Secure Split and Classification Mechanism for LoRa Networks Against Active and Reactive Interference Attacks

Omar Dario Delgado Brito
DIMES dept., University of Calabria
Rende (CS), Italy
omardario.delgado@dimes.unical.it

Floriano De Rango
DIMES dept., University of Calabria
Rende (CS), Italy
derango@dimes.unical.it

Pasquale Pace
DIMES dept., University of Calabria
Rende (CS), Italy
p.pace@dimes.unical.it

***Abstract*—In the Internet of Things (IoT) domain, resource-constrained devices are highly susceptible to malicious interference due to limited duty cycles, finite energy reserves, and an inability to perform clear channel assessment. These vulnerabilities are further exacerbated in low-power wide-area networks (LPWANs), where the absence of centralized coordination renders the network an attractive target for jamming attacks. In this work, we introduce a novel split and classification mechanism designed to enhance LoRa packet delivery under both constant and reactive jamming conditions. Our approach partitions each LoRa frame into sub-packets and applies a real-time classification algorithm to identify and mitigate corrupted segments, thereby improving the effective data extraction ratio (DER). We validate the mechanism through extensive simulated scenarios across diverse network densities. Comparative analysis against the standard LoRa protocol demonstrates a significant increase in packet success rate and a commensurate gain in DER, without incurring additional energy overhead.**

***Index Terms*—IoT, Security, Trust, LPWAN networks, LoRa, LoRaWAN, Jamming attack.**

I. Introduction

The Internet of Things (IoT) is an emerging communication paradigm that envisions a future where everyday objects, equipped with micro-controllers, transceivers, and suitable communication protocols, seamlessly integrate into the Internet, allowing interaction between them and users. This paradigm finds application in various sectors, transforming how we live and work. Some prominent examples include the automation of homes and industries, by optimizing energy management, transforming transportation with connected vehicles and intelligent traffic management systems, and many other areas [1]. IoT devices exhibit dynamic current profiles, characterized by large dynamic ranges and rapid transients. Device engineers must effectively convert measurement data into actionable insights to optimize product performance. IoT devices often operate intermittently, alternating between low-power sleep states, consuming microamperes of current, and high-power active states, drawing hundreds of milliamperes or even amperes. However, the heterogeneity and incompatibility of these devices pose challenges such as network congestion and interference issues. The emergency of ensuring the integrity and privacy of data in the face of an interference environment is fundamental. It requires having the reliability of an algorithm that ensures its delivery, taking into account the importance of information [2]. IoT applications with limited energy resources are of vital importance since long battery life without frequent replacements is a critical factor in these environments. Low-power, long-range technologies such as LoRaWAN, 6LoWPAN, and 802.15.4 are ideal for data transmission under these conditions. However, electromagnetic pollution caused by the coexistence of multiple devices in the same environment can seriously compromise the quality of communications. The presence of IoT devices, operating on overlapping frequency bands, is one of the main sources of electromagnetic interference (EMI), which can decrease the success rate of data transmission [3]. Starting from this challenging scenario, this research paper proposes and validates a strategy designed to mitigate the impact of constant and reactive jamming attacks in LoRa networks, demonstrating the need for an adaptation to a mechanism that guarantees the packet success rate of data for communications within extensive IoT networks. The proposed approach has been compared to the conventional scheme through the development of a simulation model that considers factors such as channel fading, interference, and duty cycle to replicate real-world conditions accurately, applying constant and reactive jamming attacks.

The structure of the paper is as follows: Section II presents a brief overview of the literature. Section III describes the proposed mechanism and the evaluation methodology. Section IV presents the obtained results and their analysis. The conclusions of the research are presented in Section V.

II. Literature

A substantial number of wireless IoT sensors and devices are slated for deployment within and outside a smart city's urban landscape; as a consequence, this proliferation presents a formidable challenge in establishing connectivity for all IoT sensors and devices. Wireless protocols have been devised in the last few years to meet the specific requirements of IoT applications. These emerging protocols are specifically designed to accommodate the connection of a multitude of IoT devices within expansive coverage areas while simultaneously optimizing power consumption. A term, Low Power Wide Area Network (LPWAN), has been introduced to encapsulate this category of protocols. The affordability of connectivity

979-8-3503-9281-4/25/$31.00 ©2025 IEEE

offered by this technology results in significantly reduced deployment costs for IoT sensors. LPWAN, particularly in IoT applications, and emerging low-power, long-range technologies such as LoRaWAN and Narrowband IoT (NB-IoT), are instrumental in facilitating the deployment of dense networks [4].

A. LoRaWAN MAC Layer

The LoRaWAN infrastructure hinges on a gateway that serves as an intermediary, receiving data from sensor nodes equipped with LoRa transceivers and subsequently forwarding them to a server in encrypted Internet Protocol (IP) packets via Ethernet or 3G links. However, it is imperative to note that end devices are required to adhere to a duty cycle of 1% to ensure equitable transmission rates. This restriction mandates that after a message transmission, for instance lasting 1 second, the device must observe a waiting period of approximately 99 seconds before transmitting another message [5]. From a security point of view, LoRaWAN strikes a balance between security and resource efficiency. While robust security requires powerful algorithms and hardware, LoRaWAN leverages the well-established AES standard to ensure data confidentiality and integrity. By using symmetric encryption with a 128-bit key [6] and dynamic parameters such as frame counters and random tokens, LoRaWAN safeguards communication. Additionally, message integrity checks, based on the AES-CMAC algorithm, further enhance security. These mechanisms are designed to be compatible with low-power microcontrollers, making them suitable for resource-constrained IoT devices.

B. LoRa Physical Layer

LoRa, a groundbreaking LPWAN technology developed by Semtech [7], has emerged as a promising solution for IoT applications. Operating on unlicensed ISM bands, LoRa offers long-range communication, low power consumption, and a robust modulation scheme based on Chirp Spread Spectrum (CSS). LoRa's modulation scheme involves transmitting signals with a continuously changing frequency, enabling efficient spectrum utilization and interference resistance. Key parameters determine the transmission range, data rate, and energy consumption. Transmission Power (TP) from -4 to 20 dBm, Carrier Frequency (CF) from 137 MHz to 1020 MHz, Spreading Factor (SF) from 7 to 12, Bandwidth (BW) 125 KHz, 250 KHz and 500 KHz can be set, and Coding Rate (CR) 4/5, 4/6, 4/7 and 4/8 significantly impact LoRa's performance. A higher TP and SF enhance range and reliability, but increase power consumption; on the other hand, a higher BW and lower CR improve data rate but reduce range and reliability. The optimal configuration depends on the specific application requirements, balancing the need for long-range communication with the demand for timely data delivery [8].

C. Jamming interferences

Jamming, or intentional interference, represents a critical threat to wireless communication systems. Due to their inherently open and shared nature, these systems are particularly susceptible to malicious actions aimed at degrading or entirely disrupting legitimate transmissions. Adversaries can emit interference signals within the communication channel, saturating the receiver and hindering its ability to correctly decode the intended signals. The high variability and often unpredictable nature of such interference, particularly when delivered at sufficient power, present a major challenge—rendering conventional noise mitigation and detection techniques largely ineffective [9].

Among jamming techniques, constant jamming involves the continuous emission of radio signals, either through a signal generator set to a fixed frequency or by configuring a wireless device to repeatedly transmit packets with randomized MAC addresses. This approach does not conform to MAC protocol rules and monopolizes the channel, flooding it with high-volume, non-compliant traffic. Although effective in degrading network performance, constant jamming is relatively easy to detect due to its persistent use of the channel. Conversely, reactive jamming employs a more covert strategy. The jammer remains silent during idle periods and only transmits when it detects legitimate activity on the channel. By mimicking the behavior of authorized nodes and aligning its timing with ongoing transmissions, reactive jamming significantly complicates detection and mitigation efforts [10].

D. Related Works

Recent years have seen a growing number of reverse engineering studies targeting the LoRa physical (PHY) layer, offering valuable insights into its operational behavior. In this context, the present comparative analysis aims to deepen the understanding of LoRa/LoRaWAN networks when subjected to electromagnetic interference (EMI). Notably, [11] conducted a detailed physical-layer study quantifying the impact of EMI on LoRa systems, establishing a reference framework for subsequent research.

A practical evaluation of LoRa's resilience under co-technology interference was carried out using a software-defined radio (SDR) testbed. This setup allowed precise control of parameters such as signal-to-interference ratio (SIR) and inter-signal delay without requiring a fully isolated environment. A broad spectrum of interference scenarios, varying SIR, signal-to-noise ratio (SNR), and temporal offsets, was tested. Performance was assessed through packet loss rate, calculated as the complement of the successful capture rate (SCR) and data extraction rate (DER) [12].

In terms of network-layer resilience, [13] presented an ns-3-based simulation to evaluate LoRaWAN performance under jamming attacks. Building on this, [14] proposed enhancements through the inclusion of confirmed traffic using an Aloha-t simulation framework, enabling the analysis of authenticated communication in the presence of channel-oblivious jammers.

Additionally, [15] demonstrated how a low-cost device can execute an effective jamming attack by detecting the preamble of a LoRaWAN transmission and subsequently overwhelming the channel with a stronger signal. Given the extended airtime

of LoRa packets, even with short payloads, such attacks can be highly disruptive. The literature consistently highlights LoRaWAN's vulnerability to interference and jamming. Existing mitigation strategies often rely on static adjustments such as modifying the spreading factor or increasing transmission power, which offer limited adaptability. In contrast, this work proposes a dynamic *split and classification* mechanism capable of real-time adaptation, improving network robustness under diverse interference conditions.

III. Problem formulation and proposal

LoRaWAN is particularly well-suited for applications demanding extensive communication ranges with moderate data exchange, it faces challenges related to the simplicity of its node transmission mechanisms. This simplicity, while contributing to low power consumption, also makes nodes susceptible to interference, potentially compromising the reliability of data transmission. Based on the preceding, an algorithm is proposed, specifically designed to mitigate the effects of jamming attacks in LoRa devices.

The inherent limitations of the Adaptive Data Rate (ADR) mechanism in the LoRaWAN protocol hinder its adaptability to dynamic network conditions. The ADR mechanism was designed primarily for static devices, which led to suboptimal performance and unreliable connectivity. Moreover, its reliance on the maximum signal-to-noise ratio renders it vulnerable to interference, particularly in high-noise environments or under jamming attack environments. This vulnerability can result in decreased communication range, increased packet loss, and general network performance degradation [16]; moreover, ADR performance degrades significantly when the number of devices increases [17]. The ADR mechanism is hosted on the network server, and each node is based on Thompson Sampling in multi-armed bandit settings. This algorithm is suitable for combining Spreading Factor (SF) and Transmission Power (TP) when message acknowledgments are not guaranteed. This is due to two fundamental reasons. On the one hand, the statistical model underlying both algorithms must be continuously updated using RSSI or SNR, of which end nodes are unaware. However, simple applications running on end nodes do not allow dynamic parameter selection based on the environment.

A. Success rate calculation in LoRa network

We consider a LoRa wireless sensor network with a single communication channel, with the main purpose of calculating the success rate of the network. Based on the configuration parameters, we initially determine the duration of each packet transmission. The transmission time of a single LoRa packet T_{packet} can be determined by considering the spreading factor, bandwidth, and payload size by applying the following formulas:

$$T_{\text{symbol}} = \frac{2^{\text{SF}}}{\text{BW}} \tag{1}$$

$$T_{\text{preamble}} = (n_{\text{preamble}} + 4.25) \cdot T_{\text{symbol}} \tag{2}$$

$$n_{\text{payload}} = 8 + \max\left\{\left\lceil \frac{8 \cdot \text{PL} - 4 \cdot \text{SF} + 44}{4 \cdot (\text{SF} - 2 \cdot \text{DE})} \right\rceil \cdot (\text{CR} + 4), 0\right\} \tag{3}$$

$$T_{\text{payload}} = n_{\text{payload}} \cdot T_{\text{symbol}} \tag{4}$$

$$T_{\text{packet}} = T_{\text{preamble}} + T_{\text{payload}} \tag{5}$$

Where:

- T_{symbol} => Symbol time
- SF => Spreading Factor
- BW => Bandwidth (125 kHz default)
- T_{preamble} => Preamble Time
- n_{preamble} => Symbols within preamble (8 default)
- PL => Payload size (10B used)
- DE => 0 for SF7 to SF10, 1 for SF11 and SF12
- CR => Code rate (4 default)
- T_{packet} => Packet transmission time

The default application that can run on the network server randomly selects an initial transmission time and a sleep time before starting a new transmission for each packet, resulting in a final transmission time before the window closes [18]. Devices send packets in a frame (T_{frame}) and must comply with the duty cycle restriction; to avoid excessive spectrum interference, the waiting time T_{off} is defined as:

$$T_{off} = \left(\frac{T_{\text{frame}}}{\text{DutyCycle}}\right) - T_{\text{packet}}. \tag{6}$$

The probability that a node does not collide in a transmission depends on window time, packet transmission time, and number of nodes in the same area. We are considering the probability that a specific node does not collide when there are $n-1$ additional nodes:

$$P = \left(1 - \frac{2 \cdot T_{\text{packet}}}{T_{\text{frame}}}\right)^{n-1} \tag{7}$$

Table I provides a detailed overview of the airtime transmissions for each spreading factor.

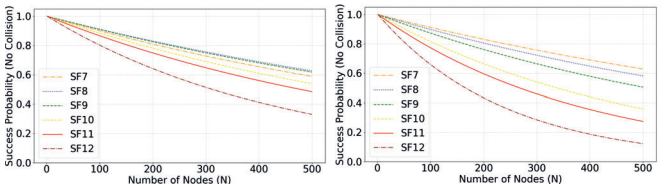
	SF 7	**SF 8**	**SF 9**	**SF 10**	**SF 11**	**SF 12**
$T_{\textbf{packet (ms)}}$	78.08	139.77	246.73	493.56	856.06	1712

TABLE I: The transmission time of a single LoRa packet.

The system's ability to handle various workloads was evaluated through a comprehensive analysis of all spreading factors, based on Equation 7. Additionally, two types of jamming attacks have been tested (constant jamming and reactive jamming) that intentionally affect the network as mentioned in the previous section; moreover, the increased collision probability is evaluated by scaling the network under constant and reactive jamming attacks.

The increase in the collision probability under a classical jamming attack is shown Fig.1(a), and it increases as the spreading factor increases. As shown in Fig.1(b), on the other hand, the reactive jamming attack increases even more the collision probability between legitimate and fake packets, further degrading network performance, which is demonstrated by

the longer channel occupancy time associated with spreading factor values.



(a) (b)

Fig. 1: No Collision Probability under a) Constant Jamming Attack; b) Reactive Jamming Attack.

The standard LoRaWAN node management mechanism, characterized by repetitive cycles of transmission and hibernation, shown in Fig.2, exposes the network to vulnerabilities to jamming attacks. The synchronization of transmissions from all nodes in the same group and time slot makes it easy for attackers to identify patterns, allowing them to interfere with communication and decrease the successful packet delivery rate.

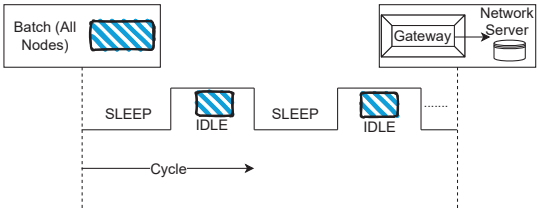


Fig. 2: Standard nodes management mechanism.

B. Dynamic mechanism of split and classification by groups

The proposed mechanism is based on a modified version of the classification algorithm [19], which is rooted in the "Hierarchical decomposition approach" paradigm commonly used in computational problem-solving. While it retains the core principle of recursive data partitioning and subsequent merging, the modification introduces a transmission-aware adaptation designed to enhance the timeliness of packet delivery from end nodes to the network server. Initially, the network nodes are hierarchically partitioned into smaller subgroups to facilitate more manageable and efficient transmission scheduling. A non-redundant iterative partitioning strategy is employed, outlined in Fig. 3, to minimize overlap and improve subgroup differentiation. Following the partitioning phase, an ascending-order sorting algorithm is applied iteratively across the resulting subgroups, using the aggregate success rate of each subgroup as the sorting criterion. This ordering ensures that subgroups with lower transmission success rates are prioritized in subsequent communication rounds, thereby promoting a more balanced and reliable data delivery across the network.

While our approach is rooted in the Merge classification algorithm, we prioritize timely packet delivery by focusing on sub-groups containing the lowest success rate, detailed in

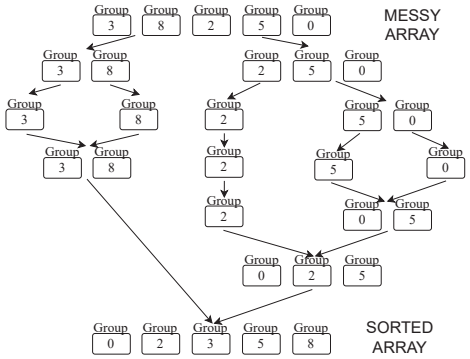


Fig. 3: A recursive algorithm to split and classify by groups.

Fig. 4. This divergence allows us to ensure efficient and timely communication, optimal transmission parameters are assigned to each group, and a new group is allocated to each node for subsequent transmissions.

The assignment of changing the spread factor, or raising the power, does not help when the network is under attack at all spread factors; on the contrary, our approach employs a randomized selection based on packet airtime for subsequent transmissions. This dynamic approach mitigates interference between terminals and within the transmission environment, thereby enhancing overall network performance. It is worth

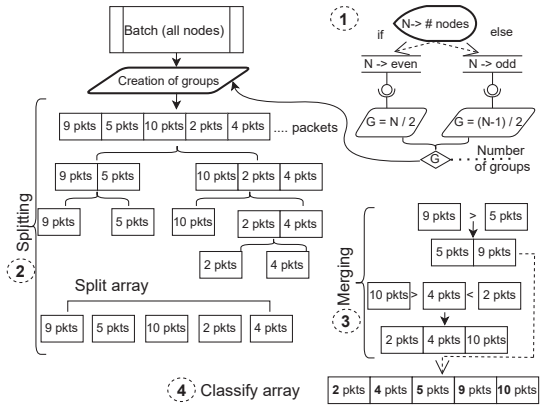


Fig. 4: Proposed mechanism to split and classify by groups.

highlighting the implementation feasibility of the mechanism in real scenarios due to the characteristics of message types in the network. The network server can easily send configuration messages to the end devices, enabling dynamic adjustments as needed. This ensures that the network can adapt to changing conditions and optimize performance in real-time.

IV. Simulation set-up and results

The proposed split and classification mechanism was simulated using the OMNeT++ discrete event simulator [20], leveraging the FLoRa (Framework for LoRa) simulation tool [21] and the INET framework. FLoRa, an open-source tool, encompasses modules for the LoRa physical layer, LoRaWAN MAC protocol, network elements, and energy consumption modeling. The

INET framework was integrated to provide a comprehensive simulation environment, particularly for the physical layer.

A. Simulation Setup

A simulation environment was established to replicate the conditions of the European 868 MHz LoRa band, adhering to regulatory constraints. Simulations were conducted for scenarios with different node densities, using the parameters exhibited in Table II, respectively, and each scenario was replicated several times with random node placements.

TABLE II: Simulation Parameters

Repetitions	25 iterations {15 days}
Area	1000 m^2
Number of legacy nodes	{50 to 500}
Legacy nodes placement	Random per replication
Initial SF for legacy nodes	randomly (7 to 12)
Initial TP for legacy nodes	14 dBm
Bandwidth	125 kHz
Center Frequency	EU Band 868 MHz {Duty Cycle 1%}

To simulate a realistic jamming environment, interference devices (constant jamming and reactive jamming) were configured with parameters identical to those of the legacy devices under test (868 MHz band, 125 kHz bandwidth, and maximum power of 14 dBm); we also consider that the jammer device does not belong to the network. The spreading factor was varied between 7 and 12 to evaluate the performance of the mechanisms under different propagation conditions. All experiments complied with the current regulations regarding the duty cycle. Furthermore, to evaluate the resilience of the proposed mechanism for LoRa networks under constant and reactive jamming attacks, a comparative analysis of the packet success rate is carried out to evaluate packets sent and lost by nodes. Moreover, we computed the percentage of use of each spreading factor to individually evaluate the impact of each different value, and the Data Extraction Rate (DER) is defined as the ratio of successfully received messages by the LoRa Gateway to transmitted messages by the LoRa node within an estimation window. In each scenario, networks with varying node densities (low, medium, high) were evaluated to analyze the impact of density on performance interference conditions under both constant and reactive jamming attacks. Several replications with random node distributions have been carried out for each configuration, providing statistically robust results.

B. Results and Discussions

In communication scenarios running without the standard ADR mechanism, they experience significant degradation in their success rate when subjected to a reactive jamming attack, as shown in Figure 5.

A computer analysis is executed of the Data Extraction Rate (DER) to evaluate the overall network performance in a numerical range between 0 and 1. The evolution of the DER as a function of node density for both the standard and proposed

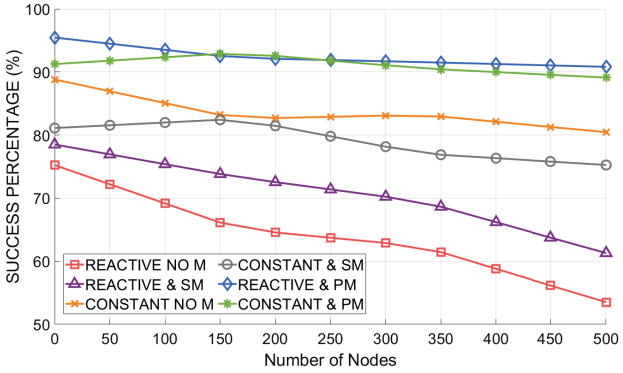


Fig. 5: Comparing Packet Success Rates under Constant and Reactive Jamming, out of mechanism (NO M), with Standard Mechanism (SM) and Proposed Mechanism (PM).

mechanisms, under constant and reactive jamming attacks, is shown in Fig.6. It is observed that, in the standard mechanism, the DER decreases significantly as node density increases, especially under reactive jamming attacks. In contrast, the proposed mechanism exhibits a more robust DER Increasing 16% that compared to the standard mechanism, experiencing a lower degradation in the face of both types of attacks, with a notable improvement in the case of constant jamming attacks.

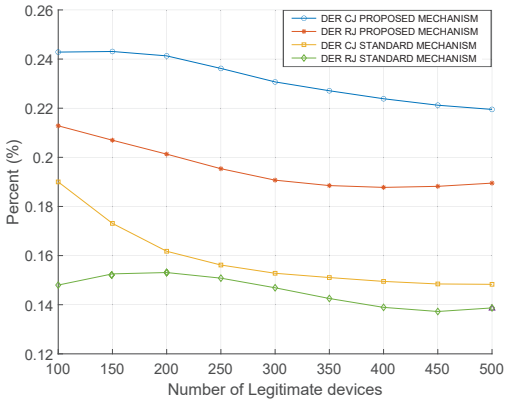


Fig. 6: Comparing Data Extraction Rate, between Standard Mechanism (SM) and Proposed Mechanism (MP), under Constant Jamming (CJ) and Reactive Jamming (RJ).

Furthermore, activating the standard mechanism slightly reduces the effects of the attack to some extent, although its effectiveness decreases as node density increases. The proposed mechanism (Split and classification) demonstrates superior performance in terms of success rate, showing greater resilience to both constant and reactive jamming attacks. To analyze the impact of node density (low, medium, and high) on the selection of the spreading factors, shown in Fig.7. The obtained results indicate that the standard mechanism shows a preference for lower spreading factors in low-density scenarios, while in high-density scenarios, there is a tendency towards higher spreading factors. On the other hand, the proposed mechanism demonstrates greater adaptability, adjusting the

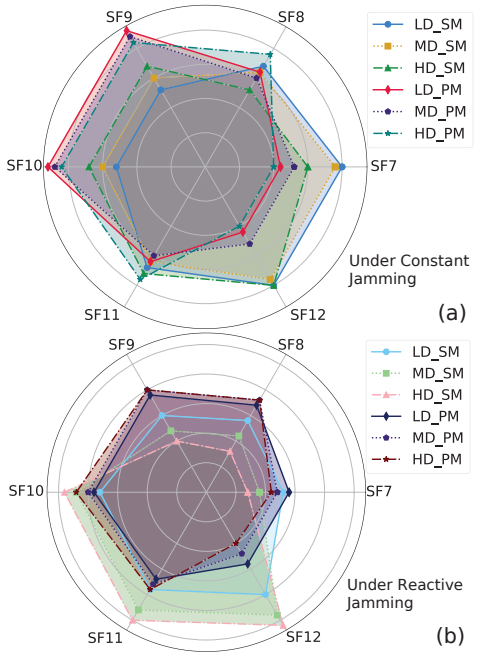


Fig. 7: Relationship between node density and spreading factor assignment, Low Density (LD), Medium Density (MD), High Density (HD); by Standard Mechanism (SM) and Proposed Mechanism (PM); under a) Constant Jamming Attack; b) Reactive Jamming Attack.

distribution of spreading factor usage based on node density and the type of attack. In fact, under reactive jamming attacks, the proposed mechanism favors the use of lower spreading factors in high-density scenarios. In contrast, under constant jamming attacks, a relatively uniform distribution of spreading factor usage is observed, regardless of node density.

V. Conclusions and Future Works

In this paper, a comparative evaluation of a novel communication mechanism has been presented and rigorously analyzed in two highly dynamic jamming attack scenarios with constant and reactive scaling density. A probabilistic analysis of packet success rate, dispersion factor utilization rate, and data extraction rate with respect to the node density has been conducted to make a comparative evaluation between the standard mechanism and the proposed *Split and classification* mechanism. The results demonstrated significant improvements, in particular, a general improvement is demonstrated in the evaluated metrics for both low and high node densities. Parameter optimization with this mechanism can improve data transmission in various LoRa-based applications. Finally, as future work, the integration of machine learning techniques holds the potential to further enhance the system's adaptability and performance in dynamic and mobile environments.

Acknowledgements

This work was partially supported by project SERICS (PE00000014) and by project Tech4You (ECS00000009, CUP H23C22000370006), under the MUR National Recovery and Resilience Plan funded by the European Union.

References

[1] R. Hassan, A. K. Sagar, and L. Banda, "Future internet of things: A framework for next generation smart cities," in *2021 IEEE 6th International Conference on Computing, Communication and Automation (ICCCA)*, pp. 106–112, 2021.

[2] Q. M. Qadir, T. A. Rashid, N. K. Al-Salihi, B. Ismael, A. A. Kist, and Z. Zhang, "Low power wide area networks: A survey of enabling technologies, applications and interoperability needs," *IEEE Access*, vol. 6, pp. 77454–77473, 2018.

[3] U. Rahamathunnisa and et. al, "Energy-efficient communication protocols for iot devices," in *2024 Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*, pp. 1–5, 2024.

[4] C. Pham and M. Ehsan, "Dense deployment of lora networks: Expectations and limits of channel activity detection and capture effect for radio channel access," *Sensors*, vol. 21, no. 3, 2021.

[5] N. Bandyopadhyay, P. Gaurav, M. Kundu, B. Misra, and B. Hoare, "Iot-based health and farm monitoring system via lora-based wireless sensor network," in *2020 4th International Conference on Electronics, Materials Engineering Nano-Technology (IEMENTech)*, pp. 1–7, 2020.

[6] "Ieee standard for low-rate wireless networks amendment 3: Advanced encryption standard (aes)-256 encryption and security extensions," *IEEE Std 802.15.4y-2021 (Amendment to IEEE Std 802.15.4-2020 as amended by IEEE Std 802.15.4z-2020 and IEEE Std 802.15.4w)*, pp. 1–23, 2021.

[7] Semtech, "Lora modulation basics an1200.22," tech. rep., 2022.

[8] Isminarti and S. et. al, "Modeling and simulation of long range (lora) communication system on smart grid," in *2022 Seventh International Conference on Informatics and Computing (ICIC)*, pp. 1–6, 2022.

[9] X. Wang, J. Wang, Y. Xu, J. Chen, L. Jia, X. Liu, and Y. Yang, "Dynamic spectrum anti-jamming communications: Challenges and opportunities," *IEEE Communications Magazine*, vol. 58, no. 2, pp. 79–85, 2020.

[10] Z. Yin, W. Wang, X. Lu, and Z. Yin, "Multi-level collaborative defense strategies against malicious traffic in wireless edge networks," in *2024 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*, pp. 185–190, 2024.

[11] A. N. de São José, C. Nathan, E. P. Simon, A. Boé, T. Vantroys, and G. et al., "A comparative analysis of lora and lorawan in the presence of jammers and transient interference," in *2022 International Symposium on Electromagnetic Compatibility – EMC Europe*, pp. 586–591, 2022.

[12] T. Elshabrawy, P. Edward, M. Ashour, and J. Robert, "Practical evaluation of lora under co-technology interference," in *2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall)*, pp. 1–5, 2020.

[13] I. Martinez and et. al, "On the performance evaluation of lorawan under jamming," in *2019 12th IFIP Wireless and Mobile Networking Conference (WMNC)*, pp. 141–145, 2019.

[14] I. Martinez and et. al, "On the performance evaluation of lorawan with re-transmissions under jamming," in *2020 IEEE Symposium on Computers and Communications (ISCC)*, pp. 1–7, 2020.

[15] T. Perković and D. Siriščević, "Low-cost lorawan jammer," in *2020 5th International Conference on Smart and Sustainable Technologies (SpliTech)*, pp. 1–6, 2020.

[16] S. Chen, H. Zhao, Z. Zhang, Y. Gong, R. Li, and L. Wang, "Improved adr and initial sf allocation in lorawan network and their simulation on ns3," in *2023 IEEE (ICSPCC)*, pp. 1–5, 2023.

[17] A. Ilarizky, A. Kurniawan, E. P. Subagyo, R. Harwahyu, and R. F. Sari, "Performance analysis of adaptive data rate scheme at network-server side in lorawan network," in *2021 2nd International Conference on ICT for Rural Development (IC-ICTRuDev)*, pp. 1–5, 2021.

[18] K. Ksiazek and K. Grochla, "Flexibility analysis of adaptive data rate algorithm in lora networks," in *2021 International Wireless Communications and Mobile Computing (IWCMC)*, pp. 1393–1398, 2021.

[19] B. Sugiarto and R. Sustika, "Data classification for air quality on wireless sensor network monitoring system using decision tree algorithm," in *2016 2nd International Conference on Science and Technology-Computer (ICST)*, pp. 172–176, 2016.

[20] A. Varga, *OMNeT++*, pp. 35–59. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010.

[21] M. Slabicki, G. Premsankar, and M. Di Francesco, "Adaptive configuration of lora networks for dense iot deployments," in *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium*, pp. 1–9, 2018.