IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/46SP/2025/4641125/
Vol. 2025 (37), Article ID 4641125

Comparative Study of Energy and Security Performance in LoRa, BLE, and Wi-Fi IoT Systems*

Karol PACYNA, Mateusz ZAWADZKI and Maciej SOBIERAJ

Poznan University of Technology, Poznan, Poland

Correspondence should be addressed to: Karol PACYNA, karolpacyna2000@gmail.com

* Presented at the 46th IBIMA International Conference, 26-27 November 2025, Ronda, Spain

Abstract

This paper presents a comparative analysis of energy consumption and security performance in IoT systems using LoRa, BLE, and Wi-Fi technologies. Current measurements were performed with an INA219 module under both unsecured and secured (encrypted/authenticated) transmission conditions. Results indicate that BLE offers the lowest energy consumption with negligible security overhead, LoRa shows moderate consumption with a strong dependence on Spreading Factor (trade-off between range and power), while Wi-Fi demonstrates the highest power demand due to TLS and session handling. Security tests involving DoS, MITM, sniffing, and data interception confirmed that encryption and authentication significantly improved system resilience. The study highlights that optimizing radio parameters and employing deep sleep modes are crucial for achieving a balance between security and energy efficiency in IoT applications.

Keywords: energy consumption, security performance, IoT system.

Introduction

The dynamic development of the Internet of Things (IoT) has led to a rapid increase in the number of network-connected devices and a broad expansion of application areas — from smart homes and healthcare, to industrial automation and precision agriculture (Evans, 2011). This unprecedented growth introduces serious security challenges Granjal, Monteiro and Silva, 2015), arising from the limited hardware resources of many IoT nodes and the heterogeneous implementation of protection mechanisms (Serror et al., 2021).

A significant number of IoT devices remain vulnerable to cyberattacks (Sicari et al., 2015), often due to the use of default passwords, lack of encryption, or inadequate authentication procedures. Such weaknesses have resulted in large-scale security incidents, exemplified by the Mirai botnet (Qian et al., 2019), which exploited poorly secured IoT devices to launch massive distributed denial-of-service (DDoS) attacks.

Therefore, designing systems that ensure robust security while maintaining low energy consumption has become a crucial research objective (Alrawais et al., 2017, Lin and Bergmann, 2016). Achieving this balance is particularly important for battery-powered and resource-constrained IoT devices, where security mechanisms must be lightweight yet effective.

The objective of this paper is to present the design and security analysis of a prototype IoT system that integrates LoRa, Wi-Fi, and Bluetooth Low Energy (BLE) communication technologies within an MQTT-based architecture. The experimental setup employs ESP32-C3 and ESP8266 microcontrollers, a Raspberry Pi as a central processing and control unit, and an InfluxDB database for data collection and monitoring. The developed

Cite this Article as: Karol PACYNA, Mateusz ZAWADZKI and Maciej SOBIERAJ, Vol. 2025 (37) "Comparative Study of Energy and Security Performance in LoRa, BLE, and Wi-Fi IoT Systems" Communications of International Proceedings, Vol. 2025 (37), Article ID 4641125, https://doi.org/10.5171/2025.4641125

test environment enabled comprehensive energy consumption measurements and security resilience evaluations, including simulated attacks and post-mitigation testing.

The article is organized as follows. Section 2 presents the system structure and implementation. In Section 3 a description of conducted researches and results are presented. Section 4 concludes the article.

System Structure and Implementation

The designed IoT system (Figure 1) consisted of three main layers: the sensor layer, the communication layer, and the data processing layer.

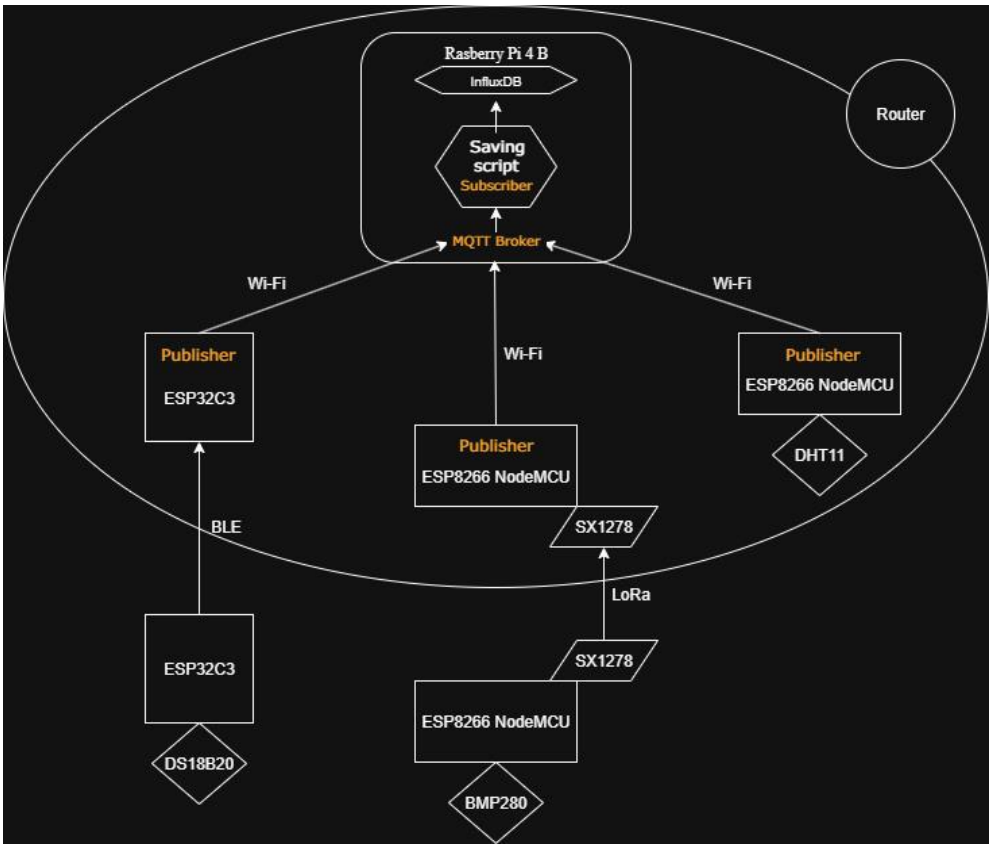

Fig 1. Structure of considered system

In the sensor layer, various environmental sensors (including temperature, humidity, and pressure sensors) were used and connected to ESP32-C3 and ESP8266 microcontrollers. These devices performed local data processing and transmitted the collected information using selected wireless communication standards – Wi-Fi, Bluetooth Low Energy (BLE), and LoRa (Haxhibeqiri et al., 2018, Sornin et al., 2017).

The communication layer enabled data exchange between the sensor nodes and the central MQTT broker, which was deployed on a Raspberry Pi computer. The system utilized the publish–subscribe model, ensuring scalability and flexibility in data transmission and integration.

In the data processing layer, an InfluxDB database was implemented to store and manage measurement data, also providing real-time visualization of results for monitoring and analysis purposes.

Experimental Study

Research Description

The conducted research focused on two key aspects of IoT system performance: energy consumption and system security.

Measurements of the current draw of microcontrollers were carried out under various operational conditions, including:

- unsecured data transmission,
- encrypted and authenticated transmission,
- variable distance between the transmitter and receiver,
- different device states (active and sleep modes).

These experiments enabled a comparative evaluation of the energy efficiency of multiple wireless communication technologies under realistic operating conditions. The measurements were performed using the INA219 current sensor module, ensuring precise monitoring of instantaneous power consumption. By analyzing both active and standby states, the study aimed to quantify the impact of security mechanisms and transmission parameters on total energy demand.

The second part of the research involved simulation of cyberattacks that are typical in IoT environments, distinguishing between unsecured and secured transmission scenarios. The following attack types were analyzed and implemented:

- Denial of Service (DoS/DDoS),
- Man-in-the-Middle (MITM),
- Sniffing,
- Data interception and capture.

The attacks were executed using publicly available penetration testing tools, replicating realistic threat conditions. After identifying system vulnerabilities, appropriate security countermeasures—including encryption at the link layer, device authentication and authorization, and traffic rate limiting—were proposed and later tested to assess their effectiveness and impact on overall system performance.

Results

Measurements were taken using the INA219 module on three types of transmitters (LoRa — SX1278 on ESP8266, BLE on ESP32-C3, and Wi-Fi on ESP8266) in two variants: unsecured transmission and secured transmission (encryption/authentication). The measurements were conducted both over short distances indoors and in open spaces; current was recorded in idle and active states.

Table 1: LoRa (distance 4 m)

	Idle		**Active**	
	Min [mA]	Max [mA]	Min [mA]	Max [mA]
Unsecured	10.7	12.6	82.7	84.6
Secured	10.7	12.6	84.7	88.3

LoRa — effect of parameters (Spreading Factor):

- For SF=7 (shorter range): e.g., 50 m → ~83.7 mA; 95 m → 105.7 mA; 190 m → 84.7 mA.
- For SF=12 (longer range): transmitter current values increase significantly (on the order of ~217–219 mA at longer distances).

This clearly shows a trade-off: greater range → substantially higher current consumption (Haxhibeqiri et al., 2018).

Table 2: Bluetooth Low Energy (BLE, 1 m)

	Idle		Active	
	Min [mA]	Max [mA]	Min [mA]	Max [mA]
Unsecured	1.2	2.1	21.6	51.7
Secured	1.4	2.1	21.6	51.9

Table 2 shows practically no significant increase. For distances of 1–6 m, active values are ~51–53 mA; a slight increase is observed through a wall.

Table 3: Wi-Fi (for distances from 2 to 6 meters, including transmission through one wall)

Idle		Active	
Min [mA]	Max [mA]	Min [mA]	Max [mA]
12.2	13	89	99.8

Based on the results presented in Tables 1–3, the following conclusions can be drawn.
Impact of Security Mechanisms:

- BLE: The introduction of authentication and session key setup procedures did not cause a significant increase in current consumption.
- LoRa: Encryption and authentication led to a small but measurable increase in current during preparation/transmission (e.g., ~2–4 mA in the tested scenario), though not dramatic for short SF configurations.
- Wi-Fi: The baseline active current is high (≈90–100 mA); the overhead caused by TLS/handshake is more noticeable in practice (due to higher traffic and longer sessions), which can reduce battery life during frequent connections. (Measured active values for secured Wi-Fi in this study confirm the high energy cost.)

Impact of Distance and Radio Parameters:

- Distance alone did not significantly affect transmitter current in the tested procedure (the transmitter sends immediately after reading data and does not wait for acknowledgements—no retransmissions). However, changes in radio parameters (e.g., SF in LoRa) have a substantial effect on transmitter current — higher SF → longer transmission time → steep increase in current consumption (Haxhibeqiri et al., 2018, Sornin et al., 2017).

Most Important Energy-Saving Factor:

- The deep sleep mode is the key factor for reducing energy use — minimizing the active time of the processor/transmitter is the dominant method of saving power, regardless of the chosen technology.

Energy consumption measurements were performed using the INA219 module for three wireless technologies: LoRa (SX1278), BLE (ESP32-C3), and Wi-Fi (ESP8266).
The results show that BLE has the lowest idle current (~1–2 mA) and moderate active current (~52 mA), LoRa has higher active current (~83–88 mA at low SF) with the possibility of a steep increase up to ~217 mA when SF is raised (at the cost of range), and Wi-Fi has a significantly higher active current (~89–100 mA).
Introducing security mechanisms (encryption, authentication) caused only a minor energy overhead for LoRa and virtually none for BLE; for Wi-Fi, the overhead is more pronounced due to the cost of TLS sessions and higher data traffic.

It is therefore recommended to use energy-saving mechanisms (deep sleep) and to select radio parameters (e.g., SF in LoRa) according to the required range (Haxhibeqiri et al., 2018) – enabling a balance between security and energy efficiency.

Conlucions

Based on the measurements conducted, BLE demonstrated the lowest energy consumption, with idle current around 1–2 mA and moderate active current near 52 mA, and the implementation of security features had negligible impact. LoRa offered longer transmission range, but increasing the Spreading Factor (SF) led to a substantial rise in current consumption, reaching up to approximately 217 mA, while security mechanisms added only a minor overhead of 2–4 mA. Wi-Fi exhibited the highest active current, ranging from 89 to 100 mA, with security overhead being more pronounced due to TLS sessions and higher traffic. Across all technologies, minimizing active time through deep sleep modes proved to be the most effective method for reducing energy consumption. Careful selection of radio parameters, such as SF in LoRa, allows for an optimal balance between range, security, and energy efficiency.

Acknowledgment

This research was funded by the Polish Ministry of Science and Higher Education under Grant 0313/SBAD/1311

References

- Alrawais, O., Alhothaily, A., Hu, C. and Cheng, X. (2017), 'Fog Computing for the Internet of Things: Security and Privacy Issues,' *IEEE Internet Computing*, 21(2), 34-42.
- Evans, D. (2011), 'The Internet of Things: How the Next Evolution of the Internet Is Changing Everything,' *Cisco White Paper*.
- Granjal, J., Monteiro, E., and Silva, J. S. (2015), 'Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues,' *IEEE Communications Surveys & Tutorials*, 17(3), 1294-1312.
- Haxhibeqiri, J., De Poorter, E., Moerman, I. and Hoebeke, J. (2018), 'A Survey of LoRaWAN for IoT: From Technology to Application,' *Sensors*, 18(11), 3995.
- Lin, H. and Bergmann, N. (2016), 'IoT Privacy and Security Challenges for Smart Home Environments,' *Information*, 7(3), 44.
- Qian, Y., Wu, D., Bao, W. and Lorenz, P. (2019) 'The Internet of Things for Smart Cities: Technologies and Applications,' *IEEE Network*, 33(2), 4-5.
- Serror, M., Hack, A., Henze, M., Schuba, M. and Wehrle, K. (2021), 'Challenges and Opportunities in Securing the Industrial Internet of Things,' *IEEE Transactions on Industrial Informatics*, 17(5), 2985-2996.
- Sicari, S., Rizzardi, A., Grieco, L. and Coen-Porisini, A. (2015), 'Security, Privacy and Trust in Internet of Things: The Road Ahead,' *Computer Networks*, 76, 146-164.
- Sornin, N., Luis, M., Eirich, T., Kramp, T. and Hersent, O. (2017), 'LoRaWAN Specification,' *LoRa Alliance*.