Scientific Journal for Publishing in Health Research and Technology

Volume 2, Issue 1, 2026, Pages: 443-449

Journal homepage: https://sjphrt.com.ly/index.php/sjphrt/en/index

Impact of Encryption Mechanisms on Power Consumption in LoRaWAN and NB-IoT Networks

MAHMUD ALI ALBRNAT *
Department of Electrical Engineering, Faculty of Engineering, Sabratha University, Libya

تأثير آليات التشفير على استهلاك الطاقة في شبكات *LoRaWAN* و *NB-IoT*

محمود علي البرناط *
قسم الهندسة الكهربائية، كلية الهندسة -رقدالين، جامعة صبراتة، ليبيا

*Corresponding author: mahmud.albrnat@ta.sabu.edu.ly

Received: January 25, 2026	Accepted: February 26, 2026	Published: March 14, 2026

Abstract:
As the Internet of Things (IoT) expands rapidly, Low Power Wide Area Networks (LPWANs) like LoRa and NB-IoT have become essential for connecting devices with limited power. However, maintaining secure applications while minimizing power consumption is a significant challenge due to the trade-off between energy efficiency and data protection. This paper investigates the impact of implementing security mechanisms, specifically transmitted data encryption, on power consumption in LoRa and NB-IoT networks. The study highlights how various encryption schemes affect battery life, latency, and connection stability. Key findings demonstrate that while NB-IoT utilizes hardware-accelerated security via cellular modules for efficiency, LoRaWAN relies on software-based AES-128 encryption which increases CPU cycles and energy usage. Experimental results for LoRaWAN show that increasing the AES key size from 128-bit to 192-bit and 256-bit leads to a substantial rise in energy consumption and processing delays. Specifically, AES-256 increased energy consumption by 30–32% and processing time by up to 32% compared to the baseline. The study concludes that while security is vital, its implementation must be carefully planned to prevent drastically lowering energy efficiency in battery-powered IoT devices. It is recommended to use AES-128 for a balance of security and power, alongside power management modes like deep sleep to further extend battery life.

Keywords: Internet of Things (IoT) ،Low Power Wide Area Networks (LPWANs) ،LoRa ، NB-IoT ،Data Encryption ،Power Consumption ،Energy Efficiency.

الملخص
مع التوسع السريع في إنترنت الأشياء(IoT) ، أصبحت شبكات الطاقة المنخفضة واسعة النطاق (LPWAN) مثل LoRa و NB-IoT ضرورية لتوصيل الأجهزة ذات القدرات المحدودة من حيث الطاقة .ومع ذلك، يبرز الحفاظ على أمن التطبيقات مع تقليل استهلاك الطاقة كتحدٍ كبير بسبب المفاضلة بين كفاءة الطاقة وحماية البيانات .تبحث هذه الورقة في تأثير تنفيذ آليات الأمن، وتحديداً "تشفير البيانات المرسلة"، على استهلاك الطاقة في شبكات LoRa و NB-IoT.تسلط الدراسة الضوء على كيفية تأثير مخططات التشفير المختلفة على عمر البطارية، وزمن الانتقال، واستقرار أداء الاتصال .وتظهر النتائج الرئيسية أنه بينما تستخدم تقنية NB-IoT أجهزة تسريع أمني عبر وحدات خلوية لضمان الكفاءة، تعتمد LoRaWAN على تشفير

AES-128القائم على البرمجيات، مما يزيد من دورات وحدة المعالجة المركزية واستهلاك الطاقة .أظهرت النتائج التجريبية لشبكة LoRaWAN أن زيادة حجم مفتاح AES من 128 بت إلى 192 بت و256 بت تؤدي إلى ارتفاع كبير في استهلاك الطاقة وتأخير المعالجة .وبشكل محدد، أدى استخدام AES-256 إلى زيادة استهلاك الطاقة بنسبة 30-32% ووقت المعالجة بنسبة تصل إلى 32% مقارنة بالمعيار الأساسي .تخلص الدراسة إلى أنه على الرغم من أهمية الأمن، إلا أن تنفيذه يحتاج إلى تخطيط دقيق لمنع خفض كفاءة الطاقة بشكل حاد في أجهزة إنترنت الأشياء التي تعمل بالبطاريات .ويُنصح باستخدام AES-128لتحقيق التوازن بين الأمن واستهلاك الطاقة، جنباً إلى جنب مع أوضاع إدارة الطاقة مثل "النوم العميق" لإطالة عمر البطارية بشكل أكبر.

الكلمات المفتاحية: إنترنت الأشياء، الشبكات واسعة النطاق منخفضة الطاقة، إنترنت الأشياء ضيق النطاق، تشفير البيانات، استهلاك الطاقة، كفاءة الطاقة.

1. Introduction

The Internet of Things' (IoT) explosive expansion has given rise to a new class of communication technologies that are intended to assist devices with long-range communication requirements and low energy budgets. Among these, two of the most popular LPWAN (Low Power Wide Area Network) technologies are LoRa (Long Range) and NB-IoT (Narrowband Internet of Things). two of the most popular LPWAN (Low Power Wide Area Network) technologies are LoRa (Long Range) and NB-IoT (Narrowband Internet of Things).

Strong security features are still difficult to integrate into LoRa and NB-IoT networks, despite their benefits. IoT devices may be left unattended for extended periods of time, transmit sensitive data, and frequently operate in hostile environments. Therefore, it is essential to guarantee data integrity, confidentiality, and authentication. However, because the majority of IoT nodes are resource-constrained and battery-powered, putting traditional security measures in place could be a waste of computational and energy resources.

This research aims to explore to what extent do encryption and other security mechanisms impact power consumption in LoRa and NB-IoT networks, analyzing the trade-offs between implementing encryption algorithms and preserving energy efficiency.

2 Background and Literature Review

2.1 LoRa Technology Overview

LoRa (Long Range) is a modulation technique developed by Semtech based on Chirp Spread Spectrum (CSS) [1][2]. It allows for long-range communication (up to 15 km in rural areas) with extremely low power consumption [1]. LoRaWAN, the network protocol built on LoRa, operates in unlicensed ISM bands and is suitable for applications that require infrequent, small data transmissions.

LoRaWAN communication protocol operates primarily in the sub-GHz industrial, scientific, and medical (ISM) bands, such as the 868 MHz band commonly used in Europe. It is characterized by uplink-dominated communication, making it highly suitable for sensor-based and monitoring applications where devices primarily transmit data to a central server. The protocol supports low data rates ranging from 0.3 to 50 kbps [2], which enhances its energy efficiency and long-range communication capabilities.

To ensure secure data transmission, LoRaWAN incorporates end-to-end encryption based on the AES-128 algorithm [2], providing a robust layer of confidentiality and integrity despite the resource-constrained nature of typical end devices.

2.2 NB-IoT Technology Overview

NB-IoT (Narrowband Internet of Things) is a cellular-based LPWAN technology standardized by 3GPP. It operates in licensed spectrum and offers better Quality of Service (QoS), mobility support, and scalability compared to LoRa. It is ideal for applications requiring periodic, reliable communication with moderate throughput.

NB-IoT operates within licensed LTE frequency bands, make use of the existing cellular infrastructure to provide reliable and wide-area connectivity. it supports bi-directional communication, enabling both uplink and downlink data transfer. This is a feature for NB-IoT that doesn't exist in many other LPWAN technologies, this is essential for applications requiring remote control or acknowledgment signaling.

Feature	LoRa	NB-IoT
Frequency Band	Unlicensed (e.g., 868 MHz)	Licensed LTE bands
Data Rate	0.3 – 50 kbps	Up to 250 kbps
Security Standard	AES-128 (LoRaWAN)	3GPP LTE Security Suite
Authentication Method	Join Request/Accept (LoRaWAN)	SIM-based (eNodeB)
Encryption Overhead	Moderate (CPU-based AES)	Lower (hardware-accelerated)
Suitable for	Static sensors, remote areas	Smart meters, city infrastructure

Table 1 : key features of LoRaWAN and NB-IoT

NB-IoT offers higher data rates, reaching up to 250 kbps [3], allowing for more complex data exchanges while maintaining energy efficiency. Security is a core component of NB-IoT, as it is built on 3GPP-standardized LTE security mechanisms, including mutual authentication and encryption, ensuring a high level of protection suitable for mission-critical and enterprise-grade IoT deployments [1][3].

3 Security Mechanisms in LoRa and NB-IoT

3.1 LoRa Security Mechanisms

LoRaWAN provides security at two layers:

- Network Security: Ensures authenticity of the node with the network server.
- Application Security: Ensures confidentiality of the data between the node and the application server.

The primary encryption mechanism is AES-128 in CTR (Counter) mode, applied to both uplink and downlink messages. The keys are:

- **AppKey** (for join procedure)
- **NwkSKey** (for MAC commands)
- **AppSKey** (for user data)

These operations are performed in software, typically requiring CPU cycles, which increases energy consumption.

LoRaWAN implement these features through mechanisms like AES-128 encryption, message integrity codes (MIC), and dynamic session key generation via Over-the-Air Activation (OTAA)[3].

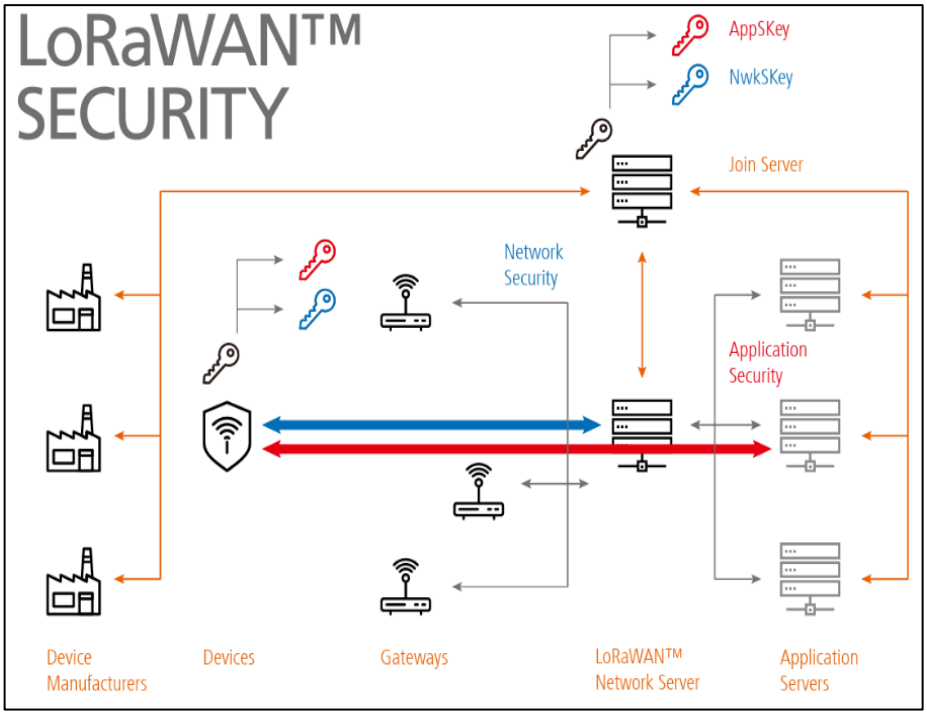

Figure 1 LoRaWAN security mechanism [3]

3.2 NB-IoT Security Mechanisms

NB-IoT leverages the security framework of LTE, including:

– Mutual authentication using SIM credentials and eNodeB.
– Encryption of both control and user planes using 128-bit SNOW 3G or AES.
– Support for integrity protection of signalling messages.

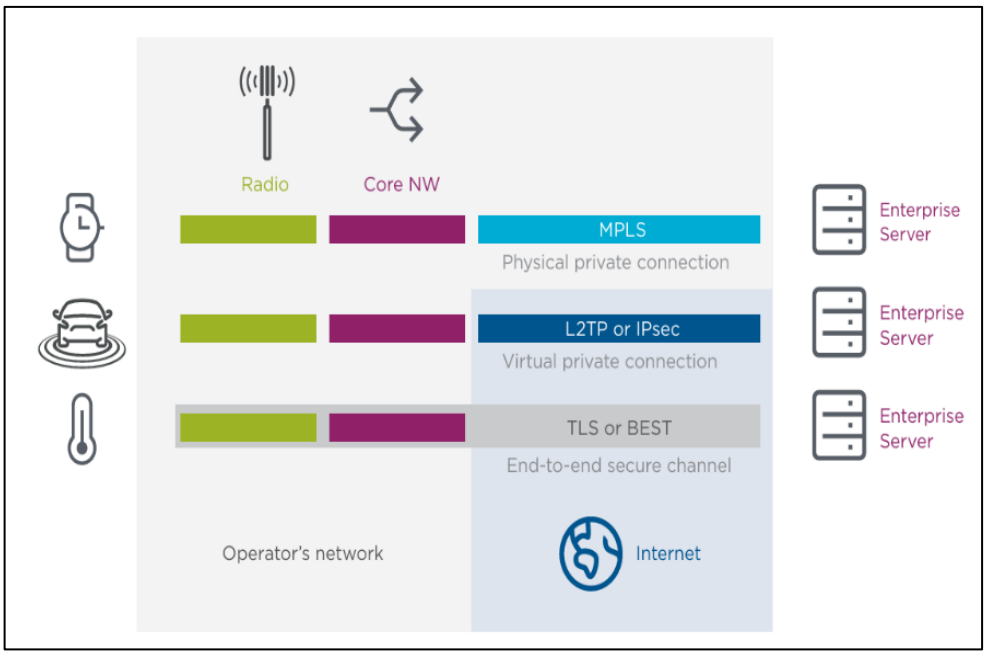

Figure 2: NB-IoT security mechanism [4]

These security processes are mostly hardware-accelerated via the cellular module and SIM, leading to more efficient power usage despite their complexity. NB-IoT, as part of the LTE family, inherits robust cellular security protocols including mutual authentication and SIM-based key management. Despite these measures, LPWANs remain vulnerable to physical tampering, replay attacks, and denial-of-service threats due to their wireless and often unattended deployment environments [6].
The security process here is hardware-accelerated via the cellular network and SIM, which makes it more energy efficient despite the complexity.

Analyzing power consumption in LoRaWAN transmission
before analysing the impacts of AES key sizes and encryption, we first understand the basic operation of LoRaWAN transmission protocol. a comprehensive study of energy usage patterns during standard LoRaWAN activities was held to discover power consumption in watts over the first 6 seconds of a node transmitting data to the gateway using joule scope js110 which is a DC energy analyser that combine multimeter and oscilloscope, it has wide dynamic range measuring currents in nanoamps(nA) [5].

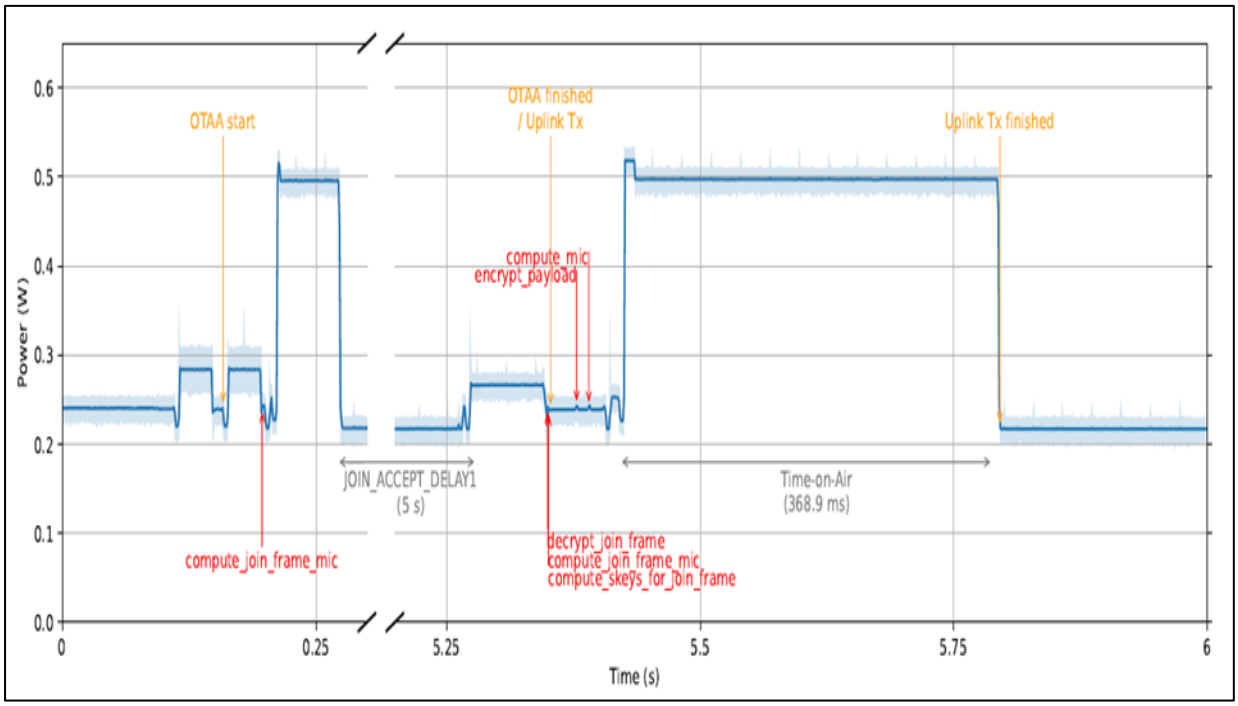

Figure 3: power consumption trace of 222byte LoRaWAN message transmission win AES 128 encryption

Figure 3 shows the energy consumption time live (power vs. time). beginning when the End Device (ED) is activated through to the transmission of its initial uplink message. This transmission contained a 222-byte payload and employed AES-128 encryption for securing the LoRaWAN communication. The horizontal axis displays time, while the vertical axis quantifies the ED's power consumption [5].

The visualization reveals distinct operational phases in the LoRaWAN communication sequence. The first segment corresponds to the Join-Request procedure, initiating the Over-the-Air Activation (OTAA) authentication. This transitions into the Join-Accept phase, which completes the OTAA process. The subsequent portion demonstrates the first data uplink transmission, where the highest power measurements correlate with the radio transmission period [7].

Power consumption test for different AES security key (128-bit, 192-bit, and 256-bit).
figure 4 presents the measured energy consumption of the End Device (ED) during experimenting difference AES key sizes across different payload [5][7]. The horizontal axis represents the payload in bytes, while the vertical axis shows corresponding energy consumption in microjoules. Three curves of the tested AES key sizes (128-bit, 192-bit, and256-bit) were plotted together to demonstrate the consumption visually.

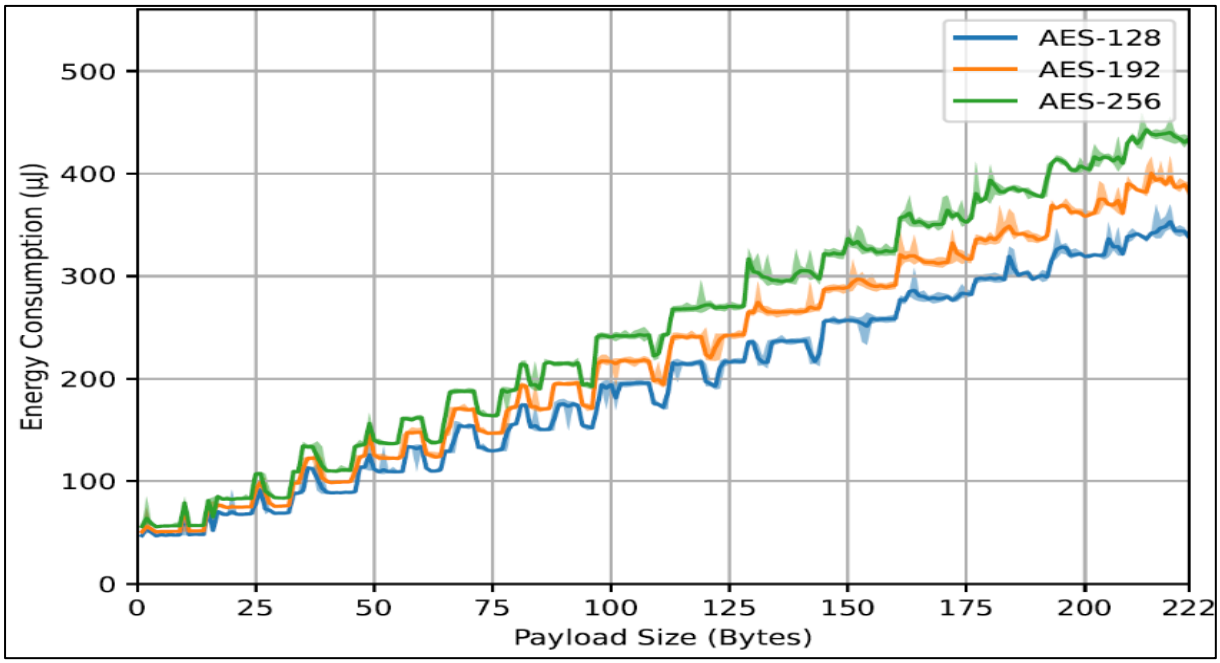

Figure 4: power consumption vs payload size for different encryption keys

The results demonstrate two expected trends: first, energy consumption rises with both larger AES key sizes and increased payload sizes. The 192-bit and 256-bit implementations consistently showed higher energy demands than the 128-bit variant across all payload sizes, attributable to the additional encryption rounds required for larger keys. Second, larger payloads required greater processing effort for data encryption, resulting in increasing the energy usage [5].

Results and Analysis
to evaluate the practical implications of enhanced cryptographic security in LoRaWAN, we analysed the energy and time overhead introduced by employing larger AES keys—specifically 192-bit and 256-bit compared to the baseline 128-bit AES standard. The analysis investigates the cryptographic performance on a LoRaWAN end device under maximum payload conditions (222 bytes).
The results show an increase in computational energy consumption and processing delay when using larger AES key sizes.
For AES-192, the energy consumption increased by approximately 13–14% relative to AES-128. Similarly, the processing time also exhibited a corresponding increase of about 13–14%. When AES-256 was utilized, the energy consumption increased by approximately 30–32%, and the processing time grew by a comparable margin of 28–32%.
These changes are severely affecting the energy cost associated with LoRaWAN radio transmissions. Specifically, the additional energy required for AES-256 encryption was estimated at 236 µJ, and the added processing time was approximately 750 µs, it is

recommended that using AES-128 provides a descent amount of security while maintaining minimum latency and power consumption requirements.

Discussion

Based upon the above analysis, maintaining a secure connection between nodes and gateways requires a significant amount of power consumption which is vital to IoT applications.
Designing power management operation modes at the microcontroller level may reduce the effect of implementing such security encryption protocols.
applying operation modes such as sleep mode where device reduce activities with quick wake-up time, deep sleep mode which provides longer idle status. and shutdown mode where all components are off excluding essential operating component, would further minimize the power consumption of each end node, also implanting polling intervals technique reduces how often sensors collects data which leads to increasing battery life significantly.

Compliance with ethical standards

Disclosure of conflict of interest

The authors declare that they have no conflict of interest.

References

[1] Semtech Corporation, "LoRa and LoRaWAN: A Technical Overview," White Paper, 2020.
[2] LoRa Alliance, "LoRaWAN™ 1.1 Specification," Oct. 2017. [Online]. Available: https://lora-alliance.org/resource_hub/lorawan-specification-v1-1/
[3] 3GPP, "Security architecture and procedures for 5G system," TS 33.501, v16.1.0, 2019.
[4] N. Sornin, M. Luis, T. Eirich, T. Kramp, and C. Hersent, "LoRaWAN Specification," LoRa Alliance, Inc., 2015.
[5] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125-1142, Oct. 2017.
[6] R. Ratasuk, B. Vejlgaard, N. Mangalampalli, J. P. Martel, and A. Prasad, "NB-IoT system for M2M communication," *2016 IEEE Wireless Communications and Networking Conference*, Doha, Qatar, 2016, pp. 1-5.
[7] K. Q. Abdelfadeel, V. Cionca, and D. Pesch, "A Fair and Reliable Adaptive Data Rate for LoRaWAN," *2018 IEEE 19th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, Chania, Greece, 2018.

