International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

An Efficient and Optimized Backoff Scheme for Disseminating Heterogeneous Traffic for Multiple Instances of LLN-Based Industrial IOT Networks.

Animesh Giri[1*] **and Dr Annapurna**[2]

Submitted: 05/02/2024 **Revised**: 13/03/2024 **Accepted**: 19/03/2024

Abstract: With numerous devices being connected to the Internet to create a network of smart things, the Internet of Things (IoT) has experienced rapid growth in recent years. However, because of their constrained power, processing, and bandwidth, these devices frequently require assistance with network efficiency and dependability.

In order to overcome the difficulties of distributing heterogeneous traffic across numerous instances of low power and Lossy-IoT networks, this research suggests an effective, optimized backoff scheme. The suggested method makes use of backoff algorithms in conjunction with network coding to increase network efficiency and reliability while decreasing transmission delay.

The binary exponential-backoff (BEB) algorithm and the truncated binary exponential backoff (TBEB) algorithm are two of the backoff algorithms used in the suggested scheme. The BEB algorithm is used to resolve collisions during transmission, while the TBEB algorithm is used to reduce the backoff stage and the transmission delay.

The suggested scheme also makes use of network coding, which raises the network's dependability by enabling multiple nodes to work collectively to transmit data, reducing the likelihood of data loss, and guaranteeing that the data reaches its target location.

Extensive simulations are used to evaluate the performance of the proposed scheme, and the results show that it performs better than traditional backoff algorithms in terms of network efficiency, reliability, and transmission delay. The outcomes also show that the suggested method can manage heterogeneous traffic, which qualifies it for IoT networks with a variety of devices and applications. In conclusion, the suggested effective, optimized backoff scheme offers a potentially viable answer to the problems faced by lossy, low-power IoT networks. The scheme's combination of backoff algorithms and network coding enhances network efficiency and reliability while reducing transmission delay, making it an attractive option for IoT network deployments.

Keywords: *IIoT, Heterogeneous Traffic, MAC Layer Prioritization, Multi-Instances, RPL*

1 Introduction

The classic CSMA/CA (Carrier-Sense Multiple Access / Collision Avoidance) protocols [1], while containing the Binary Exponential Backoff (BEB) algorithm to manage colliding packets, lacks prioritization techniques. Consequently, all packets are treated equally, disregarding any inherent distinctions. Our research addresses this limitation by introducing a data prioritization framework within the CSMA MAC layer. This introduction is beneficial, especially to an Industrial IoT setup, since various devices provide various kinds of data. Some data streams carry time-critical data, while others have periodic characteristics.

1.1 Prioritization of Heterogeneous Data in RPL

RPL(Routing Protocol for low power and lossy networks) [2] is an optimal choice for environments constrained by time, power, and resources. When integrating data prioritization inside the MAC (Medium Access Control) layer of IoT [3] devices, RPL (Routing Protocol for Low-Power and Lossy Networks) has shown to be quite beneficial, especially in the context of industrial settings. Due to the network hierarchy's smooth alignment with data prioritization, higher-priority data may be distributed to higher levels of the network hierarchy. Because RPL's goal functions are programmable, it is possible to pick a customized route based on criteria like reliability and latency, efficiently prioritizing pathways that serve various data priority levels. Multiple instance support allows RPL to accept different priority assignments within the network, and its constraint optimization techniques guarantee effective data transfer with little resource use.

An Objective Function [4] is a set of rules that define the routing behaviour of the network, including selecting the most appropriate paths for data transmission based on various metrics, such as hop count, latency, and reliability. MRHOF (Minimum Rank with Hysteresis

---

[1*] *Research Scholar, Department of Computer Science and Engineering, PESIT - Bangalore South Campus, Bengaluru, 560100, Karnataka, India Visvesvaraya Technological University, Belagavi, 590018, Karnataka, India. animeshgiri@pes.edu*

[2] *Professor, Department of Computer Science and Engineering, PESIT Bangalore South Campus, Bengaluru, 560100, Karnataka, India. annapurnad@pes.edu*

***Corresponding Author:** *Animesh Giri*

**Research Scholar, Department of Computer Science and Engineering, PESIT - Bangalore South Campus, Bengaluru, 560100, Karnataka, India Visvesvaraya Technological University, Belagavi, 590018, Karnataka, India. animeshgiri@pes.edu*

Objective-Function) and OF0 (Objective-function 0) are the most common objective functions. MRHOF optimizes the overall ETX, while OF0 focuses on reducing hop counts. We shall be using instances of both MRHOF and OF0 in our framework to make the overall network more efficient.

1.2 Why Standard IEEE 802.15.4

The standard IEEE 802.15.4 [5] defines the physical and medium-access control (MAC) layers for low rate wireless personal area networks (LR-WPANs), does not consider data prioritisation for several reasons:

1. Focus on simplicity: The primary focus of the IEEE 802.15.4 standard is simplicity, has low power consumption, and low cost. As such, the standard does not include complex mechanisms for data prioritization, which would increase the cost and complexity of the network.

2. Limited network resources: LR-WPANs are designed to operate with limited network resources, such as bandwidth and battery power. Because the network's limited resources are shared by all devices, data priority is not a crucial element in these networks.

3. Non-real-time applications: The majority of LR-WPAN applications are nonreal-time in nature, such as building automation, home automation, and sensor networks. In these types of application, data prioritization is not considered a critical factor as the network is designed to support low-rate and low-latency data transmission.

4. Open loop architecture: IEEE 802.15.4 standard uses an open-loop architecture where the MAC layer does not provide feedback to the higher layers. This makes data prioritisation difficult to achieve since the MAC layer cannot alter the transmission rate based on data priority.

In conclusion, the IEEE 802.15.4 standard does not take into consideration data prioritization due to its focus on simplicity, limited network resources, non-real-time applications, and open-loop architecture. However, some of the IoT networks may require data prioritization, which can be achieved through additional protocols or network management techniques as implemented by us.

IEEE 802.15.4 is a standard for low rate - wireless personal area networks (LRWPANs). It defines the physical and data link layer specifications. The standard uses Carrier sense Multiple access with collision avoidance (CSMA/CA) as the Medium Access Control (MAC) protocol to avoid collisions between devices and efficiently share the channel.

1.3 Use of our complex backoff algorithm estimating backoff time-slots

The standard CSMA protocol [6] is unable to distinguish between data streams with different priorities, which causes delays in the transmission of crucial data. Furthermore, because it assumes that a clear communication channel denotes availability, it is ineffective in situations where multiple devices are competing for access with varying priorities, increasing contention and latency. Although fair, the protocol's equal-access approach fails when some devices need more frequent or dependable access because of their importance in transmitting mission-critical data.

An approach for determining the appropriate backoff time slots for prioritised data in low power and lossy IoT networks has been developed to address this issue. The backoff algorithm regulates the transmission rate of different types of data based on their priority and the available network resources.

A shorter backoff interval is given to data with higher priority, enabling faster transmission. In contrast, data that is less important is given a longer backoff period, which lowers the transmission rate and lowers the chance of network congestion. In order to ensure that crucial data is transmitted quickly and reliably, low-power and lossy IoT networks can be made much more effective by using a complex backoff algorithm. Non-critical data, on the other hand, is transmitted more slowly, reducing the possibility of network congestion and enhancing overall network performance.

2 Related Work

Shagufta Henna, et al [7] introduced an intelligent protocol named RAI-MAC which adjusts retransmission priorities based on past failures, reducing collisions and delays. RAI-MAC is an adaptive protocol for IEEE 802.5.4- based WBANs.

Anjum I et al [8] in their paper introduced the concept of PLA-MAC which is a priority based , traffic-load adaptive protocol for heterogeneous BSNs. Classification of data packets is based on QoS, calculates priorities, and dynamically adjusts the superframe structure. The protocol improves QoS by adaptive transmission scheduling , outperforming existing protocols and prioritized .

Sahoo et al [9] in their paper introduced a novel synchronous MAC protocol for wireless sensor network. It's emphasis is on energy efficient real time data transmission. The approach includes efficient channel access and relay node selection.

The challenges related to cross-platform implementations of MAC protocols like timing bugs, hardware-dependent issues, and performance variations are addressed by Bauwens Jan et al [10] in their paper. They proposed a methodology to overcome these challenges and enhance cross-platform MAC development.

Li S et al [11] in their paper explored the challenges associated with energy efficient and quality-of-services(QoS) capable of wireless multimedia sensor networks (WMSNs). They highlighted the unique characteristics and requirements of WMSNs, surveyed existing solutions and reviewed recent research efforts in energy-efficient communication protocols which include MAC protocols and disjoint multipath routing protocols

Kim et al [12] introduced a protocol which adjusts radio duty-cycles and contention window sizes based on traffic congestion for efficient IoT data transmission. Their proposed approach effectively reduces delays and energy consumption of the sensor nodes in IoT environments.

S Homayouni et al [13] in their paper introduced adaptive radio duty cycling for IoT networks, which dynamically adjusts RDC frequencies based on battery levels and radioactivity , thereby enhancing energy efficiency and reduced delay in low traffic networks

Fasee Ullah et al [14] in their paper introduced TraySL-MAC, a novel MAC protocol for WBANs which addressed contention and delay issues. Adaptive slot allocation algorithm prioritized data based on criticality , improving performance metrics significantly in biomedical scenarios.

An enhanced version of IEEE 802.15.4 MAC protocol for healthcare Wireless Body Area Networks (WBANs) is introduced by Rajini Gupta and Biswas S [15]. They suggest dynamic GTS allocation based on traffic levels and priority. Their simulations demonstrated enhanced energy efficiency and delay under critical conditions.

3 System Model

3.1 Traffic Classification

In the rapidly evolving landscape of Low Power and Lossy Internet-of-Things (IoT) networks, traffic classification is pivotal in optimizing communication efficiency and reliability. To achieve seamless data exchange and address the diverse requirements of IoT applications, data is categorized based on four types of priorities, enabling the network to allocate resources strategically. By prioritizing traffic, the network ensures that critical data receives the utmost attention while non-urgent information is handled efficiently, balancing resource allocation and data importance.

In industrial IoT applications [16], the significance of traffic prioritization becomes even more pronounced due to the unique challenges posed by the environment. Four instances, each with distinct characteristics, are key to understanding the importance of traffic prioritization:

Instance 1 (I1) caters to critical real-time traffic in industrial IoT applications, where time-sensitive information is paramount. It handles crucial data from safety critical systems, ensuring prompt and reliable transmission. For example, in an automated manufacturing plant, I1 is responsible for managing real-time feedback from sensors and immediate control commands to prevent accidents or disruptions in the production process. The minimal transmission delay, typically within one to five seconds, ensures that control commands and sensor data from vital machinery are promptly relayed, enabling timely decision-making and preventing potential hazards. Moreover, the small packet size optimization further enhances data delivery efficiency, minimizing the risk of data loss and guaranteeing the uninterrupted operation of industrial processes.

Instance 2 (I2) addresses non-critical real-time traffic in the industrial IoT setting. While less time-sensitive than I1, this data type remains crucial for maintaining operational visibility and allowing supervisors to monitor plant conditions. For example, I2 handles non-urgent status updates and control commands for lighting and climate control in a smart building system. The moderate delay requirements, ranging from 15 to 30 seconds, ensure reliable and timely communication, supporting efficient data exchange for process monitoring and non-critical control tasks.

Instance 3 (I3) is tailored for periodic traffic in industrial IoT applications, involving data transmission at regular intervals to support time-sensitive periodic updates. In predictive maintenance systems, for instance, sensor readings are periodically transmitted to monitor equipment health. Although I3 data may not require immediate transmission, high reliability remains essential to maintaining accurate records and ensuring timely maintenance actions. The transmission delay for I3 is typically around 180 seconds, facilitating periodic data updates, and the moderate packet size optimization enables efficient handling of cyclic data patterns, thus enhancing the predictability and effectiveness of maintenance operations.

Instance 4 (I4) caters to low-priority traffic in the industrial IoT landscape, where non-essential data can tolerate longer transmission delays. Applications like environmental monitoring or non-critical parameter logging rely on I4 to handle periodic data with time intervals of up to 360 seconds. As these data updates do not require immediate attention, I4 allows devices to conserve energy and operate in low-power modes to extend battery life. The higher packet size optimization in

I4 accommodates the periodic collection of a larger volume of data in a single transmission, striking a balance between energy efficiency and communication performance for non-urgent data.

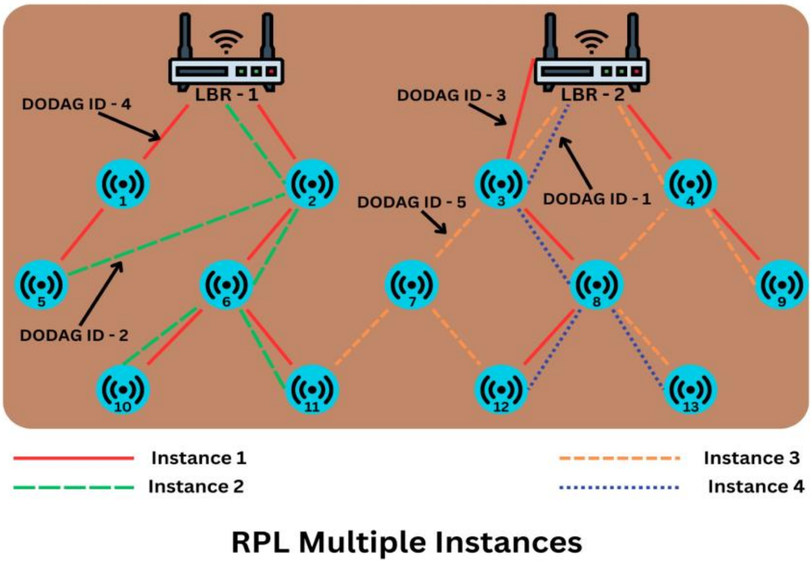

Fig. 1 Network Architecture

The prioritization of traffic based on these instances as also shown in Figure 1 becomes a critical aspect in industrial IoT environments, where communication's reliability, efficiency, and responsiveness directly impact the performance and safety of critical systems. By aligning network resources with the specific requirements of each data type, traffic prioritization optimizes the flow of information, ensures timely responses to critical events, and enhances overall communication reliability and efficiency in industrial settings.

3.2 Importance of Prioritizing Traffic Based on Its Characteristics

Traffic prioritization is a crucial strategy in low-power and lossy industrial IoT networks, optimizing resource allocation and enhancing communication reliability. It ensures timely delivery of critical data, manages congestion, minimizes latency, conserves energy, and meets quality of service requirements. Networks ensure efficient operation even during congestion by assigning higher resources and reliability to high-priority data, like critical information and real-time control commands. This approach improves user experience, extends device battery life, and maintains data integrity. In applications ranging from healthcare to industrial automation, prioritizing traffic based on characteristics enhances network efficiency, responsiveness, and sustainability.

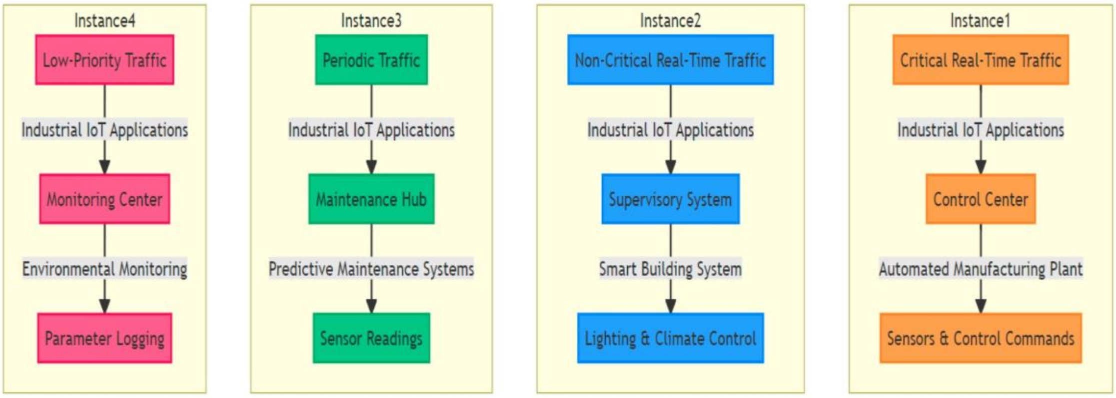

Fig. 2 Network Architecture

4 Proposed Backoff Scheme

4.1 Scheme Overview

The proposed scheme aims to efficiently address heterogeneous network traffic by introducing a priority-based approach and an optimized backup scheme. The primary goal is to manage network traffic more effectively and ensure that high-priority data precedes lower-priority data.

Each packet is assigned a priority level in this scheme, reflecting its importance and urgency. Upon receiving data for transmission, the system first checks its priority. If the data belongs to a higher-priority category, it is allocated a shorter backoff interval, allowing it to be transmitted sooner. Conversely, a longer backoff interval is assigned for data of lower priority. This deliberate delay ensures that high-priority packets can be transmitted without contention from lower-priority data.

After the designated backoff interval, the channel is examined again to determine if it is available for transmission. High-priority data has a higher chance of accessing the channel promptly due to the shorter backoff interval assigned to it. Conversely, lower-priority data will retry the message after its longer backoff interval, allowing high-priority traffic to be efficiently accommodated.

Algorithm 1.1 Initialization

```
BLE ⇐ false                      ▷ Bluetooth Low Energy is initially disabled
CW ⇐ 2                           ▷ Contention Window starts with a value of 2
NB ⇐ 0                           ▷ Number of backoffs initiated is initially 0
macMinBE ⇐ 1                     ▷ Minimum Backoff Exponent
macMaxBE ⇐ 5                     ▷ Maximum Backoff Exponent
macMaxCSMABackoffs ⇐ 4           ▷ Maximum number of backoff attempts allowed
```

Algorithm 1.2 Main Process

```
INIT CW = 2                      ▷ Set Contention Window to its initial value (2)
BLE = false                      ▷ Disable Bluetooth Low Energy (BLE) by default
```

Algorithm1.3 Determine Backoff Stage

```
if Nd with priority == 0 then ▷ High Priority Data Backoff
    BE = 1 ▷ Set Backoff Exponent (BE) to 1 for high priority data
    NB = 0 ▷ Reset the number of backoff attempts to 0
else if Nd with priority == 1 then ▷ Low Priority Data Backoff
    priority = 1 ▷ Set Priority to 1 for non-critical data
else if Nd with priority == 2 then
    priority = 2 ▷ Set Priority to 2 for periodic data
else if Nd with priority == 3 then
    priority = 3 ▷ Set Priority to 3 for low-priority data
end if
```

Algorithm 1.4 Backoff Calculation and Execution

```
while $NB \le macMaxCSMABackoffs$ do
    if Nd with priority == 0 then
        $BP = random(priority \cdot (BE + 1) + 1, 2 \cdot BE + 4 \cdot priority + 2)$ ▷Compute BP for high priority
    else
        $BP = random(2 \cdot BE + 4 \cdot priority + 2)$ ▷ Compute BP for other priorities
    end if
    if Transmission medium IDLE then
        CW = max(CW - 1, 0)                ▷ Decrement CW or reset if idle
    else
```

```
        if $CW == 0$ then
            Transmit-Data                         ▷ Transmit data when CW reaches 0
        else
            $CW = 2$                              ▷ Reset CW to its initial value
        end if
    end if
    WAIT for BP                                   ▷ Wait for the chosen Backoff Period
end while
```

Algorithm 1.5 Handling Failures and Retries

```
if $NB > macMaxCSMABackoffs$ then
    STOP with error ”Failed access to transmission medium”
else
    if $BE == 2$ then
        $BP = random((priority + 2) \cdot 2 \cdot BE - 3, 2 \cdot BE + 4 \cdot priority + 4)$
        $NB = 1$
    else if $BE == 3$ then
        $BP = random((priority + 2) \cdot 2 \cdot BE - 4 \cdot priority - 7, 2 \cdot BE + 4 \cdot priority + 4)$
        $NB = 2$
    else if $BE == 4$ then
        $BP = random(2 \cdot (BE - 1) + 4 \cdot (priority + 2) - 3, 2 \cdot BE + 4 \cdot priority)$
        $NB = 3$
    else
        $BP = random(2 \cdot (BE - 1) + 4 \cdot priority + 1, 2 \cdot (BE - 1) + 4 \cdot priority + 4)$
        $NB = 4$
    end if
end if
Perform CCA with new BP
WAIT for BP
```

The network can allocate resources more effectively using this priority-driven and optimized backoff scheme. Overall, this approach enables the network to balance the demands of heterogeneous traffic while maximizing efficiency and meeting the specific needs of various applications and services. As a result, the network becomes more robust, adaptive, and responsive, offering an enhanced user experience and improved overall performance.

Overall, adding priority to packets in IoT networks helps optimize data delivery, improve resource utilization, and enhance the network’s overall performance, ensuring that critical data is handled appropriately. This process is also depicted in Figure 3.

5 Performance Evaluation

5.1 Simulation Setup

This experiment uses the COOJA simulator, which comes bundled with the Contiki OS, as the platform for conducting simulations. The simulations are carried out using Z1 Zolertia motes, providing a reliable hardware setup. The wireless channel model chosen for the experiments is UGDM (Loss of Distance in the Unit Disk Graph Medium), ensuring a realistic representation of wireless communication characteristics. The simulation covers an area of 300m x 300m and runs for 1 hour, providing insights into the network’s performance. Each mote has a transmission range of 50 meters, allowing it to communicate with nearby nodes within this distance.

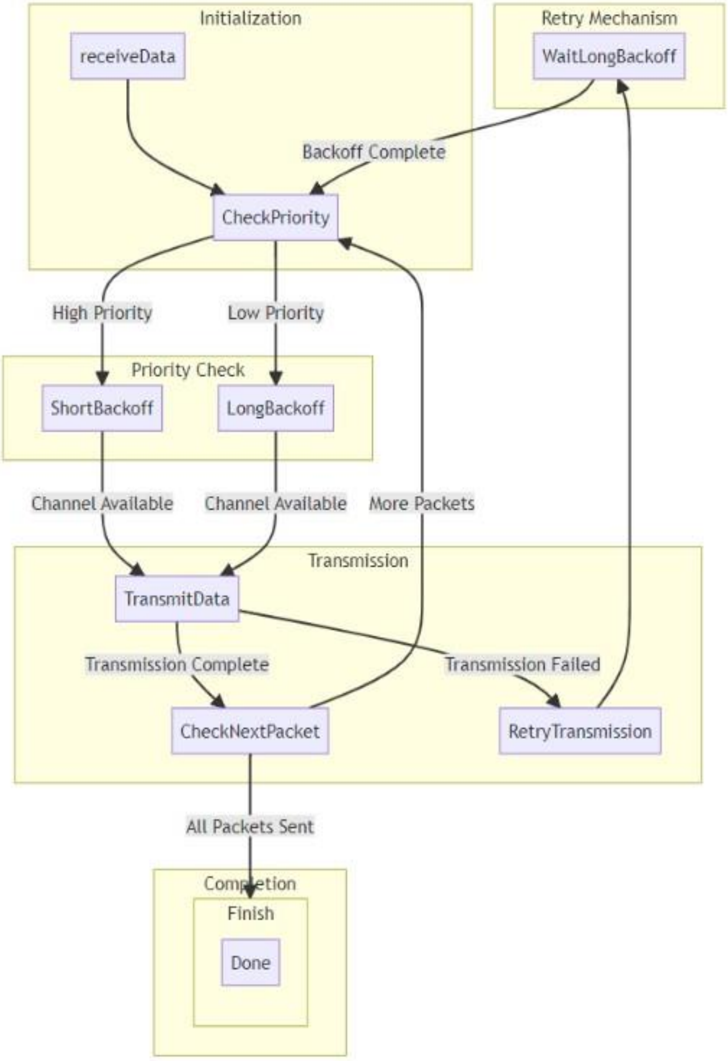

Fig. 3 Flow Chart for Proposed Scheme to Calculate Backoff Interval for Various Instances

Additionally, the interference range is set to 100 meters. The TX (transmission) ratio for all motes is fixed at 100%, ensuring that every node sends data with a high probability. The reception ratios are modified between 30%, 50%, 70%, 85%, and 100% to emulate varying reception capabilities. The 6LowPAN adaptation layer and RPL operating at the network layer facilitate seamless encapsulation and transmission of IPv6 packets over low power networks, promoting efficient data transfer. The Radio Duty Cycling (RDC) layer operates using the ContikiMAC driver, strategically alternating between active and sleep states to reduce power consumption during idle periods. The CSMA/CA protocol at the MAC layer ensures an efficient mechanism to manage access to the shared wireless medium. Table 1 shows all the parameters varied in this simulation.

Table 1 Network Simulation Environment

Simulation Parameter	**Values**
Operating System	Contiki 3.0 on Ubuntu 21.04
Mote Device Model	Z1 Zolertia
Objective Function (OF)	MHROF – ETX, OF0 – Hop Count
Wireless Channel	Unit Disk Graph Medium (UDGM)
Deployment Coverage Area	300 X 300 m
Simulation duration	3600 Seconds
TX Range	100 m
INT range	150 m
TX Ratio	Fixed at 100 %

RX Ratio	Varying as 30%, 50%, 70%, 85%, and 100%
Sender Nodes	25,50 & 75
Sink Node	2
Network Layer	IPv6, ContikiRPL
MAC Layer	Modified CSMA/CA
Adaption Layer	6LoWPAN
Radio-Duty Cycle	NullMAC / ContikiMAC
Physical Layer	IEEE 802.15.4 (Channel 26) with CC2420 2.4 GHz

Before transmitting data, a device using CSMA/CA listens to the wireless medium to detect if it is busy or idle. To avoid collisions, such devices perform a ”backoff” procedure. It chooses a random backoff time and waits for that duration before attempting to transmit. This random backoff helps to prevent multiple devices from simultaneously choosing the same transmission time, thus reducing the likelihood of collisions. Separate simulations are conducted for each instance of RPL traffic to thoroughly analyse its impact on the network. Each simulation is being carried out with different numbers of sender motes, specifically 25, 50, and 75, to investigate the network’s behavior under varying traffic instances. Furthermore, for each simulation, we employ two sink motes, which serve as the destinations for the data generated by the sender motes as seen in Fig 4.

5.2 Objective Function Selection (MRHOF vs. OF0)

5.2.1 Instances using MRHOF (ETX):

In the instances where MRHOF with the ETX (Expected Transmission-Count) metric is selected, the focus is on optimizing energy efficiency and reliability for data traffic. MRHOF efficiently finds routes with the minimum energy consumption, making it a suitable choice for scenarios with critical and time-sensitive data, such as Instance 1 and Instance 2. In these cases, where data is labelled ”Critical” and ”Non-Critical,” respectively, frequent and reliable data transmissions are crucial for monitoring and control. The ETX metric, which estimates link quality and reliability, enables the selection of paths with better transmission performance, ensuring timely and efficient data delivery. The choice of MRHOF (ETX) in these instances aligns with the requirements of low-power IoT devices, where conserving energy is essential for extending the network’s lifespan and ensuring continuous data connectivity.

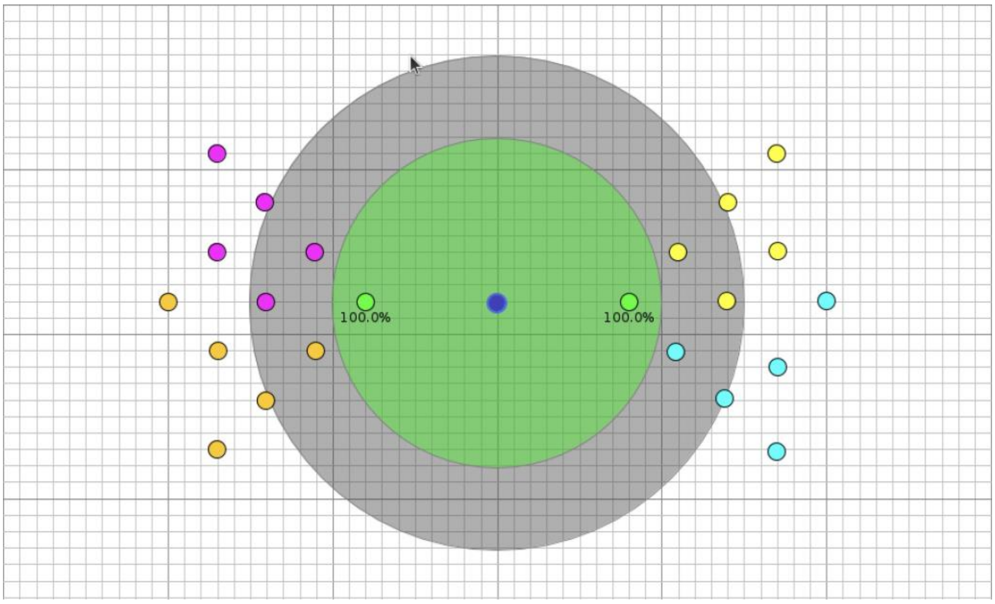

Fig. 4 Cooja Simulator Topology

5.2.2 Instances using OF0 (HC):

For instances where OF0 (Objective Function Zero) with the HC (Hop Count) metric is chosen, the emphasis is on simplicity in routing decisions, especially regarding hop count. OF0 is a straightforward objective function that only considers the hop count when selecting routes. It is well-suited for scenarios with ”Periodic” and ”LowPriority” data, such as Instance 3 and Instance 4. In these situations, the data transmissions occur at less frequent intervals, and the data may not be as time-sensitive or critical as in other instances. By selecting OF0 with HC, the routing protocol reduces computational overhead and complexity, making it more suitable for applications where low latency is not the primary concern. The HC metric ensures that routes with the least number of hops are chosen, potentially optimizing the overall path length and reducing transmission delays for less critical data updates.

5.3 Radio Duty Cycling (ContikiMAC vs. NullMAC)

5.3.1 ContikiMAC:

ContikiMAC is used as the Radio Duty Cycling (RDC) protocol when low-power and energy-efficient operation is desired. ContikiMAC employs duty cycling techniques, which enable IoT devices to shift between active and sleep modes in order to save energy. This makes it an appropriate choice for instances with ”Critical,” ”Non-Critical”, ”Periodic”, and ”Low-Priority Traffic” data traffic, such as Instance 1, Instance 2, Instance 3, and Instance 4. In these scenarios, energy efficiency is crucial due to frequent data transmissions or continuous monitoring requirements. ContikiMAC ensures that devices can conserve energy during periods of inactivity, extending the battery life of IoT devices and enabling longer network operation without sacrificing data connectivity.

5.3.2 NullMAC:

In Instance 1, where the data traffic is ”Critical,” both ContikiMAC and NullMAC are considered RDC protocols. However, the choice of NullMAC could be based on specific requirements related to power resources and simplicity. NullMAC operates more straightforwardly by eliminating duty cycling. This means that devices using NullMAC will not enter sleep states, and radio operations will always be active. NullMAC may be chosen in instances where the devices have ample power supply or emphasize simplicity, such as critical applications where the devices are directly powered, or energy consumption is not a primary concern. However, in critical scenarios where energy efficiency is paramount, ContikiMAC might still be preferred for its energy-saving capabilities.

5.4 Scenario Explanation

In this study, the Cooja Simulator, an integral component of the Contiki OS, was employed to conduct the experiment. The focus was on four distinct instances—I-1, I-2, I-3, and I-4—arranged in descending order of priority. Each instance generated packets with differing sizes and exhibited varying transmission intervals. Packets with higher priority underwent more frequent transmissions as they are time-critical data packets, while the low-priority packets underwent less frequent transmissions. Thus, the packet size for high-priority packets is kept smaller than that of low-priority packets.

The four priority data examples in an industrial IoT setting come from several sources. Instance 1 (I1) manages vital real-time data for manufacturing safety-critical systems, providing fast transmission of sensor feedback and control orders to prevent accidents. For non-critical real-time operations like lighting and climate management in smart buildings, instance 2 (I2) controls the data. As sensor readings are often transmitted in predictive maintenance systems, Instance 3 (I3) is designed for periodic data updates. Low-priority data are catered for by instance 4 (I4), including environmental monitoring. This allows devices to save energy by gathering less-urgent data at regular intervals.

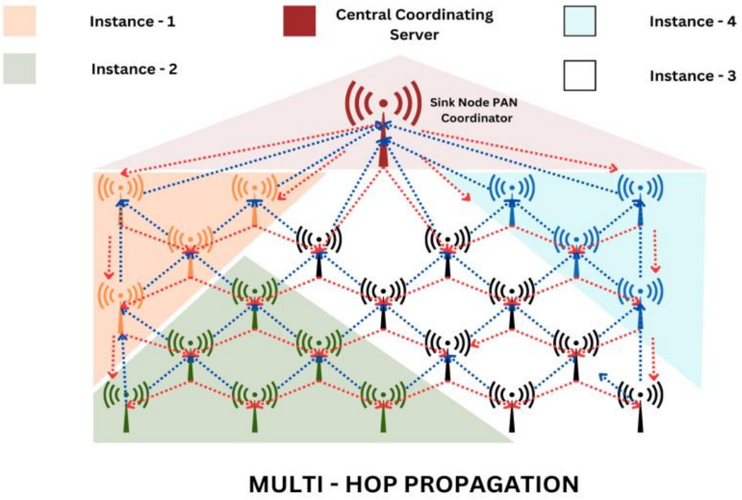

Fig. 5 Multi-Hop Propagation

For the simulation, 25,50, and 75 motes were employed for each instance type. To gather data from both MRHOF and OF0, two sink motes were utilized, accommodating both objective function types. These sink motes were subsequently linked to a border router for subsequent processing and analysis. Table 2 shows the simulation parameters used.

Table 2 PACKET SPECIFICATION

RPL Instances	Type of Data	Period	Packet Size	RDC Protocol	Objective Function
Instance 1	Critical	15	16 bytes	NullMAC/ContikiMAC	MHROF (ETX)
Instance 2	Non-Critical	30	32 bytes	ContikiMAC	MHROF (ETX)
Instance 3	Periodic	180	48 bytes	ContikiMAC	OF0 (HC)
Instance 4	Low-Priority	360	64 bytes	ContikiMAC	OF0 (HC)

6 Performance Metrics

The proposed traffic prioritization scheme in low-power and lossy IoT networks is evaluated using several performance metrics [17]that measure its efficiency and effectiveness. These metrics enable a comprehensive assessment of the scheme's impact on various aspects of network communication. The following performance metrics are instrumental in gauging the success of the prioritization scheme:

6.1 Packet Delivery Ratio (PDR)

Packet Delivery Ratio (PDR) is a critical performance metric that plays a major role in evaluating the effectiveness of the proposed traffic prioritization scheme in low-power and lossy IoT networks. PDR measures the success rate of data delivery by calculating the percentage of packets that successfully reach their intended destination out of the total packets sent by all network nodes. A higher PDR indicates a more reliable network where critical data is delivered with a higher degree of success, ensuring data integrity and reducing the likelihood of data loss during transmission.

In industrial IoT applications, where real-time and safety-critical information is prevalent, achieving a high PDR is paramount. For instance, in an automated manufacturing plant, the prioritization scheme's ability to ensure a high PDR for high-priority data instances (e.g., I1) can significantly impact the safety and efficiency of the production process. These high-priority data instances may include real-time sensor feedback, immediate control commands, or critical system status updates. The successful and timely delivery of such data is crucial for enabling prompt responses to critical events and preventing potential hazards that could result in production disruptions or accidents.

The prioritization scheme aims to optimize the allocation of network resources to prioritize high-priority data, such as I1 and I2, which require low latency and reliable communication. By dedicating ample resources and providing preferential treatment to high-priority data packets, the scheme ensures they experience lower chances of collisions, buffering delays, or packet losses, thereby contributing to a higher PDR.

Furthermore, the high PDR achieved for critical data instances directly impacts the overall performance of mission-critical applications in industrial settings. For example, in smart city [18] applications, where real-time sensor data from various IoT devices is used for traffic management or environmental monitoring, a high PDR ensures that the data is delivered reliably to the central monitoring system. This reliable delivery of critical data aids in making informed decisions promptly, leading to better traffic management, improved environmental monitoring, and enhanced overall user experience.

6.2 Latency

In the context of industrial IoT applications, latency is a crucial performance metric that directly impacts the responsiveness and efficiency of the network. Latency refers to the time taken for data packets to travel from the source node to the sink node, and it plays a significant role in real-time data communication. Prompt responses to critical events, timely decision-making, and seamless control of industrial processes heavily rely on minimizing latency.

To improve overall network performance, the prioritisation strategy focuses on reducing both end-to-end and average latency. End-to-end latency for high-priority data instances like I1 and I2 is especially important in industrial IoT scenarios where real-time data transmission is needed. End-to-end latency, for example, is critical in a smart manufacturing plant to ensure real-time sensor feedback is immediately supplied to the control system. The idea provides quick responses to sensor readings by minimising the time it takes for this important data to reach the destination, allowing the control system to make immediate modifications to the manufacturing process to avoid defects or dangers.

At the same time, the average latency statistic provides an exhaustive overview of network performance by taking into account all packets sent and received across the whole system. This larger view is crucial for determining how well the prioritisation method handles critical and non-critical data instances. While high-priority data instances aim for low end-to-end latency, non-critical data like I4 may have more lenient latency requirements. The prioritization scheme optimizes the average latency by allocating resources and managing data transmission to ensure that all data types, regardless of their priority, experience acceptable communication delays.

Achieving low average latency is essential in industrial IoT applications to maintain smooth and reliable communication across the entire network.

6.3 Energy Consumption

In smart industrial systems, energy efficiency is crucial in ensuring uninterrupted operations and minimizing downtime. The industrial IoT environment often consists of many sensors, actuators, and control devices distributed across the manufacturing plant. These devices are typically battery-powered or operate on low-power sources. Hence, optimizing their energy consumption is paramount to extending battery life and reducing overall operational costs.

The prioritization scheme in industrial IoT networks focuses on managing energy consumption effectively by identifying the priority levels of data traffic and adjusting transmission parameters accordingly. For instance, high-priority data instances, such as I1, which carry critical real-time feedback and control commands, are allocated more resources and transmitted with minimal delays to ensure prompt and reliable communication. On the other hand, low-priority data instances, like I4, dealing with non-critical parameter logging, can be aggregated and transmitted in larger packets with longer intervals. This approach allows devices to conserve energy and enter low power modes when not actively communicating, effectively prolonging their battery life and reducing the frequency of battery replacements.

7 Results and Analysis

The simulation setup analyses four distinct packet instances traversing the network. Instance 1 packets carry critical real-time data, having the highest priority, while Instance 4 packets accommodate lower-priority information. This paper investigates the network's response to the inclusion of packet prioritization. Network performance evaluation can be done through two key metrics: Latency and PDR. Latency pertains to the time elapsed between packet transmission and its eventual reception. PDR, on the other hand, calculates the proportion of successfully delivered packets.

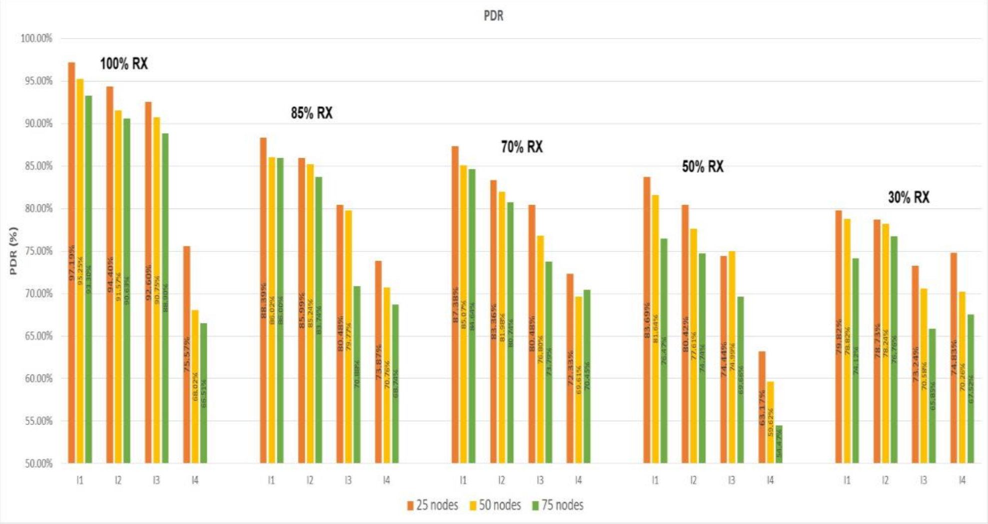

Fig. 6 PDR

In Fig. 6, the comparative analysis of Packet Delivery Ratio (PDR) reveals distinctive performance trends among different instances. Notably, Instance 1 exemplifies its excellence in critical real-time data handling, boasting a robust average PDR of 95.83% across all reception ratios. Impressively, this effectiveness translates to varying network sizes, maintaining a consistently high average PDR of 95.9% across different numbers of motes, highlighting its proficiency in ensuring data delivery irrespective of reception conditions or network scale. Conversely, Instance 2 manages non-critical real-time tasks, demonstrating an average PDR of 85.76% across reception ratios. Its versatility is emphasized by an average PDR of 87.14% across all numbers of motes, reaffirming its capability to deliver data reliably in diverse non-critical real-time scenarios. Meanwhile, Instance 3, optimized for periodic updates, showcases its adaptability with an average PDR of 78.79% across reception ratios, and maintains data delivery consistency across all numbers of motes, with an average PDR of 81.79%. Lastly, Instance 4, tailored for low-priority monitoring, exhibits flexibility across reception capabilities, maintaining an average PDR of 69.29% across reception ratios. This adaptability extends to different numbers of motes, resulting in an average PDR of 59.87%, underscoring its efficacy in various network sizes and reception conditions.

From the graph shown in Fig 7 it is evident how packet priority and delay relate to one another. As packet priority decreases, a distinct trend appears as latency values rise. This effect is most noticeable when we look at examples with different amounts of motes.

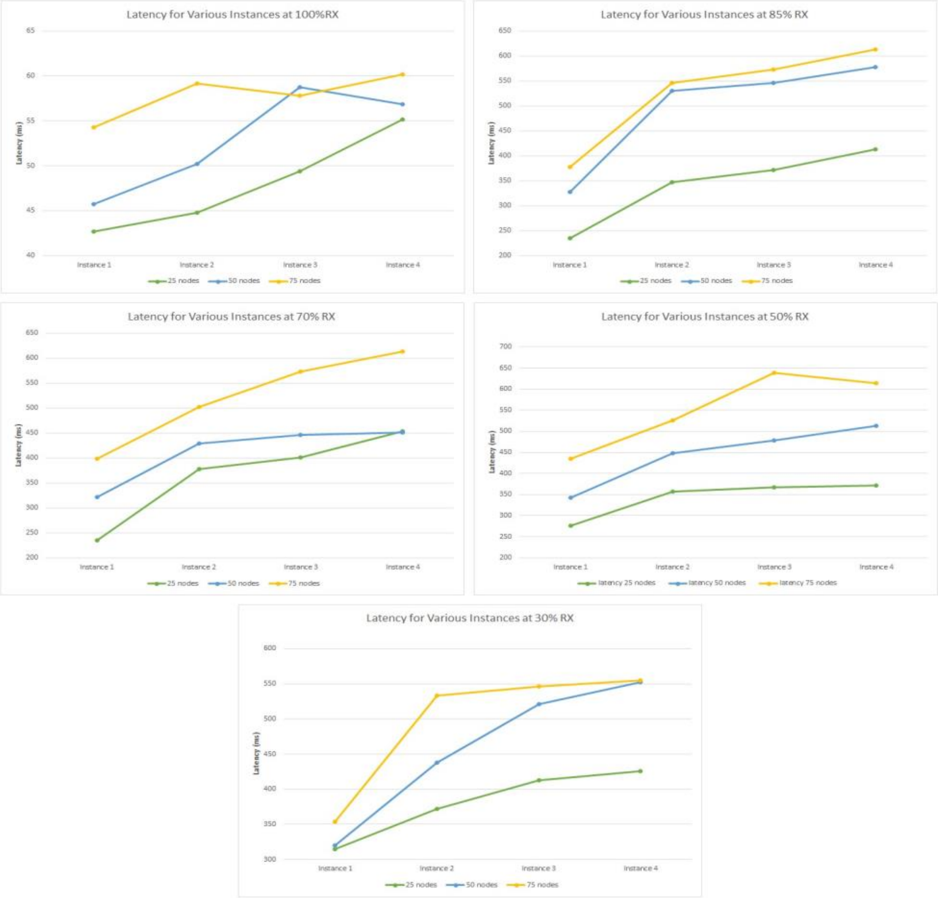

Fig. 7 Latency

Consider the observations for Instance 1, with 25 motes, as an example. At a 100% reception ratio (RX ratio), the latency is at its lowest point, recorded as 42.7 ms. However, as we progress through Instances 2, 3, and 4, latencies rise successively to 44.8 ms, 49.3 ms, and 55.1 ms, respectively. Moreover, it becomes evident that elevating the number of motes in the simulation further increases latency. This situation is mostly related to increased network congestion. Congestion increases as more motes compete to transmit data at the same time, resulting in increasing delay.

By reducing the RX ratio to 85%, 70%, 50%, and 30%, the escalation of latency persists. This outcome arises due to the combined effects of multiple retransmissions and the processing overhead incurred as a result of the reduced reception ratio. Notably, the most substantial latency values are observed at 30% RX ratio. For Instance 1, the latency peaks at 315.0 ms, while Instance 2 reaches 372.1 ms. Similarly, Instance 3 registers 413.0 ms, and Instance 4 reaches 425.4 ms. These greater latency values for lower RX ratios and higher mote counts demonstrate the complex connection between reception ratio and latency.

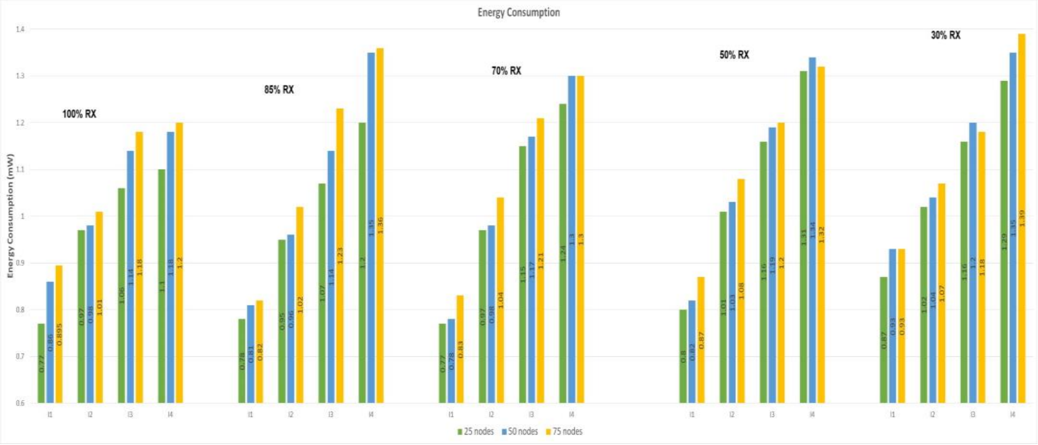

Fig. 8 Energy Consumption

From the graph in Fig 8 for Energy across various instances for different mote counts for various Reception Ratios we can see that there is a trend of rise in energy consumption as the priority of the packet decreases. Furthermore, the energy consumption also increases as the RX ratio is decreased. This is primarily because due to reduced reception ratio, there is more packet loss and hence more retransmission of packet, in turn increases the overall power consumption.

Fig 8 shows the energy consumption across various instances for different mote counts for various reception ratios. The analysis of energy consumption across different instances, considering varying mote counts and reception ratios, reveals a consistent trend. As the packet priority is downgraded, there is a noticeable upward trajectory in energy consumption. This phenomenon is compounded by the decrease in reception ratio: as the RX ratio diminishes, energy consumption also rises.

The effects of lower reception ratios are at the basis of this trend. The chance of packet loss increases as the RX ratio decreases, requiring an increase in the frequency of packet retransmissions. This increased retransmission activity correlates directly to increased power usage. As a result, in scenarios with lower packet priority and lower reception ratios, overall energy usage rises.

8 Conclusion

In conclusion, the suggested priority-based strategy and optimized backoff scheme serve as a reliable and practical response to the issues posed by spreading heterogeneous traffic in Industrial IoT (IIoT) contexts. This study proposes a unique architecture that seamlessly combines a smart backoff mechanism with data packet prioritization to significantly enhance key performance indicators.

The proposed approach was compared to conventional methods and found to be superior in several ways. First, the priority-driven strategy guarantees that high-priority data is sent with the least amount of conflict, resulting in a notable improvement in the packet delivery ratio (PDR). This is especially important in IIoT, where it is necessary to reliably and quickly transmit time-critical information, such as safety-critical sensor data and control orders, in order to avoid possible dangers and guarantee smooth production operations.

Additionally, the optimized backoff interval's achievement of a reduction in latency is quite significant in IIoT applications. For prompt decision-making and precise predictive maintenance, situations like important real-time traffic (Instance 1) and periodic updates (Instance 3) demand quick data transfer. The proposed method's ability to prioritize and accelerate such data transfers significantly reduces latency, assuring maximum operational effectiveness and minimizing downtime.

Through the suggested plan, energy efficiency, a crucial problem in IIoT, also significantly improves. Devices can operate in low-power modes to save energy by allowing low-priority data (Instance 4) to be transferred less often. This wise energy use increases battery life and complies with industrial installations sustainability objectives.

In conclusion, this research establishes the groundwork for a very strong solution that handles the particular difficulties of spreading diverse traffic in IIoT networks. The suggested solution not only outperforms conventional approaches but also makes a strong case for improving the performance and flexibility of IIoT networks thanks to its priority-driven approach, optimized backoff intervals, and noticeable reductions in PDR, latency, and energy consumption. It is positioned as a significant addition to the changing environment of industrial connectivity because of its personalized approach to data prioritization and effective resource utilization.

9 Future Work

The future scope in this work would be exploring the dynamic adaptation of priority levels based on real-time network conditions, integrating machine learning techniques for more accurate priority assignment, and investigating the scheme’s scalability for larger industrial IoT networks. Additionally, extending the framework to hybrid communication models involving both wired and wireless technologies could enhance reliability further, while cross-domain applicability across sectors like smart cities and healthcare offers exciting avenues for research and implementation.

References

[1] A. Koubaa, M. Alves, and E. Tovar. ”A comprehensive simulation study of slotted CSMA/CA for IEEE 802.15. 4 wireless sensor networks.” 2006 IEEE international workshop on factory communication systems. IEEE, 2006.

[2] H. Kharrufa, HAA. Al-Kashoash, and AH. Kemp. ”RPL-based routing protocols in IoT applications: A review.” IEEE Sensors Journal 19.15 (2019): 5952-5967.

[3] S. Madakam, V. Lake. ”Internet of Things (IoT): A literature review.” Journal of Computer and Communications 3, no. 05 (2015): 164.

[4] H. Lamaazi, and N. Benamar. ”A comprehensive survey on enhancements and limitations of the RPL protocol: A focus on the objective function.” Ad Hoc Networks 96 (2020): 102001.

[5] Kivinen, T., and P. Kinney. IEEE 802.15. 4 Information Element for the IETF. No. rfc8137. 2017.

[6] A. Koubaa, M. Alves, and E. Tovar. ”A comprehensive simulation study of slotted CSMA/CA for IEEE 802.15. 4 wireless sensor networks.” 2006 IEEE international workshop on factory communication systems. IEEE, 2006.

[7] S. Henna, MA. Sarwar, ”An Adaptive Backoff Mechanism for IEEE 802.15.4 Beacon-Enabled Wireless Body Area Networks”, Wireless Communications and Mobile Computing, vol. 2018, Article ID 9782605, 15 pages, 2018.

[8] Anjum I, Alam N, Razzaque MdA, Mehedi Hassan M, Alamri A. ”Traffic Priority and Load Adaptive MAC Protocol for QoS Provisioning in Body Sensor Networks. International Journal of Distributed Sensor Networks”. 2013;9(3). doi:10.1155/2013/205192

[9] Sahoo, Prasan Kumar, Sudhir Ranjan Pattanaik, and Shih-Lin Wu. ”A novel synchronous MAC protocol for wireless sensor networks with performance analysis.” Sensors 19.24 (2019): 5394.

[10] Bauwens, Jan, B. Jooris, S. Giannoulis, I. Jabandˇzi´c, I. Moerman, and ED. Poorter. ”Portability, compatibility and reuse of MAC protocols across different IoT radio platforms.” Ad Hoc Networks 86 (2019): 144-153.

[11] S. Li, JG. Kim, DH. Han, and KS. Lee. ”A survey of energy-efficient communication protocols with QoS guarantees in wireless multimedia sensor networks.” Sensors 19, no. 1 (2019): 199.

[12] G. Kim, JG. Kang, and M. Rim ”Dynamic duty-cycle MAC protocol for IoT environments and wireless sensor networks.” Energies 12.21 (2019): 4069.

[13] S. Homayouni and R. Javidan, ”ERA-ContikiMAC: An adaptive radio duty cycling layer in Internet of Things,” 2018 9th International Symposium on Telecommunications (IST), Tehran, Iran, 2018, pp. 74-79, doi: 10.1109/ISTEL.2018.8661144.

[14] F. Ullah, , AH. Abdullah, O. Kaiwartya, and MM. Arshad. ”Traffic priority-aware adaptive slot allocation for medium access control protocol in wireless body area network.” Computers 6, no. 1 (2017): 9.

[15] R. Gupta, S. Biswas ”Priority based IEEE 802.15.4 MAC by varying GTS to satisfy heterogeneous traffic in healthcare application. Wireless Netwwork” 26, 2287–2304 (2020). https://doi.org/10.1007/s11276-019-02149-6

[16] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson. ”The industrial internet of things (IIoT): An analysis framework.” Computers in industry 101 (2018): 1-12.

[17] MF Khan, EA. Felemban, S. Qaisar, and S. Ali. ”Performance analysis on packet delivery ratio and end-to-end delay of different network topologies in wireless sensor networks (WSNs).” In 2013 IEEE 9th International Conference on Mobile Ad-hoc and Sensor Networks, pp. 324-329. IEEE, 2013.

[18] K. Muhammad, J. Lloret, and SW Baik. ”Intelligent and energy-efficient data prioritization in green smart cities: Current challenges and future directions.” IEEE Communications Magazine 57.2 (2019): 60-65.

[19] M. Zhao, Ho, I.W.H. and Chong, P.H.J., 2016. ”An energy-efficient region-based RPL routing protocol for low-power and lossy networks”. IEEE Internet of Things Journal, 3(6), pp.1319-1333.

[20] P. Karkazis, Leligou, H.C., Sarakis, L., Zahariadis, T., Trakadas, P., Velivassaki, T.H. and Capsalis, C., 2012, July. ”Design of primary and composite routing metrics for RPL-compliant wireless sensor

networks.” In 2012 international conference on telecommunications and multimedia (TEMU) (pp. 13-18). IEEE.

[21] Gonizzi, P., Monica, R. and Ferrari, G., 2013, July. ”Design and evaluation of a delay-efficient RPL routing metric”. In 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC) (pp. 1573-1577). IEEE.

[22] X. Huang,K. Xie, Leng, S., Yuan, T. and Ma, M., 2018. ”Improving Quality of Experience in multimedia Internet of Things leveraging machine learning on big data.” Future Generation Computer Systems, 86, pp.1413-1423.

[23] Sandur, Anshu, and Animesh Giri. ”Performance Analysis of the merged 6L0WPAN-CoAP and RPL-CoAP with different combination of MAC and RDC layer protocols.” In 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon), pp. 1-6. IEEE, 2022.

[24] Charles, A.J. and Kalavathi, P., 2018. ”QoS measurement of RPL using Cooja simulator and Wireshark network analyser.” International Journal of Computer Sciences and Engineering, 6(4), pp.283-291.

[25] S. Katsikeas, K. Fysarakis, A. Miaoudakis, AV Bemten, I. Askoxylakis, I. Papaefstathiou, and A. Plemenos. ”Lightweight & secure industrial IoT communications via the MQ telemetry transport protocol.” In 2017 IEEE Symposium on Computers and Communications (ISCC), pp. 1193-1200. IEEE, 2017.

[26] WZ Khan, M. H. Rehman, HM Zangoti, MK. Afzal, N. Armi, and K. Salah.

[27] ”Industrial internet of things: Recent advances, enabling technologies and open challenges.” Computers & electrical engineering 81 (2020): 106522.

[28] Q. Qi, Z. Xu, and P. Rani. ”Big data analytics challenges to implementing the intelligent Industrial Internet of Things (IIoT) systems in sustainable manufacturing operations.” Technological Forecasting and Social Change 190 (2023): 122401.

[29] S. Beitelspacher, M. Mubashir, KM Besher, and M.Z Ali. ”Prioritizing health care data traffic in a congested IoT cloud network.” In 2020 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), pp. 1-6. IEEE, 2020.

[30] F. Dobslaw, M. Gidlund, and T. Zhang. ”Challenges for the use of data aggregation in industrial Wireless Sensor Networks.” 2015 IEEE International Conference on Automation Science and Engineering (CASE). IEEE, 2015.

[31] S. Bhandari, S.K. Sharma, and X. Wang. ”Latency minimization in wireless IoT using prioritized channel access and data aggregation.” In GLOBECOM 20172017 IEEE Global Communications Conference, pp. 1-6. IEEE, 2017.

[32] I. Dbibih, I. Iala, D. Aboutajdine, and O. Zytoune. ”Collision avoidance and service differentiation at the MAC layer of WSN designed for multi-purpose applications.” In 2016 2nd International Conference on Cloud Computing Technologies and Applications (CloudTech), pp. 277-282. IEEE, 2016.

[33] C.D. Devi, and K. Vidya. ”A survey on cross-layer design approach for secure wireless sensor networks.” In International Conference on Innovative Computing and Communications: Proceedings of ICICC 2018, Volume 1, pp. 43-59. Springer Singapore, 2019.