IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 11 December 2023, accepted 25 December 2023, date of publication 29 December 2023,
date of current version 8 January 2024.

Digital Object Identifier 10.1109/ACCESS.2023.3348416

RESEARCH ARTICLE

Enhancing LoRaWAN Security: An Advanced AES-Based Cryptographic Approach

SAMIRA ABBOUD[1] **AND NABIL ABDOUN**[2]
[1]École Supérieure d'Électronique de l'Ouest (ESEO), Angers, 49107 Angers, France
[2]Department of Liberal Education, School of Arts and Sciences, Lebanese American University (LAU), Beirut 1102-2801, Lebanon

Corresponding author: Nabil Abdoun (nabil.abdoun@lau.edu.lb)

ABSTRACT The unique set of LoRaWAN design prerequisites, which include low power consumption, cost-effectiveness, and high scalability, requires its security protocols to be equally robust and enduring, especially since devices are often deployed for extended durations in the field. This research paper elucidates a novel cryptographic method for LoRaWAN, hinged on the Advanced Encryption Standard (AES) employing a 256-bit key. The efficacy and efficiency of the proposed cryptographic solution are analyzed through a comprehensive performance evaluation. Key performance indicators include the security metric, network throughput, and energy utilization of end-devices. It was observed that augmenting the key size from 128 to 256 bits notably bolsters the resilience of LoRaWAN against various cyber attacks. The results also indicate a marginal disparity between the proposed AES256-based method and the existing AES128-based method with regards to network throughput and energy consumption. However, the enhanced security provided by the AES256 standard underscores its potential as a viable cryptographic method for LoRaWAN, providing a favorable balance between improved security and operational performance.

INDEX TERMS LoRa, LoRaWAN, cryptography, AES, throughput, energy consumption.

I. INTRODUCTION

LoRaWAN (Long Range Wide Area Network) [1] is a low-speed communication protocol in Low Power Wide Area Network (LPWAN) using Long Range (LoRa) modulation technology developed by Semtech [2]. It is one of the choices made in the development of Internet of Things (IoT) networks [3]. The applications for LoRaWAN are broad. They include trucking and logistics, smart city and parking, agriculture and farming, smart construction, localization, monitoring remote objects like garbage, animals, etc. [4].

LoRa serves as the physical layer in LPWAN, facilitating long-distance transmissions of 3 to 8 km in urban settings and 15 to 20 km in rural areas, while maintaining low power consumption that can extend battery life up to 20 years, depending on usage. Conversely, LoRaWAN is a Media Access Control (MAC) protocol developed by the LoRa Alliance, as detailed in [5]. It builds upon LoRa technology to enable communication between end-devices and a network server via gateways.

This paper introduces a novel approach by comparing the performance of two AES encryption standards, specifically cipher-text with padding under AES128 and AES256. It focuses on several key areas: the energy consumption of end-devices, security metrics, and network throughput. Additionally, it examines the rate of data expansion and how the inclusion of padding in cipher-text under both AES128 and AES256 affects transmission time. Furthermore, the paper delves into the balance between security and performance within LoRaWAN networks, offering valuable insights into achieving sustainable security for long-term IoT applications [6].

Another novelty of this paper is that it includes an analysis of the AES256 encryption standard, which has not been extensively studied in the context of LoRaWAN. This is significant because AES256 is a more secure encryption standard than AES128 and is used in many other security applications. By comparing the performance of both

The associate editor coordinating the review of this manuscript and approving it for publication was Shuangqing Wei.

encryption standards, the paper provides valuable insights into the trade-offs between security and performance in LoRaWAN and highlights the potential benefits of using more secure encryption standards.

This paper is organized into six distinct sections. The Background and Motivations section sets the context and the driving factors behind the research. The Preliminaries section covers the LoRaWAN architecture, operation classes, modulation characteristics, and security aspects, including security features, activation modes, and analyses of encryption using AES and authentication using CMAC. The Literature Survey section provides a review of existing research related to the topic. The Methodology and Implementation of AES256 Variant in LoRaWAN section details the approach and practical application of the AES256 variant within LoRaWAN. The Results and Discussion section focuses on evaluating LoRaWAN's performance in terms of security analysis, data payload size, total transmission time, packet loss rate, network throughput, and energy consumption. It includes comparative analysis and discussion on the trade-offs between security and performance. The Conclusion and Directions for Future Research section summarizes the key findings of the study and discusses potential implications, setting a course for future research endeavors.

II. BACKGROUND AND MOTIVATIONS

Addressing the AES128 algorithm vulnerability is essential to decrease the potential security attacks that may arise against LoRaWAN data. End-devices are equipped with low computing resources and are unable to compute heavy cryptography algorithms. The key length used in the encryption determines the practical feasibility of performing a brute-force attack, with longer keys exponentially more difficult to crack than shorter ones. Brute-force attacks involve systematically checking all possible key combinations until the correct key is found and is one way to attack when it is not possible to take advantage of other weaknesses in an encryption system.

Although LoRaWAN offers security in data transmission where it uses AES128 in the encoding and decoding processes, some studies have reported a security vulnerability in the LoRaWAN technology known as "Bit-flipping", which can be exploited by brute force attack. In [7], the author highlights the vulnerability of the LoRaWAN frame payload to brute-force attacks. Building on this, a benchmark test for a brute-force attack on AES128 using off-the-shelf components was conducted in [8], revealing the susceptibility of AES when integrated with a LoRa module. Furthermore, in [9] authors emphasize the potential risk of a bit-flipping attack, a type of man-in-the-middle attack that actively manipulates data and changes the encrypted text, impacting all versions of LoRaWAN. This attack may occur between servers, worsening the security situation. The authors proposed a countermeasure named "Circular shift to the left" to mitigate this risk. However, this countermeasure, upon analysis, revealed an unintentional generation of a number of session keys, introducing new vulnerabilities. Considering the ongoing concerns, authors in [10] delve into the analysis of the bit-flipping attack risk in LoRaWAN and introduces a countermeasure aimed at preventing its occurrence.

Besides, it is worth mentioning that software implementation of AES128 for LoraWAN introduces data processing and transmission delay, as well as an increase in energy consumption [11]. In order to ensure data confidentiality and privacy, LoRa adopts encryption, however, works should be proposed to design methods/models that will consume minimal power with least computation. The traditional AES128 encryption consumes too much computation and energy for low powered LoRaWAN end-devices.

Moreover and despite of the LoRaWAN security mechanism, devices are susceptible to jamming attack, compromising device and network keys, replay attack and wormhole attack [12]. Therefore, switching to AES256 could be a better solution against cracking LoRaWAN ciphered data and/or weak keys. AES256 is still a safer encryption protocol since the encryption key is twice as long, meaning it is much harder to crack. Additionally, the increased key length gives way to a higher number of processing rounds, which can also lower the chance of successful brute-force attacks. Because of this, AES256 encryption is more resilient, against brute-force attacks, than AES128.

III. PRELIMINARY

This section provides a comprehensive overview of LoRaWAN, detailing its architecture and operational classes, as well as exploring the specifics of data rates and spreading factors that are central to its functionality. Additionally, this section delves into the encryption process for AES, underpinning the security scheme essential for secure LoRaWAN communications. Each of the following subsections is designed to give you a detailed understanding of the various aspects of LoRaWAN.

A. LoRaWAN ARCHITECTURE

In general, a standard LoRaWAN architecture consists of numerous end-devices, gateways, network servers and application servers. End-devices transmit up-link data packets to gateways. A gateway acts as a bridge that collects data from end-devices and relays them to the application servers through the network server as illustrated in Figure 1 [13], [14]. Therefore, a network server is configured to direct messages to appropriate application servers for processing. Servers can send messages back to the end-devices through the gateways in down-link communications.

In the context of the Open Systems Interconnect (OSI) model, LoRa defines the physical layer, whereas LoRaWAN pertains to the data link and network layers [15], [16], establishing a layered approach to network security as shown in Figure 2.

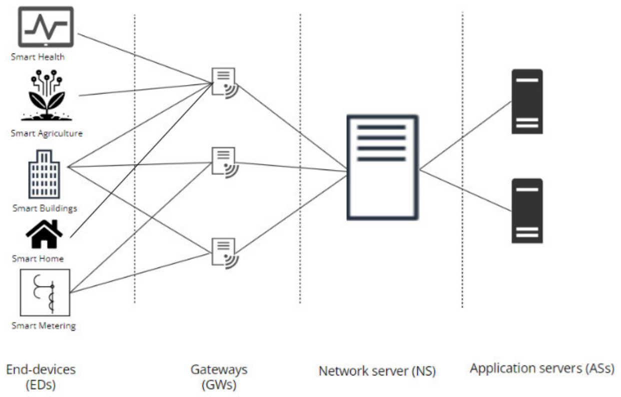

FIGURE 1. Architecture of a LoRaWAN Network.

B. LoRAWAN OPERATION CLASSES

In LoRaWAN, end-devices transmit their data message to one or more gateways, and the gateways forward the message to the Network Server as shown in Figure 1. The end-devices follow one of the three possible classes of operation: Class A, Class B, or Class C to address the diverse application needs [4].

In this article, we adapted the mandatory Class A, where the end-devices allow for bi-directional communications whereby each end-device‘s up-link transmission is followed by two short down-link receive windows called $RX1$ and $RX2$ for the acknowledgments (ACK) [17]. $RX2$ is opened only if no ACK is successfully received during $RX1$. $RX1$ opens after a delay called $RECEIVE\_DELAY1$ (in seconds) and $RX2$ opens exactly 1 second after the first one opens. In other words, the end-device waits one second after $RX1$ closes before opening $RX2$. This means that $RECEIVE\_DELAY2 = RECEIVE\_DELAY1 + 1\ sec$ as shown in Figure 3. As stated previously, if no ACK is received during $RX1$, the end-device listens for possible $ACKs$ during $RX2$. If no ACK is received during $RX2$, then the up-link packet is considered lost and the end-device transmits it again. The maximum number of re-transmissions in LoRaWAN is set to 8 attempts by default [18].

Class B mode allows end-devices to receive downlink communications at predetermined times, providing predictable and limited delays. Conversely, Class C mode keeps the end-devices' receive windows open at all times, except during their own transmission periods, allowing for constant communication. The choice between Class A, Class B and Class C operation has implications for the network's data rates and spreading factors, which we will explore in the next subsection.

C. LoRA MODULATION CHARACTERISTICS

The data rates in Europe for LoRaWAN are determined by the Data Rate (DR) parameter, which represents the processing of bits per unit of time and ranges from 0.3 kbps to 50 kbps. Within this range, DR0 to DR5 utilize a channel bandwidth of 125 kHz, while DR6 uses a wider bandwidth of 250 kHz [19].

The Spreading Factor (SF) indicates how quickly the signal frequency changes across the channel's bandwidth. For DR0, SF is set to 12, and for each subsequent increase in DR until DR5 (inclusive), the SF decreases by one [20]. There is a noticeable relationship between the spreading factor and data rate, whereby higher spreading factors lead to lower data rates. Table 1 [21] shows the six different spreading factors that can be used on a 125 KHz channel. It shows the maximum payload size, the signal to noise ratio (SNR) limit, the time-on-air (ToA), values for the maximum payload as well as the equivalent bit rate for each of the six spreading factors.

Opting for a slower data transmission rate enhances the signal's reception and distinguishability from background noise. However, this also results in a longer transmission time, causing greater device utilization and higher power consumption. Conversely, higher data rates correspond to lower spreading factors, but this increases the likelihood of packet loss. Hence, it is crucial to strike a balance and determine the optimal spreading factor parameter that aligns with specific requirements. While lower spreading factors contribute to a more efficient network, their universal use across all scenarios may not be practical or feasible.

Besides, in LoRaWAN wireless communications, a receiver needs a good SNR to separate the original signal from the modulated carrier. The SNR is the ratio of the received signal power to the noise level. It is commonly used to determine the quality of the received signal. Typical LoRa SNR values are between $-20\ dB$ and $+10\ dB$. A value closer to $+10\ dB$ means that the received signal is less corrupted. LoRa can actually demodulate signals that are $-7.5\ dB$ to $-20\ dB$ below the noise floor.

D. LoRaWAN SECURITY

LoRaWAN provides long-range wireless connectivity for IoT devices. Due to its low-power and long-range capabilities, LoRaWAN has gained significant traction in various industries, including agriculture, healthcare, and smart cities. To ensure secure communication between LoRaWAN devices and gateways, cryptographic methods are employed.

1) GENERAL LoRaWAN SECURITY FEATURES

LoRaWAN is designed with a strong focus on security, adopting sophisticated cryptographic mechanisms to protect the data transmission between end-devices and the network. At the core of its security architecture are two primary keys provided to each end-device: the network layer key $NwkKey$ and the application layer key $AppKey$, together termed as root keys [22]. These keys facilitate the usage of the Advanced Encryption Standard (AES) algorithm for robust data encryption and authentication at both the network and application layers [23].

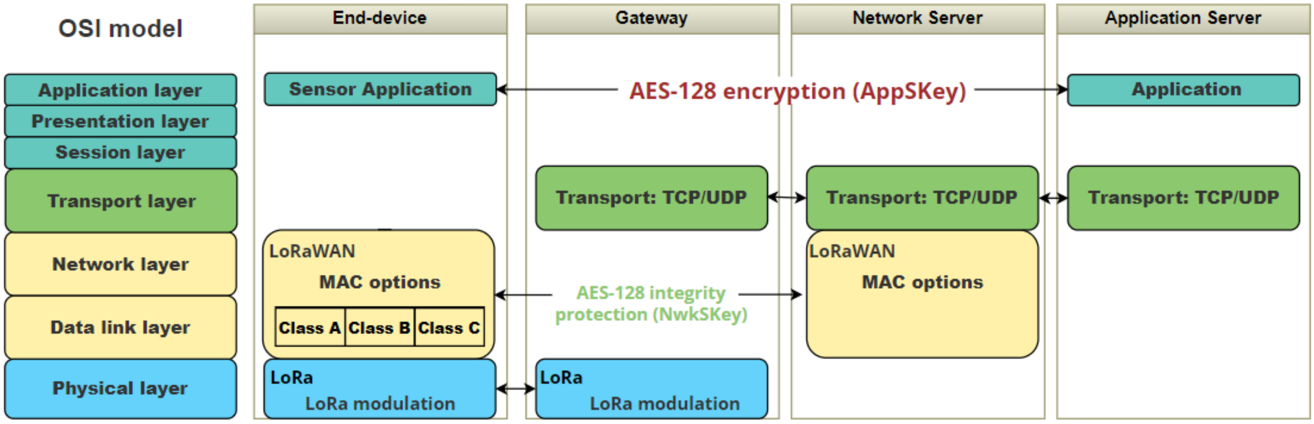

FIGURE 2. Comparison of LoRaWAN with the OSI model.

TABLE 1. LoRa modulation characteristics for EU863-870 band on a 125 KHz channel.

Data Rate (DR)	Spreading Factor (SF)	Max payload [bytes]	Signal to Noise Ratio (SNR) limit [dB]	Time-on-air [ms]	Bitrate [bps]
5	7	230	-7.5	56	5470
4	8	230	-10	103	3125
3	9	123	-12.5	205	1760
2	10	59	-15	371	980
1	11	59	-17.5	741	440
0	12	59	-20	1483	250

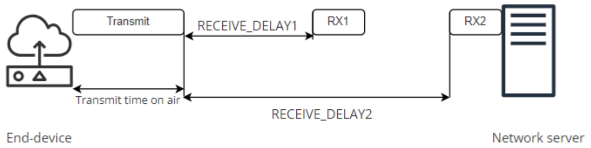

FIGURE 3. Transmission and reception slot timing for Class-A end-device in LoRaWAN.

Secure communication is further reinforced by generating two session-specific keys from the root keys: the Network Session Key *NwkSKey* for securing the exchange between end-devices and the network server, and the Application Session Key *AppSKey* for encrypting and decrypting the payloads.

Activation of an end-device is imperative for network participation, ensuring the device is registered with a unique 4-byte end-device address *DevAddr* and the necessary session keys. Non-activated devices are unable to send data frames that the network server will acknowledge [24].

The security protocol in LoRaWAN operates on two principal layers. Payload encryption is conducted using AES Counter Mode (*AES-CTR*) with the 128-bit *AppSKey*, while the integrity of the messages is upheld through a Message Integrity Code *MIC*, computed using AES Cipher-based Message Authentication Code (*AES-CMAC*) with the 128-bit *NwkSKey*. A frame counter provides defense against replay attacks, and the *MIC* guards against tampering. This dual-layer protection ensures the confidentiality, integrity of data within the network, and the authenticity of message received network and application servers from end-devices.

Encryption of the frame payload *FRMPayload* is executed by preparing a sequence of 128-bit blocks A_i for each message, with $i = 1, \ldots, k$ indexing the blocks and k representing the total number of blocks needed, which is the ceiling of the payload length divided by 16: $k = ceil[length(FRMPayload)/16]$. Each A_i block is composed of various elements including the direction of the data *Dir* (with 0 indicating uplink and 1 indicating downlink), the device address *DevAddr*, and the corresponding counter *ctr* (*FCntUp* for uplink or *FCntDown* for downlink), along with the block index i [25]. These blocks are then individually encrypted to form a corresponding encrypted blocks S_i, $i = 1, \ldots, k$. Then calculating a stream of keys (a sequence S of blocks S_i) by encryption the sequence of blocks A_i. The *FRMPayload* is then encrypted, to produce *EncFRMPayload*, by xoring S with the *FRMPayload* as presented in Algorithm 1.

Following the encryption of the frame payload, an integrity check is performed by calculating the 4-byte *MIC* for messages transmitted within the LoRaWAN network using the AES128-CMAC mode as presented in Algorithm 2.

Algorithm 1 AES128-CTR Algorithm for Encrypting LoRaWAN Frame Payload Using *AppSKey*

```
Input: $FRMPayload, AppSKey, keySize$
Output: $EncFRMPayload$
    $Initialisation: k = ceil[length(FRMPayload)/16]$
                     $keySize = 128$
  Function AES_CTR($FRMPayload, AppSKey, keySize, k$):
    for $i = 1$ to $k$ do
        $Ai = 0 \times 01 \parallel 0 \times 00 \parallel 0 \times 00 \parallel 0 \times 00 \parallel 0 \times 00 \parallel \mathrm{Dir} \parallel \mathrm{DevAddr} \parallel \mathrm{ctr} \parallel 0 \times 00 \parallel \mathrm{i}$
        $Si = AES_{CTR}(AppSKey, Ai)$
    end
    $S = [S_1][S_2]\ldots[S_k]$
    $EncFRMPayload = S \oplus FRMPayload$
    return $EncFRMPayload$
End Function
```

Algorithm 2 AES128-CMAC Algorithm to Generate *MIC* of LoRaWAN Frame Payload Using *NwkSKey*

```
Input: $EncFRMPayload,$
       $LoRaWAN\_Header, NwkSKey, keySize$
Output: $MIC$
    $Initialisation: keySize = 128$
  Function AES_CMAC($EncFRMPayload, NwkSKey, keySize$):
    $MIC = AES_{CMAC}(NwkSKey, LoRaWAN\_Header$
              $|| EncFRMPayload)$
    return $MIC$
End Function
```

After calculating the *MIC*, the LoRaWAN frame is constructed according to Equation 1 as follows:

$$LoRaWANFrame = LoRaWAN\_Header \, || \, EncFRMPayload \, || \, MIC \tag{1}$$

When considering AES variants, AES128, AES192, and AES256 are differentiated by their key sizes - 128, 192, and 256 bits, respectively - and the number of encryption/decryption rounds they perform as represented in Table 2 [26].

The number of rounds - 10 for AES128, 12 for AES192, and 14 for AES256 - correlates with the increasing complexity and security level provided by each AES variant [27]. These rounds include several processing steps that involve substituting bytes, shifting rows, mixing columns, and XORing data blocks with round keys.

In summary, LoRaWAN's employment of AES128 with CMAC and CTR modes establishes a robust, secure communication framework that strikes a balance between security imperatives and the operational efficiency of network-connected devices. However, it is important to note that this system is still susceptible to various types of attacks, necessitating ongoing vigilance and enhancements in security measures to safeguard against potential vulnerabilities.

TABLE 2. Parameters of the three AES variants.

Algorithm	Key length [bits]	Number of rounds	Block size [bits]
AES128	128	10	128
AES192	192	12	128
AES256	256	14	128

2) LoRaWAN ACTIVATION MODES

LoRaWAN supports two modes of activating a new end-device when it is added to a LoRa network [28]:

1) Activation By Personalization (ABP): in this activation mode, an end-device is pre-provisioned with the two essential session keys - *NwkSKey* for network services and *AppSKey* for application services - as well as the device address *DevAddr*. These keys, which are typically embedded into the device during the manufacturing process, are used to create a key-stream for the encryption of data. Utilizing ABP means that the end-device is configured with these session keys from the outset, allowing it to skip the join procedure and enabling immediate communication with the network.
2) Over-The-Air Activation (OTAA): in this activation mode, end-devices must first go through an activation process known as a "join procedure" to connect with the network server before they can start exchanging data. To initiate this process, each end-device must be pre-configured with three unique credentials: a globally unique end-device identifier *DevEUI*, an application identifier *AppEUI*, and a unique 128-bit AES key *AppKey*. When an end-device attempts to join the network using OTAA, the *AppKey* is employed to generate the two session keys, *NwkSKey* and *AppSKey*, which are then used to secure network communications and application data, respectively. The properties of these session keys are detailed in Table 3 as per the citation from Oniga [29].
   Upon activation, the node sends a "join request" to the LoRaWAN server through a gateway. Each request includes a *DevNonce*, a unique 16-bit counter value that starts at 0 and increments with each join request. This ensures the authenticity of each connection attempt. Following a successful request, the Network Server responds with an encrypted "join accept" message, which not only secures the connection but also verifies the end-device's identity. Indeed, the end-device opens $RX1$ after a delay of

TABLE 3. Session Keys in LoRaWAN.

Properties	Application Session Key ($AppSKey$)	Network Session Key ($NwkSKey$)
Purpose of Key	Encrypts and decrypts data message payloads between Application Server and end-device	Calculates and verifies MIC between Network Server and end-device
Key Application Scope	End-device, Application Server	End-device, Network Server
Key Distribution Method	Generated via OTAA; Pre-set for ABP	Generated via OTAA; Pre-set for ABP

TABLE 4. Comparison of LoRaWAN Activation Modes: ABP vs. OTAA.

Properties	Activation By Personalization (ABP)	Over-The-Air Activation (OTAA)
Session Keys	End-devices are pre-provisioned with static session keys for their entire operational lifetime	Dynamically generates and periodically renews session keys for end-devices
Network Connection	End-devices are permanently associated with a specific network	End-devices have the flexibility to switch between networks dynamically
Join Procedure	No join procedure required	Join procedure mandatory
Security Level	Basic security due to static keys	Enhanced security through dynamic key generation
Configuration Complexity	Relatively simple to configure	More complex to configure

*JOIN_ACCEPT_DELAY*1 (default value is 5*s* for the EU863-870MHz band), in order to listen to the join accept packet. If the join-accept is not received during *RX*1, a second receive window RX2 is opened after a *JOIN_ACCEPT_DELAY*2 from the end of the join-request transmission (default value is 6*s* for the EU863-870 MHz band) [30].

The OTAA mode is considered a more secure method for activating end-devices within a network and is preferable for applications that require robust security measures. This mode mandates the safeguarding of root keys within the end-device, which is critical since unauthorized access to these keys could allow an attacker to mimic a legitimate device and generate corresponding session keys [31]. Conversely, the ABP mode is simpler to deploy as it does not require a join procedure; however, this simplicity comes at the expense of security. In ABP mode, end-devices retain the same session keys for their entire operational lifespan, making the method less secure in comparison to OTAA [32], [33]. The key distinctions between OTAA and ABP activation modes are outlined in Table 4, which provides a summary of their differences.

IV. LITERATURE SURVEY

Organizations such as those in large-scale industrial or agricultural sectors, utility companies, and local governments frequently adopt LoRaWAN for its ability to support low-powered devices spread across vast areas. Despite the wide distribution, there might be a tendency within these enterprises to deprioritize full security measures for the devices and the network as a whole. Nevertheless, compromised LoRaWAN devices can become instruments in attacks leading to operational disruptions, data breaches, or the dissemination of inaccurate information. For a more detailed understanding, Table 5 compiles various research papers that have explored and analyzed the array of possible physical and network attacks targeting LoRaWAN, highlighting the importance of robust security strategies in these environments.

These attacks on LoRaWAN networks represent a significant threat, as they can exploit vulnerabilities to disrupt service, intercept sensitive data, or manipulate transmitted information. They range from passive eavesdropping to active interference, such as jamming signals or replaying messages, and can compromise not just individual devices but the integrity of the entire network. It is essential for organizations using LoRaWAN to understand these risks and implement comprehensive security measures to protect against potential breaches. This not only involves securing the devices themselves but also ensuring that communication protocols and network infrastructure are resilient to such malicious activities. The studies listed in Table 5 serve as a critical resource, shedding light on the methods attackers may use and the best practices for defense, thereby helping to maintain the reliability and trustworthiness of LoRaWAN deployments.

Many previous works have studied LoRaWAN security and proposed improvements to its specification. Some of these improvements have been included in LoRaWAN v1.1. Here, we review some works on the previous version of LoRaWAN (v1.0). This anteriority work remains useful to learn about the state of progress of the specification and to have an overview of previous attacks and proposals for improvements.

TABLE 5. Overview of Reviewed Network-Layer and Physical-Layer Attacks Against LoRaWAN.

Paper	Network layer attacks	Physical layer attacks
Aras et al. [16]	• Replay and wormhole attacks	• Jamming attack • Hijacking of EDs
JungWoon et al. [34]	• Bit flipping attack	
Yang [35]	• Replay attack for ABP activated end-devices • Eavesdropping • Bit flipping attack • ACK spoofing • Attacks toward LoRaWAN Class B	
Yang et al. [36]	• Replay attack for ABP activated nodes • Eavesdropping • Bit flipping attack • Plain-text recovery • Malicious message modification • Falsification of delivery reports	• Finding or spoofing the location of a LoRa gateway • Battery exhaustion attack
Gresak et al. [37]	• ABP Replay attack	
Van Es et al. [38]		• In the context of DoS attacks: – Beaconing vulnerability – Down-link routing vulnerability – Join Accept replay vulnerability
Ingham et al. [11]	• AES128 Encryption and protocol vulnerability • Replay attack • Bit flipping attack • Eavesdropping attack	• LoRaWAN keys management • DoS attacks via signal jamming and replay attacks
De Moraes et al. [39]	• A lack of end-to-end integrity protection • Join and rejoin request messages are not encrypted • Join accept is not linked to join request • Counter mode encryption executes only XOR operation • Beacons for Class B are not encrypted	• LoRaWAN does not feature over-the-air device firmware update • The message integrity code has a short length • AppNonce is not registered by end-device • Key provisioning, storage and usage is not specified
Prasad et al. [40]		• DoS via jamming attacks
Ruotsalainen et al. [41]		• Key Extraction Attacks • Sniffing attacks • Jamming attacks • Wormhole attacks • Covert Channels • Energy Attacks
Donmez et al. [42]	• Replay attack for the network join procedure	
Loubet et al. [43]	• Native Security Features • Re-use of nonce values • Frame counter management • Lack of end-to-end integrity protection • Packet and payload vulnerabilities • Credentials Misconfiguration • Bit flipping attack • Acknowledgement spoofing • Eavesdropping (sniffing, relay attack or man-in-the middle).	• Physical access to devices • Radio jamming

TABLE 5. ***(Continued.)*** **Overview of Reviewed Network-Layer and Physical-Layer Attacks Against LoRaWAN.**

Paper	Network layer attacks	Physical layer attacks
Noura et al. [44]	• Man-in-the-middle attack • Security parameter extraction and device cloning or firmware replacement • Replay attack • Down-link routing attack • Join-accept replay attack • Beacon synchronization attack • ACK spoofing attack • Bit flipping attack • Eavesdropping	• Destroy, remove, or steal ED • Jamming attack
Qadir et al. [45]		• ED physical attacks (extraction of the device root keys) • Weak key generation • Weak key updating • Compromised server
Torres et al. [46]	• Bit flipping attack • Jamming attack • Replay attack • Wormhole attack • Denial of Service attack	• Theft of devices • Social Engineering • Sleep Deprivation attack • Malicious Node Injection • Environment
Eldefrawy et al. [47]	• Cryptographic primitives • Key preloading	• Infrastructure trust
Sahraoui et al. [9]	• Bit flipping attack	

In 2015, Antipolis and Girard [47] addressed a critical issue in the key management system of the initial LoRaWAN version 1.0. The protocol's design at that time tasked the network server with the generation of both session keys: *NwkSKey* and *AppSKey*. This posed a security risk, as the network server's access to *AppSKey* meant it could potentially decrypt and read any transmitted message. To mitigate this risk, the authors suggested an overhaul of the LoRaWAN network architecture, incorporating a Public Key Infrastructure (PKI) to serve as a trusted third party. This security gap—specifically, the lack of separation between root keys—was subsequently addressed in LoRaWAN version 1.1, which introduced a system where *NwkSKey* and *AppSKey* are derived from separate root keys, thus enhancing the overall security of the network.

Kim and Song [48] introduced a scheme that enhances the security of end-device activation in LoRaWAN by using two distinct keys, aiming to segregate the trust involved in session key management more effectively. This concept of dual keys was later reflected in LoRaWAN version 1.1, which introduced a separate root key (*NwkKey*)) dedicated to generating the (*NwkKey*). The updated protocol ensures that the application and network session keys are independently generated from their respective root keys during the OTAA phase. Moreover, while Kim et al.'s work proposed an advancement over version 1.0 by suggesting the separation of root keys, it's important to note that LoRaWAN version 1.1 had already incorporated this security enhancement.

The *DevNonce* required in LoRaWAN v1.0 is a random number created by end-devices. It is used to circumvent replay attacks during the key generation phase. Zulian [7] showed that with the *DevNonce* generation system of LoRaWAN v1.0, after a certain period of time, the end-device can be unavailable with a certain probability. To get around this problem, the author suggested increasing the size of the *DevNonce* field up to 24-32 bits.

LoRaWAN end-devices must perform a join procedure for participating in the network. Attackers could exploit the join procedure because it has vulnerability in terms of security. Replay attack is a method of exploiting the vulnerability in the join procedure. Hence, Na et al. [49] proposed an attack scenario and a countermeasure against replay attack that may occur in the join request transfer process.

In 2020, Noura et al. [43] found that effective countermeasures are highly needed to enable LoRaWAN's wide adoption in the IoT domain. They reviewed the LoRaWAN architecture, applications, and security threat with risk assessment. In addition, they listed several possible countermeasures to address the existing LoRaWAN vulnerabilities in order to prevent the potential related attacks.

In [29], Oniga et al. performed an analysis of the main aspects of LoRaWAN security and proposed an extended architecture by adding a typical approach based on certificates and transport layer security. Although this solution can be a complementary approach for the development of high-level services, key aspects of management are not taken into account at the LoRaWAN level. The previous related works provide valuable insights into the security issues of LoRaWAN and proposes various solutions and countermeasures to address these issues. However, some of these works are based on the older version of LoRaWAN (v1.0), and their proposed solutions may not be relevant to the latest version (v1.1) of the protocol, which has already addressed some of these vulnerabilities.

In [44], Qadir et al. state that the end-devices residing on the edge of the network represent a primary target for cyber-attackers. Therefore, they present a solution called the Key Generation and Distribution "KGD" mechanism that mitigates cyber-attacks in the light of secure key management. The KGD algorithm is accomplished in three steps. At first, it generates the secret keys with a cryptographically secured deterministic random bit generator method. The generated keys are then exchanged between the ED and join server using the Elliptic-Curve Diffie-Hellman (ECDH) method. Afterwards, a key authentication process named Elliptic Curve Digital Signature Algorithm (ECDSA) is considered to verify if the keys were exchanged with the legitimate parties. Results show that their proposed KGD is secure against cyber-attacks and has authentication, integrity and transmission secrecy.

In [50], Aliyu et al. state that the ever-increasing penetration of IoT applications across various sectors and industries, require better information and communications security for IoT devices. Physical Unclonable Function (PUF) circuits are considered as an inexpensive method for generating unique responses, ideal for key generation and device authentication in high-performance microprocessors. PUFs are extracted from manufacturing variations embedded in the hardware of accessible devices, thereby requiring no additional modification. Static Random Access Memory (SRAM) PUFs are widely used with keys generated from power-on values for authentication. In this context, authors worked on improving the authentication of LoRa devices. They leverage the integration of Carrier Frequency Offsets (CFOs) and SRAM PUF to create a two-step authentication security solution for LoRaWAN called LoRa-PUF. The power-on state value of SRAM chips were analyzed for SRAM PUF properties, and 36000 packets of CFOs of four LoRa device types have been analyzed for LoRa-PUF. Results indicate that LoRa SRAMs serve as reliable challenge-response pair sources for PUFs, and the CFOs of the LoRa device type can be classified during communication with more than 70% accuracy which can be implemented on LoRa microcontrollers with limited resources.

In [51], Povalac et al. monitored and analyzed LoRaWAN traffic in four European cities, making the obtained data and post-processing scripts publicly available. They developed an open source sniffer that can capture all LoRaWAN communications in the EU868 band. They discovered significant issues in current LoRaWAN deployments, including violations of fundamental security principles, such as the use of default and exposed encryption keys, potential violations of spectrum regulations, including cycle violations service issues, and misaligned Class B beacons. This misalignment can make class B unusable because the beacons cannot be validated. Additionally, they enhanced Wireshark's LoRaWAN protocol dissector to accurately decode recorded traffic. They also proposed passive reception of Class B beacons as an alternative time base source for devices operating in LoRaWAN coverage, assuming that the problem of misaligned beacons can be resolved or mitigated in the future.

In [52], Rodic et al. studied privacy leakage of LoRaWAN smart parking communication devices. They state that when a vehicle as a metallic obstacle obscures the LoRaWAN smart parking device, the signal strength will be reduced on the receiver side. Therefore, the variation in the signal strength of LoRaWAN parking systems transmits information about parking space occupancy, allowing the implementation of a passive side-channel attack at large distances. Using supervised machine learning techniques based on Neural Network, the attacker can estimate parking lot occupancy with very high accuracy up to 97%, while Random Forrest approach reaches the accuracy over 98%.

Additionally, some of the proposed solutions in the previous related work, such as employing Public Key Infrastructure, may introduce additional complexities and overheads to the LoRaWAN network. Therefore, a careful trade-off between security and practicality needs to be considered when implementing these solutions. Moreover, while some of the proposed solutions address specific security issues, they may not provide a comprehensive and integrated approach to LoRaWAN security. Therefore, there is a need for a holistic view of LoRaWAN security, considering all aspects of the protocol, from the device to the application layer, and taking into account the unique characteristics and constraints of IoT networks.

The state-of-the-art literature includes review and survey papers with references to vulnerabilities and countermeasures on different communication layers. For instance,few works [43], [53], [54] delivered brief reviews on the relevant physical-layer attacks and mentioned some countermeasures. Nevertheless, none of these works treated these topics comprehensively and they also lacked discussion on wireless physical-layer techniques. Ruotsalainen et al. [40] have presented a consistent review of the relevant physical-layer vulnerabilities and protection topics.

Table 6 compiles key scholarly articles that have examined network layer attacks on LoRaWAN, also outlining possible countermeasures. Although existing literature offers a solid base for grasping the security vulnerabilities inherent in LoRaWAN, there is a need for ongoing research. This future research should aim to establish a holistic security framework

TABLE 6. Review of Papers on Network Layer Security in LoRaWAN.

Paper	Mitigation techniques	Description
Kim et al. [56]	Replay attack prevention scheme	Follow the existing packet structure and deal with exceptional situations such as device reset.
Han et al. [57]	Root key update scheme	High randomness degree
Sanchez-Iborra et al. [58]	Lightweight and authenticated key management	EDHOC update session keys and SCHC for IPv6
Feichtinger et al. [59]	Enhancement to the OTAA join procedure	Hybrid crypto-system to encrypt the OTAA join-request by using the already implemented symmetric crypto-system and the existing $AppKey$
Dönmez et al. [60]	Delegated key management	Master device manages lifetime keys
Xing et al. [61]	Improved secure key management	HD wallet for key management, ECDH for key agreement
Chen et al. [62]	Fast session key generation	High computing efficiency and key randomness
Gunathilake et al. [63]	Lightweight Cryptography (LWC) algorithms	Several block ciphers are compared against AES
Danish et al. [64]	Two-factor authentication mechanism based on block-chain	Integrate the standard authentication of the join procedure with a block-chain-based authentication. A special node, called agent node, is used to mediate the communication between the block-chain and LoRaWAN nodes
Tsai et al. [65]	Session key generation method	Integrating elliptic curve cryptography and AES128
Ribeiro et al. [66]	Secure architecture for key management	Permissioned block-chain using open-source tools and commodity hardware
Naoui et al. [67]	Novel enhanced solution to secure the smart home remote control	Using a rigorous informal security analysis and a formal security verification via Scyther tool
Anantachaisilp et al. [68]	A security scheme based on AES to secure transmitted data in the private LoRaWAN-server via satellite GWs	Develop payload for CubeSat in the low-earth orbit to receive up-link between LoRa module and private LoRaWAN-server on CubeSat to store data and then use S-band transceiver to down-link the data to ground station
Noura et al. [69]	Dynamic key derivation algorithm for ABP EDs	Use of a dynamic key approach, and dynamic network and application keys are produced for each reset operation. The dynamic key derivation approach updates the network and application keys after each reset operation for ABP EDS.
Claverie et al. [70]	—	Presenting an environment based on hardware, software and SDR to study the radio layer of the protocol
Goulart et al. [71]	Application of the CIA triad	Classify lightweight security approaches for AES and ECC
Fan et al. [72]	Efficient authentication scheme for massive EDs in LoRaWAN join procedure	Allow several EDs of the same GW to generate group keys
Mohamed et al. [73]	Novel certificate authentication technique that enhances the cyber security of gateways in LoRaWAN	Considering a public key infrastructure (PKI) solution that considers a two-tier certificate authority (CA) setup, such as a root-CA and intermediate-CA.
Qadir et al. [45]	Lightweight Secure Key Management Scheme	key generation and distribution (KGD) mechanism to securely exchange the root key between the ED and the AS
Aliyu et al. [51]	Two-Step Security Solution	Improving device authentication by creating a two-step authentication security solution called LoRa-PUF while exploiting the integration of Carrier Frequency Offsets (CFOs)
Povalac et al. [52]	Enhancing Wireshark's LoRaWAN dissector to accurately decode recorded traffic Proposing the passive reception of Class-B beacons as an alternative time-base source	Monitoring and analyzing LoRaWAN traffic to reveal security and system challenges by developing an open-source sniffer capable of capturing all LoRaWAN communication within the EU868 band
Rodic et al. [53]	Deep learning algorithms based on neural networks and random forest	Investigating and analyzing variations in signal strength that result from vehicles as a metallic obstacle obscuring smart parking sensors
Czeczot et al. [74]	—	Structure the knowledge in LoRaWAN security, based on previous publications, in order to identify challenges
Richardson [75]	Jamming Detection and Mitigation Using Machine Learning in the Cloud	Using real-time jamming attack implementation. Performing a jamming attack on a LoRaWAN testbed. Implementing a countermeasure via Amazon Web Service
Hayati et al. [76]	Novel secure root key updating scheme that involves periodically changing the root key value based on the CTR_AES DRBG 128 algorithm	The scheme consists of two sequential phases: the initialization process that occurs at the end-device and the root key update process that occurs at the join server
Wei et al. [77]	Proposition of a Directed Acyclic Graph (DAG) based LoRaWAN system	Distributed LoRa gateways and network servers record data transmissions in tangle network to make LoRa data traceable and avoid single point of failure

for LoRaWAN that addresses the nuances of the most recent protocol iteration and the specific security demands of IoT networks. Our present study assesses the implications of adopting AES256 for LoRaWAN security, specifically focusing on the associated energy consumption, transmission delay, and network throughput. This transition to AES256 is implemented within the LoRaWAN protocol, particularly at the data link and network layers, rather than at the LoRa physical layer. Essentially, our research is concentrated on the encryption and decryption processes that occur at the LoRaWAN MAC layer.

V. METHODOLOGY AND IMPLEMENTATION OF THE AES256 VARIANT IN LoRaWAN

In this section, we provide an overview of the parameters and configurations employed in our simulations, setting the stage for a comprehensive evaluation of the AES256 encryption process in LoRaWAN communications. Our simulations involve a network composed of a single gateway ($x = 1$) and varying numbers of end-devices ($n \in \{1, 4, 16, 64, 256\}$), each following a 1% duty cycle. The end-devices employ spreading factors SF7 and SF12, with a bandwidth of 125 KHz and a transmission power of 14 dBm (the default for LoRaWAN end-devices). The data transmission spans 24 hours, with results averaged over ten thousand samples. The RC-SM1276-868 model, a 868MHz LoRa Module based on SX1276 and controllable via an SPI interface, serves as our LoRa module. Its characteristics are detailed in Table 7. Our simulations are conducted using a Python simulator developed in version 3.11.5, adhering to LoRaWAN specification v.1.0.3 [1]. Additionally, we introduce the AES256 encryption process steps, essential for understanding the subsequent analyses:

1) Key Generation: Utilize a 32-byte key (256 bits).
2) Data Organization: Organize the 16 bytes (128 bits) of plain-text into a 4 × 8 block matrix.
3) Transformations: Apply 14 rounds of transformations to the state, incorporating round keys.
4) Cipher-text Retrieval: Retrieve 16 bytes of cipher-text from the block matrix.

Our proposed implementation of AES256, illustrated in Figure 4 and outlined in Algorithm 3, represents our contribution and underscores the novelty of our research approach.

Algorithm 3 AES256 Algorithm for Encrypting LoRaWAN Frame Payload and Generating *MIC* Using *AppSKey* and *NwkSKey* During the OTAA Process

```
Input: $FRMPayload, AppSKey, NwkSKey, keySize$
Output: $EncFRMPayload, MIC$
    Initialisation: $k = ceil[length(FRMPayload)/16]$
                    $keySize = 256$
  $EncFRMPayload=$
      $AES\_CTR(FRMPayload, AppSKey, keySize, k)$
  $MIC=$
      $AES\_CMAC(EncFRMPayload, NwkSKey, keySize)$
```

Algorithm 3 illustrates the encryption of the LoRaWAN frame payload using AES256. The process begins with initialization, where the number of blocks (k) is determined based on the payload length. The payload is then encrypted using the AES-CTR mode with the *AppSKey*, and the *MIC* is generated using the AES-CMAC mode with the *NwkSKey*.

TABLE 7. Characteristics of the SX1276 LoRa Module.

Current	12mA
Frequency	868MHz
Sensibility	-139dBm
RF Power	+19dBm

VI. RESULTS AND DISCUSSION

In this section, we consolidate and present the outcomes of our evaluation, focusing on cipher-text data transmission in LoRaWAN communications using both AES128 and AES256 encryption modes. The findings are systematically organized into distinct subsections for clarity and depth. First, we explore the "Effect of AES256 Encryption on Performance Metrics," analyzing how this encryption standard impacts various performance indicators in the LoRaWAN network. Following this, the "Comparative Analysis" subsection presents a detailed comparison between AES128 and AES256, highlighting their operational differences and similarities. We then delve into the "Discussion of the Trade-offs between Security and Performance," where we critically evaluate the balance between the heightened security of AES256 and its effects on network efficiency. Lastly, the "Limitations" subsection addresses the constraints and potential areas for future research, providing a comprehensive and transparent overview of our study's scope.

A. EFFECT OF AES256 ENCRYPTION ON PERFORMANCE METRICS

In this section, we provide a detailed exploration of various performance metrics to evaluate the efficacy of these two encryption methods in a LoRaWAN communication. These metrics serve as critical indicators, shedding light on the operational implications of integrating our proposed AES256 algorithm in contrast to the traditionally used AES128. By delving into these metrics, we aim to offer comprehensive insights into how AES256 encryption affects data transmission times, throughput, energy consumption and overall network performance.

1) SECURITY ANALYSIS

The most commonly used cryptographic methods for LoRaWAN include Advanced Encryption Standard (AES), Message Integrity Code (MIC), and Nonce. AES is a widely used symmetric key algorithm that provides strong encryption and decryption capabilities. MIC ensures message integrity and detects any tampering or alteration of messages during transmission. Nonce, on the other hand, ensures that the same message cannot be transmitted twice, which prevents replay attacks.

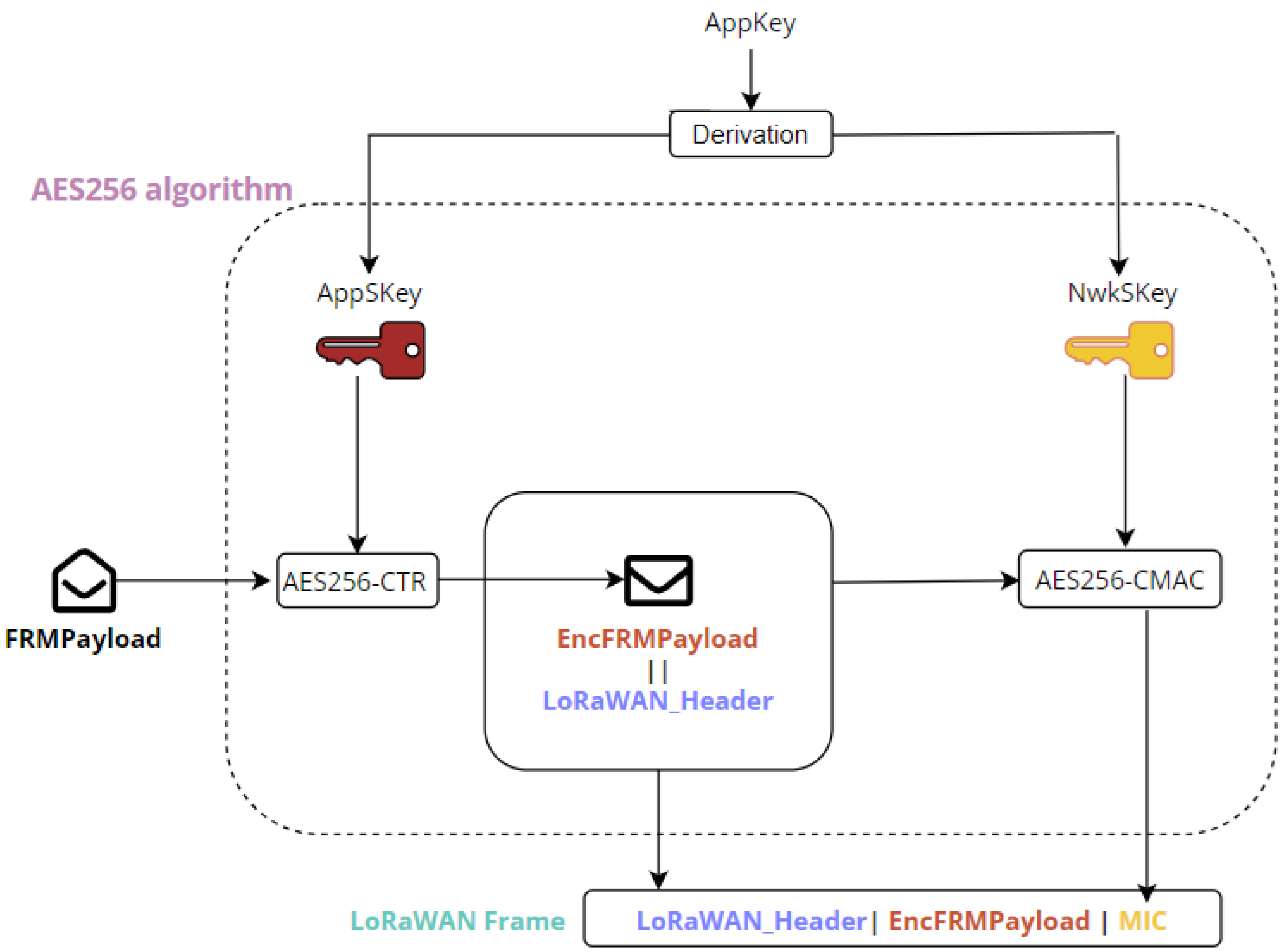

FIGURE 4. AES256 algorithm for encrypting LoRaWAN frame payload and generating *MIC* using *AppSKey* and *NwkSKey* during the OTAA process.

While these cryptographic methods provide a good level of security for LoRaWAN, they may have some limitations in certain scenarios. For example, the use of AES can increase the power consumption of IoT devices, which may not be desirable in low-power applications. Additionally, some attacks may exploit vulnerabilities in the implementation of cryptographic methods, such as key management or random number generation.

To address these limitations, researchers are constantly exploring new cryptographic methods for LoRaWAN. One such method is based on the concept of lightweight cryptography, which aims to provide efficient and secure cryptographic primitives suitable for resource-constrained IoT devices. Another approach is to use post-quantum cryptography, which is resistant to attacks by quantum computers, which may become a threat in the future.

In summary, the current cryptographic methods used in LoRaWAN, such as AES, MIC, and Nonce, provide adequate security for most use cases. However, with the increasing adoption of IoT devices and the growing threat landscape, it is essential to continually evaluate and improve the security measures employed in LoRaWAN.

2) DATA PAYLOAD SIZE

The observed increase in data size when using AES encryption in LoRaWAN communications, as detailed in Tables 8 and 9, can primarily be attributed to the padding necessary to complete the final block. This expansion is a result of the encryption process employing the CBC (Cipher Block Chaining) mode of operation with AES128 and AES256. These encryption standards translate plaintext into ciphertext, often resulting in a payload that is marginally larger than the original plaintext. Theoretically, AES encryption should not significantly expand data size, except for a few bytes of padding added to the end of the last block. This padding is essential for aligning the data with the size of a block, especially when the data length is not an exact multiple of the block size. Therefore, the slight increase in data size observed can be understood as a necessary aspect of ensuring proper data alignment and completeness in the encryption process.

TABLE 8. Cipher-Text Size at Spreading Factor 12 (SF12).

CT AES128	CT AES256
0.022	0.023
0.033	0.035
0.042	0.043
0.054	0.055

TABLE 9. Cipher-Text Size at Spreading Factor 7 (SF7).

CT AES128	CT AES256
0.021	0.0218
0.032	0.033
0.044	0.045
0.060	0.062
0.064	0.064
0.078	0.079
0.082	0.0828
0.100	0.103
0.108	0.118

3) TOTAL TRANSMISSION TIME

In the context of LoRaWAN, the total transmission times for two different activation modes, ABP and OTAA, are calculated considering various factors. For the ABP mode, the total transmission time, denoted as $totalTransTime_{ABP}$, comprises the time on air ToA and the encryption processing time $procEncTime$:

$$totalTransTime_{ABP} = ToA + procEncTime \tag{2}$$

where the $procEncTime$ represents the time it takes for the AES encryption algorithm to convert plaintext to ciphertext.

In contrast, the OTAA mode requires additional steps for activation. The total transmission time in OTAA, denoted as $totalTransTime_{OTAA}$, includes the time for a join request $joinRequestTime$, the time for a join accept $joinAcceptTime$, and the total transmission time of ABP mode $totalTransTime_{ABP}$ calculated in equation 2:

$$\begin{aligned} totalTransTime_{OTAA} &= joinRequestTime \\ &+ joinAcceptTime \\ &+ totalTransTime_{ABP} \end{aligned} \tag{3}$$

For our analysis, we first measured the total transmission time for both AES128 and AES256 encryption modes under Spreading Factor 12 (SF12) and Spreading Factor 7 (SF7). Our findings, as shown in Tables 10 and 11, indicate the average time spent for the transmission of encrypted data under each encryption mode, and the difference in transmission time between them. For SF12, our analysis reveals that the AES256 algorithm generally requires more time than AES128. This is attributed to the higher number of encryption rounds in AES256 and the increased payload size in the CT, as previously detailed in Table 8. Similarly, for SF7, the transmission time for CT under AES256 exceeds that of AES128, with an average increase of approximately 0.57 *ms*.. Therefore, it is evident that using AES256 results in a slight increase in transmission delay compared to AES128, regardless of whether SF12 or SF7 is used.

TABLE 10. Total transmission time (in *ms*) for cipher-text under AES128 and AES256 at SF12.

	with AES128	with AES256	Difference
	1321.10	1322.04	0.94
	1651.25	1653.24	1.99
	1975.40	1976.35	0.95
	2304.60	2306.11	1.51
Average	1813.09	1814.44	1.35

TABLE 11. Total transmission time (in *ms*) for cipher-text under AES128 and AES256 at SF7.

	with AES128	with AES256	Difference
	57.01	58.05	1.04
	72.33	72.93	0.60
	83.21	83.28	0.07
	98.74	98.90	0.16
	113.32	113.69	0.37
	130.55	131.85	1.30
	145.08	145.50	0.42
	160.42	161.26	0.84
	177.08	177.40	0.32
Average	115.30	115.87	0.57

4) PACKET LOSS RATE

Packet loss occurs when one or more packets across networks drop before reaching destination [77]. Packet loss in LoRaWAN can occur due to various factors, including network congestion, interference from other wireless devices, physical obstructions that disrupt signal paths, limited signal range, especially in large or complex environments, hardware malfunctions, and firmware issues in end-devices or gateways. Environmental factors like extreme weather conditions can also impact signal strength and quality, leading to packet loss. Additionally, configuration errors or inadequate network planning, resulting in suboptimal placement of nodes and gateways, can further exacerbate this issue.

It is obvious that the delays caused by the AES encryption and decryption operations can increase the packet loss rate due to the fact that these AES operations force the packets to spend more time in LoRaWAN channels, which can result in a congestion of these channels and possibly packet losses. It is obvious that the number of packets lost or dropped during transmission must be kept low.

The LoRaWAN packet loss rate, measured as a percentage of packets lost with respect to packets sent, is represented by

Equation 4 [78]:

$$packetLossRate = \frac{LP}{RP + LP} * 100 \tag{4}$$

where LP represents the number of lost packets, and RP the number of received packets. Our findings indicate that the average packet loss rate is approximately 2.4% with AES128, and marginally higher at 2.41% when utilizing AES256. This slight and negligible difference demonstrates that transitioning to the AES256 encryption algorithm does not lead to a significant increase in packet loss, implying that both encryption standards exhibit nearly equivalent performance in this aspect.

5) NETWORK THROUGHPUT

The network throughput of data transmission defines how much data can be successfully transmitted in a given time period. From the execution time results, the throughput of the network is calculated to indicate the performance and transmission speed using Equation 5 as follows:

$$Throughput[bits/s] = \frac{Total\ transmitted\ data\ [bits]}{Total\ transmission\ time\ [s]} \tag{5}$$

To enhance Quality of Service (QoS) in packet-switched networks, the primary goal is to maximize throughput while minimizing packet loss and delay, as highlighted in [79]. Higher throughput is indicative of superior network performance. According to the data in Tables 12 and 13, CT under AES256 demonstrates the highest throughput for both SF12 and SF7. Notably, CT without padding can result in lower throughput, attributed to incomplete bytes per block leading to timeouts and consequent transmission delays. However, this issue is mitigated by incorporating padding, which aligns the data size per block and effectively prevents delays and timeouts in transmission, as supported by the findings in [80]. Additionally, within the same security method, using a longer key length has been observed to increase throughput, illustrating a direct correlation between key length and throughput efficiency.

TABLE 12. Throughput [*bits*/*s*] at SF12.

	AES128	AES256	Difference
	1.33	1.39	0.06
	1.55	1.61	0.06
	1.76	1.87	0.11
	1.97	1.96	0.01
Average	1.65	1.71	0.06

6) ENERGY CONSUMPTION

Energy consumption is one of the main metrics to consider in LoRaWAN. The power-intensive operation of sensor end-devices placed in a harsh industrial environment or in inaccessible locations (e.g., in many industrial monitoring use cases) makes regular battery replacement impossible.

TABLE 13. Throughput [*bits*/*s*] at SF7.

	AES128	AES256	Difference
	29.47	30.04	0.57
	35.56	36.16	0.6
	42.41	43.27	0.86
	48.98	50.36	1.38
	45.31	45.31	0
	48.00	48.24	0.24
	45.24	45.53	0.29
	50.00	51.18	1.18
	48.81	53.27	4.46
Average	43.75	44.81	1.06

The energy consumption is mainly from data communication and data processing, including the amount of transmission data, data encoding, etc. Therefore, it is essential to always consider a way to keep the energy consumed as low as possible [81]. In this part, we will present the analysis of the energy consumption per end-device obtained by 10000 simulations, concerning the number of packets frequency.

The energy consumption of LoRaWAN end-devices can be illustrated by classifying the phases in which the device operates, and then the power consumed at each of these phases, as proposed in several publications on sensor networks [82]. In other words, the distribution of the dissipated energy consumption is divided according to the phases the end-device goes through. We have previously seen that the LoRaWAN end-device goes in several phases of operations (join request, join accept, data transmission phase and AES procedure). The total energy consumed EC_{OTAA} by LoRaWAN end-devices is given by Equation 6 [82], [83] as follows:

$$EC_{OTAA}[\mu J] = P * totalTransTime_{OTAA} \tag{6}$$

where P represents the power consumption.

The $totalTransTime_{OTAA}$ is the total transmission time of the different phases of the end-devices (i.e., the join request, the join accept, the data transmission phase (ToA) and the AES procedure as previously shown in Equations 2 and 3).

The study, illustrated in Figures 5 and 6, examines the energy consumption of end-devices in a network, focusing on the comparison between AES128 and AES256 encryption modes under SF7 and SF12 conditions, with energy measured in microjoules (μJ).

The research, involving 1, 4, 16, and 64 end-devices, reveals a 2.12% difference in average energy consumption between AES128 and AES256. A significant increase in energy consumption occurs when the number of devices rises from 64 to 256, showing increases of 4.7% under AES128 and 10.17% under AES256, in comparison to the energy consumption observed without encryption. The study also finds that energy consumption escalates with the frequency of communication, especially under AES256, highlighting its inefficiency in scenarios with frequent transmissions and a large number of devices. This inefficiency is crucial in energy-constrained devices like smart meters, where preserving energy and extending battery life are essential, underscoring the impact of encryption mode, device count, and communication frequency on energy usage. Table 14 presents our summary results obtained for AES128 and AES256 encryption techniques regarding execution time (or latency), network throughput, energy consumption of EDs and security level.

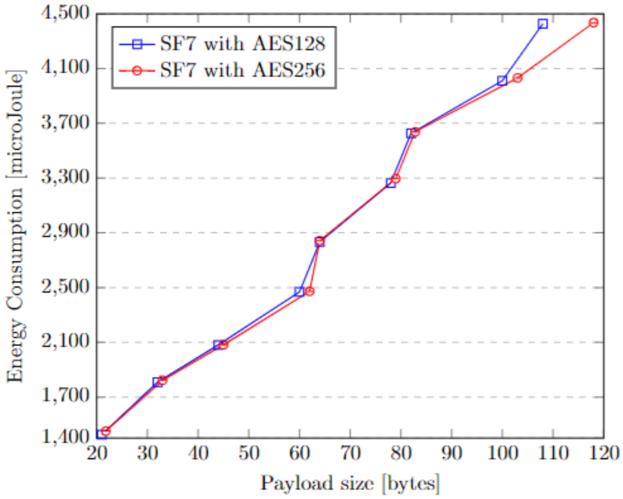

FIGURE 5. Energy Consumption of End-Device in Relation to Payload Size for AES128 and AES256 Encryption Modes Under SF7.

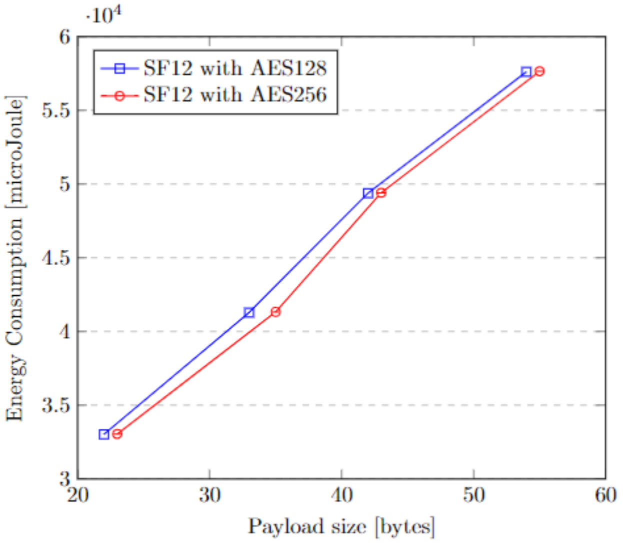

FIGURE 6. Energy Consumption of End-Device in Relation to Payload Size for AES128 and AES256 Encryption Modes Under SF12.

B. COMPARATIVE ANALYSIS

Among works done for enhancing IoT security, Bui et al. [84] presented a low power AES architecture for IoT applications by utilizing simple shift registers and permutation for key/data storage to reduce circuit size and power consumption. Authors also proposed a low-power technique, named clock gating, for power saving on S-box. Trappe et al. [85] pointed out that IoT end-devices have limited energy and memory space, and conventional cryptography is inappropriate for IoT systems. They suggested reusing existing functions, e.g., using physical layer information to check the location of transmitter and receiver.

TABLE 14. Impacts of the two AES variants in LoRaWAN.

Metrics	AES128	AES256
Execution time	Less ✓	More ✗
Throughput	Less ✗	More ✓
Energy consumption	Less ✓	More ✗
Level of security	Considered secure ✓	Much stronger ✓✓

Among previous works done for enhancing LoRaWAN security, studies such as [56] and [63] have evaluated their proposed solutions based on some metrics such as latency and throughout as we did in the current paper.

Han et al. [56] proposed a key management scheme for updating root keys in LoRaWAN 1.1. This scheme consists of a two step Key Derivation Function (KDF). The KDF begins with a randomness extraction step, followed by a key expansion step. The Rabbit stream cipher is used as a pseudo-random number generator for the two steps. Performance results show that the KDF proposed scheme presents a lower execution times when compared to other schemes.

Danish et al. [63] proposed a two-factor authentication mechanism based on block-chain to improve LoRaWAN security of the Join procedure. The additional security layer inserted into the system allows to increase trust on EDs. Their proposed scheme integrates the standard authentication of the join procedure with a block-chain-based authentication. A special node, called agent node, is used to mediate the communication between the block-chain and LoRaWAN nodes (e.g., NSs, gateways). Results obtained from the experiments demonstrate the efficiency of the solution, with respect to latency and throughput. Nonetheless, a considerable amount of delay is introduced in the first joint request, due to the mining procedure executed in the block-chain network.

To our understanding, there is a lack of existing research regarding the energy consumption associated with the implementation of new security schemas in LoRaWAN. Furthermore, the effects of these new security schemas on the energy usage of end-devices have not been extensively studied.

C. DISCUSSION OF THE TRADE-OFFS BETWEEN SECURITY AND PERFORMANCE

In the context of LoRaWAN networks, there is a trade-off between security and performance. On the one hand, strong encryption and authentication mechanisms provide higher security, but on the other hand, they can significantly reduce the network's performance. This is because encryption and decryption operations require additional processing time and energy consumption, which can lead to longer transmission times and shorter battery life for LoRaWAN devices.

Therefore, it is important to balance the level of security with the practical constraints of the LoRaWAN network. For example, some LoRaWAN applications may require high security, such as those involving sensitive data or critical infrastructure, while others may prioritize performance, such as those involving real-time monitoring or tracking.

To address this trade-off, new cryptographic methods for LoRaWAN should aim to provide a reasonable level of security while minimizing the impact on performance. This can be achieved through the use of efficient algorithms, optimized implementations, and hardware acceleration. It is also important to consider the specific requirements and constraints of the application and network, such as the number of devices, data rate, and transmission distance, when selecting and implementing cryptographic methods.

A careful balance between security and performance is crucial for the successful implementation of cryptographic methods in LoRaWAN.

D. LIMITATIONS

Communications security is an important element of LoRaWAN networks, and cryptography is one of the main techniques used for this purpose. Despite an increase in publications and solutions offered, concerns pertaining to the physical and network layers, as well as potential advancements and expansions of existing standards, continue to be the main themes of discussion. The existing studies of weaknesses and threats have not been put into practice. This paper has described in details two modes of AES encryption for LoRaWAN network layer. It was observed from the results that the duration of the encryption and decryption process is related to the key size. Nevertheless, it is necessary to provide studies to see whether the encryption and decryption process under AES256 may be also affected by the hardware and the type of the used LoRa module. Additionally, studies should be conducted to determine whether there is a likelihood that a particular attack could crack AES256-based hardware.

VII. CONCLUSION AND DIRECTIONS FOR FUTURE RESEARCH

In this study, we have introduced and thoroughly evaluated a novel AES256 encryption mode for LoRaWAN, comparing its performance with the standard AES128 mode. Our unique contribution lies in the implementation of AES256, which, despite increasing transmission time and energy consumption compared to AES128 and plain-text, offers significantly enhanced security. We observed that while transmitting cipher-text, AES256 incurs an average delay of approximately 4.01 ms at SF12, a modest increase over AES128's 2.66 ms, but crucially provides stronger protection against security threats. The implementation of robust security measures in LoRaWAN is non-negotiable, especially considering the growing reliance on IoT devices in sensitive sectors such as healthcare and defense. While network performance does experience some impact due to the heightened security, the trade-off is essential and worthwhile. Our findings suggest that the choice between AES128 and AES256 should be context-dependent: AES256 is preferable for devices handling sensitive data due to its superior security, whereas AES128 is more suitable for scenarios prioritizing energy efficiency. Currently, while AES128 is the norm in LoRaWAN devices, our work paves the way for the integration of AES256, broadening the scope of LoRaWAN's applicability. This advancement is particularly relevant for applications requiring high-security standards. Looking forward, there is a pressing need for a balance between high performance and robust security in LoRaWAN networks. Our research underscores the importance of continually evaluating the impact of encryption protocols on network performance. Future work should focus on refining LoRaWAN's MAC protocol, enhancing security without significantly compromising performance. This ongoing development is crucial for advancing the capabilities and applications of LoRaWAN in an increasingly interconnected world.

REFERENCES

[1] *LoRaWAN 1.0.3 Specification*. Accessed: Nov. 20, 2023. [Online]. Available: https://lora-alliance.org/wp-content/uploads/2020/11/lorawan1.0.3.pdf

[2] *Platform for IoT*. Accessed: Nov. 20, 2023. [Online]. Available: https://www.semtech.com/lora

[3] A. Lavric and A. I. Petrariu, "LoRaWAN communication protocol: The new era of IoT," in *Proc. Int. Conf. Develop. Appl. Syst. (DAS)*, May 2018, pp. 74–77.

[4] J. Haxhibeqiri, E. De Poorter, I. Moerman, and J. Hoebeke, "A survey of LoRaWAN for IoT: From technology to application," *Sensors*, vol. 18, no. 11, p. 3995, Nov. 2018.

[5] G. P. Reddy and Y. V. Pavan Kumar, "Demystifying LoRa wireless technology for IoT applications: Concept to experiment," in *Proc. 4th Int. Symp. Adv. Electr. Commun. Technol. (ISAECT)*, Dec. 2021, pp. 01–06.

[6] N. Abdoun, S. El Assad, T. M. Hoang, O. Deforges, R. Assaf, and M. Khalil, "Secure and resilient authenticated encryption approach based on chaotic neural networks and duplex construction," in *Advances and Challenges in Science and Technology*, vol. 6. BP International, 2023, pp. 146–191.

[7] S. Zulian, "Security threat analysis and countermeasures for LoRaWAN join procedure," Tech. Rep., 2016.

[8] A. Iqbal and T. Iqbal, "Low-cost and secure communication system for remote micro-grids using AES cryptography on ESP32 with LoRa module," in *Proc. IEEE Electr. Power Energy Conf. (EPEC)*, Oct. 2018, pp. 1–5.

[9] Z. Sahraoui and A. Chekirine, "On the risk analysis and countermeasure for bit-flipping attack in LoRaWAN," in *Proc. Int. Conf. Comput. Syst. Appl.* Cham, Switzerland: Springer, 2022, pp. 311–321.

[10] J. Lee, D. Hwang, J. Park, and K.-H. Kim, "Risk analysis and countermeasure for bit-flipping attack in LoRaWAN," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2017, pp. 549–551.

[11] M. Ingham, J. Marchang, and D. Bhowmik, "IoT security vulnerabilities and predictive signal jamming attack analysis in LoRaWAN," *IET Inf. Secur.*, vol. 14, no. 4, pp. 368–379, Jul. 2020.

[12] S. Chacko and M. D. Job, "Security mechanisms and vulnerabilities in LPWAN," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 396, Aug. 2018, Art. no. 012027.

[13] J. Prasetyo, M. Musayyanah, and J. Jusak, "A novel multiple access communication protocol for LoRa networks without LoRaWAN," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 30, no. 3, p. 1440, Jun. 2023.

[14] J. P. Shanmuga Sundaram, W. Du, and Z. Zhao, “A survey on LoRa networking: Research problems, current solutions, and open issues,” *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 371–388, 1st Quart., 2020.

[15] C. Sun, F. Zheng, G. Zhou, and K. Guo, “Design and implementation of cloud-based single-channel LoRa IIoT gateway using raspberry Pi,” in *Proc. 39th Chin. Control Conf. (CCC)*, Jul. 2020, pp. 5259–5263.

[16] E. Aras, G. S. Ramachandran, P. Lawrence, and D. Hughes, “Exploring the security vulnerabilities of LoRa,” in *Proc. 3rd IEEE Int. Conf. Cybern. (CYBCONF)*, Jun. 2017, pp. 1–6.

[17] S. Abboud, N. el Rachkidy, A. Guitton, and H. Safa, “Gateway selection for downlink communication in LoRaWAN,” in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2019, pp. 1–6.

[18] S. Abboud, N. E. Rachkidy, and A. Guitton, “Efficient decoding of synchronized colliding LoRa signals,” in *Proc. IEEE 91st Veh. Technol. Conf. (VTC-Spring)*, May 2020, pp. 1–5.

[19] S. Kim, H. Lee, and S. Jeon, “An adaptive spreading factor selection scheme for a single channel LoRa modem,” *Sensors*, vol. 20, no. 4, p. 1008, Feb. 2020.

[20] S. Maudet, G. Andrieux, R. Chevillon, and J.-F. Diouris, “Refined node energy consumption modeling in a LoRaWAN network,” *Sensors*, vol. 21, no. 19, p. 6398, Sep. 2021.

[21] F. Valois, “Optimization and experimental characterization of low power wide area networks,” Ph.D. dissertation, Grenoble INP, Grenoble, France, 2021.

[22] M. Jouhari, N. Saeed, M.-S. Alouini, and E. M. Amhoud, “A survey on scalable LoRaWAN for massive IoT: Recent advances, potentials, and challenges,” *IEEE Commun. Surveys Tuts.*, vol. 25, no. 3, pp. 1841–1876, 2023, doi: 10.1109/COMST.2023.3274934.

[23] N. Abdoun, S. El Assad, T. M. Hoang, O. Deforges, R. Assaf, and M. Khalil, “Authenticated encryption based on chaotic neural networks and duplex construction,” *Symmetry*, vol. 13, no. 12, p. 2432, Dec. 2021.

[24] K.-L. Tsai, Y.-L. Huang, F.-Y. Leu, I. You, Y.-L. Huang, and C.-H. Tsai, “AES-128 based secure low power communication for LoRaWAN IoT environments,” *IEEE Access*, vol. 6, pp. 45325–45334, 2018.

[25] S. Loukil, L. C. Fourati, A. Nayyar, and K.-W.-A. Chee, “Analysis of LoRaWAN 1.0 and 1.1 protocols security mechanisms,” *Sensors*, vol. 22, no. 10, p. 3717, May 2022.

[26] L. Thulasimani and M. Madheswaran, “Design and performance analysis of unified reconfigurable data integrity unit for mobile terminals,” 2010, *arXiv:1003.1514*.

[27] N. Abdoun, S. El Assad, T. M. Hoang, O. Deforges, R. Assaf, and M. Khalil, “Designing two secure keyed hash functions based on sponge construction and the chaotic neural network,” *Entropy*, vol. 22, no. 9, p. 1012, Sep. 2020.

[28] A. M. Da Rocha, M. A. De Oliveira, P. J. Fm, and G. G. H. Cavalheiro, “ABP vs. OTAA activation of LoRa devices: An experimental study in a rural context,” in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2023, pp. 630–634.

[29] B. Oniga, V. Dadarlat, E. De Poorter, and A. Munteanu, “Analysis, design and implementation of secure LoRaWAN sensor networks,” in *Proc. 13th IEEE Int. Conf. Intell. Comput. Commun. Process. (ICCP)*, Sep. 2017, pp. 421–428.

[30] LoRa Alliance. (2018). *LoRaWAN Regional Parameters v1.0.3revA*. [Online]. Available: https://lora-alliance.org/resource_hub/lorawan-regional-parameters-v1-0-3reva/

[31] LoRa Alliance, *LoRaWAN 1.1 Specification*, document 2018-04, Version 1.1, 2017.

[32] M. Mehic, M. Duliman, N. Selimovic, and M. Voznak, “LoRaWAN end nodes: Security and energy efficiency analysis,” *Alexandria Eng. J.*, vol. 61, no. 11, pp. 8997–9009, Nov. 2022.

[33] G. Dandachi, Y. Hadjadj-Aoul, P. Maille, and R. E. Navas, “Lightweight learning algorithms for massive IoT and analysis of their performance,” Ph.D. dissertation, INRIA Rennes-Bretagne Atlantique, Univ. Rennes, Rennes, France, 2022.

[34] X. Yang, “LoRaWAN: Vulnerability analysis and practical exploitation,” M. S. thesis, Math. Comput. Sci., Delft Univ. Technol., Delft, The Netherlands, 2017.

[35] X. Yang, E. Karampatzakis, C. Doerr, and F. Kuipers, “Security vulnerabilities in LoRaWAN,” in *Proc. IEEE/ACM 3rd Int. Conf. Internet-of-Things Design Implement. (IoTDI)*, Apr. 2018, pp. 129–140.

[36] E. Gresak and M. Voznak, “Protecting gateway from ABP replay attack on LoRaWAN,” in *Proc. Recent Adv. Electr. Eng. Rel. Sci. (AETA)*. Cham, Switzerland: Springer, 2020, pp. 400–408.

[37] E. van Es, H. Vranken, and A. Hommersom, “Denial-of-service attacks on LoRaWAN,” in *Proc. 13th Int. Conf. Availability, Rel. Secur.*, Aug. 2018, pp. 1–6.

[38] P. de Moraes and A. F. da Conceição, “A systematic review of security in the LoRaWAN network protocol,” 2021, *arXiv:2105.00384*.

[39] N. Prasad and P. Lynggaard, “LoRaWan sensitivity analysis and prevention strategies against wireless DoS attacks,” *Wireless Pers. Commun.*, vol. 126, no. 4, pp. 3663–3675, Oct. 2022.

[40] H. Ruotsalainen, G. Shen, J. Zhang, and R. Fujdiak, “LoRaWAN physical layer-based attacks and countermeasures—A review,” *Sensors*, vol. 22, no. 9, p. 3127, Apr. 2022.

[41] T. C. M. Dönmez and E. Nigussie, “Security of LoRaWAN v1.1 in backward compatibility scenarios,” *Proc. Comput. Sci.*, vol. 134, pp. 51–58, Jan. 2018.

[42] G. Loubet, E. Alata, A. Takacs, and D. Dragomirescu, “A survey on the security challenges of low-power wireless communication protocols for communicating concrete in civil engineerings,” *Sensors*, vol. 23, no. 4, p. 1849, Feb. 2023.

[43] H. Noura, T. Hatoum, O. Salman, J.-P. Yaacoub, and A. Chehab, “LoRaWAN security survey: Issues, threats and possible mitigation techniques,” *Internet Things*, vol. 12, Dec. 2020, Art. no. 100303.

[44] J. Qadir, I. Butun, P. Gastaldo, O. Aiello, and D. D. Caviglia, “Mitigating cyber attacks in LoRaWAN via lightweight secure key management scheme,” *IEEE Access*, vol. 11, pp. 68301–68315, 2023.

[45] N. Torres, P. Pinto, and S. I. Lopes, “Security vulnerabilities in LPWANs—An attack vector analysis for the IoT ecosystem,” *Appl. Sci.*, vol. 11, no. 7, p. 3176, Apr. 2021.

[46] M. Eldefrawy, I. Butun, N. Pereira, and M. Gidlund, “Formal security analysis of LoRaWAN,” *Comput. Netw.*, vol. 148, pp. 328–339, Jan. 2019.

[47] S. Antipolis and P. Girard, “Low power wide area networks security,” Gemalto, Amsterdam, The Netherlands, White Paper, 2015.

[48] J. Kim and J. Song, “A dual key-based activation scheme for secure LoRaWAN,” *Wireless Commun. Mobile Comput.*, vol. 2017, pp. 1–12, Nov. 2017.

[49] S. Na, D. Hwang, W. Shin, and K.-H. Kim, “Scenario and countermeasure for replay attack using join request messages in LoRaWAN,” in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2017, pp. 718–720.

[50] M. B. Aliyu, M. Hafeez, and A. Johnson, “LoRa-PUF: A two-step security solution for LoRaWAN,” in *Proc. IEEE 97th Veh. Technol. Conf. (VTC-Spring)*, Jun. 2023, pp. 1–6.

[51] A. Povalac, J. Kral, H. Arthaber, O. Kolar, and M. Novak, “Exploring LoRaWAN traffic: In-depth analysis of IoT network communications,” *Sensors*, vol. 23, no. 17, p. 7333, Aug. 2023.

[52] L. D. Rodić, T. Perković, M. Škiljo, and P. Šolić, “Privacy leakage of LoRaWAN smart parking occupancy sensors,” *Future Gener. Comput. Syst.*, vol. 138, pp. 142–159, Jan. 2023.

[53] I. Butun, N. Pereira, and M. Gidlund, “Security risk analysis of LoRaWAN and future directions,” *Future Internet*, vol. 11, no. 1, p. 3, Dec. 2018.

[54] F. Kuntke, V. Romanenko, S. Linsner, E. Steinbrink, and C. Reuter, “LoRaWAN security issues and mitigation options by the example of agricultural IoT scenarios,” *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 5, p. e4452, May 2022.

[55] J. Kim and J. Song, “A simple and efficient replay attack prevention scheme for LoRaWAN,” in *Proc. 7th Int. Conf. Commun. Netw. Secur.*, Nov. 2017, pp. 32–36.

[56] J. Han and J. Wang, “An enhanced key management scheme for LoRaWAN,” *Cryptography*, vol. 2, no. 4, p. 34, Nov. 2018.

[57] R. Sanchez-Iborra, J. Sánchez-Gómez, S. Pérez, P. Fernández, J. Santa, J. Hernández-Ramos, and A. Skarmeta, “Enhancing LoRaWAN security through a lightweight and authenticated key management approach,” *Sensors*, vol. 18, no. 6, p. 1833, Jun. 2018.

[58] K. Feichtinger, Y. Nakano, K. Fukushima, and S. Kiyomoto, “Enhancing the security of over-the-air-activation of LoRaWAN using a hybrid cryptosystem,” *Int. J. Comput. Sci. Netw. Secur.*, vol. 18, pp. 1–9, Feb. 2018.

[59] T. C. M. Dönmez and E. Nigussie, “Key management through delegation for LoRaWAN based healthcare monitoring systems,” in *Proc. 13th Int. Symp. Med. Inf. Commun. Technol. (ISMICT)*, May 2019, pp. 1–6.

[60] J. Xing, L. Hou, K. Zhang, and K. Zheng, “An improved secure key management scheme for LoRa system,” in *Proc. IEEE 19th Int. Conf. Commun. Technol. (ICCT)*, Oct. 2019, pp. 296–301.

[61] X. Chen, J. Wang, and L. Wang, "A fast session key generation scheme for LoRaWAN," in *Proc. Austral. New Zealand Control Conf. (ANZCC)*, Nov. 2019, pp. 63–66.

[62] N. A. Gunathilake, W. J. Buchanan, and R. Asif, "Next generation lightweight cryptography for smart IoT devices: Implementation, challenges and applications," in *Proc. IEEE 5th World Forum Internet Things (WF-IoT)*, Apr. 2019, pp. 707–710.

[63] S. M. Danish, M. Lestas, W. Asif, H. K. Qureshi, and M. Rajarajan, "A lightweight blockchain based two factor authentication mechanism for LoRaWAN join procedure," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2019, pp. 1–6.

[64] K.-L. Tsai, F.-Y. Leu, L.-L. Hung, and C.-Y. Ko, "Secure session key generation method for LoRaWAN servers," *IEEE Access*, vol. 8, pp. 54631–54640, 2020.

[65] V. Ribeiro, R. Holanda, A. Ramos, and J. J. P. C. Rodrigues, "Enhancing key management in LoRaWAN with permissioned blockchain," *Sensors*, vol. 20, no. 11, p. 3068, May 2020.

[66] S. Naoui, M. E. Elhdhili, and L. Azouz Saidane, "Novel enhanced LoRaWAN framework for smart home remote control security," *Wireless Pers. Commun.*, vol. 110, no. 4, pp. 2109–2130, Feb. 2020.

[67] P. Anantachaisilp, M. Muangkham, N. Punpigul, and M. Thammawichai, "Store and forward cubesat using LoRa technology and private LoRaWAN-server," Tech. Rep., 2020.

[68] H. Noura, O. Salman, T. Hatoum, M. Malli, and A. Chehab, "Towards securing LoRaWAN ABP communication system," in *Proc. 10th Int. Conf. Cloud Comput. Services Sci.*, 2020, pp. 440–447.

[69] T. Claverie and J. L. Esteves, "A LoRaWAN security assessment test bench," in *Proc. GNU Radio Conf.*, 2021, vol. 2, no. 1, pp. 1–3.

[70] A. Goulart, A. Chennamaneni, D. Torre, B. Hur, and F. Y. Al-Aboosi, "On wide-area IoT networks, lightweight security and their applications—A practical review," *Electronics*, vol. 11, no. 11, p. 1762, Jun. 2022.

[71] C.-I. Fan, E.-S. Zhuang, A. Karati, and C.-H. Su, "A multiple end-devices authentication scheme for LoRaWAN," *Electronics*, vol. 11, no. 5, p. 797, Mar. 2022.

[72] A. Mohamed, F. Wang, I. Butun, J. Qadir, R. Lagerström, P. Gastaldo, and D. D. Caviglia, "Enhancing cyber security of LoRaWAN gateways under adversarial attacks," *Sensors*, vol. 22, no. 9, p. 3498, May 2022.

[73] G. Czeczot, I. Rojek, and D. Mikołajewski, "Analysis of cyber security aspects of data transmission in large-scale networks based on the LoRaWAN protocol intended for monitoring critical infrastructure sensors," *Electronics*, vol. 12, no. 11, p. 2503, Jun. 2023.

[74] S. G. Richardson, "LoRaWAN sensor network jamming detection and mitigation using machine learning in the cloud," Ph.D. dissertation, Dept. Elect. Comput. Eng., Morgan State Univ., Baltimore, MD, USA, 2023.

[75] N. Hayati, K. Ramli, S. Windarta, and M. Suryanegara, "A novel secure root key updating scheme for LoRaWANs based on CTR_AES DRBG 128," *IEEE Access*, vol. 10, pp. 18807–18819, 2022.

[76] Y. Wei, K. F. Tsang, and H. Wang, "An efficient and secure DAG-based LoRaWAN system," in *Proc. IEEE 32nd Int. Symp. Ind. Electron. (ISIE)*, Jun. 2023, pp. 1–5.

[77] D. R. Bhadra, C. A. Joshi, P. R. Soni, N. P. Vyas, and R. H. Jhaveri, "Packet loss probability in wireless networks: A survey," in *Proc. Int. Conf. Commun. Signal Process. (ICCSP)*, Apr. 2015, pp. 1348–1354.

[78] P. Spadaccino, F. G. Crinó, and F. Cuomo, "LoRaWAN behaviour analysis through dataset traffic investigation," *Sensors*, vol. 22, no. 7, p. 2470, Mar. 2022.

[79] B. Preveze, "A novel method for performance improvement of slow start congestion control method in packet switched networks," *Uludağ Üniversitesi Mühendislik Fakültesi Dergisi*, vol. 24, no. 3, pp. 451–468, 2019.

[80] P. Thota and Y. Kim, "Implementation and comparison of M2M protocols for Internet of Things," in *Proc. 4th Int. Conf. Appl. Comput. Inf. Technol./3rd Int. Conf. Comput. Sci./Intell. Appl. Inform./1st Int. Conf. Big Data, Cloud Comput., Data Sci. Eng. (ACIT-CSII-BCD)*, Dec. 2016, pp. 43–48.

[81] Z. Ali, S. Henna, A. Akhunzada, M. Raza, and S. W. Kim, "Performance evaluation of LoRaWAN for green Internet of Things," *IEEE Access*, vol. 7, pp. 164102–164112, 2019.

[82] T. Bouguera, J.-F. Diouris, J.-J. Chaillout, R. Jaouadi, and G. Andrieux, "Energy consumption model for sensor nodes based on LoRa and LoRaWAN," *Sensors*, vol. 18, no. 7, p. 2104, Jun. 2018.

[83] H. Rajab, T. Cinkler, and T. Bouguera, "Evaluation of energy consumption of LPWAN technologies," Tech. Rep., 2021.

[84] D.-H. Bui, D. Puschini, S. Bacles-Min, E. Beigné, and X.-T. Tran, "Ultra low-power and low-energy 32-bit datapath AES architecture for IoT applications," in *Proc. Int. Conf. IC Design Technol. (ICICDT)*, Jun. 2016, pp. 1–4.

[85] W. Trappe, R. Howard, and R. S. Moore, "Low-energy security: Limits and opportunities in the Internet of Things," *IEEE Secur. Privacy*, vol. 13, no. 1, pp. 14–21, Jan. 2015.