Journal of
Sensor and Actuator Networks

MDPI

Article

Priority-Based Data Flow Control for Long-Range Wide Area Networks in Internet of Military Things

Rachel Kufakunesu *, Herman C. Myburgh and Allan De Freitas

Department of Electrical, Electronic and Computer Engineering, University of Pretoria, Pretoria 0002, South Africa; herman.myburgh@up.ac.za (H.C.M.); allan.defreitas@up.ac.za (A.D.F.)
* Correspondence: rachel.kufakunesu@tuks.co.za

Abstract: The Internet of Military Things (IoMT) is transforming defense operations by enabling the seamless integration of sensors and actuators for the real-time transmission of critical data in diverse military environments. End devices (EDs) collect essential information, including troop locations, health metrics, equipment status, and environmental conditions, which are processed to enhance situational awareness and operational efficiency. In scenarios involving large-scale deployments across remote or austere regions, wired communication systems are often impractical and cost-prohibitive. Wireless sensor networks (WSNs) provide a cost-effective alternative, with Long-Range Wide Area Network (LoRaWAN) emerging as a leading protocol due to its extensive coverage, low energy consumption, and reliability. Existing LoRaWAN network simulation modules, such as those in ns-3, primarily support uniform periodic data transmissions, limiting their applicability in critical military and healthcare contexts that demand adaptive transmission rates, resource optimization, and prioritized data delivery. These limitations are particularly pronounced in healthcare monitoring, where frequent, high-rate data transmission is vital but can strain the network's capacity. To address these challenges, we developed an enhanced sensor data sender application capable of simulating priority-based traffic within LoRaWAN, specifically targeting use cases like border security and healthcare monitoring. This study presents a priority-based data flow control protocol designed to optimize network performance under high-rate healthcare data conditions while maintaining overall system reliability. Simulation results demonstrate that the proposed protocol effectively mitigates performance bottlenecks, ensuring robust and energy-efficient communication in critical IoMT applications within austere environments.

Keywords: data flow control; data transmission; internet of military things; LoRaWAN; priority-based traffic

Academic Editor: Stefan Fischer

Received: 27 February 2025
Revised: 5 April 2025
Accepted: 11 April 2025
Published: 16 April 2025

Citation: Kufakunesu, R.; Myburgh, H.C.; De Freitas, A. Priority-Based Data Flow Control for Long-Range Wide Area Networks in Internet of Military Things. *J. Sens. Actuator Netw.* **2025**, *14*, 43. https://doi.org/10.3390/jsan14020043

1. Introduction

The rapid expansion of the Internet of Things (IoT) has fundamentally transformed data-driven decision-making in various sectors, facilitating the seamless integration of sensors, actuators, and analytics platforms. Among the numerous IoT communication protocols available, Low-Power Wide Area Network (LPWAN) technologies such as Sigfox, NBIoT, and Ingenu RPMA [1–3], stand out due to their design for long-range and low-power communication. These protocols are particularly well-suited for IoT applications, as they enable devices to transmit small data packets over extensive distances while consuming minimal energy, thereby optimizing operational efficiency and extending the lifespan of battery-operated devices. Long-Range Wide Area Network (LoRaWAN) has emerged as a

cornerstone technology for low-power, long-range applications, exploiting its proprietary chirp spread spectrum (CSS) modulation at the physical layer to achieve robust signal penetration and energy efficiency [4]. LoRaWAN's star-of-stars architecture, where end devices (EDs) transmit data to gateways (GWs) that relay information to a centralized network server (NS), supports deployments spanning tens of kilometers with minimal infrastructure [5]. These features have made LoRaWAN indispensable in smart cities (e.g., waste management, traffic control) [6], precision agriculture (e.g., soil moisture monitoring) [7], and industrial Internet of Things (IIoT) (e.g., predictive maintenance) [8,9]. However, its adoption in mission-critical domains such as military operations, healthcare monitoring, and disaster response demands rethinking its default "best-effort" data transmission model to accommodate heterogeneous traffic with varying urgency levels.

In military scenarios, the Internet of Military Things (IoMT) represents a significant technological advancement in modern defense operations, enabling the real-time exchange of data among sensors, actuators, and decision-making systems. These networks enhance situational awareness, resource management, and tactical decision-making, all of which are critical in military environments where rapid and informed responses can significantly impact mission success. IoMT networks rely on LoRaWAN to monitor troop vitals, track equipment status, and detect security breaches in remote border regions [10]. Similarly, healthcare systems utilize wearable LoRaWAN sensors to transmit real-time physiological data, such as heart rate and blood oxygen levels, for remote patient monitoring [11]. These applications generate a mix of high-priority alerts such as cardiac emergencies, unauthorized border crossings, and routine telemetry, necessitating dynamic prioritization to ensure critical data are delivered without delays. However, traditional LoRaWAN implementations assume uniform, periodic transmissions, which is insufficient for dynamic and priority-based applications that require adaptive data flow control, leading to inefficiencies.

A major challenge in military border security is ensuring timely and reliable communication in remote and high-risk environments. Sensors deployed along borders detect unauthorized crossings, environmental threats, and troop movements, necessitating a data prioritization mechanism to ensure that critical alerts are transmitted promptly. Similarly, the healthcare monitoring of military personnel requires the frequent transmission of high-priority physiological data, such as vital signs and emergency alerts. While LoRaWAN is suitable for low-data-rate applications, these use cases introduce challenges related to network congestion, latency, and energy consumption, especially when handling a mix of high- and low-priority data.

Existing LoRaWAN network simulation models, such as those in ns-3, primarily support fixed-interval data transmissions, which limits their applicability in IoMT scenarios that require adaptive transmission rates and priority-based traffic management. Current solutions lack mechanisms for dynamically adjusting transmission parameters based on the importance of real-time data, which is crucial for enhancing efficiency and reliability in military and healthcare applications. This study addresses these gaps by introducing a priority-based flow control (PFC) protocol, which optimizes network performance by prioritizing critical data transmissions while maintaining energy efficiency. A traffic generator model is developed using the Kronecker delta function δ to mathematically express the conditional increase in priority based on sensor readings. We employed a simulation-based approach to model and evaluate priority-based traffic for IoMT applications.

Beyond military and healthcare use cases, the proposed protocol has implications for smart cities, prioritizing emergency alerts (e.g., fire detection) over routine environmental data; and IIoT, ensuring the timely transmission of equipment failure warnings in

automated factories; as well as environmental monitoring, which expedites flood or wildfire alerts in remote sensor networks. By integrating these advancements, our work bridges the gap between LoRaWAN's low-power design and the rigorous demands of mission-critical IoT, providing a scalable framework for managing heterogeneous data traffic.

To the best of our knowledge, such a framework has not previously been developed in the literature. The principal contributions of this work are summarized as follows:

- Design and implementation of an enhanced ns-3 LoRaWAN simulation module that supports event-driven and priority-based traffic modeling.
- Development of a priority-based flow control (PFC) algorithm that dynamically adjusts data transmission rates based on sensor priority levels.
- Proposal of an adaptive priority-based communication protocol to improve the efficiency of LoRaWAN in military and healthcare applications.
- A comprehensive evaluation of the proposed framework through simulation, demonstrating improvements in packet delivery ratio, energy consumption, and network reliability.

The remainder of this article is organized as follows: Section 2 provides a technological overview of LoRaWAN and its applicability to IoMT. Section 3 reviews the related literature. Section 4 describes the design and implementation of the enhanced sensor data generator. Section 5 provides the system model. Section 6 presents the proposed schemes. Section 7 presents and discusses the simulation results. Section 8 concludes the article with future directions.

2. Technological Overview

LoRaWAN is a proprietary trademark synonymous with LoRa and a member of low-power wide area network (LPWAN) technology in the Internet of Things (IoT). It connects numerous end devices (EDs) with low-cost, low-data-rate, long-range, and long-lasting batteries suitable for various IoT applications with varying levels of QoS in various industries such as smart agriculture, smart metering, smart cities, and smart healthcare [6,7,11,12]. Unlike NBIoT [13] and Sigfox [1], which are proprietary, LoRaWAN operates in the Industrial, Scientific, and Medical (ISM) band. LoRa employs a physical (PHY) layer chirp spread spectrum (CSS) modulation technology that provides the highest receiver sensitivity while consuming the least power compared to other LPWAN technologies [4]. The CSS enables the demodulation of data packets with a low signal-to-noise ratio (SNR) at lower data rates. EDs sense the environment and communicate with the network server (NS) via the gateway (GW). Depending on the distance from the gateway and the propagation conditions, transmission parameters are set, namely, spreading factor (SF), transmission power (TP), bandwidth (BW), and coding rate (CR). These transmission parameters have an impact on energy consumption [14].

LoRaWAN employs the adaptive data rate (ADR) scheme, an essential element that regulates these transmission parameters to optimize resource allocation. The key objective of the ADR scheme is to optimize the network for maximum capacity, ensuring that EDs continuously transmit with optimal transmission parameters. Since the lifetime of the ED battery is limited, charging or replacing batteries may be impossible in some harsh environments; thus, energy efficiency is considered to avoid network lifetime degradation in a LoRaWAN network. The work in [15] details the network architecture and key features like adaptive data rate and device classes, and it highlights LoRaWAN's strengths in energy efficiency and wide coverage. Our work in [16,17] optimized ADR for energy efficiency. Simulation tools were employed to deploy and evaluate our LoRaWAN network. We reviewed the available LoRaWAN simulators in the literature, such as [18–20], and settled on an open-source simulation tool that accurately models the behavior of LoRaWAN networks, including factors like signal propagation, interference, collisions, data rates,

and network congestion. We sought features that enable easy customization of network topology and node behaviors, allowing for the modification of various parameters, such as transmission power, spreading factor, data rates, and network configurations. The NS-3 simulation tool was selected as the platform for implementation. However, within ns-3, several modules were implemented, such as [5,21–23]. The LoRaWAN module by [5], available in [24], was selected due to the availability of a supportive community, user forums, and documentation associated with the simulator. The frequent updates, ongoing maintenance, and bug fixes provided by the simulator's developers ensure compatibility with new protocol versions and improvements in simulation capabilities, making it a suitable choice. However, the existing model has some limitations. The current Periodic Sender Application only allows for fixed-interval data transmission, failing to capture the dynamic and often unpredictable data patterns of austere security and healthcare applications. The model does not allow for prioritizing critical data, such as emergency alerts or urgent patient updates, which is crucial in security and healthcare scenarios.

While LoRaWAN is generally well-suited for applications with low data rate requirements, like many border security use cases, healthcare monitoring often demands higher data rates, leading to several potential effects on LoRaWAN's performance:

- Higher data rates in LoRaWAN require the use of smaller spreading factors, which decrease receiver sensitivity, requiring higher transmission power for successful communication. This increased transmission power directly translates to higher energy consumption by the end devices. This is a critical consideration for remote and austere environments, where emergency dispatchers (EDs) may rely on batteries with a limited lifespan.
- LoRaWAN exploits the orthogonality of different spreading factors to allow multiple EDs to transmit concurrently without interference. However, fewer orthogonal channels are available when EDs transmit at higher data rates. This can lead to increased collisions and congestion, reducing the overall network capacity and the number of devices that can be effectively supported.
- Higher data rates imply a shorter time on air for individual packets. However, in the context of healthcare monitoring, where more frequent transmissions might be needed, the overall airtime used by these transmissions could still increase, potentially leading to higher latency for other applications sharing the LoRaWAN infrastructure.
- In LoRaWAN, data rate and coverage have an inherent trade-off. Lower data rates provide a more extended range, while higher data rates limit the range. If healthcare monitoring applications demand higher data rates, it could impact the achievable coverage area for these applications within a LoRaWAN deployment.

In this work, we attempted to address these challenges by developing an improved sensor data sender application and a priority-based communication protocol. We contribute to realizing dependable and robust LoRaWAN solutions for these critical applications.

3. Related Literature

The military sector has long relied on diverse wireless communication technologies, each tailored to specific operational requirements. While LoRaWAN offers distinct advantages for low-power, long-range sensor networks in IoMT applications, it is important to contextualize its role alongside established military-grade wireless solutions. Mobile Ad Hoc Networks (MANETs), such as those employing the Optimized Link State Routing Protocol (OLSR) [25], form the backbone of tactical communication systems. These self-configuring networks excel in dynamic environments where infrastructure is absent or compromised, enabling peer-to-peer connectivity among soldiers, vehicles, and command centers. MANETs support high mobility and robust data throughput, making them ideal for

real-time voice and video transmission. However, their energy-intensive routing protocols and scalability limitations in large-area deployments [26,27] render them less suitable for low-power, wide-area sensor networks where LoRaWAN thrives. Tactical Cognitive Radio Networks (CRNs) represent a paradigm shift in military communications, enabling the dynamic access to underutilized spectrum to avoid jamming and interception. These networks are particularly valuable in electronic warfare scenarios, where maintaining secure and reliable links is paramount. Studies have demonstrated CRNs' ability to maintain connectivity even in contested spectral environments [28], but their computational complexity and power consumption exceed the capabilities of resource-constrained LoRaWAN end devices. Mesh networks support advanced applications, such as real-time situational awareness and drone control, with throughput orders of magnitude higher than LoRaWAN [29,30]. However, their infrastructural requirements and energy demands limit their use for persistent, wide-area sensor monitoring, precisely the area where LoRaWAN's energy efficiency and scalability prove advantageous.

Recent advancements in wireless sensor networks have demonstrated significant improvements, establishing this technology as a new, energy-efficient solution for low-data-rate applications. The growing adoption of LoRaWAN in mission-critical applications has highlighted the need for intelligent priority-based traffic management. Current approaches to data prioritization in IoT networks vary significantly in their design philosophies, performance characteristics, and suitability for different deployment scenarios. While its adoption in healthcare monitoring is well-documented [31], recent studies highlight its growing role in mission-critical domains such as military operations [32], border security [33], and industrial automation [34]. These applications require adaptive data flow control to handle heterogeneous traffic, where high-priority alerts, such as unauthorized border crossings and equipment failures, must coexist with routine telemetry. The simplest approach to traffic management employs static priority assignments, where data categories are predefined based on application requirements. For instance, in healthcare monitoring systems, vital signs may be permanently classified as high-priority while routine telemetry receives low priority. While our focus is on the priority of data transmission, certain applications, such as those in the military and healthcare sectors, require an additional consideration of the security aspect [35]. LoRaWAN utilizes AES-128 encryption to secure the payload with the AppSKey, ensuring message integrity and authenticity with the NwkSKey. However, security remains an active research area, with studies focusing on enhancing resilience under adversarial attacks and evolving threat mitigation strategies [36–38].

The work in [39] presents a novel Data Transmission Protocol using Priority Approach (DTP-PA) designed for low-rate wireless sensor networks (LR-WSNs) with heterogeneous traffic. The authors addressed challenges in transmitting priority-based traffic in multi-hop sensor networks while minimizing energy consumption and delay. The proposed solution comprises three algorithms that dynamically adjust reporting rates based on decision intervals specified by the sink node. It prioritizes packet scheduling based on hop count and data priority to ensure the timely delivery of critical packets while also optimizing buffer occupancy and data flow by adjusting reporting rates in response to network conditions. Simulation and testbed evaluations demonstrated significant performance improvements in priority packet delivery and overall network throughput compared to traditional methods. The innovative scheduling prioritizes long-distance, high-priority packets, reducing delays for critical applications. The algorithms minimize energy consumption through dynamic reporting rates and distributed decision-making. While the protocol reduces delay for priority packets, comprehensive delay constraints for heterogeneous traffic flows are not addressed, and the solution focuses on multi-hop

networks, limiting its direct applicability to other network architectures. This method benefits from straightforward implementation and predictable network behavior, making it suitable for basic IoT deployments with consistent traffic patterns. However, its rigidity becomes problematic in dynamic environments where data criticality may change rapidly. During emergency situations in military or healthcare scenarios, the inability to dynamically reprioritize data flows can result in either excessive resource allocation to non-critical transmissions or insufficient bandwidth for urgently needed information. Moreover, fixed-priority schemes often fail to account for changing network conditions, such as congestion or node mobility, which can potentially exacerbate performance degradation during peak loads or topological changes.

More sophisticated solutions, such as the Priority-Based Energy-Efficient Routing Protocol (PEERP), attempt to address these limitations through conditional routing strategies [40]. The authors present an innovative routing protocol for healthcare systems that utilize IoT. The proposed PEERP protocol classifies health information into two categories: emergency situation (P1) and vital health data (P2). Critical data, P1, are transmitted using direct communication for minimal delay, while less time-sensitive data, P2, are sent via multi-hop communication to optimize energy consumption. PEERP introduces a cost-based mechanism to select forwarder nodes based on residual energy and communication distance, thereby ensuring balanced energy usage and prolonging the network's lifetime. This work supports delay-sensitive (emergency) and energy-sensitive (continuous monitoring) applications, ensuring broad applicability. While effective in small-scale simulations, PEERP's performance in large-scale IoT deployments with a greater number of nodes remains unexplored. A slightly higher path loss than ATTEMPT in prolonged scenarios may impact reliability in specific applications. The accuracy of forwarder node selection heavily depends on the cost function parameters, which may need to be tuned for different environments. This approach demonstrates particular effectiveness in healthcare applications, where it balances the need for rapid emergency response with energy conservation for routine monitoring. The protocol incorporates a cost-based forwarding mechanism that considers both residual energy and communication distance when selecting relay nodes, theoretically prolonging network lifetime. The binary priority classification proves inadequate for complex scenarios requiring finer granularity in urgency levels, such as distinguishing between life-threatening emergencies and important but non-critical alerts.

A novel cache replacement technique for industrial IoT applications was developed in [10]. The approach integrates a periodic popularity prediction with content size caching to optimize data transmission and reduce latency in IIoT environments. The method assigns values to cached content based on popularity, size, and time update characteristics. When cache replacement is needed, the least valuable information is removed first. Simulation results demonstrated that the proposed technique improves cache hit rates and reduces transmission delay compared to classical caching algorithms, including GDS, MPC, LRU, FIFO, and LFU. The proposed approach achieved a 15.3% higher hit rate than GDS, 17.3% higher than MPC, 20.1% higher than LRU, 22.3% higher than FIFO, and 24.8% higher than LFU in scenarios involving 350 different information categories. The study's findings are applicable to various fields, including supply chain management, smart manufacturing, automation, energy optimization, intelligent logistics, and e-healthcare applications. A Priority-Based Energy-Efficient Metaheuristic Routing Approach for Smart Healthcare Systems (SHS) is proposed in [41]. This approach utilizes a hybrid Duty-Cycled Ant Colony Optimization Routing (DC-ACOP) mechanism to optimize data transmission in IoT-enabled smart healthcare systems. Their primary focus was reducing transmission delay and energy consumption while ensuring prioritized data delivery for critical healthcare applications.

They proposed the DC-ACOP method, which integrates dynamic duty cycling where sensor nodes activate their communication units only on demand to save energy. The method integrates priority-based routing, where data packets are categorized based on criticality using the IP packet's Type of Service (ToS) field. This ensures that high-priority healthcare data are transmitted first. They employed metaheuristic optimization, specifically Ant Colony Optimization (ACO), which determines efficient routing paths dynamically based on parameters such as residual energy, mobility, and path length. The ACO-based routing approach requires additional processing, which may not be ideal for resource-constrained sensor nodes. While practical, assigning priority labels and dynamically adjusting routing behavior adds protocol complexity.

The article entitled "Reducing Operational Expenses of LoRaWAN-Based Internet of Remote Things Applications" [42] focuses on optimizing scheduled transmissions in LoRaWAN networks that rely on LEO satellite links instead of terrestrial backhauls. To minimize operational costs—specifically the airtime billed by satellite operators—the authors proposed a cost-efficient transmission scheduling algorithm that organizes when and how end devices send data through LoRaWAN gateways to satellites. Simulation results demonstrated that this scheduling approach significantly reduced airtime and, therefore, operational expenses, without compromising data delivery reliability. The approach assumes predictable and timely satellite pass availability, which may not be practical in dynamic or emergency scenarios. The solution relies on strategically placed LoRaWAN gateways with satellite connectivity, which may pose logistical or financial barriers in certain contexts. The work in [10] addresses challenges in IIoT sensing networks, particularly the uncertainty in data transmission caused by limited resources and dynamic environments. The authors propose a priority-based transmission algorithm (PBTA) that enhances data certainty by prioritizing data packets based on the urgency and importance of the IIoT application. The drawback is that the computational overhead caused by the priority calculation and dynamic slot allocation may introduce processing delays, especially in low-power IIoT devices.

A priority-driven transmission model for wearable sensors in healthcare systems is developed in [43]. The model employs a Type-2 Fuzzy Logic System (FLS) for real-time congestion detection and utilizes active queue management (AQM) to dynamically regulate transmission rates. Their key focus is on reducing congestion and minimizing transmission delay while ensuring reliable data delivery. The proposed method integrates selective decision modes, including congestion mitigation and perfect queuing, to enhance network efficiency. The fixed-priority assignment is a drawback, as there is no priority reassignment mechanism to adjust to changing patient conditions. The CBT-based slot allocation may become inefficient if network traffic experiences unexpected spikes. The study evaluates its approach through simulations in OMNeT++, demonstrating improved queue utilization (37.18%), higher success rates (3.67%), and a reduced transmission delay (23.69%) compared to existing methods. The study in [44] introduces LoRa-REP, a redundancy-based transmission mechanism designed to enhance communication reliability and resilience in LoRaWAN networks for mixed-criticality applications. Traditional LoRaWAN suffers from high failure probabilities due to its simple ALOHA MAC protocol, which lacks built-in mechanisms for prioritizing transmissions and ensuring reliable retransmission. The proposed LoRa-REP solution addresses these limitations by replicating critical messages across multiple spreading factors, reducing transmission failures. The authors implemented message replication using multiple SF values, ensuring orthogonality and minimizing interference. They utilized virtual nodes to mimic independent devices, achieving backward compatibility with existing LoRaWAN deployments. The optimization of uplink and downlink transmission scheduling was implemented to minimize transaction

delays. Experimental results using a real-world LoRaWAN testbed showed that LoRa-REP reduced the failure probability of critical transactions from 78% (single SF) to below 2.5%, significantly improving reliability in mixed-criticality scenarios. The drawback of this solution is increased energy consumption, as it requires multiple transmissions for message redundancy, potentially draining the battery of battery-powered devices more quickly. While LoRa-REP improves reliability for a few critical nodes, excessive redundant transmissions may increase network congestion in dense deployments. The multiple SF replications consume more transmission slots, reducing overall network capacity. The SF replication strategy is fixed and is not dynamically adjusted based on network conditions. Furthermore, the approach demonstrates poor scalability as the number of critical nodes increases, with the network capacity diminishing rapidly due to the multiplicative effect of redundant transmissions.

These limitations make pure redundancy-based solutions impractical for large-scale deployments with mixed criticality requirements. Unlike the static priority assignments, our work employs dynamic thresholds that continuously evaluate sensor data against clinically or operationally significant parameters. This real-time assessment, implemented through Kronecker delta functions, enables automatic priority escalation when measurements exceed predefined thresholds. We propose a priority-based protocol that considers energy efficiency.

4. The Enhanced Sensor Data Generator for LoRaWAN

In a typical ns-3 LoRaWAN simulation scenario, the end devices are equipped with the Periodic Sender Application. Each device generates packets at the defined interval and sends them to the network server through the gateways. The simulation then tracks these sent and received packets to compute network statistics. The application is quite basic and assumes a uniform periodic transmission pattern, which might not be suitable for more complex or realistic scenarios where data generation is event-driven or has a variable rate. It does not adapt to changing network conditions or data importance. In real-world applications, data may need to be prioritized or sent only if certain conditions are met; however, the "periodic sender" simply sends data at fixed intervals without any intelligence or adaptability. The "periodic sender" does not simulate a higher-level application logic that may be present in real IoT applications, such as data aggregation, compression, or decision-making based on sensor readings. This is insufficient for more detailed simulations requiring a more sophisticated application layer or custom data generation patterns.

Figure 1 presents a class structure from [45] that explains the way in which different components of the current ns-3 implementation of LoRaWAN [24] are organized. The packets generated by the Periodic Sender at the EDs end up at the network server.

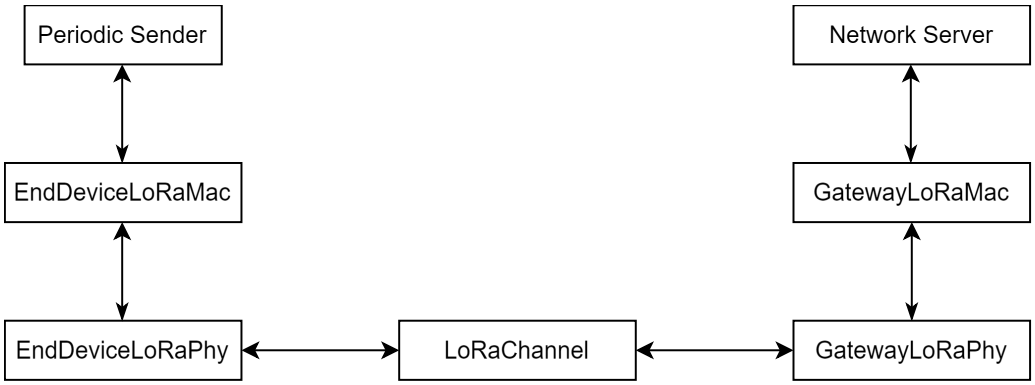

Figure 1. The Periodic Sender in the class structure [45].

4.1. Structure of the Existing Periodic Sender

1. Configure Sender:
   - Set how often to send data (data interval).
   - Set initial delay before starting.
   - Decide on the basic size of data packets.
   - Optionally, allow for random packet size variation.
2. Start Sending:
   - Wait for the initial delay.
   - Create a packet.
   - Attach LoRaWAN mac and frame Headers.
   - Package the data into the packet
   - Transmit/Send the packet
   - Wait for the set interval
   - Repeat
3. Stop sending:
   - Stop sending packets.

Because the current implementation of the Periodic Sender lacks the necessary options to handle more realistic sensor data, we propose improvements to this data sender application in this work.

4.2. Improved Data Sender Application for Border and Body Sensor End Devices

The proposed application enhances the standard ns-3 Periodic Sender Application by incorporating priority differentiation based on sensor data. Additional headers are included as shown in Figure 2 to structure and transmit sensor readings over the network. The Body Sensor Data Generation Algorithm is designed to simulate the generation and transmission of physiological sensor data in a medical monitoring system. It operates under specific conditions and assigns priority levels based on abnormal readings. The new data generator requires custom headers, including ApplicationHeader, BorderSensorDataHeader, and BodySensorDataHeader, to structure and transmit sensor readings over the network. These headers include fields for specific sensor values. In the PeriodicSender::SendPacket() function, the application creates a new packet. Depending on the sensor type (m_appType), it generates random sensor data using appropriate probability distributions (e.g., UniformRandomVariable for border sensor data, NormalRandomVariable for body sensor data) and populates the corresponding custom header. The custom header is then added to the packet using packet->AddHeader() to indicate whether the packet is originating from a border security sensor or a body sensor end device. An additional custom header, SensorAppHeader, is used to convey the application type (m_sensorAppType) and priority (m_priority). The priority is dynamically determined based on sensor readings and predefined thresholds. For border sensors, exceeding thresholds for human detection, vibration, acoustic level, or detecting motion increases the priority. For body sensors, a high body temperature (fever), a high blood pressure, a low oxygen level, or an abnormal heart rate triggers a higher priority. The SensorAppHeader is added to the packet, embedding the priority information. The packet, now containing both sensor data and priority, is sent using m_mac->Send(packet). This algorithm effectively simulates the generation and transmission of real-time physiological data in a medical monitoring system. By dynamically computing priority based on abnormal values, it ensures that critical health conditions are identified and prioritized for further analysis or emergency response.

The algorithm for a simple body sensor data generation is shown in Algorithm 1 below. If the application type is BodySensor, then it generates sensor data using normal distributions. The priority determination logic is added to the algorithm, incorporating both the condition checks and the Kronecker delta function for mathematical representation, which returns 1 if the condition is true and 0 otherwise. We include the sections for creating and adding headers before transmission. The next data packet transmission is scheduled after a predefined time interval (Δt), ensuring continuous monitoring of physiological parameters. The packet containing the sensor data and headers is transmitted via the MAC (Medium Access Control) layer to ensure communication with the monitoring system. The main improvement over the basic Periodic Sender is the dynamic assignment and transmission of priority levels. This enables the simulation to distinguish between routine and critical data, which is crucial for accurately modeling austere security and healthcare scenarios. The use of thresholds for priority assignment introduces flexibility. Other researchers can adjust these thresholds to model different scenarios and analyze their impact on network performance.

Algorithm 1 Body Sensor Data Generation Algorithm

Require: $m\_appType$ (Application Type Indicator)
Ensure: Generate sensor data and determine priority

if $m\_appType = 2$ **then**
  Generate Sensor Data:
  $T \sim \mathcal{N}(37.0, 0.4)$ {Body Temperature (°C)}
  $P \sim \mathcal{N}(120.0, 10.0)$ {Blood Pressure (mmHg)}
  $O_2 \sim \mathcal{N}(98.0, 2.0)$ {Oxygen Level (%)}
  $HR \sim \mathcal{N}(75.0, 5.0)$ {Heart Rate (bpm)}
  Determine Priority:
  $priority \leftarrow 0$
  if $T > 38.0$ **then**
    $priority \leftarrow priority + 1$
  end if
  if $P > 140.0$ **then**
    $priority \leftarrow priority + 1$
  end if
  if $O_2 < 90.0$ **then**
    $priority \leftarrow priority + 1$
  end if
  if $HR > 100.0$ **then**
    $priority \leftarrow priority + 1$
  end if
  Compute priority mathematically:
  $priority \leftarrow priority + (\delta_{T>38.0} + \delta_{P>140.0} + \delta_{O_2<90.0} + \delta_{HR>100.0})$
  Define Kronecker delta function:

$$\delta_{condition} = \begin{cases} 1, & \text{if condition is true} \\ 0, & \text{if condition is false} \end{cases}$$

  Create and Add Headers:
  Set fields in BodySensorDataHeader: T, P, O_2, HR
  Set fields in SensorAppHeader: $SensorAppType = m\_appType$, $priority$
  Add both headers to the packet
  Send the Packet:
  Transmit the packet via MAC layer
  Schedule Next Transmission:
  Schedule next packet transmission after predefined interval Δt
end if

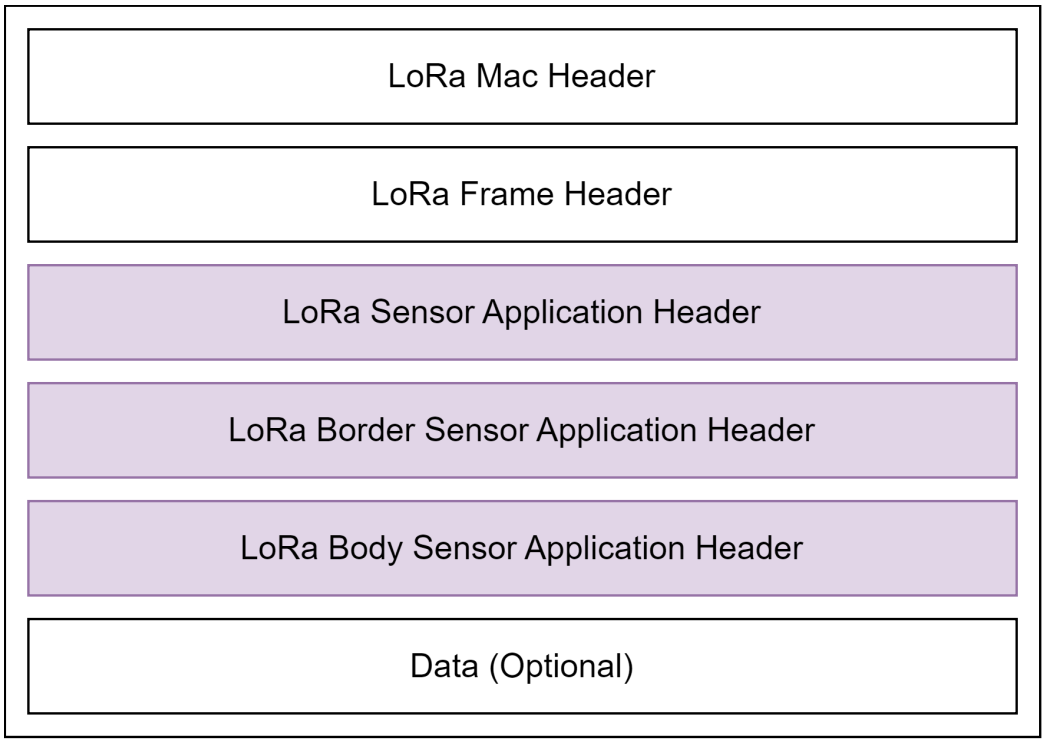

Figure 2. The Periodic Sender in the class structure [45].

5. System Model

Having developed a more realistic data generator, we implemented it in our border control application scenario, where fixed and mobile end devices were used by the military to secure the border. Figure 3 is a NetAnim output of the ns-3 simulation [46] showing the proposed two-dimensional network topology area of the US–Mexico border. The small red dots around the side of the US borderline denote the LoRaWAN static EDs deployed for border security operations. The militant icons denote the mobile EDs. The network consists of a network server, gateways, static EDs monitoring the environment, and mobile body-sensor EDs monitoring the vitals of the patrolling soldiers. We considered a LoRaWAN network using European regional parameters with confirmed traffic transmissions for Class A end devices. The network uses modulation with a fixed bandwidth of 125 kHz and consists of three GWs positioned along the coverage within 5 km of the border (Table 1). The EDs are heterogeneous, that is, mobile and static, and located randomly with a uniform distribution in the coverage area. The simulation tool mimics the SX1301 digital baseband chip used for GW capabilities and SX1272 [47,48] for the ED transceiver. The network spans a topographical area of 10 km by 20 km. The EDs generate packets of fixed payload for a given SF at different application data intervals, regardless of proximity to the GW. In our algorithm, the NS uses the average SNR values [49,50] of the previous four packets sent by the ED to approximate the link quality, in comparison with the standard ADR protocol that uses the maximum SNR value of twenty packets, saving on computational costs [16]. We utilized the log–distance propagation path loss model [51]. This model enables the estimation of signal strength decay as it travels over a distance, considering factors such as attenuation and interference. The system model incorporates the interference arising from simultaneous uplink transmissions on a specific appropriate uplink transmission. A transmitted packet is received or dropped based on the sensitivity values provided in Table 2. Therefore, SF should be allocated to an ED guaranteeing that the received signal strength is higher than the receiver sensitivity as shown in (1) below.

$$SNR_{margin} = SNR_{avg} - SNR_{thresh} - D_{margin}, \quad (1)$$

where SNR_{avg} denotes the average SNR of the packets in the ReceivedPacketList, SNR_{thresh} is the minimum SNR threshold, and D_{margin} is the device margin.

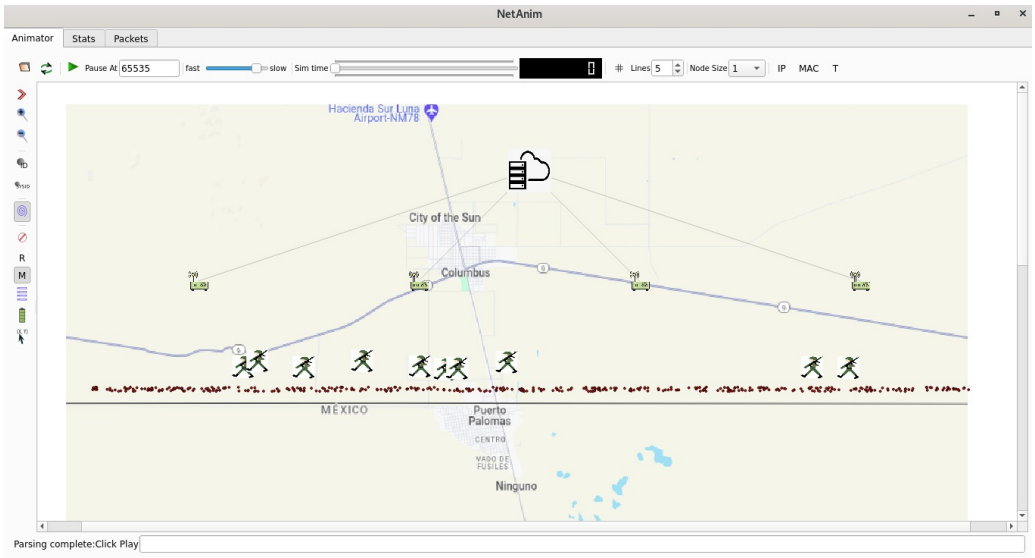

Figure 3. The simulated LoRaWAN border security and healthcare monitoring network scenario.

The received signal power at the GW in dB is given in (2):

$$P_{rx(dB)} = P_{tx}(dB) + G_a(dB) - L_p(dB)\,, \quad (2)$$

where P_{tx} is the transmit power at the ith ED, G_a is the antenna gain, and L_p is the path loss.

The path loss propagation is given by

$$L_p = -10\log_{10}(d_i^{\alpha} f_c^2 * 10^{-2.8})\,, \quad (3)$$

where d_i is the distance between the ith ED and the gateway, α is the path loss exponent (3.76), and f_c is the carrier frequency (868.1 MHz).

We assumed a simple energy consumption model comprising four states: transmit, idle, receive, and sleep. The energy model links each of the aforementioned states with a different voltage and current utilization as shown in Table 3. We monitored the energy usage of each node throughout the simulation period to determine the network's overall energy consumption. The model calculates the device's energy consumption and estimates the ED's battery life. The total energy consumption for each ED is given by (4)

$$E_{ED} = E_{tx} + E_{rx} + E_i + E_s\,, \quad (4)$$

where E_{tx} is the energy consumed when the ED is transmitting a packet, E_{rx} is the energy consumed when the ED is receiving an incoming packet, E_i is the energy consumed when listening for incoming packets, and E_s is the energy consumed when the ED is in sleep mode.

Table 1. Simulation parameters.

Parameter	Value
Frequency	868 MHz
Number of Border Sensor Nodes	50, 100, 200, 400
Number of BSN Mobile Nodes	10, 20, 30, 40, 50
Border Area Length	20,000 m
Border Area Width	5000 m
Number of GWs	3
Number of NS	1
BorderSensorNodeDeployment Area Width	100 m
Simulation Runs	10
Simulation Time	6 h
Border Sensor Data Interval	1 packet per 1200 s, 1800 s, 2400 s, 3000 s
BSN Mobile Sensor Data Interval	60 s

Table 2. SNR and sensitivity thresholds per spreading factor [48].

Spreading Factor	Required SNR [dB]	Sensitivity [dBm]
7	−7.5	−123
8	−10	−126
9	−12.5	−129
10	−15	−132
11	−17.5	−134.5
12	−20	−137

Table 3. Energy Model Parameters.

Parameter	Value
Initial Energy of EDs	10,000 J
Supply Voltage	3.3 V
Standby Current	0.0014 A
Tx Current	0.028 A
Sleep Current	0.0000015 A
Rx Current	0.0112 A

6. The Proposed Priority-Based Flow Control Protocol for LoRAWAN

The use of mobile body sensor nodes generates data at high rates. This influx of data challenges the performance efficiency of LoRaWAN, particularly since it is primarily optimized for low-data-rate transmissions. These sensor nodes continuously monitor vital signs and relay this information through the protocol stack. When a packet is received at the Medium Access Control (MAC) layer, the first step involves examining its priority field. This priority value plays a crucial role in determining how the packet will be handled during subsequent stages of processing and forwarding. Depending on the priority assigned to the packet, the MAC layer may prioritize it over other packets, ensuring that critical data are transmitted in a timely manner. This prioritization process helps optimize network performance by reducing delays for high-priority packets while effectively managing lower-priority traffic. Ultimately, the handling and forwarding decisions based on the priority value can significantly impact overall network efficiency and responsiveness. While LoRaWAN's architecture is ideally suited for intermittent, low-volume data, the demands presented by high data rate applications risk escalating energy consumption and compromising overall system performance. To address these challenges, we advocate for the implementation of a priority-based flow control protocol. This innovative approach

aims to streamline data transmission processes, thereby optimizing network performance while minimizing resource consumption.

6.1. The Priority-Based Flow Control (PFC) Algorithm

The proposed priority-based flow control dynamically assigns data transmission priorities based on real-time sensor readings and predefined thresholds. The priority-based flow control algorithm determines whether a data packet should be forwarded based on its assigned priority level and the current time. The number of priorities and delay intervals that can be assigned to priority packets is $n - 1$. For the purposes of testing our model, three priorities were used: Pr = 0, 1, 2 and k = 0, 1, 2. The packet priorities and delay intervals for priority packets were assigned in ascending order.

1. Priority Assignment:
   - High Priority (Pr = 2): Triggered when sensor values exceed critical thresholds (e.g., body temperature > 38 °C, heart rate > 100 bpm). These packets are transmitted immediately.
   - Medium Priority (Pr = 1): Generated when sensor readings approach warning thresholds (e.g., blood pressure > 140 mmHg). Transmitted every k_1 seconds if no high-priority traffic exists.
   - Low Priority (Pr = 0): Routine data (e.g., stable vitals, environmental telemetry). Transmitted every k_2 seconds to conserve energy.
2. Dynamic Thresholds:
   - Priorities are recalculated using a Kronecker delta function. Example: A soldier's elevated heart rate (HR > 100) and low oxygen (O_2 < 90%) would yield Pr = 2 (immediate transmission).

$$\delta_{condition} = \begin{cases} 1, & \text{if condition is true} \\ 0, & \text{if condition is false} \end{cases}$$

3. Time Interval Selection:
   - k_1 / k_2 intervals were empirically derived from simulations to balance latency and energy consumption. We started with conservative defaults and iteratively made refinements via simulations. $k_0 = 0$ means immediate transmission, $k_2 = 2k_1$.
   - Low-priority packets are delayed to reduce collisions, while critical data bypass queues.

   The Algorithm 2 begins by initializing two critical time intervals: k_1 seconds for medium-priority packets and k_2 seconds for low-priority packets. If a packet has high priority (Pr = 2), it is forwarded immediately. For packets that are not high priority, forwarding occurs when the current time is a multiple of k_1 seconds. Similarly, low-priority packets (Pr = 0) are forwarded only if the current time is a multiple of k_2 seconds. If none of these conditions are met, the packet is discarded. This structured approach ensures that high-priority packets are transmitted without delay while lower-priority packets are sent periodically to optimize network efficiency. The algorithm ensures an efficient and controlled transmission mechanism, prioritizing urgent data while managing network congestion for lower-priority packets.

Algorithm 2 Priority-Based Flow Control Algorithm

Require: T (Body Temperature), P (Blood Pressure), O (Oxygen Level), H (Heart Rate)
Require: n (Number of priorities)
Require: t: Current time (seconds)
Require: Pr: Priority Level ($n-1$ = highest, 0 = lowest)
Require: k_1: Base delay interval (applies to Pr = $n-2$)
Ensure: Forward True/False (Decision to forward or discard the packet)
1: $f(Pr) \leftarrow 0$ {Initialize forwarding decision}
2: **if** $Pr = n-1$ **then**
3: $f(Pr) \leftarrow 1$ {High Priority − Forward immediately}
4: **else if** $Pr =< n-1$ and
5: $k_i = (n-1-Pr) * k_1$ { Compute delay interval e.g., Pr = $n-2 \rightarrow k_1$; Pr = $n-3 \rightarrow k_1 = 2 * k_1$}
6: Forward if $(t \mod k_1 = 0)$ **then**
7: **return** forward
8: **end if**

6.2. The Priority-Based Flow Control (PFC) with Dynamic Confirmed Data Update (PFC_DCDU)

The model is designed to prioritize the forwarding of data packets based on their priority level. It ensures that high-priority packets are transmitted immediately while medium- and low-priority packets are forwarded at specific intervals. This approach is particularly useful in systems where resource allocation (e.g., bandwidth, processing power) needs to be optimized based on the urgency of the data. At the application layer, the body sensors periodically read the data from the sensors and report them to the remote server. Frequent data updates can lead to increased overhead and negatively impact LoRaWAN's overall performance. The previous model presents a simple priority-based flow control model implemented at the MAC layer of LoRa end devices. We introduced a controlling "Dynamic Confirmed Data Update (DCDU) Mechanism", which, when a packet is forwarded by the node as a high-priority packet, sets the "Confirmed Data Update (CDU) field" of the packet to true. This results in the NS sending an acknowledgment to the corresponding ED, ensuring that important packets are delivered without loss. The model controls the data forwarded to the network server based on priority and, therefore, reduces the data rate. The Priority-Based Packet Forwarding Algorithm 3 with Dynamic Confirmed Data Update (PFC_DCDU) protocol determines when packets should be forwarded based on their priority levels and time intervals. It incorporates a CDU flag to manage packet forwarding behavior efficiently. The algorithm classifies packets into three priority levels: High ($Pr = 2$), Medium ($Pr = 1$), and Low ($Pr = 0$). It utilizes two critical intervals: k_1 seconds for medium-priority packets and k_2 seconds for low-priority packets. The CDU flag is dynamically updated based on packet forwarding decisions. The algorithm operates by assessing the priority of incoming packets and deciding their forwarding schedule accordingly. High-priority packets ($Pr = 2$) are forwarded immediately upon arrival to ensure minimal latency and maximum responsiveness. Medium-priority packets ($Pr = 1$) are transmitted at regular intervals of k_1 seconds, ensuring a balance between timely delivery and network efficiency. Similarly, low-priority packets ($Pr = 0$) are sent only at k_2-second intervals to further optimize resource allocation. If the time condition is not met, medium- and low-priority packets are not forwarded, conserving bandwidth. The CDU flag plays an important role in controlling network behavior. When set to false, it temporarily disables confirmed data updates, preventing unnecessary retransmissions and optimizing network load. When no packet is forwarded, the CDU flag remains true, This algorithm ensures efficient packet transmission by prioritizing high-importance data while conserving network resources for lower-priority packets. The CDU flag helps

manage network performance by dynamically enabling or disabling updates based on forwarding decisions.

Algorithm 3 Priority-Based Packet Forwarding with CDU Logic

Require: T (Body Temperature), P (Blood Pressure), O (Oxygen Level), H (Heart Rate)
Require: n (Number of priorities)
Require: t: Current time (seconds)
Require: Pr: Priority Level ($n-1$ = highest, 0 = lowest)
Require: k_1: Base delay interval (applies to Pr = $n-2$)
Require: $CDUFlag$ (Confirmed Data Update flag)
Ensure: Forward True/False (Decision to forward or discard the packet)
CDUflag $\leftarrow$ true
$f(Pr) \leftarrow 0$ {Initialize forwarding decision}
if $Pr = n - 1$ **then**
    $f(Pr) \leftarrow 1$ {High Priority - Forward immediately}
    CDUflag $\leftarrow$ false {Disable CDU}
else if $Pr =< n - 1$ and
$k_i = (n - 1 - Pr) * k_1$ { Compute delay interval e.g., Pr = $n - 2 \rightarrow k_1$; Pr = $n - 3 \rightarrow k_2 = 2 * k_1$}
Forward if $(t \mod k_1 = 0)$ **then**
    CDUflag $\leftarrow$ false {Disable CDU}
else
    CDUflag $\leftarrow$ true
    return forward and CDUflag
end if

7. Results and Discussion

An evaluation of the proposed algorithm is presented in this section based on the results derived from the simulations. The performance analysis of the LoRaWAN network primarily focuses on four key metrics: confirmed packet success rate (CPSR), uplink packet delivery ratio (UL-PDR), total energy consumption (ET), and interference ratio (IR). In the first evaluation scenario, we varied the number of static border EDs while maintaining a fixed number of BSN EDs (50), an application data packet rate of 60 s for mobile BSN EDs, and 1200 for the fixed border EDs. In the second evaluation scenario, we varied the number of BSN EDs while maintaining a constant application data interval for both BSN EDs and border EDs and a fixed number of static border EDs. The main findings of our study indicate that our proposed protocols, PFC and PFC-CDU, performed significantly better than the case where no "flow control" was used in terms of packet delivery ratio, while also demonstrating reduced interference rates and energy consumption.

7.1. Performance with Varying Number of Static Border Sensor EDs

This section presents an analysis of the impact of increasing the number of border sensor nodes (No.BorderEDs) on various network performance metrics for different data flow control mechanisms, as illustrated in Figure 4. The evaluation compares three data flow control mechanisms: No Flow Control (NFC), priority-based flow control (PFC), and PFC with Dynamic CDU (PFC_DCDU). This analysis considers a 60-second data interval for mobile EDs and a 1200-second data interval for static EDs.

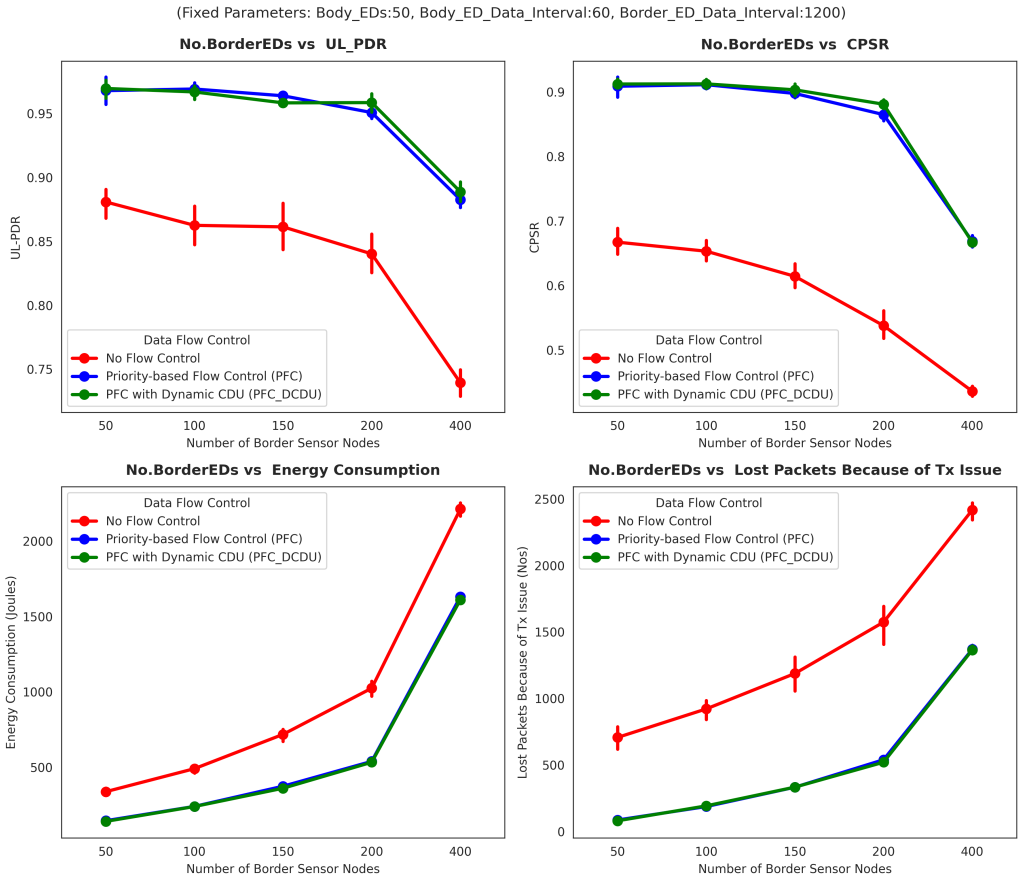

Figure 4. Performance analysis of LoRaWAN with different numbers of border sensor EDs.

7.1.1. No.BorderEDs vs. UL_PDR (Uplink Packet Delivery Ratio)

The uplink packet delivery ratio is the ratio of the number of packets successfully received at the GW to the number of packets generated by the ED. The results indicate that an increase in the number of border sensor nodes results in a decrease in the uplink packet delivery ratio, primarily due to network congestion and increased packet collisions. However, the implementation of flow control mechanisms significantly mitigates the decline. NFC exhibits a substantial decrease in UL_PDR, dropping to approximately 0.75 at 400 nodes, which highlights severe congestion and frequent packet losses. PFC and PFC_DCDU maintain high reliability (0.95) up to 300 nodes but experience a slight decline at 400 nodes due to increased contention for network resources. The vertical bars on the graphs indicate the range between the lowest and highest recorded values from the multiple simulation runs, and the spread of the data points around the mean. The error bars indicate high variability in NFC, suggesting unstable packet delivery performance due to retransmissions, whereas PFC_DCDU exhibits smaller error margins, demonstrating consistent reliability. A marginal improvement in UL_PDR between PFC and PFC_DCDU is attributed to the dynamic confirmed data update mechanism.

7.1.2. No.BorderEDs vs. CPSR (Confirmed Packet Success Rate)

The confirmed packet success rate is the probability that the transmitted uplink packets and their corresponding downlink packets are received by the network server and the ED, respectively, in at least one of the available transmission attempts. The analysis of the results reveals that NFC experiences a sharp decline in CPSR, from 0.65 to 0.45, as node density increases, indicating severe network degradation due to congestion and retransmission overhead. PFC and PFC_DCDU maintain CPSR values above 0.9 up to 300 nodes, with a minor decline at 400 nodes, suggesting that the intelligent scheduling

of packets preserves network efficiency under high node densities. The error bar analysis shows that PFC_DCDU has smaller variations, reinforcing its robustness and stability in high-density deployments.

7.1.3. No.BorderEDs vs. Energy Consumption

The total energy consumption comprises the energy utilized by all the EDs. Energy efficiency is a critical factor in IoMT networks. Figure 4 illustrates the relationship between node density and energy consumption, showing that NFC leads to excessive energy consumption, exceeding 2000 J at 400 nodes, primarily due to inefficient retransmissions and packet losses. PFC and PFC_DCDU exhibit significantly lower energy consumption owing to effective congestion control and prioritization mechanisms that reduce unnecessary transmissions. The error bars for NFC are relatively large, reflecting the inconsistent nature of energy expenditure due to unpredictable retransmissions. PFC_DCDU exhibits the smallest error bars, suggesting predictable and controlled energy utilization, which is crucial for energy-constrained applications.

7.1.4. No.BorderEDs vs. Lost Packets Because of Tx Issue

Packet loss due to transmission failures is a key indicator of network performance under heavy traffic. NFC results in an exponential increase in lost packets, exceeding 2500 at 400 nodes, making it unsuitable for large-scale deployments. PFC and PFC_DCDU significantly reduce packet losses, maintaining a stable and efficient transmission environment. The error bar analysis indicates that NFC experiences substantial fluctuations, signifying unreliable network performance. PFC_DCDU achieves the lowest packet loss with minimal variance, reinforcing its efficiency in handling increasing node density.

7.2. Performance at Varying Mobile Body Sensor EDs

The analysis depicted in Figure 5 provides insights into the effectiveness of different flow control strategies under varying numbers of body sensor nodes while keeping border sensor node parameters fixed. While the performance gains achieved by the PFC_DCDU model may not be substantial in every context, they are nevertheless impactful in scenarios characterized by a high node density, indicating its potential for optimizing system performance in such environments.

7.2.1. No.BodyEDs vs. Uplink Packet Delivery Ratio

UL_PDR, as depicted in the top-left graph, demonstrates the proportion of successfully received packets at the gateway. As the number of body sensor nodes increases, UL_PDR declines, particularly in the case of the "No Flow Control" approach. This degradation is attributed to network congestion, increased collisions, and excessive retransmissions, leading to packet loss. The priority-based flow control (PFC) and PFC with Dynamic CDU (PFC_DCDU) exhibit superior performance, maintaining a high UL_PDR above 95%. The effectiveness of these mechanisms is attributed to their ability to manage transmission scheduling and data prioritization, thereby reducing congestion and enhancing reliability.

7.2.2. No.BodyEDs vs. Confirmed Packet Success Rate

The CPSR, shown in the top-right graph, represents the successful reception rate of high-priority packets. The "No Flow Control" approach exhibits a sharp decline in CPSR as the number of body sensor nodes increases, dropping from approximately 0.9 to nearly 0.5. This indicates that without an intelligent flow control mechanism, critical data are severely impacted by network congestion. On the other hand, both PFC and PFC_DCDU demonstrate robustness in maintaining a CPSR above 90%. The slight decline observed in these schemes is attributed to increasing network contention; however, the proactive traffic

management employed ensures that critical packets receive a higher transmission priority, thereby sustaining reliability.

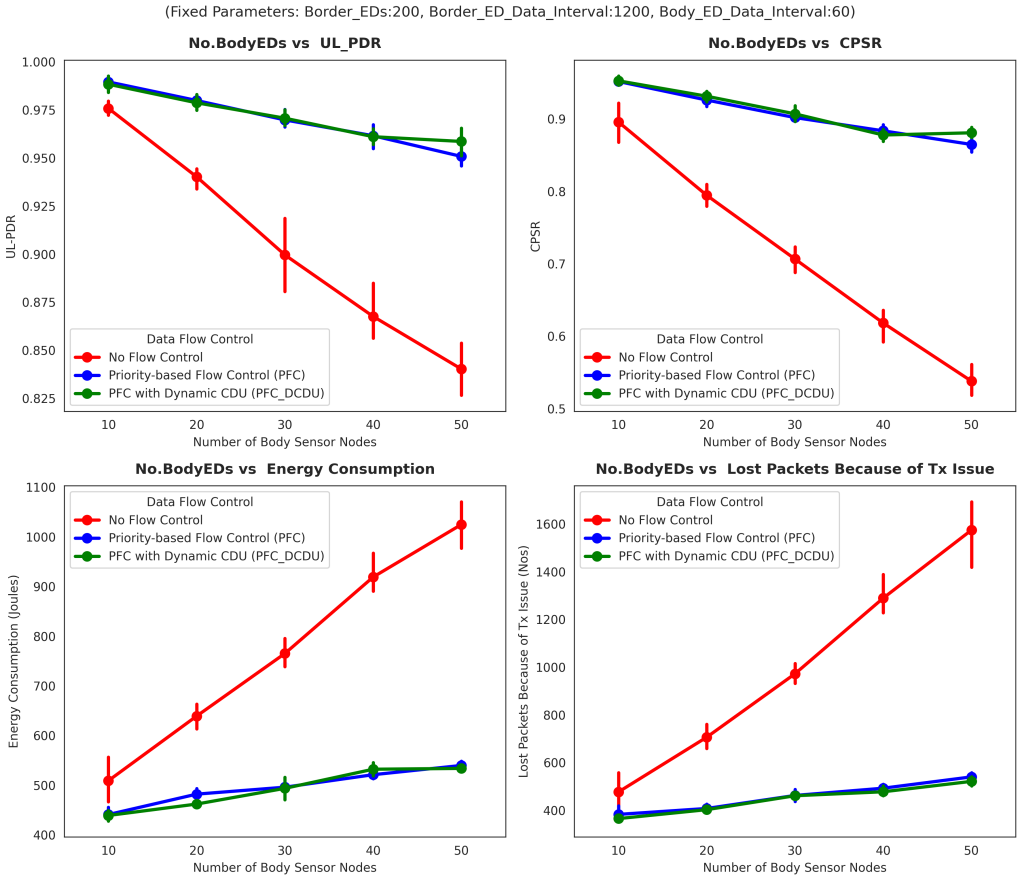

Figure 5. Performance analysis of LoRaWAN with different numbers of body sensor EDs.

7.2.3. No.BodyEDs vs. Energy Consumption

The bottom-left graph illustrates energy consumption across different flow control strategies. The "No Flow Control" scheme results in significantly higher energy consumption, increasing steeply with the number of body sensor nodes. This is due to excessive retransmissions, idle listening, and unnecessary packet forwarding, resulting in the rapid depletion of node batteries. Conversely, PFC and PFC_DCDU consume substantially less energy, with PFC_DCDU demonstrating the lowest energy usage. This efficiency is because the dynamic CDU optimizes transmission intervals and adaptively controls duty cycles, reducing redundant transmissions and conserving energy.

7.2.4. No.BodyEDs vs. Lost Packets Due to Transmission Issues

The bottom-right graph provides insights into the number of packets lost due to transmission failures. The "No Flow Control" strategy suffers from severe packet losses, escalating dramatically with increasing body sensor nodes. This further corroborates the earlier findings that network congestion and excessive retransmissions lead to deteriorating performance. In contrast, PFC and PFC_DCDU significantly mitigate packet losses, with PFC_DCDU performing slightly better. These mechanisms' proactive congestion management and intelligent transmission scheduling ensure more efficient channel utilization, reducing the likelihood of packet drops.

7.3. Performance at Varying Static Border Sensor Data Intervals

Figure 6 presents the results, which provide insights into the effectiveness of the proposed protocol's performance under varying border sensor intervals in terms of key performance metrics, including UL_PDR, CPSR, energy consumption, and lost packets due to transmission issues. The analysis compares the three different data flow control mechanisms.

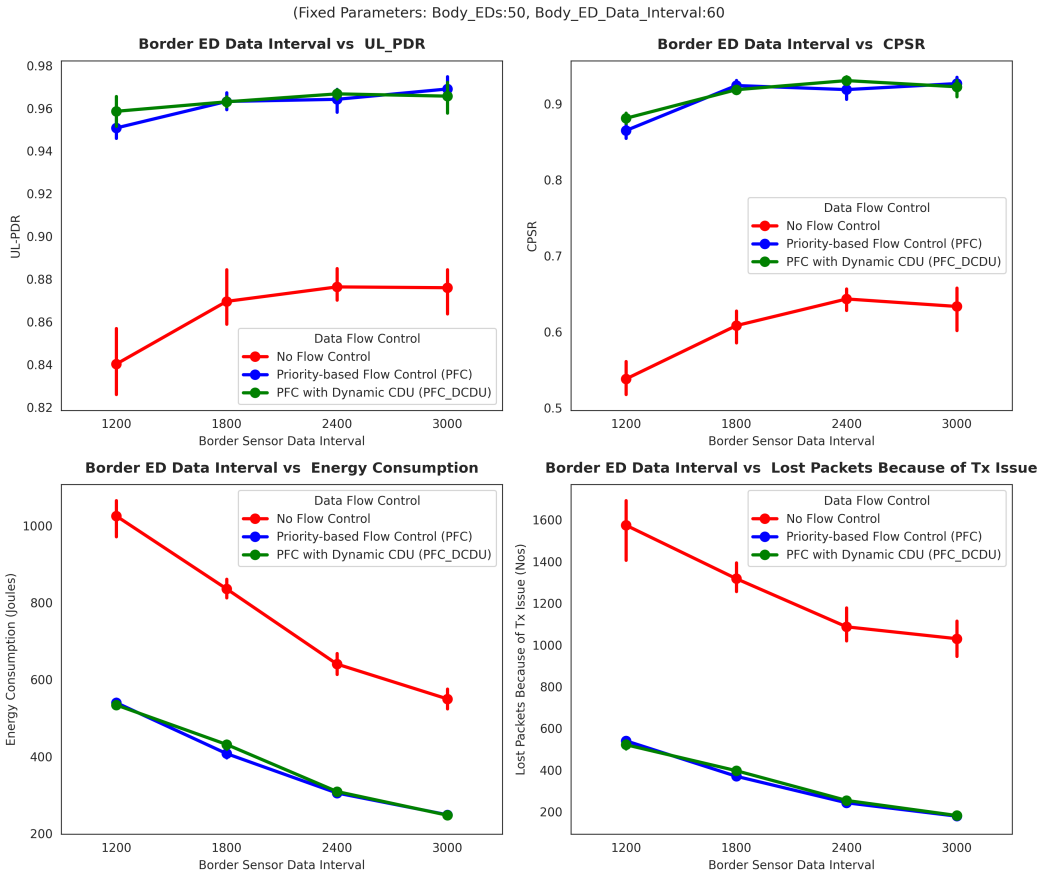

Figure 6. Performance analysis of LoRaWAN with different border sensor data intervals.

7.3.1. Impact on Uplink Packet Delivery Ratio

The figure illustrates the relationship between the border sensor data interval and UL_PDR. The results indicate that UL_PDR improves with increasing data intervals, showing a consistent upward trend. Notably, the No Flow Control exhibits significantly lower UL_PDR values compared to the flow control mechanisms, indicating its inefficiency in handling network congestion. Both PFC and PFC_DCDU demonstrate superior performance, with PFC_DCDU marginally outperforming PFC. This suggests that the dynamic CDU mechanism further enhances data packet delivery reliability by effectively managing network resources.

7.3.2. Impact on Confirmed Packet Success Rate

The CPSR results follow a trend similar to UL_PDR, where increasing data intervals lead to improved control packet success rates. The No Flow Control scheme performs significantly worse, stabilizing below 0.6, whereas both PFC and PFC_DCDU maintain a CPSR above 0.85, reflecting their ability to manage packet transmissions efficiently. The slight advantage of PFC_DCDU over standard PFC suggests that dynamic CDU mechanisms optimize control packet delivery.

7.3.3. Impact on Energy Consumption

The energy consumption results exhibit a downward trend, implying that increasing the data interval reduces energy expenditure across all schemes. This reduction is most pronounced for the No Flow Control scheme, which initially consumes the highest energy (above 1000 J at the smallest interval) but gradually decreases as the interval increases. The PFC and PFC_DCDU schemes consistently exhibit significantly lower energy consumption. Among them, PFC_DCDU achieves the lowest energy usage, reinforcing its efficiency in balancing transmission needs and energy expenditure. These results confirm that flow control strategies improve network longevity by reducing unnecessary retransmissions and collisions.

7.3.4. Impact on Lost Packets Due to Transmission Issues

The bottom-right plot quantifies the number of packets lost due to transmission failures. The No Flow Control mechanism exhibits the highest packet loss, with over 1600 packets lost at the smallest interval. As the interval increases, packet loss decreases; however, it remains significantly higher than the flow-controlled approaches. Both PFC and PFC_DCDU maintain substantially lower lost packet counts, with PFC_DCDU showing a slight edge over standard PFC. These findings suggest that flow control mechanisms—especially those incorporating dynamic CDU—effectively mitigate packet loss by optimizing transmission efficiency.

The results conclusively demonstrate that employing a data flow control mechanism significantly improves network reliability, reduces energy consumption, and enhances packet delivery efficiency. Among the evaluated approaches, the PFC_DCDU scheme consistently outperforms the others, achieving optimal trade-offs between energy efficiency and data reliability. The findings emphasize the necessity of adaptive flow control techniques in large-scale IoT deployments, particularly in mission-critical applications such as health monitoring and emergency response systems.

7.4. Priority-Based Performance Metrics

This section comprehensively evaluates throughput performance under the priority-based flow control (PFC) protocol, examining how priority levels (Pr = 0, 1, and 2) influence network efficiency and reliability. Throughput is measured as the number of successful packets delivered per minute per gateway, taking into account collision rates, transmission intervals, and confirmed delivery mechanisms. Table 4 summarizes the analysis of the simulation results.

Table 4. Priority-based performance metrics.

Metric	Pr = 2	Pr = 1	Pr = 0
Interval (s)	0 (immediate)	300	600
Avg. Throughput	12–15 pkts/min	3–5 pkts/min	1–2 pkts/min
Packet Loss	<5%	8–12%	15–20%
Energy/packet	0.46 mJ	0.32 mJ	0.18 mJ
Latency	<100 ms	<5 min	<10 min

For high-priority traffic (Pr = 2), the protocol achieves near-real-time delivery (12–15 packets per minute per gateway) with consistent sub-100ms latency, even in dense deployments of up to 400 nodes. This is accomplished through immediate transmission, prioritized channel access, and the use of minimal spreading factors (SF7). Medium-priority traffic (Pr = 1) maintains a balance between data freshness and network efficiency, delivering 3–5 packets per minute with controlled latency under 5 min, while the dynamic 300 s

transmission interval adapts to network load. Low-priority traffic (Pr = 0) operates with intentional packet dropping (15–20%) during congestion, which preserves higher-priority throughput and stabilizes overall network interference. The results confirm that PFC's tiered approach successfully meets the distinct requirements of critical, important, and background data flows.

The protocol's performance remains robust across different network densities and mobility scenarios. Even at peak loads, the Pr = 2 throughput shows only minimal degradation ($\leq$10% at 400 nodes), while Pr = 1 maintains reliable service through adaptive intervals and PFC_DCDU's confirmed delivery mechanism. The strategic dropping of Pr = 0 packets during congestion prevents network overload while still capturing 90% of sensor trends. These results validate that PFC's design choices, including priority-specific transmission intervals, dynamic spreading factor selection, and controlled packet dropping, collectively optimize the trade-offs between latency, throughput, and energy efficiency. The protocol's ability to maintain stratified quality-of-service levels makes it particularly suitable for mixed-criticality IoMT applications where both urgent alerts and routine monitoring must coexist on resource-constrained networks.

7.5. Generalization to Alternative Topologies

While the PFC_DCDU protocol is designed for LoRaWAN's star-of-stars topology, its priority-based flow control principles could extend to other IoT network architectures, albeit with distinct trade-offs. In mesh networks, PFC's interval-based prioritization could integrate with multi-hop routing to enforce end-to-end priority handling, although latency may increase for high-priority packets due to hopping. Cluster-tree topologies naturally align with PFC's tiered priorities, where cluster heads can locally schedule traffic. However, bottlenecks near the root may require dual-homing for critical nodes. For MANETs, dynamic topology changes would necessitate cross-layer coordination to maintain priority queues across transient links, potentially combining PFC's intervals with location-aware priority assignment. In cellular IoT, PFC could be mapped to existing QoS classes, although energy costs may increase for low-priority devices. Hybrid topologies such as mesh-star would require gateway-based priority translation to ensure consistent behavior across segments. Across all architectures, PFC's core mechanism—dynamic interval tuning based on priority—remains applicable; however, its efficacy depends on topology-specific adaptations to address challenges such as resource allocation fairness, priority inversion, and mobile node management. This flexibility suggests PFC could serve as a template for priority-aware IoT communication beyond LoRaWAN, with implementation suggestions guided by deployment conditions.

8. Conclusions

In this work, we developed an enhanced sensor data sender application capable of simulating priority-based traffic within LoRaWAN, specifically targeting use cases such as border security and healthcare monitoring. We introduced a priority-based data flow control protocol designed to optimize network performance under high data rate conditions typical in healthcare without compromising overall system reliability and efficiency. The simulation results demonstrate that the proposed protocol effectively mitigates performance bottlenecks, ensuring robust and energy-efficient communication in critical IoMT applications operating in austere environments. Through simulations, we demonstrated that the PFC and PFC_DCDU models significantly improved the uplink packet delivery ratio (by up to 20%), confirmed packet success rate (by up to 30%), and reduced network congestion (by 25%) compared to conventional fixed-interval transmission approaches. The findings indicate that adaptive flow control mechanisms reduce

unnecessary retransmissions by 40%, enhance energy efficiency by 15%, and optimize data prioritization for mission-critical IoMT applications. Notably, the PFC_DCDU model exhibited superior performance in high-density environments, suggesting its suitability for large-scale deployments that require robust real-time communication. While the proposed protocol improves network performance and energy conservation, it does not account for dynamic mobility patterns that could affect network stability and packet delivery. To address this limitation, future research will focus on exploring a cross-layer optimization approach to enhance adaptability across different network conditions and resource constraints, the integration of machine learning techniques to further optimize data rate adaptation, and dynamic priority scheduling. Future work could also explore the impact of different topologies on the proposed priority-based approach.

Author Contributions: R.K.: Conceptualization, Methodology, Writing—original draft, Writing—review and editing. H.C.M.: Conceptualization, Writing—review and editing. A.D.F.: Conceptualization, Writing—review and editing. All authors have read and agreed to the published version of the manuscript.

Funding: The research was sponsored by ARO, accomplished under Grant Number: W911NF-22-1-0006. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of ARO or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for government purposes notwithstanding any copyright notation herein.

Data Availability Statement: The original contributions presented in the study are included in the article. Further inquiries can be directed to the corresponding author.

Acknowledgments: This research is limited to the academic field of priority-based communication protocols for low-power IoT networks, which aims to improve emergency response efficiency in healthcare and remote monitoring scenarios. While the proposed protocol is evaluated in a simulated military IoT context (border security and soldier health monitoring), its primary purpose is to enhance life-saving capabilities through reliable data transmission in austere environments and does not pose a threat to public health or national security. The authors acknowledge the dual-use potential of research involving wireless surveillance technologies and confirm that all simulations are conducted in controlled academic environments (ns-3) without connection to physical hardware or real-world deployments. As an ethical responsibility, authors strictly adhere to relevant national and international laws about DURC. The authors advocate for responsible deployment, ethical considerations, regulatory compliance, and transparent reporting to mitigate misuse risks and foster beneficial outcomes.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Lavric, A.; Petrariu, A.I.; Popa, V. SigFox Communication Protocol: The New Era of IoT? In Proceedings of the 2019 International Conference on Sensing and Instrumentation in IoT Era (ISSI), Lisbon, Portugal, 29–30 August 2020; pp. 1–4.
2. Routray, S.K.; Mohanty, S. *Principles and Applications of Narrowband Internet of Things (NBIoT)*; IGI Global: Hershey, PA, USA, 2021.
3. *How RPMA Works*; White Paper; Ingenu Inc.: San Diego, CA, USA, 2016.
4. Mekki, K.; Bajic, E.; Chaxel, F.; Meyer, F. Overview of Cellular LPWAN Technologies for IoT Deployment: Sigfox, LoRaWAN, and NB-IoT. In Proceedings of the 2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Athens, Greece, 19–23 March 2018; pp. 197–202.
5. Magrin, D.; Centenaro, M.; Vangelista, L. Performance Evaluation of LoRa Networks in a Smart City Scenario. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017; pp. 1–7.
6. Basford, P.J.; Bulot, F.M.; Apetroaie-Cristea, M.; Cox, S.J.; Ossont, S.J. LoRaWAN for Smart City IoT Deployments: A Long Term Evaluation. *Sensors* **2020**, *20*, 648. [CrossRef] [PubMed]
7. Arshad, J.; Aziz, M.; Al-Huqail, A.A.; Zaman, M.H.; Husnain, M.; Rehman, A.U.; Shafiq, M. Implementation of a LoRaWAN Based Smart Agriculture Decision Support System for Optimum Crop Yield. *Sustainability* **2022**, *14*, 827. [CrossRef]

8. Shahjalal, M.; Islam, M.M.; Alam, M.M.; Jang, Y.M. Implementation of a Secure LoRaWAN System for Industrial Internet of Things Integrated with IPFS and Blockchain. *IEEE Syst. J.* **2022**, *16*, 5455–5464. [CrossRef]
9. Manikandan, P.; Patel, R.; Gopalakrishnan, S.; Palaniswamy, K. Revolutionizing Industrial IoT with LoRaWAN for Smarter and Greener Industries. In Proceedings of the 2024 IEEE East-West Design & Test Symposium (EWDTS), Yerevan, Armenia, 13–17 November 2024; pp. 1–5.
10. Nalbant, K.G.; Almutairi, S.; Alshehri, A.H.; Kemal, H.; Alsuhibany, S.A.; Choi, B.J. An Efficient Algorithm for Data Transmission Certainty in IIoT Sensing Network: A Priority-Based Approach. *PloS ONE* **2024**, *19*, e0305092. [CrossRef]
11. Alshehri, F.; Muhammad, G. A Comprehensive Survey of the Internet of Things (IoT) and AI-Based Smart Healthcare. *IEEE Access* **2020**, *9*, 3660–3678. [CrossRef]
12. Slaný, V.; Lučanský, A.; Koudelka, P.; Mareček, J.; Krčálová, E.; Martínek, R. An Integrated IoT Architecture for Smart Metering Using Next Generation Sensor for Water Management Based on LoRaWAN Technology: A Pilot Study. *Sensors* **2020**, *20*, 4712. [CrossRef]
13. Gbadamosi, S.A.; Hancke, G.P.; Abu-Mahfouz, A.M. Building Upon NB-IoT Networks: A Roadmap Towards 5G New Radio Networks. *IEEE Access* **2020**, *8*, 188641–188672. [CrossRef]
14. Kufakunesu, R. Energy-Efficient Adaptive Data Rate Optimisation Scheme for LoRaWAN. Ph.D. Thesis, University of Pretoria, Pretoria, South Africa, 2023.
15. Haxhibeqiri, J.; De Poorter, E.; Moerman, I.; Hoebeke, J. A Survey of LoRaWAN for IoT: From Technology to Application. *Sensors* **2018**, *18*, 3995. [CrossRef]
16. Kufakunesu, R.; Hancke, G.P.; Abu-Mahfouz, A. A Fuzzy-Logic Based Adaptive Data Rate Scheme for Energy-Efficient LoRaWAN Communication. *J. Sens. Actuator Netw.* **2022**, *11*, 65. [CrossRef]
17. Kufakunesu, R.; Hancke, G.P.; Abu-Mahfouz, A.M. Collision Avoidance Adaptive Data Rate Algorithm for LoRaWAN. *Future Internet* **2024**, *16*, 380. [CrossRef]
18. da Silva, J.C.; Flor, D.d.L.; de Sousa Junior, V.A.; Bezerra, N.S.; de Medeiros, A.A. A Survey of LoRaWAN Simulation Tools in ns-3. *J. Commun. Inf. Syst.* **2021**, *36*, 17–30. [CrossRef]
19. Marais, J.M.; Abu-Mahfouz, A.M.; Hancke, G.P. A Review of LoRaWAN Simulators: Design Requirements and Limitations. In Proceedings of the 2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC), Vanderbijlpark, South Africa, 21–22 November 2019; pp. 1–6.
20. Idris, S.; Karunathilake, T.; Förster, A. Survey and Comparative Study of LoRa-Enabled Simulators for Internet of Things and Wireless Sensor Networks. *Sensors* **2022**, *22*, 5546. [CrossRef] [PubMed]
21. Reynders, B.; Wang, Q.; Pollin, S. A LoRaWAN Module for ns-3: Implementation and Evaluation. In *Proceedings of the 10th Workshop on ns-3*, ACM: 2018, Surathkal, India, 13–14 June 2018 ; pp. 61–68.
22. Van den Abeele, F.; Haxhibeqiri, J.; Moerman, I.; Hoebeke, J. Scalability Analysis of Large-Scale LoRaWAN Networks in ns-3. *IEEE Internet Things J.* **2017**, *4*, 2186–2198. [CrossRef]
23. To, T.H.; Duda, A. Simulation of LoRa in NS-3: Improving LoRa Performance with CSMA. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–7.
24. Magrin, D.; Capuzzo, M. LoRaWAN ns-3 Module. Available online: https://github.com/signetlabdei/lorawan (accessed on 17 April 2020).
25. Clausen, T.; Jacquet, P. *RFC3626: Optimized Link State Routing Protocol (OLSR)*; Technical Report; Internet Engineering Task Force (IETF): Fremont, CA, USA, 2003.
26. Ramanathan, R.; Redi, J. A Brief Overview of Ad Hoc Networks: Challenges and Directions. *IEEE Commun. Mag.* **2002**, *40*, 20–22. [CrossRef]
27. Rath, M.; Pattanayak, B.K.; Pati, B. Energy Efficient MANET Protocol Using Cross Layer Design for Military Applications. *Def. Sci. J.* **2016**, *66*. [CrossRef]
28. Speybrouck, V.; Despoux, E.; Kim, Y. A Study on The Use of Cognitive Radio Networks in The Military Operation Environment. *J. Converg. Inf. Technol.* **2021**, *11*, 106–114.
29. Parvin, J.R. An Overview of Wireless Mesh. In *Wireless Mesh Networks: Security, Architectures and Protocols*; IntechOpen: London, UK, 2020 ; pp. 1–16.
30. Dubey, R.; Louis, S.J.; Sengupta, S. Evolving Dynamically Reconfiguring UAV-hosted Mesh Networks. In Proceedings of the 2020 IEEE Congress on Evolutionary Computation (CEC), Glasgow, UK, 19–24 July 2020; pp. 1–8.
31. Musa, U.; Shah, S.M.; Majid, H.A.; Mahadi, I.A.; Rahim, M.K.A.; Yahya, M.S.; Abidin, Z.Z. Design and Implementation of Active Antennas for IoT-Based Healthcare Monitoring System. *IEEE Access* **2024**, *12*, 48453–48471. [CrossRef]
32. Kufakunesu, R.; Myburgh, H.; De Freitas, A. The Internet of Battle Things: A Survey on Communication Challenges and Recent Solutions. *Discov. Internet Things* **2025**, *5*, 3. [CrossRef]

33. Koppaka, A.; Aravindh, P.; Aneesh, M.; Valsan, V. Navigating the Waves: IoT Border Alert System for Maritime Safety. In Proceedings of the 2024 International Conference on Advances in Computing Research on Science Engineering and Technology (ACROSET), Indore, India, 27–28 September 2024; pp. 1–8.
34. Babayigit, B.; Abubaker, M. Industrial Internet of Things: A Review of Improvements Over Traditional Scada Systems for Industrial Automation. *IEEE Syst. J.* **2023**, *18*, 120–133. [CrossRef]
35. Koutras, D.; Stergiopoulos, G.; Dasaklis, T.; Kotzanikolaou, P.; Glynos, D.; Douligeris, C. Security in IoMT Communications: A survey. *Sensors* **2020**, *20*, 4828. [CrossRef]
36. Mohamed, A.; Wang, F.; Butun, I.; Qadir, J.; Lagerström, R.; Gastaldo, P.; Caviglia, D.D. Enhancing Cyber Security of LoRaWAN Gateways under Adversarial Attacks. *Sensors* **2022**, *22*, 3498. [CrossRef] [PubMed]
37. Hessel, F.; Almon, L.; Hollick, M. LoRaWAN Security: An Evolvable Survey on Vulnerabilities, Attacks and Their Systematic Mitigation. *ACM Trans. Sens. Netw.* **2023**, *18*, 1–55. [CrossRef]
38. Dave, J.; Choudhury, N. Security Enhancement of OTAA based Joining Procedure in LoRaWAN for Satellite Communication. In Proceedings of the 2024 IEEE 99th Vehicular Technology Conference (VTC2024-Spring), Singapore, 24–27 June 2024; pp. 1–5.
39. Sarode, S.S.; Bakal, J.W. A Data Transmission Protocol for Wireless Sensor Networks: A Priority Approach. *J. Telecommun. Electron. Comput. Eng. (JTEC)* **2018**, *10*, 65–73.
40. Bahattab, A.A.; Trad, A.; Youssef, H. PEERP: An Priority-Based Energy-Efficient Routing Protocol for Reliable Data Transmission in Healthcare Using the IoT. *Procedia Comput. Sci.* **2020**, *175*, 373–378.
41. Rana, B.; Singh, Y.; Singh, P.K.; Hong, W.C. A Priority Based Energy-Efficient Metaheuristic Routing Approach for Smart Healthcare System (SHS). *IEEE Access* **2024**, *12*, 85694–85708. [CrossRef]
42. Finochietto, M.; Santos, R.; Ochoa, S.F.; Meseguer, R. Reducing Operational Expenses of LoRaWAN-Based Internet of Remote Things Applications. *Sensors* **2022**, *22*, 7778. [CrossRef]
43. Alsiddiky, A.; Awwad, W.; Fouad, H.; Hassanein, A.S.; Soliman, A.M. Priority-Based Data Transmission Using Selective Decision Modes in Wearable Sensor Based Healthcare Applications. *Comput. Commun.* **2020**, *160*, 43–51. [CrossRef]
44. Carvalho, D.F.; Ferrari, P.; Sisinni, E.; Flammini, A. Improving Redundancy in LoRaWAN for Mixed-Criticality Scenarios. *IEEE Syst. J.* **2020**, *15*, 3682–3691. [CrossRef]
45. Magrin, D. LoRaWAN Simulations Using ns-3. Available online: https://www.nsnam.org/tutorials/consortium19/wns3-lorawan.pdf (accessed on 17 November 2024).
46. NS3 NetAnim Animator. Available online: https://www.nsnam.org/wiki/NetAnim (accessed on 20 October 2024).
47. Semtech. SX1301 Data Sheet_v2.4. 2017. Available online: https://www.semtech.com/products/wireless-rf/lora-core/sx1301 (accessed on 8 June 2022).
48. Semtech. SX1272 Data Sheet_v4. 2019. Available online: https://www.semtech.com/products/wireless-rf/lora-core/sx1272 (accessed on 8 June 2022).
49. Slabicki, M.; Premsankar, G.; Di Francesco, M. Adaptive Configuration of LoRa Networks for Dense IoT Deployments. In Proceedings of the NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium, Taipei, Taiwan, 23–27 April 2018; pp. 1–9.
50. Hauser, V.; Hégr, T. Proposal of Adaptive Data Rate Algorithm for LoRaWAN-Based Infrastructure. In Proceedings of the 2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud), Prague, Czech Republic, 21–23 August 2017; pp. 85–90.
51. Gaussian Waves Log Distance Model. Available online: https://www.gaussianwaves.com/2013/09/log-distance-path-loss-or-log-normal-shadowing-model/ (accessed on 14 August 2021).