InMAC: An Interference-Aware MAC Protocol for 2.4 GHz LoRaWAN

Chenglong Shao, *Senior Member, IEEE*, Tongyang Xu, *Member, IEEE*, and Xianpeng Wang, *Member, IEEE*

***Abstract*—Recent years have seen the rapid development of long-range wide area network (LoRaWAN) operating in region-specific sub-GHz frequency bands (*e.g.,* 868 MHz in Europe and 915 MHz in North America). To achieve global deployment, LoRaWAN has been extended to operate in the globally available 2.4 GHz unlicensed band. However, this shift exposes LoRaWAN to significant interference from coexisting Wi-Fi networks, which share the same band and typically transmit at much higher power levels. To address this problem, this paper presents InMAC, an interference-aware medium access control (MAC) protocol designed to improve coexistence between LoRaWAN and Wi-Fi networks. To the best of our knowledge, InMAC is the first MAC protocol specifically tailored to mitigate Wi-Fi interference for 2.4 GHz LoRaWAN. InMAC enhances LoRaWAN communication by probabilistically exploiting the silent time in Wi-Fi traffic, leveraging a Wi-Fi traffic profiling mechanism at LoRaWAN gateways and a packet length adaptation strategy at end devices. In addition to mitigating external interference from Wi-Fi, InMAC also tackles internal interference caused by signal collisions among LoRaWAN end devices. It incorporates a novel channel access mechanism based on Channel Activity Detection, a carrier-sensing technique adapted specifically for LoRaWAN. Experimental results demonstrate that InMAC reduces both external Wi-Fi interference and internal LoRaWAN collisions, achieving up to a 111% throughput boost over existing approaches.**

***Index Terms*—LoRaWAN, Wi-Fi, coexistence, interference, collision, medium access control layer.**

I. Introduction

LOW-power wide area networks (LPWANs) have emerged as one of the key wireless networking technologies for the Internet of Things (IoT) in recent years [1], [2]. LPWAN devices can achieve communication ranges from several hundred meters up to tens of kilometers while maintaining extremely low power consumption. This characteristic makes LPWANs highly suitable for diverse IoT applications, including large-scale agricultural automation, long-distance asset tracking, and remote waste bin management. In this context, numerous LPWAN technologies have been introduced, each offering distinct networking characteristics and catering to various market needs. Among them, long-range WAN (LoRaWAN) has become one of the most prominent technologies, attracting growing interest from academia and industry [3]–[6].

Similar to conventional wireless sensor networks, LoRaWAN typically consists of numerous distributed end devices that collect physical-world data. One or more gateways act as intermediaries, forwarding the collected data to back-end network and application servers. LoRaWAN commonly operates in unlicensed sub-GHz frequency bands. These unlicensed bands allow users to deploy networks without prior approval from regulatory authorities, enabling the construction of private LoRaWAN in various environments. However, sub-GHz bands are allocated differently across regions (*e.g.,* 470-510 MHz in China, 863-870 MHz in Europe, and 902-928 MHz in North America) [7]. As a result, region-specific parameters such as channel frequency, duty cycle limits, and transmission power must be carefully accounted for when designing LoRaWAN hardware and communication protocols.

To enable region-independent LoRaWAN development using uniform parameters, a new approach utilizing the globally available 2.4 GHz ISM (industrial, scientific, and medical) band for LoRaWAN communication has been introduced and is receiving increasing attention from both academic and industrial communities [8]–[14]. Compared to sub-GHz LoRaWAN, 2.4 GHz LoRaWAN increases the maximum channel bandwidth from 500 KHz to 1625 KHz, leading to a substantial improvement in data rates [15]–[19]. Additionally, it offers the advantage of reduced packet transmission latency, as the 2.4 GHz band does not impose duty-cycle limitations. These features make 2.4 GHz LoRaWAN an attractive option for applications requiring higher throughput and lower delay. However, a major challenge that must be addressed is signal interference caused by coexisting Wi-Fi networks [20]–[25][1]. This interference occurs because Wi-Fi systems also operate in the 2.4 GHz band, typically transmitting at higher power levels than 2.4 GHz LoRaWAN. To date, only a limited number of studies have focused on resolving this coexistence issue [26]–[28]. Specifically, [26] and [27] propose physical-layer techniques to extract 2.4 GHz LoRaWAN signals from Wi-Fi interference, while [28] introduces a medium access control

This work was supported in part by JSPS KAKENHI Grant Number 24K20765 and Takahashi Industrial and Economic Research Foundation.

C. Shao is with the Department of Computer Science and Networks, Kyushu Institute of Technology, Iizuka, Japan (E-mail: shao@csn.kyutech.ac.jp).

T. Xu is with the Department of Electronic and Electrical Engineering, University College London, London, UK (E-mail: tongyang.xu.11@ucl.ac.uk).

X. Wang is with the School of Information and Communication Engineering, Hainan University, Haikou, China (E-mail: wxpeng2016@hainanu.edu.cn).

[1] In this work, we focus specifically on the impact of Wi-Fi interference on 2.4 GHz LoRaWAN communications, as Wi-Fi is the most dominant and widespread source of interference in typical deployment scenarios. While other wireless technologies, such as Bluetooth and ZigBee, also operate in the 2.4 GHz band, their traffic patterns, duty cycles, and channel access mechanisms differ significantly from Wi-Fi, requiring separate analysis and design considerations. Extending this work to study coexistence with these technologies represents a valuable direction for future research.

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2025.3641235

(MAC) protocol that reserves part of the Wi-Fi channel to ensure interference-free 2.4 GHz LoRaWAN communication.

In this work, by substantially extending our previous work [29], we take a different approach to develop a LoRaWAN[2]-oriented interference-aware MAC protocol named InMAC to improve coexistence between LoRaWAN and Wi-Fi networks. For interference-aware LoRaWAN communication under the coexistence with Wi-Fi networks, InMAC aims at the avoidance of both external interference from Wi-Fi and internal interference caused by signal collisions among LoRaWAN end devices. Regarding the former issue, InMAC has LoRaWAN gateways perform a Wi-Fi traffic profiling technique to characterize the silent time of Wi-Fi traffic. The corresponding result is used for LoRaWAN end devices to adapt their packet length so that their transmissions are likely to proceed during the Wi-Fi silent time. Regarding the internal LoRaWAN signal collisions, InMAC resorts to Channel Activity Detection (CAD) that is tailor-made for carrier sensing in LoRaWAN [30], [31]. Based on this technique, a carrier-sense multiple access (CSMA) protocol is designed to adjust the channel access behaviors of end devices. The main contributions of this work are as follows.

- To our best knowledge, this work is the first research effort to resolve both external Wi-Fi interference and internal LoRaWAN signal collisions when LoRaWAN and Wi-Fi networks coexist.
- This paper proposes InMAC as the first-ever LoRaWAN-oriented MAC protocol to enable interference-aware LoRaWAN communication in the 2.4 GHz band.
- We build LoRaWAN testbeds in different real-world environments and conduct practical experiments to prove the feasibility and superiority of InMAC.

The rest of this paper is organized as follows. Section II provides a comprehensive review of existing techniques and studies addressing the coexistence challenges between LoRaWAN and Wi-Fi networks. In Section III, we introduce essential background knowledge and system assumptions that form the foundation for understanding the design of InMAC. Section IV presents the detailed design and operational principles of InMAC, including its core mechanisms for interference avoidance. In Section V, we discuss several noteworthy considerations and potential limitations related to the implementation and deployment of InMAC in practical environments. Section VI presents the details of our real-world testbeds, while Section VII reports the experimental results. Finally, Section VIII draws the conclusion.

II. Related Work

In LoRaWAN, the issue of signal interference caused by coexisting Wi-Fi networks has been discussed and experimentally analyzed in several prior research efforts [20]–[25]. These studies primarily focus on characterizing and quantifying the impact of Wi-Fi interference on LoRaWAN communication performance. They do not propose concrete mechanisms or protocol-level solutions to actively mitigate this problem. To the best of our knowledge, concrete solutions to mitigate this problem have been proposed in only a few studies [26]–[28]. Focusing on the physical layer of LoRaWAN, the method introduced in [26] is designed to separate contaminated LoRaWAN signal samples from Wi-Fi interference. Specifically, it applies short-time Fourier transform (STFT) to each received LoRaWAN signal symbol to identify interference-free samples. These intact samples are then selectively forwarded to the standard LoRaWAN signal decoding pipeline, enabling partial symbol recovery while discarding corrupted portions. Similarly, [27] proposes a frequency bin masking technique that is generated based on the detected preamble field of a LoRaWAN signal. The mask is subsequently applied to facilitate more reliable decoding of the following payload field within the same signal, thereby improving demodulation accuracy under Wi-Fi interference.

In contrast to these physical-layer approaches, a MAC-layer protocol is introduced in [28] as a different strategy to avoid Wi-Fi interference in LoRaWAN communication. This protocol operates by having each Wi-Fi transmitter detect the presence of LoRaWAN transmissions and dynamically vacate a portion of its channel bandwidth to create interference-free communication opportunities for LoRaWAN devices. While InMAC shares a similar objective with this method, *i.e.,* enhancing coexistence between LoRaWAN and Wi-Fi networks, it is fundamentally different in its design philosophy. InMAC is specifically developed as a LoRaWAN-oriented MAC protocol implemented directly at LoRaWAN devices, whereas the solution in [28] is Wi-Fi-oriented and requires modifications at the Wi-Fi transmitter side. In other words, InMAC reexamines the coexistence challenge from the perspective of channel access management within LoRaWAN itself, rather than relying on cooperative behavior from Wi-Fi networks. This distinction makes InMAC more practical in scenarios where Wi-Fi network configurations cannot be modified or controlled by LoRaWAN operators.

Recent studies have also explored machine learning-based adaptive MAC protocols for LoRaWAN. Several works employ Q-learning to optimize channel access parameters such as channel selection, backoff timing, or transmission settings under dynamic interference [32], [33]. More advanced approaches integrate deep reinforcement learning to jointly tune spreading factor and transmit power for improved scalability [34]. These learning-based schemes provide long-term adaptability through experience-driven optimization, but often require exploration periods or assume relatively stable interference patterns. In contrast, InMAC reacts immediately to cross-technology interference using real-time Wi-Fi traffic profiling and dual carrier sensing, making it complementary to these learning-driven approaches.

III. Preliminary

Before presenting the detailed design of InMAC, we first provide a brief overview of LoRaWAN networking, clearly define the specific coexistence problem addressed in this work, and describe the underlying motivation that guides the development of InMAC.

[2] If not specified, we make no distinction between the terms “LoRaWAN” and “2.4 GHz LoRaWAN” in the rest of this paper for brevity.

A. Basics of LoRaWAN Networking

In LoRaWAN, wireless signals are divided into multiple segments of equal duration, with each segment referred to as a chirp or symbol. Fundamentally, the frequency of each chirp increases linearly across a specified bandwidth, which can typically be 203 KHz, 406 KHz, 812 KHz, or 1625 KHz, depending on the configuration. The duration of each chirp is controlled by a parameter known as the spreading factor (SF), which generally takes values in the range of $[7, 12]$ [8]. SF not only determines the length of each chirp but also defines how much data is embedded within it. Specifically, a higher SF results in a longer chirp duration, making the transmission more robust against interference but reducing the data rate. For signal demodulation, each incoming chirp is down-sampled and multiplied by a predefined reference chirp. The result of this multiplication is then processed using fast Fourier transform (FFT), through which a peak FFT bin emerges. The frequency index of this peak bin corresponds to the specific data symbol encoded in the chirp.

Regarding channel access mechanisms at LoRaWAN end devices, the ALOHA protocol is predominantly adopted because of its simplicity and ease of deployment. However, ALOHA inherently suffers from a high probability of signal collisions, as end devices transmit their packets without sensing whether the channel is already occupied by another transmission. To address this limitation, a specialized carrier-sensing method called CAD has been developed for use in LoRaWAN [30], [31]. Unlike conventional carrier-sensing techniques such as those based on received signal strength (RSS) used in Wi-Fi and ZigBee, CAD operates by correlating received signals with one or more locally generated chirps. If a significant peak correlation result is detected, it indicates the presence of an ongoing LoRaWAN transmission, signaling to other end devices that the channel is currently busy. Although CAD is implemented at the transceiver level and is not specific to the LoRaWAN protocol, it has been widely adopted in LoRaWAN systems as an effective CSMA mechanism. This allows end devices to defer their transmissions until the channel becomes free, thereby reducing the likelihood of signal collisions and improving overall network efficiency.

B. Problem Domain

This work focuses on enabling interference-aware LoRaWAN communication in environments where a LoRaWAN coexists with one or more Wi-Fi networks operating in the same frequency band. The considered LoRaWAN setup consists of a gateway and multiple end devices, all configured with identical signal parameters such as SF, center frequency, and channel bandwidth. Each end device performs uplink transmissions to the gateway and subsequently awaits a 1-bit downlink acknowledgment message as confirmation of successful signal reception at the gateway.

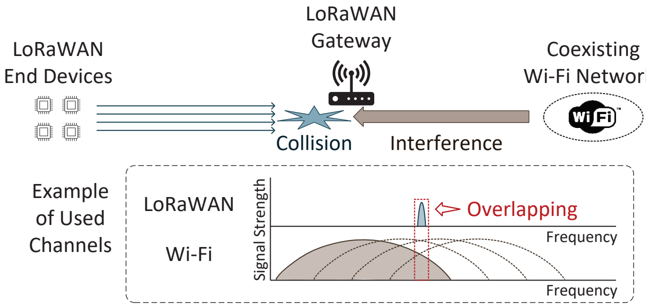


Fig. 1. Targeted coexistence problem between LoRaWAN and Wi-Fi networks. We aim to enable interference-aware LoRaWAN communication by mitigating both external Wi-Fi interference and internal LoRaWAN signal collisions at the gateway.

Targeted Problems: As illustrated in Fig. 1, the operating channels of LoRaWAN and Wi-Fi networks overlap, leading to potential coexistence issues. Specifically, due to the typically higher transmission power of Wi-Fi signals, there is a significant risk that Wi-Fi traffic interferes with the reception of LoRaWAN uplink signals at the gateway, degrading communication reliability. It is important to note that the downlink acknowledgment messages from the gateway to end devices are generally very short. Therefore, the impact of Wi-Fi interference on the acknowledgment message transmissions is relatively minor and will be validated in Section VII-A. Additionally, within the LoRaWAN itself, multiple end devices may transmit simultaneously, resulting in internal signal collisions, which further hampers communication efficiency.

Design Goals: This work aims to mitigate both external interference from Wi-Fi and internal interference due to LoRaWAN signal collisions by dynamically adjusting the channel access behavior of end devices. For handling Wi-Fi interference, we introduce a Wi-Fi traffic profiling mechanism at the gateway alongside an adaptive algorithm that adjusts LoRaWAN packet lengths based on observed Wi-Fi silent time. This allows LoRaWAN end devices to probabilistically align their transmissions with periods of reduced Wi-Fi activity, improving transmission success rates. To address internal LoRaWAN signal collisions, we propose a CAD-based CSMA protocol. This protocol requires each end device to perform a clear channel assessment before initiating any transmission, ensuring that the channel is free and minimizing the likelihood of signal collisions among end devices.

C. Motivation for InMAC

To mitigate external Wi-Fi interference in LoRaWAN, a straightforward approach is to let LoRaWAN end devices perform RSS-based carrier sensing to detect ongoing Wi-Fi signals before initiating their own transmissions. While this method can reduce some interference, it does not fully prevent Wi-Fi from disrupting LoRaWAN communications. This is because Wi-Fi transmitters, due to their typically higher power and independent management, usually cannot sense the much weaker LoRaWAN signals, leading to unavoidable interference at the LoRaWAN gateway. Additionally, LoRaWAN signals generally have much longer airtime compared to Wi-Fi signals, making them more vulnerable to being overlapped by multiple Wi-Fi transmissions. To further minimize interference, InMAC is designed to utilize the silent time (*i.e.,* idle periods) of Wi-Fi traffic for scheduling LoRaWAN transmissions. However,

This article has been accepted for publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2025.3641235

predicting Wi-Fi silent time is inherently challenging because Wi-Fi networks are often managed independently by different operators, preventing coordinated control. To tackle this, InMAC incorporates a Wi-Fi traffic profiling mechanism that characterizes Wi-Fi silent time in a probabilistic manner rather than requiring precise prediction. Details of this profiling process are described in Section IV-B.

To handle internal LoRaWAN signal collisions caused by simultaneous transmissions from multiple end devices, InMAC can theoretically be designed using schemes such as time-division multiple access (TDMA), frequency-division multiple access (FDMA), or CSMA. However, both TDMA and FDMA require tight clock synchronization and additional coordination signaling between gateways and end devices, which significantly increases overhead and system complexity especially in large-scale LoRaWAN deployments. In contrast, CSMA allows end devices to perform carrier sensing independently and asynchronously, offering a simpler and more scalable solution. Based on this insight, InMAC is developed following the general principles of CSMA, consisting of a carrier-sensing phase and a signal transmission phase. Specifically, the carrier sensing in InMAC relies on the CAD technique, which is specially adapted for LoRaWAN signal characteristics.

IV. Design of InMAC

As a MAC protocol, InMAC adjusts the channel access behaviors of end devices to combat Wi-Fi interference and LoRaWAN signal collisions.

A. Overview of InMAC

InMAC is implemented collaboratively at both LoRaWAN gateways and end devices with the objective of mitigating two major challenges: external interference from coexisting Wi-Fi networks and internal signal collisions among LoRaWAN end devices. To keep end devices informed about the current Wi-Fi traffic conditions, each gateway periodically broadcasts beacons that carry information about the silent time status of Wi-Fi traffic, denoted as Ω. This parameter Ω represents the probabilistically characterized idle periods in Wi-Fi transmissions, during which LoRaWAN devices are encouraged to transmit to reduce the likelihood of interference.

To maintain accurate and up-to-date values of Ω, the gateway continuously performs a Wi-Fi traffic profiling process (described in detail in Section IV-B) during the interval between beacon transmissions. This ensures that the silent time information remains reflective of real-time network conditions. Additionally, to account for potential clock drifts between gateways and end devices, the gateway transmits the same beacon three times consecutively. This redundancy enhances the reliability of beacon reception by ensuring that even if one transmission is missed or lost due to timing offsets, the end devices still have multiple opportunities to receive a valid beacon. Importantly, end devices maintain coarse synchronization with the gateway based on these beacons, without the need for precise timing alignment. The gateway continuously listens on the LoRaWAN channel for uplink transmissions from end devices and issues a one-bit acknowledgment packet (Ack) to confirm successful packet reception.

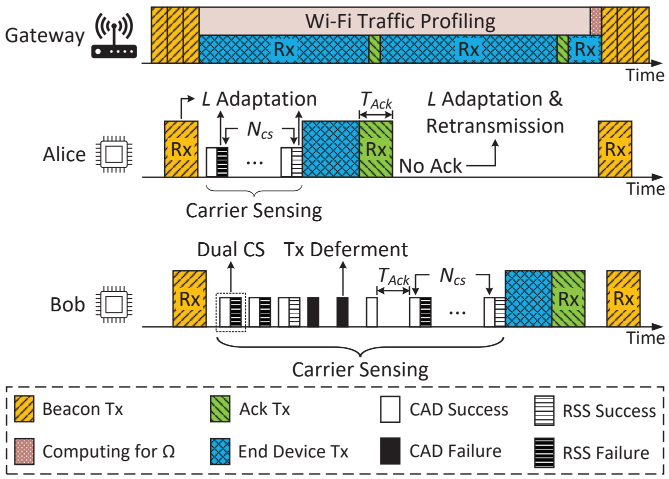


Fig. 2. An example of InMAC operation involving a gateway and two end devices (Alice and Bob). The results of RSS-based sensing (*i.e.,* success or failure) are affected by the timing of coexisting Wi-Fi traffic and are illustrated as an example here. Tx: Transmission; Rx: Reception; CS: Carrier sensing.

When an end device receives a beacon, it immediately updates its local value of Ω and adapts its packet length, represented as L, accordingly. The value of L is adjusted to match the estimated silent time in Wi-Fi traffic, improving the probability that the end device's transmission is completed within a Wi-Fi idle slot. Before initiating transmission, the end device must assess the channel's current status to check for ongoing LoRaWAN or Wi-Fi transmissions. InMAC introduces a dual carrier sensing mechanism combining two techniques: CAD for detecting LoRaWAN signals and RSS-based sensing for detecting Wi-Fi signals.

The dual carrier sensing process operates as follows. First, the end device performs CAD to detect any ongoing LoRaWAN transmissions. If a LoRaWAN signal is detected via CAD, it is regarded as a CAD failure (*i.e.*, channel busy), prompting the end device to defer its transmission attempt. If CAD does not detect any LoRaWAN signal, it is considered a CAD success (*i.e.*, channel free), but the end device is required to perform N_{cs} consecutive successful CAD checks before finally determining the channel as idle. This process reduces the likelihood of transmitting in a briefly idle channel. The counter for consecutive CAD checks resets to N_{cs} each time a CAD failure occurs. Notably, when CAD fails, only CAD-based sensing is used in subsequent checks until CAD succeeds again and RSS sensing is skipped in this case.

Once CAD is successful, the end device proceeds with RSS-based sensing to detect the presence of Wi-Fi signals. If the measured RSS value exceeds a predefined threshold (typically set near the noise floor level), it is classified as an RSS failure (*i.e.*, Wi-Fi detected), and the device reduces its packet length L according to the updated Ω value. If the RSS is below the threshold, it is treated as an RSS success (*i.e.*, no Wi-Fi detected), allowing the device to increase L according to Ω. Through this adaptive adjustment of L, InMAC tries to dynamically align LoRaWAN packet durations with Wi-Fi silent periods, reducing the likelihood of interference.

After a successful transmission, the end device waits for a fixed duration denoted as T_{Ack} to receive an Ack. During this waiting period, the device can either listen continuously or wake up at two predefined receive windows as specified in the LoRaWAN Class A standard [35]. For simplicity and reliability, InMAC adopts continuous listening throughout T_{Ack}. If no Ack is received within this period, the end device interprets the transmission as failed, reduces its packet length L further, and initiates a packet retransmission attempt. Both dual carrier sensing and L adaptation are performed again as part of the retransmission process. Specific details of the L adaptation logic are provided in Section IV-C.

To illustrate InMAC's operation, Fig. 2 presents an example involving two end devices, Alice and Bob. After receiving a beacon from the gateway, Alice initiates dual carrier sensing using CAD followed by RSS sensing. Based on each RSS result, Alice updates L dynamically, following the adaptation rules described earlier. After observing N_{cs} consecutive successful CAD results, Alice determines the channel is idle and immediately begins transmission. Meanwhile, Bob performs CAD but encounters two consecutive CAD failures due to Alice's ongoing transmission. Once Alice's transmission concludes, Bob observes a CAD success, waits for T_{Ack}, and then restarts dual carrier sensing. After obtaining N_{cs} consecutive successful dual carrier sensing results, Bob judges the channel as idle and initiates its own transmission.

B. Wi-Fi Traffic Profiling

To obtain the silent time status (Ω) of coexisting Wi-Fi traffic, a straightforward and intuitive method is for a LoRaWAN gateway to actively scan all Wi-Fi channels that overlap with the target LoRaWAN channel. This scanning is combined with Wi-Fi signal recognition using specialized algorithms, such as the well-known Schmidl-Cox algorithm [36], which is designed for efficient detection and synchronization of Wi-Fi preambles. This approach allows the gateway to precisely identify the presence and timing of Wi-Fi transmissions across a broad frequency range. Notably, this method can be implemented using commercial off-the-shelf LoRaWAN chipsets like the Semtech LR1120, which supports both LoRaWAN communications and Wi-Fi scanning within the 2.4 GHz frequency band [17]. While this comprehensive signal recognition technique is effective for accurately generating Ω, the primary objective of Wi-Fi traffic profiling in InMAC is not to decode or fully recognize Wi-Fi signals occupying a large bandwidth. Instead, it aims to gain a lightweight understanding of when Wi-Fi interference occurs specifically within the relatively narrow bandwidth of the LoRaWAN channel to facilitate timely interference avoidance.

Accordingly, InMAC adopts a more lightweight and practical approach for Wi-Fi traffic profiling by focusing solely on monitoring signal strength within the target LoRaWAN channel itself, without the need for complex Wi-Fi signal decoding. More specifically, whenever a signal is detected with strength exceeding a predefined threshold (usually set close to the noise floor), InMAC interprets this as the presence of Wi-Fi interference. It then records the precise timestamp and duration of this detected interference event. If the signal detected is identified by the LoRaWAN signal decoder at the gateway as a legitimate LoRaWAN transmission rather than Wi-Fi, InMAC disregards this event and continues to monitor the channel without marking it as interference. By continuously performing this lightweight sensing during the interval between beacon transmissions, InMAC constructs a dataset containing n Wi-Fi interference events.

From this dataset, InMAC derives a Wi-Fi silent time set $S = \{s_1, ..., s_i, ..., s_{n-1}\}$ where s_i denotes the time interval between the i-th and the $(i+1)$-th Wi-Fi interference events. Using S, InMAC generates the Wi-Fi silent time status Ω as

$$\Omega = \{\mu, \alpha, \beta\}, \tag{1}$$

where

$$\begin{aligned} \mu &= \frac{1}{n-1}\sum_{i=1}^{n-1} s_i, & (2)\\ \alpha &= \max(s_1, ..., s_i, ..., s_{n-1}), & (3)\\ \beta &= \min(s_1, ..., s_i, ..., s_{n-1}). & (4) \end{aligned}$$

In other words, μ represents the mean silent time calculated over all values in S, α denotes the maximum silent time in S, and β corresponds to the minimum silent time in S. This statistical characterization enables InMAC to probabilistically estimate the potential transmission opportunities in the LoRaWAN channel during Wi-Fi silent periods. By leveraging these three parameters (*i.e.,* average, longest, and shortest silent times) in Ω, InMAC can dynamically adapt LoRaWAN transmission behaviors to improve coexistence with unpredictable Wi-Fi activity.

It is also important to note that given three consecutive beacon transmissions by the gateway, InMAC performs the Ω update process immediately before sending the first beacon. This ensures that the silent time information communicated to the end devices remains current and reflective of the most recent Wi-Fi traffic conditions, thereby enhancing the effectiveness of interference-aware channel access decisions. We further note that the values of μ, α, and β are inherently influenced by the temporal variability of surrounding Wi-Fi traffic. In highly bursty environments (e.g., indoor office scenarios), larger fluctuations are observed between α and β, indicating a wider range of silent intervals. In such cases, InMAC adopts more conservative packet length adaptation to reduce the risk of collision. In contrast, in more stable environments (*e.g.,* controlled outdoor interference), μ, α, and β exhibit lower variance and tighter clustering, allowing InMAC to select longer transmission opportunities with higher confidence. This adaptive response to the statistical variability of Wi-Fi silent intervals contributes to the robustness of InMAC under diverse and time-varying interference conditions.

C. Packet Length Adaptation

To probabilistically avoid Wi-Fi interference, InMAC requires each end device to dynamically adjust its packet length (L) so that its signal transmission is more likely to occur during the silent periods of surrounding Wi-Fi traffic. By tailoring

L to align with observed idle times, InMAC minimizes the probability that a LoRaWAN signal overlaps with active Wi-Fi transmissions. As illustrated in Fig. 2, packet length adaptation in InMAC is triggered under the following three specific cases.

- Case 1: A beacon from the gateway is just received.
- Case 2: RSS-based carrier sensing fails or succeeds.
- Case 3: A packet retransmission becomes necessary.

In Case 1, immediately after receiving a beacon, the end device initializes its packet length by setting L to L^{μ}. Here, L^{μ} refers to the packet length corresponding to an airtime that is closest to the mean silent time μ contained in the received beacon. This approach ensures that the initial packet length is proportionally aligned with the average idle period observed in the Wi-Fi traffic. The specific value of L^{μ} is determined based on the predefined LoRaWAN parameters such as SF, channel bandwidth, and coding rate. These parameters dictate the time-on-air for a given payload size, allowing L^{μ} to be calculated by adjusting the payload length, as exemplified in [37]. For clarity and conciseness, the detailed formula and step-by-step calculation procedure for L^{μ} are omitted here.

In Case 2, InMAC utilizes an adaptive packet length adjustment mechanism based on the outcome of RSS-based carrier sensing. To facilitate this process, InMAC defines an L adaptation range, denoted as κ, calculated as

$$\kappa = \min\left(\frac{\alpha - \mu}{N_{cs}}, \frac{\mu - \beta}{N_{cs}}\right). \tag{5}$$

The parameter κ ensures that the adjustment step size is proportionally bounded by both the observed silent time variability and N_{cs}. When RSS-based carrier sensing fails (*i.e.*, a Wi-Fi transmission is detected), the end device reduces its current packet length by one step, updating L as $L - L^{\kappa}$. Conversely, when RSS-based carrier sensing succeeds (*i.e.*, no Wi-Fi signal is detected), the end device increases its packet length as $L + L^{\kappa}$. In this way, after each RSS-based sensing result, the packet length is incrementally tuned using a step size of L^{κ}, promoting adaptive alignment with the fluctuating nature of Wi-Fi idle times.

In Case 3, when a packet retransmission is necessary due to the absence of an Ack from the gateway, InMAC assumes that the packet loss is likely caused by the relatively long airtime of the initial transmission, increasing its vulnerability to Wi-Fi interference. To address this, InMAC reduces the length of the previously transmitted packet by half, using this reduced length as the new initial value for the retransmission attempt.

It is also important to highlight two key constraints enforced by InMAC on packet length adaptation. First, the adapted packet length L must not exceed L^{α}, which is defined as the packet length corresponding to the longest silent time α observed in Wi-Fi traffic. This upper limit ensures that even after multiple increments due to successful RSS sensing, packet airtime does not exceed the empirically observed maximum idle period. If, at any point, the calculated L surpasses L^{α}, InMAC forcibly limits it to L^{α} regardless of further RSS sensing outcomes. Second, regarding the minimum packet length after adaptation, InMAC enforces a lower bound. Specifically, the packet length must include the fixed size of packet metadata (*e.g.,* preamble, sync word, and packet header) plus a minimum of one payload signal symbol. This rule ensures that even under severe channel conditions requiring minimal airtime, the transmitted packet maintains meaningful payload content and remains decodable.

To further validate the choices of the minimum (1) and maximum (L^{α}) values of L, we conducted practical experiments by varying them in steps of one payload signal symbol. While omitted here for clarity, the results show that i) when the maximum is fixed to L^{α}, adopting minimum values in the range of $[1, 7]$ does not significantly change the throughput, and ii) when the minimum is fixed to 1, choosing maximum values within $[L^{\alpha} - 5, L^{\alpha}]$ achieves comparable throughput performance. Beyond these ranges, throughput degradation is observed because a higher minimum value increases collision probability with Wi-Fi signals, while a lower maximum reduces the opportunity to fully exploit Wi-Fi silent periods. Based on these observations, in this work we adopt the minimum value of L as 1 and the maximum as L^{α}. We also note that the optimal choices of these bounds may vary across deployment environments, depending on factors such as the number of LoRaWAN end devices and Wi-Fi traffic density. Additionally, adapted packet lengths in InMAC must comply with the maximum payload size limits defined by the LoRaWAN standard [11]. All the operations in the packet length adaptation mechanism is summarized in Algorithm 1.

Algorithm 1: Packet length adaptation in InMAC

```
Input: Silent time parameters $(\mu, \alpha, \beta)$, current $L$,
       $N_{cs}$, LoRaWAN payload limit $L^{\text{maxLoRaWAN}}$
Output: Updated packet length $L$
Case 1: On beacon reception:
$L \leftarrow L^{\mu}$;
Case 2: RSS-based sensing result:
$\kappa \leftarrow \min\left(\frac{\alpha-\mu}{N_{cs}}, \frac{\mu-\beta}{N_{cs}}\right)$;
if RSS failure (Wi-Fi detected) then
    $L \leftarrow L - L^{\kappa}$;
else
    $L \leftarrow L + L^{\kappa}$;
Case 3: Retransmission (no Ack):
$L \leftarrow \lfloor L/2 \rfloor$;
Enforce constraints:
$L \leftarrow \min(L, L^{\alpha})$;
$L \leftarrow \max(L, L^{\text{min}})$;
$L \leftarrow \min(L, L^{\text{maxLoRaWAN}})$;
return $L$;
```

V. Discussion

A few points regarding the current design of InMAC are worth mentioning.

A. Adaptive Activation of InMAC

InMAC is designed to operate as an on-demand MAC protocol alongside basic channel access modes such as ALOHA at LoRaWAN gateways and end devices. Rather than serving as a permanent replacement, InMAC can be selectively activated depending on network conditions. For instance, when a gateway communicates with only a limited number of end devices and detects that the traffic load from coexisting Wi-Fi networks is minimal, end devices can continue using the simpler ALOHA protocol for channel access. This flexible approach helps balance system complexity and performance. The specific benchmarks for switching between ALOHA and InMAC (*e.g.,* thresholds for end device population or Wi-Fi interference level) can be configured by network operators, application developers, or end users according to system requirements and deployment scenarios.

B. Energy Consumption Considerations at End Devices

InMAC performs Wi-Fi traffic profiling entirely at the gateway side, and end devices only receive the resulting silent-time parameter Ω through periodic beacons. Thus, the profiling mechanism incurs no additional energy overhead at end devices. For channel sensing, InMAC adopts a hierarchical design in which CAD is used as the primary sensing technique while RSS-based sensing is performed only when CAD successfully detects activity. According to the specifications of the Semtech SX128x chipset series, a typical CAD operation consumes approximately 4.5–6.0 mA for 64–96 μs, corresponding to 0.3–0.6 μJ per CAD operation [15], [16]. In contrast, a single LoRaWAN transmission, lasting 20–40 ms at +6 dBm, consumes around 30–60 mJ. Hence, even if InMAC performs multiple CAD checks per packet, the sensing overhead remains several orders of magnitude smaller than the cost of a single transmission, contributing well under 0.01% of the total energy used per packet.

ALOHA incurs no sensing energy, because it transmits immediately without performing CAD or RSS-based checks. In contrast, InMAC introduces a minimal sensing overhead due to CAD and occasional RSS measurements. However, the additional energy consumed by these sensing operations is extremely small (on the order of microjoules per packet) compared with the energy required for packet retransmissions. Under moderate Wi-Fi interference, ALOHA may require multiple retransmissions (2–4 attempts), each costing tens of millijoules. InMAC's design aligns transmissions with Wi-Fi silent periods and reduces internal collisions, substantially lowering the retransmission rate. Consequently, the overall energy consumption per delivered message is expected to be lower for InMAC than ALOHA, despite InMAC's small sensing overhead. In other words, InMAC trades microjoules of sensing for millijoules of retransmission savings, leading to net energy benefits.

Although the above analysis leverages vendor-provided SX128x specifications, the current study does not include direct measurements of energy-per-bit or energy-per-delivered-message due to the lack of on-board current-sensing hardware. In future work, we will instrument end devices with external power monitoring modules (*e.g.,* INA226 or Nordic Power Profiler Kit) to provide fully measured comparisons of InMAC and ALOHA under identical coexistence scenarios.

C. Packet Length Adaptation at Application Layer

While InMAC primarily targets improving LoRaWAN performance (*e.g.,* throughput and reliability) under coexistence with Wi-Fi networks at the MAC layer, its application in real-world IoT systems requires careful consideration at the application layer. In particular, the packet length adaptation mechanism in InMAC may affect application data consistency, as varying packet sizes could fragment larger application-layer data units. To mitigate this, developers should implement application-layer mechanisms such as packet segmentation and reassembly. These functions ensure that larger messages are divided into InMAC-compatible packets during transmission and accurately reassembled at the receiving end, preserving data integrity and consistency across the system. Moreover, by aligning packet transmissions with Wi-Fi silent periods and reducing collisions and retransmissions, InMAC can enhance effective delivery reliability and latency, even under heavy interference. For highly time-critical or mission-critical applications, additional measures such as tuning adaptation parameters, prioritization, or redundancy mechanisms may be necessary to meet strict latency and integrity requirements. Detailed application-layer design is beyond the scope of this work and will be explored in future studies.

D. CAD, Synchronization, and Class-Level Extensions

In practical deployments, several additional aspects warrant consideration. First, the performance of CAD may degrade in environments with strong multipath propagation or severe signal reflections, potentially leading to occasional false detections or missed channels. Second, as the network scales to a large number of end devices, beacon-based synchronization and the dissemination of Ω may become more challenging due to timing drift and increased contention, requiring more robust synchronization strategies. Finally, while this work focuses on uplink-dominated communication under LoRaWAN Class A, extending InMAC to support more intensive bidirectional traffic and to operate under Class B (beacon-synchronized ping slots) and Class C (continuous reception) could further enhance downlink reliability in coexistence scenarios, at the cost of increased complexity and energy consumption.

VI. Implementation

For the evaluation of InMAC, we implement a LoRaWAN prototype consisting of one gateway and 20 end devices. This experimental scale is consistent with prior studies: four end devices in [26], 20 end devices in [27], and one end device in [28]. The hardware used for both the gateway and end devices is the Semtech LR1120DVK1TCKS development kit, equipped with an LR1120 radio chip and an STM32L476RGT6 microcontroller [38]. Each end device is assigned a unique identifier (E1-E20) and includes it in the header of each uplink packet. The gateway employs two LR1120DVK1TCKS devices: one for Wi-Fi traffic profiling and beacon transmissions, and the other for communication with end devices. Both devices are managed by the same laptop to support InMAC functionality. It is worth noting that InMAC is inherently hardware-agnostic, relying on standard

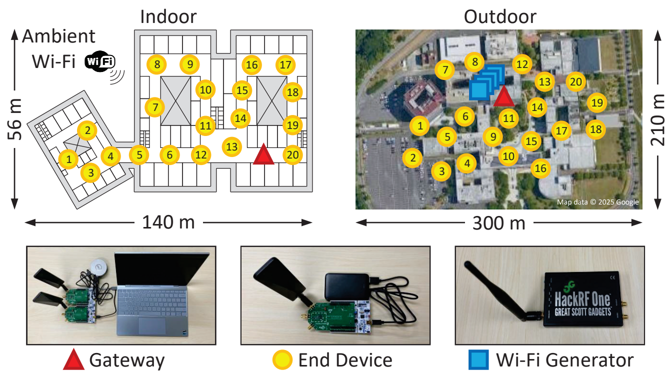


Fig. 3. Evaluation scenarios (indoor and outdoor) with one gateway and 20 end devices (E1-E20). Wi-Fi interference arises from ambient Wi-Fi networks in the indoor environment and from four dedicated Wi-Fi generators in the outdoor environment.

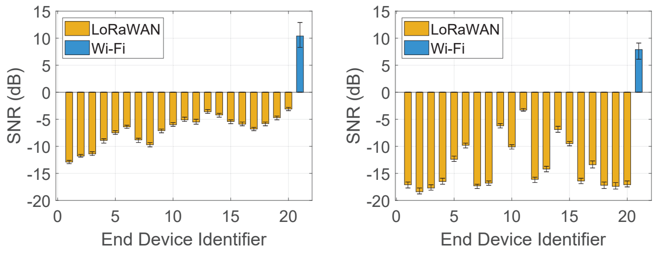
LoRaWAN features such as CAD and RSS-based sensing. Porting InMAC to other LoRa-compatible radios, including the SX1280 and SX1281, is therefore straightforward [15], [16]. Comprehensive evaluation across multiple hardware platforms will be pursued in future work.

We evaluate InMAC in both indoor and outdoor environments as illustrated in Fig. 3. The indoor environment is a typical office building covering 4500 m^2, with end device-to-gateway distances ranging from $[20, 100]$ meters. Wi-Fi interference indoors originates from ambient Wi-Fi infrastructure. To estimate Wi-Fi activity, we perform a rough scan of Wi-Fi Channels 1-13 in the 2.4 GHz band. Frequent transmissions are detected across all channels, indicating significant interference affecting LoRaWAN signals, as discussed in Section VII-B. The indoor experiments are conducted on weekdays between 9:00-11:00 am, which corresponds to peak usage hours with a large number of active users. During this period, we observe heterogeneous, bursty, and mobility-driven Wi-Fi traffic from existing infrastructure. To further intensify Wi-Fi activity, we additionally generate traffic ourselves by downloading a 5 GB movie file and continuously streaming multimedia content via Netflix, in parallel with background traffic from other users. These conditions expose InMAC to realistic traffic rates, multimedia flows, channel conditions, and highly variable interference patterns. Detailed information about the ambient Wi-Fi networks (*e.g.,* number of networks, coverage areas, channels, and transmitter locations) is unavailable, as these networks are independently managed.

The outdoor evaluation is conducted on a university campus spanning 63000 m^2, where the end device-to-gateway distance ranges from $[25, 130]$ meters. We employ four HackRF One software-defined radios (SDRs) as Wi-Fi traffic generators to emulate controlled interference conditions, enabling systematic analysis of InMAC's coexistence behavior under repeatable and measurable settings [39]. This approach is primarily adopted because the campus Wi-Fi networks are deployed mainly indoors (*e.g.,* laboratories, classrooms, and meeting rooms). As a result, most outdoor end devices are unable to detect Wi-Fi transmissions, which would not realistically represent the coexistence between LoRaWAN and Wi-Fi networks. To address this, additional Wi-Fi generators are placed around the gateway to produce sufficient and detectable Wi-Fi traffic for all end devices. Their transmission functionality is based on the GNU Radio Wi-Fi transceiver implementation described in [40]. Each generator transmits packets containing 100-500 random payload bytes at uniform intervals. While this setup provides controlled and repeatable interference, it represents a simplified model of Wi-Fi activity. Nonetheless, InMAC is inherently capable of adapting to more complex traffic patterns through continuous Wi-Fi traffic profiling and dual carrier sensing, as demonstrated in the indoor evaluation.

For LoRaWAN communication, each end device transmits payload data at uniformly distributed time intervals after receiving an Ack. The payload size is determined by μ, as indicated in the latest beacon received from the gateway. The beacon length is 6 bytes and is transmitted thrice every two minutes with SF = 12 and a bandwidth of 812 KHz, which corresponds to less than 1% of total channel usage. Unless otherwise specified, LoRaWAN operates on a channel centered at 2.425 GHz with an 812 KHz bandwidth. The four Wi-Fi generators are configured on Channels 2-5 (20 MHz bandwidth), partially overlapping with the LoRaWAN channel. LoRaWAN data communication is conducted with SF = 9 and a coding rate of 4/8. Importantly, InMAC preserves the autonomy of end devices: beacons provide optional Wi-Fi silent-time information (Ω), but each end device independently decides whether and how to use this information for packet length adaptation and channel access. No centralized scheduling or unsolicited coordination is imposed by the gateway, and the beacon overhead remains negligible (less than 1% of channel resources). By lowering collisions and retransmissions, InMAC enhances both reliability and energy efficiency without restricting end device autonomy.

It is worth noting that our experiments involve 20 end devices, consistent with the experimental scale adopted in state-of-the-art studies: 4 in [26], 20 in [27], and 1 in [28]. Although our testbed includes only 20 end devices, InMAC is designed to scale efficiently to much larger deployments comprising hundreds or even thousands of end devices. The Wi-Fi traffic profiling and Ω beaconing mechanism at the gateway is independent of the number of end devices, allowing each end device to adapt its transmission timing and packet length locally. Similarly, the dual carrier sensing and packet length adaptation are performed individually at each end device, so scaling primarily affects network-level contention rather than per-end-device operations. As the number of end devices increases to hundreds or thousands, we anticipate a gradual increase in contention among LoRaWAN transmissions, but the dual carrier sensing design will continue to reduce collisions by probabilistically aligning transmissions with Wi-Fi silent periods. The packet length adaptation mechanism further mitigates the impact of high end device density by dynamically shortening transmissions when channel contention is detected, reducing the likelihood of retransmissions. At very high densities, both ALOHA and InMAC approach saturation due to channel capacity and duty-cycle limits, but InMAC is still expected to reduce retransmissions and channel waste. We also state that further scaling beyond hundreds of end



(a)

(b)

Fig. 4. SNR of LoRaWAN and Wi-Fi signals observed at the gateway. (a) Indoor. (b) Outdoor.

devices can be achieved through multi-channel/multi-gateway operation, which is identified as future work.

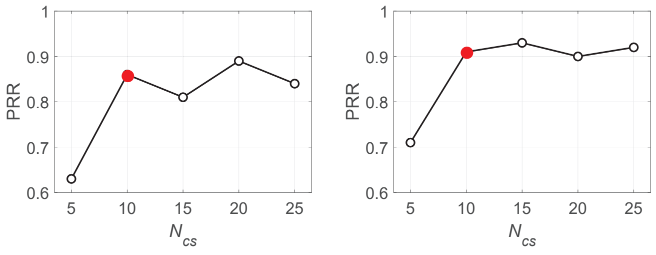
VII. Performance Evaluation

Based on the indoor and outdoor evaluation scenarios described in Section VI, we conduct extensive experiments to show the feasibility and superiority of InMAC for enabling interference-aware LoRaWAN communication. Before conducting a detailed evaluation of InMAC, we first analyze the SNR of both LoRaWAN and Wi-Fi signals as measured at the gateway. Fig. 4 shows the SNR of each transmitted LoRaWAN and Wi-Fi signal in indoor and outdoor scenarios, respectively. Wi-Fi transmissions consistently exhibit higher SNRs than LoRaWAN signals in both indoor (Fig. 4 (a)) and outdoor (Fig. 4 (b)) environments. This is consistent with expectations, as Wi-Fi signals from ambient Wi-Fi networks (indoor) or dedicated Wi-Fi generators (outdoor) generally have higher transmission power than LoRaWAN signals. For LoRaWAN, the 20 end devices show average SNRs ranging from -12.9 to -3.1 dB indoors and from -18.4 to -3.3 dB outdoors. As anticipated, outdoor SNRs tend to be lower due to increased transmission distance and more pronounced channel fading.

A. InMAC Evaluation

The performance of InMAC is evaluated using three primary metrics: packet reception ratio (PRR), Ack reception ratio (ARR), and channel access latency (CAL). PRR is defined as the ratio between the number of successfully received LoRaWAN packets and the total number of transmitted packets from the 20 end devices. ARR is defined as the ratio between the number of successfully received Ack packets (collected from all end devices) and the total number of transmitted Ack packets (managed by the gateway). Note that an Ack is transmitted from the gateway only when the corresponding uplink signal is successfully decoded. CAL refers to the total elapsed time for carrier sensing before a signal transmission.

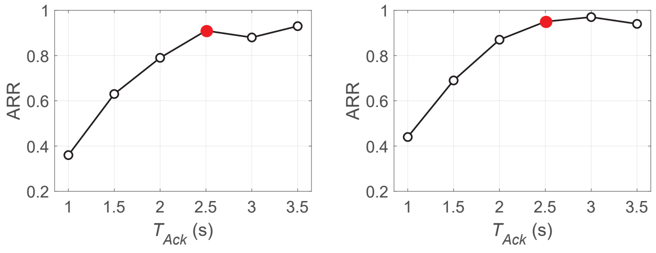
Fig. 5 shows the achieved PRR under different settings of N_{cs}. We observe that increasing N_{cs} from 5 to 10 significantly improves PRR in both the indoor and the outdoor environments. This indicates that adapting the LoRaWAN packet length more times during the dual carrier sensing process can increase the chance of avoiding Wi-Fi interference. However, the improvement becomes less notable when N_{cs} is further increased beyond 10. This is because taking more time for packet length adaptation may cause the end devices to miss the silent periods of Wi-Fi traffic. Based on this result, we set N_{cs} to be 10 in our experiments, and it may change depending on the tested environments. In addition, PRR performance differs between the indoor and outdoor scenarios. In the indoor environment, PRR is slightly lower and exhibits more pronounced fluctuations due to denser and uncontrollable Wi-Fi deployments, as well as more dynamic usage patterns from heterogeneous users and devices. In contrast, the outdoor experiments involve only four Wi-Fi generators, leading to smoother PRR behavior.



(a)

(b)

Fig. 5. PRR via InMAC under varying N_{cs}. (a) Indoor. (b) Outdoor.



(a)

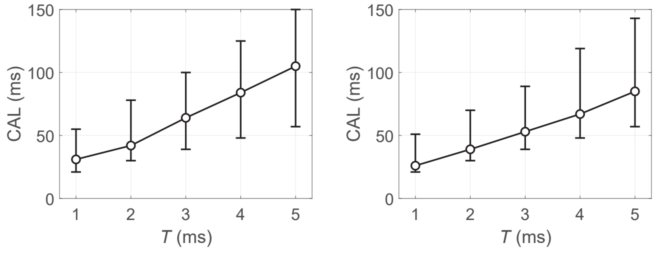
(b)

Fig. 6. ARR via InMAC under varying T_{Ack}. (a) Indoor. (b) Outdoor.

Fig. 6 shows the achieved ARR under different settings of T_{Ack}. We find that most Ack packets can be successfully received at the end devices in both the indoor and the outdoor environments when T_{Ack} is larger than 2.5 seconds. In the case where $T_{Ack} < 2.5$ seconds, a significant decrease in ARR is observed since the end devices experience considerable delay in receiving Ack packets due to several inevitable factors at the gateway, such as signal decoding and Ack packet preparation. Based on this result, we set T_{Ack} to be 2.5 seconds in our experiments, and it may change depending on the experimental settings. By observing the ARR results when $T_{Ack} > 2.5$ seconds, we confirm that Ack reception is not significantly affected by Wi-Fi interference because of its short airtime. It is also worth noting that in extremely congested environments, ACK loss may still occur. In such cases, standard LoRaWAN fallback mechanisms, such as uplink retransmissions triggered by missing ACKs, are naturally applied. For other LoRaWAN classes, further differences can be expected: Class B, with beacon-synchronized ping slots, may improve downlink reliability under heavy coexistence, while Class C, with continuous reception, can further increase the probability of successful ACK reception at the cost of higher energy consumption.

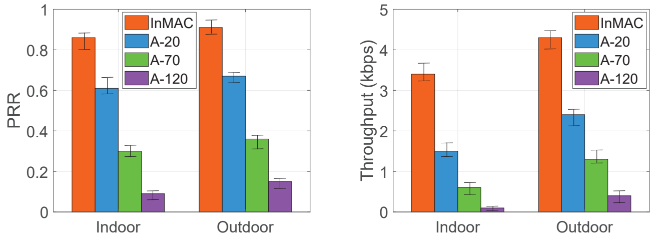
TABLE I
STATISTICAL RESULTS OF PRR AND THROUGHPUT IN TERMS OF STANDARD DEVIATION (σ), VARIANCE (σ^2), AND 95% CONFIDENCE INTERVAL (CI).

	PRR (Indoor)			PRR (Outdoor))			Throughput (Indoor)			Throughput (Outdoor))		
	σ	σ^2	95% CI	σ	σ^2	95% CI	σ	σ^2	95% CI	σ	σ^2	95% CI
InMAC	0.015	0.00023	[0.80,0.89]	0.010	0.00010	[0.89,0.95]	0.12	0.0144	[3.21,3.74]	0.08	0.0064	[4.04,4.47]
A-20	0.020	0.00040	[0.59,0.66]	0.013	0.00017	[0.65,0.69]	0.15	0.0225	[1.43,1.71]	0.10	0.0100	[2.16,2.53]
A-70	0.018	0.00032	[0.28,0.33]	0.015	0.00023	[0.31,0.38]	0.18	0.0324	[0.42,0.73]	0.12	0.0144	[1.21,1.53]
A-120	0.022	0.00048	[0.07,0.10]	0.020	0.00040	[0.11,0.16]	0.20	0.0400	[0.05,0.13]	0.16	0.0256	[0.27,0.51]



(a) (b)

Fig. 7. CAL via InMAC under varying T. (a) Indoor. (b) Outdoor.



(a) (b)

Fig. 8. Performance comparison of (a) PRR and (b) throughput measured at the gateway under the default experimental settings.

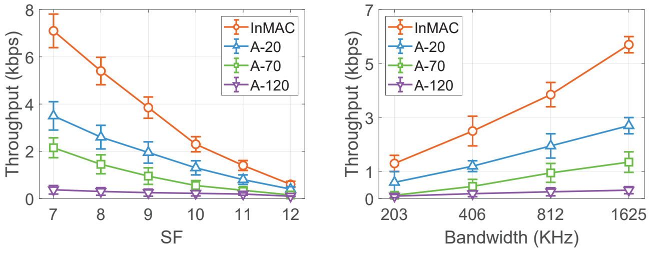
With the interval for the dual carrier sensing in InMAC set to be T ms, Fig. 7 shows the CAL experienced at the 20 end devices in the indoor and the outdoor environments. We can see that the end devices experience a longer CAL on average as T increases, since using a larger T makes the end devices wait for a longer time before starting another round of dual carrier sensing. In particular, the minimum CAL under a given T is the same for the indoor and the outdoor cases. This CAL corresponds to the total elapsed time for N_{cs} dual carrier sensing. Therefore, this indicates the existence of signal transmissions before which N_{cs} consecutive CAD operations are successful in both the indoor and the outdoor cases. Furthermore, we observe that the CAL in the outdoor environment is slightly shorter than that in the indoor environment. This is because CAD-based carrier sensing in the outdoor case is slightly less effective than that in the indoor case due to relatively severe channel fading among the outdoor end devices.

B. Performance Comparison

Recent studies [26]–[28] have also investigated the coexistence issues between LoRaWAN and Wi-Fi but from different design perspectives. As explained in Section II, the methods in [26], [27] enhance the physical layer of LoRaWAN by applying STFT-based selective forwarding or frequency bin masking to mitigate interference, requiring modifications to the signal processing chain. In contrast, [28] proposes a Wi-Fi-oriented MAC solution in which Wi-Fi transmitters vacate bandwidth to accommodate LoRaWAN transmissions, assuming cooperative behavior from Wi-Fi infrastructure. By comparison, InMAC adopts a LoRaWAN-oriented MAC-layer strategy. It is implemented entirely at LoRaWAN devices and leverages native mechanisms such as CAD to coordinate channel access, without requiring changes to the physical layer or to Wi-Fi networks. This design makes InMAC more practical for real-world deployments where LoRaWAN operators typically cannot influence Wi-Fi configurations. We therefore view InMAC as complementary to the physical-layer approaches in [26], [27] and the Wi-Fi-oriented MAC solution in [28], collectively enriching the spectrum of strategies available for reliable coexistence between LoRaWAN and Wi-Fi. For this reason, we adopt ALOHA, the default LoRaWAN channel access scheme, as the baseline for performance comparison, ensuring a fair and representative evaluation of our contributions.

From the gateway's perspective, we evaluate InMAC and ALOHA in terms of PRR and throughput. Since InMAC incorporates packet length adaptation to exploit silent periods in Wi-Fi traffic, we configure ALOHA with different fixed packet lengths to enable a fair comparison. Specifically, we set the packet payload size to 20 Bytes, 70 Bytes, and 120 Bytes, referring to these configurations as A-20, A-70, and A-120, respectively. Note that in each version of ALOHA, the packet length is fixed across all 20 end devices. Fig. 8 (a) presents the observed PRR in both indoor and outdoor environments. Across all repeated trials, InMAC consistently outperforms every ALOHA configuration. The mean PRR improvement is statistically significant, as confirmed by the small standard deviations shown in Table I. The 95% confidence intervals of InMAC do not overlap with those of A-20, A-70, or A-120 in any tested environment, indicating statistically significant differences. These results demonstrate that i) InMAC's packet length adaptation effectively mitigates Wi-Fi interference, and ii) its dual carrier sensing reliably reduces signal collisions among the 20 end devices. Among the three ALOHA variants, A-120 exhibits the lowest PRR, as the longer payload length and airtime make LoRaWAN transmissions more vulnerable to both Wi-Fi interference and internal signal collisions.

Throughput results follow the same trend. With $T = 1$ ms, Fig. 8 (b) shows the throughput achieved by InMAC and the three ALOHA variants. InMAC provides significantly



(a)

(b)

Fig. 9. Throughput comparison under varying (a) SF and (b) bandwidth.

higher mean throughput in both indoor and outdoor scenarios. The statistical variation is again small as shown in Table I. Moreover, the 95% confidence intervals of InMAC do not overlap with those of any ALOHA variant, confirming statistically significant gains. Consistent with the results in Section VII-A, PRR and throughput are generally higher outdoors compared to indoors. This is primarily because the indoor environment experiences denser ambient Wi-Fi traffic, while the outdoor setup uses only four Wi-Fi transmitters for Wi-Fi traffic generation.

Additionally, we examine throughput performance under different SF and bandwidth settings. The tested SF values range from 7 to 12, as typically used in LoRaWAN, as described in Section III-A. Besides the default 812 KHz bandwidth, we also consider 203 KHz, 406 KHz, and 1625 KHz bandwidth settings supported by the LR1120 radio chip. Fig. 9 presents the corresponding results, where each line shows the average throughput across both indoor and outdoor environments. InMAC consistently achieves higher throughput than the benchmark approaches across all SF and bandwidth configurations. As shown in Fig. 9 (a), throughput decreases as SF increases, reflecting the lower data rate associated with larger SF values. Conversely, as illustrated in Fig. 9 (b), increasing channel bandwidth improves data rate and thus enhances throughput. Notably, InMAC boosts throughput by up to 111% compared to A-20 when the bandwidth is set to 1625 KHz, as indicated in Fig. 9 (b).

Based on these observations, we conclude that InMAC inherently provides a degree of indirect fairness among end devices. By reducing both Wi-Fi interference and LoRaWAN signal collisions, InMAC increases the likelihood of successful transmissions for all end devices, including those experiencing weaker channel conditions or located farther from the gateway. This improvement holds across varying SF and bandwidth configurations, ensuring that performance gains are more evenly distributed compared to standard ALOHA, which does not account for coexistence or dynamic adaptation.

VIII. Conclusion and Future Work

This paper presents InMAC, the first LoRaWAN-oriented MAC protocol specifically designed to enable interference-aware LoRaWAN communication in environments where Wi-Fi networks coexist. To reduce the impact of external Wi-Fi interference, InMAC introduces a Wi-Fi traffic profiling mechanism at gateways and a packet length adaptation strategy at end devices, increasing the likelihood of aligning LoRaWAN transmissions with the silent time of Wi-Fi traffic. To prevent internal signal collisions among end devices, InMAC modifies their channel access behavior through a CAD-based CSMA protocol. Experimental evaluations in diverse real-world environments demonstrate that InMAC substantially enhances LoRaWAN performance, maintaining high reliability and throughput even in the presence of Wi-Fi interference.

Looking ahead, several extensions can be built atop InMAC.

- Integration with Adaptive Data Rate (ADR): InMAC's Wi-Fi-aware packet length adaptation can be jointly optimized with ADR mechanisms to simultaneously adjust SF, transmit power, and packet duration. A unified ADR-InMAC controller could, for example, reduce packet airtime in highly congested Wi-Fi periods or boost SF only when InMAC detects persistent interference patterns.
- Inter-gateway cooperation: Multi-gateway deployments could share Wi-Fi traffic fingerprints, CAD statistics, and channel occupancy maps through a lightweight backhaul protocol. Such cooperation would enable coordinated back-off windows, interference-aware gateway selection, and distributed scheduling that minimizes redundant sensing and reduces network-wide collision probability.
- Hybrid TDMA/CSMA operation for ultra-dense networks: In extremely dense deployments (hundreds of end devices per gateway), a hybrid scheme can be introduced where InMAC provides CSMA-based access during light/moderate congestion, while gateways periodically broadcast micro-TDMA beacons to reserve short contention-free slots for end devices experiencing repeated failures. This hybrid design would allow deterministic latency and collision-free transmissions during peak interference while preserving CSMA flexibility in normal conditions.

By incorporating these extensions, InMAC can evolve into a fully adaptive interference-resilient MAC framework, paving the way for reliable and energy-efficient LoRaWAN operation in future ultra-dense and highly heterogeneous unlicensed spectrum environments.

References

[1] A. Ikpehai, B. Adebisi, K. M. Rabie, K. Anoh, R. E. Ande, M. Hammoudeh, H. Gacanin, and U. M. Mbanaso, "Low-power wide area network technologies for Internet-of-Things: A comparative review," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2225–2240, Apr. 2019.

[2] The Business Research Company – Low Power Wide Area Network (LPWAN) Global Market Report 2025. [Online]. Available: https://www.thebusinessresearchcompany.com/report/low-power-wide-area-network-lpwan-global-market-report.

[3] M. Jouhari, E. M. Amhoud, N. Saeed, and M.-S. Alouini, "A survey on scalable LoRaWAN for massive IoT: Recent advances, potentials, and challenges," *arXiv:2202.11082*, Feb. 2022.

[4] C. Li and Z. Cao, "LoRa networking techniques for large-scale and long-term IoT: A down-to-top survey," *ACM Comput. Surv.*, vol. 55, no. 3, pp. 1–36, Feb. 2022.

[5] Z. Sun, H. Yang, K. Liu, Z. Yin, Z. Li, and W. Xu, "Recent advances in LoRa: A comprehensive survey," *ACM Trans. Sens. Netw.*, vol. 18, no. 4, pp. 1–44, Nov. 2022.

[6] P. Maurya, A. Hazra, P. Kumari, T. B. Sørensen, and S. K. Das, "A comprehensive survey of data-driven solutions for LoRaWAN: Challenges and future directions," *ACM Trans. Internet Things*, vol. 6, no. 1, pp. 1–36, 2025.

[7] The Things Network - LoRaWAN Frequency Plans by Country. [Online]. Available: https://www.thethingsnetwork.org/docs/lorawan/frequencies-by-country/.

[8] G. H. Derévianckine, A. Guitton, O. Iova, B. Ning, and F. Valois, "Opportunities and challenges of LoRa 2.4 GHz," *IEEE Commun. Mag.*, vol. 61, no. 10, pp. 164–170, Oct. 2023.

[9] R. Falanji, M. Heusse, and A. Duda, "Range and capacity of LoRa 2.4 GHz," in *Proc. of EAI MobiQuitous*, 2022.

[10] Semtech Wireless RF - LoRa 2.4GHz. [Online]. Available: https://www.semtech.com/products/wireless-rf/lora-24ghz.

[11] Semtech, "Physical layer proposal: 2.4GHz ISM band," *Technical Paper*, Mar. 2021.

[12] Semtech, "Semtech and Sonova create new hearing aid solutions for better IoT connectivity," Mar. 2019. [Online]. Available: https://www.semtech.com/company/press/semtech-and-sonova-create-new-hearing-aid-solutions-for-better-iot-connectivity.

[13] J. Aufranc (CNXSOFT), "LoRa 2.4GHz is now supported by The Things Network," Feb. 2021. [Online]. Available: https://www.cnx-software.com/2021/02/03/lora-2-4ghz-is-now-supported-by-the-things-network/.

[14] M. Lozada, "Semtech showcases next-gen LoRa technology at IoT Solutions World Congress 2025," May 2025. [Online]. Available: https://www.businesswire.com/news/home/20250508714723/en/Semtech-Showcases-Next-Gen-LoRa-Technology-at-IoT-Solutions-World-Congress-2025.

[15] Semtech SX1280 2.4GHz Wireless RF Transceiver. [Online]. Available: https://www.semtech.com/products/wireless-rf/lora-24ghz/sx1280.

[16] Semtech SX1281 2.4GHz Wireless RF Transceiver. [Online]. Available: https://www.semtech.com/products/wireless-rf/lora-24ghz/sx1281.

[17] Semtech LR1120 for Multi-Band Worldwide Asset Management. [Online]. Available: https://www.semtech.com/products/wireless-rf/lora-edge/lr1120.

[18] Semtech LR2021 Fourth-generation LoRa IP. [Online]. Available: https://www.semtech.com/products/wireless-rf/lora-plus/lr2021.

[19] Semtech, "Semtech LoRa® Gen 4 addresses low-power wireless range and speed limitations," Sept. 2025. [Online]. Available: https://www.semtech.com/company/press/semtech-lora-gen-4-addresses-low-power-wireless-range-and-speed-limitations.

[20] T. Wendt, F. Volk, and E. Mackensen, "A benchmark survey of long range (LoRaTM) spread-spectrum-communication at 2.45 GHz for safety applications," in *Proc. of IEEE WAMICON*, 2015.

[21] Semtech, "Application note: Wi-Fi immunity of LoRa at 2.4 GHz," *White Paper*, June 2017.

[22] L. Polak and J. Milos, "Performance analysis of LoRa in the 2.4 GHz ISM band: Coexistence issues with Wi-Fi," *Telecommun. Syst.*, vol. 74, pp. 299–309, Mar. 2020.

[23] C. F. Hernández, G. Hochet Derévianckine, A. Guitton, O. Iova, and F. Valois, "Indoor performance evaluation of LoRa® 2.4 GHz," in *Proc. of IEEE WCNC*, 2023.

[24] G. Hochet Derevianckine, A. Guitton, O. Iova, B. Ning, and F. Valois, "Hate or love in the 2.4 GHz ISM band: The story of LoRa™ and IEEE 802.11g," *ACM Trans. Internet Things*, to be published.

[25] R. Saduakhas, Y. Kadirzhanov, and D. Zorbas, "LoRa and WiFi at 2.4 GHz: A cross-technology interference evaluation," in *Proc. of IEEE CSCN*, 2025.

[26] K. Sun, Z. Yin, W. Chen, S. Wang, Z. Zhang, and T. He, "Partial symbol recovery for interference resilience in low-power wide area networks," in *Proc. of IEEE ICNP*, 2021.

[27] C. Shao, K. Tsukamoto, Y.-W. Ma, Y. Hua, and X. Wang, "CoWiL: Combating cross-technology interference in LoRaWAN," in *Proc. of ICCCN*, 2024.

[28] G. Chen, W. Dong, and J. Lv, "LoFi: Enabling 2.4GHz LoRa and WiFi coexistence by detecting extremely weak signals," in *Proc. of IEEE INFOCOM*, 2021.

[29] C. Shao, T. Xu, and Q. Du, "Toward collision-free LoRaWAN communication under the coexistence with Wi-Fi networks," in *Proc. of CANDAR*, 2024.

[30] A. Gamage, J. Liando, C. Gu, R. Tan, M. Li, and O. Seller, "LMAC: Efficient carrier-sense multiple access for LoRa," *ACM Trans. Sen. Netw.*, vol. 19, no. 2, pp. 1–27, Feb. 2023.

[31] C. Shao, O. Muta, K. Tsukamoto, W. Lee, X. Wang, M. Nkomo, and K. R. Dandekar, "Toward improved energy fairness in CSMA-based LoRaWAN," *IEEE/ACM Trans. Netw.*, vol. 32, no. 5, pp. 4382–4397, Oct. 2024.

[32] B. Abu-Elkheir and M. A. Abdelghany, "Q-learning based adaptive channel selection for LoRaWAN networks," in *Proc. of ACM/IEEE IoTDI*, 2020.

[33] C. Goursaud and F. N. Koukoumidis, "Learning-based adaptive MAC for LoRa networks," in *Proc. of IEEE ICC*, 2018.

[34] M. Selim and K. A. Harras, "Deep reinforcement learning for joint SF and power optimization in LoRaWAN," *IEEE Trans. Green Commun. Netw.*, vol. 6, no. 3, pp. 1842–1855, 2022.

[35] The Things Network - LoRaWAN Device Classes. [Online]. Available: https://www.thethingsnetwork.org/docs/lorawan/classes/.

[36] T. M. Schmidl and D. C. Cox, "Robust frequency and timing synchronization for OFDM," *IEEE Trans. Commun.*, vol. 45, no. 12, pp. 1613–1621, Dec. 1997.

[37] LoRa Calculator. [Online]. Available: https://www.semtech.com/design-support/lora-calculator.

[38] Semtech LR1120DVK1TCKS Development Kit. [Online]. Available: https://www.semtech.com/products/wireless-rf/lora-edge/lr1120dvk1tcks.

[39] Great Scott Gadgets HackRF One. [Online]. Available: https://greatscottgadgets.com/hackrf/one/.

[40] B. Bloessl, M. Segata, C. Sommer, and F. Dressler, "Performance assessment of IEEE 802.11p with an open source SDR-based prototype," *IEEE Trans. Mob. Comput.*, vol. 17, no. 5, pp. 1162–1175, May 2018.

Chenglong Shao (Senior Member) is an Associate Professor in the Department of Computer Science and Networks at Kyushu Institute of Technology, Japan, a position he has held since 2026. He received his B.S. in Information and Communications Engineering from Xi'an Jiaotong University, China, in 2010, and his Ph.D. in Computer Science and Engineering from Korea University, South Korea, in 2019. He previously served as a Research Professor at Korea University in 2019, a JSPS International Research Fellow at Kyushu University from 2021 to 2023, and a Visiting Scholar at the University of California, Riverside, in 2024. His research interests span wireless networking, IoT-enabled mobile computing, wireless security, and networked embedded systems. He has authored over 30 first-author papers in leading international journals and conferences, including IEEE Transactions on Mobile Computing and IEEE/ACM Transactions on Networking. His work has been recognized with more than 10 international awards, such as the CANDAR 2022 Best Paper Award, the 25th Samsung Humantech Paper Award – Bronze Prize in 2019, and the 1st Place Transactions Award of 2018 Annual IEEE Consumer Electronics Society Chester W. Sall Memorial Awards in 2018. He serves as an editor for Computers, Materials & Continua (CMC) and the Journal of Information and Intelligence. He is an active member of the research community, contributing as a TPC member at over 20 international conferences and as a reviewer for more than 40 academic journals.

Tongyang Xu (Member) received the B.Eng. degree in Electronic Information Engineering from Xidian University, Xi’an, China, in 2011, the M.Sc. degree (Distinction) in Telecommunications, and the Ph.D. degree (Lombardi Prize) in Electronic and Electrical Engineering from University College London (UCL), London, U.K., in 2012 and 2017, respectively. He is currently an Assistant Professor in the Department of Electronic and Electrical Engineering at UCL. Dr. Xu has authored and co-authored over 100 SCI- and EI-indexed papers as first or corresponding author, along with two invited book chapters, in the areas of 6G signal waveform design, 5G/6G wireless and optical communications, machine learning, IoT, secure communications, integrated sensing and communications (ISAC), MIMO beamforming and transmission, software-defined radio (SDR), FPGA, and real-time testbed prototyping. With over 13 years of experience in ‘non-orthogonal signal’ design, Dr. Xu has developed more than 22 pre-commercial hardware prototyping platforms for industry partners. He has served as Principal Investigator (PI) and Co-Investigator (Co-I) on multiple projects funded by the Engineering and Physical Sciences Research Council (EPSRC) and various industrial projects, with total funding over £1m. Dr. Xu served as TPC Chair for IEEE ICT 2024, Publicity Chair and the Special Session Track chair for IEEE PIMRC 2020. He is a Fellow of the Higher Education Academy (HEA) and the member of EPSRC expert panels. He was a recipient of the Best Paper Award in IEEE ICT-2025 and the Organizing Committee Award in IEEE ICT-2024. He was the recipient of the Lombardi Prize and the National Instrument (NI) academic award. He is currently the Associate Editor for IEEE Wireless Communications Letters and the Associate Editor for IEEE Transactions on Mobile Computing.

Xianpeng Wang (Member) received the M.S. and Ph.D. degrees from the College of Automation, Harbin Engineering University, Harbin, China, in 2012 and 2015, respectively. He was a full-time Research Fellow with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, from 2015 to 2016. He is currently a Professor with the School of Information and Communication Engineering, Hainan University, Haikou, China. He is the author of more than 100 papers published in related journals and international conference proceedings. He was a reviewer of more than 30 journals. His major research interests include communication systems, array signal processing, radar signal processing, and compressed sensing and its applications.