ADVANCES IN CYBER-PHYSICAL SYSTEMS

Vol. 10, No. 1, 2025

CREATING SECURE COMMUNICATION CHANNEL WITH LoRa TECHNOLOGY

Nazarii Yuzvak[1], *Roman Banakh*[1], *Abdallah A. Z. A. Ibrahim*[2]

[1] *Lviv Polytechnic National University, 12, S. Bandery str., Lviv, 79013, Ukraine,*
[2] *Suez Canal University, El Sheikh Zayed, El Salam District, IsmailiaБ 8366004, Egypt*
Authors' e-mails: *nazarii.yuzvak.kb.2021@lpnu.ua, roman.i.banakh@lpnu.ua, abdallah.ibrahim@ci.suez.edu.eg*

https://doi.org/10.23939/acps2025.01.111

Submitted on 16.04.2025

***Abstract*: This article addresses secure information transmission using LoRa technology in peer-to-peer mode, without relying on LoRaWAN. Such communication is vital in areas lacking centralized network infrastructure, such as rural, remote, emergency, or combat situations, where confidential data must be exchanged over several kilometers. The study explores methods for secure data transmission with LoRa devices, focusing on improving efficiency by optimizing encoding for higher data rates within limited byte sizes. Measurements of the maximum transmission rate and longest successful distance have been provided. A message-type-based encoding method has been proposed to optimize data transmission between the sender and receiver under limited channel bandwidth conditions.**

***Index terms*: LoRa, cybersecurity, encryption, wireless networks.**

I. INTRODUCTION

Wireless communication is a fundamental component of modern society, enabling the transfer of data without physical connections. Our everyday lives heavily rely on technologies powered by radio communication, such as mobile networks, the internet, satellite television, and radio broadcasting [1]. These technologies, though diverse in their applications, all operate using radio waves, which differ in frequency and wavelength. These physical characteristics directly affect signal propagation, data transmission speed, and coverage range [2].

Radio waves are typically classified by wavelength into long, medium, short, and ultra-short bands. Each class supports different use cases, from global radio broadcasts to high-speed data links. Wireless technologies such as Wi-Fi, GPS, and Bluetooth are designed with specific trade-offs: for example, Wi-Fi offers high transmission speeds at the cost of limited range, while Bluetooth supports only short-distance communication and is optimized for low power consumption [3].

When transmitting small data over long distances in remote or infrastructure-limited areas, traditional technologies like Wi-Fi and Bluetooth are unsuitable. LoRa (Long Range) addresses this gap with low-power, long-range wireless technology for efficient IoT data transmission. LoRa enables devices to communicate over several kilometers while consuming minimal energy [4]. In scenarios where the transmitted information is sensitive, it is essential to also ensure the confidentiality and security of the communication channel.

This paper investigates practical methods to improve the security of LoRa-based communication while considering the technology's limitations in terms of data rate and bandwidth. It aims to explore how encryption can be applied without compromising efficiency, and to examine the maximum effective range of LoRa in a semi-urban environment.

II. LITERATURE REVIEW AND PROBLEM STATEMENT

LoRa is a wireless communication technology based on radio modulation, enabling reliable data transmission over long distances in unlicensed frequency bands (169 MHz, 433 MHz, 868 MHz, 915 MHz). It is used in smart city lighting, agriculture, logistics, hydrology, engineering, medicine, and for transmitting natural disaster alerts [5].

LoRa's low energy requirements make it ideal for IoT devices needing long battery life. Unlike LoRaWAN, which includes infrastructure and security, LoRa is a physical layer communication method [6]. LoRa's signal quality is influenced by factors like frequency, transmission power, modulation type (Chirp Spread Spectrum), and environmental conditions, including terrain and weather [7–8]. Antenna placement and the Fresnel zone are crucial for optimizing performance [9].

In the article [10], the authors demonstrate that encryption does not affect data transmission performance. However, the study is limited to basic interception tests and does not consider potential key attacks or resource-constrained scenarios, which may be crucial when transmitting sensitive data. The article [11] provides a practical demonstration of using AES-128 for securing LoRa-based IoT data transmissions, highlighting successful system integration and real-world tests. However, the study lacks comprehensive analysis of cryptographic overhead, energy consumption, and robustness under adversarial conditions, limiting its applicability in large-scale or hostile environments.

However, the low data transmission rate of LoRa presents a challenge, as encryption methods must not significantly increase the size of transmitted data, and messages must remain efficient to avoid overloading the limited bandwidth.

III. SCOPE OF WORK AND OBJECTIVES

This study aims to enhance the security of information transmission over LoRa by developing and applying encryption methods suitable for low data rates.

The objectives of this research are twofold: first, to find ways to optimize the data transmission rate within the limitations of LoRa technology, ensuring that encryption does not significantly impact the speed; and second, to investigate the maximum transmission range in an urban fringe environment. By achieving these goals, the study seeks to establish practical solutions for improving the security and efficiency of LoRa-based communication systems.

IV. SECURE COMMUNICATION USING LORA TECHNOLOGY

Encryption in LoRa must balance cryptographic strength and payload constraints. LoRaWAN provides end-to-end encryption and scalable management, but adds latency due to gateway routing [12]. Compared to Sigfox and NB-IoT [13], LoRa offers stronger resistance to interference and jamming, making it more reliable in dense or contested radio environments, including those affected by electronic warfare [14].

LoRaWAN's scalability and security are offset by latency and limited throughput, making point-to-point links more effective in offline use cases. Therefore, this study uses E32-433T30D modules operating at the physical layer without LoRaWAN support [15]. Periodic key rotation limits key compromise risk. AES-CMAC and similar MACs ensure message integrity with a verification tag from a shared key [16]. Replay attacks can be mitigated with counters or unique packet IDs. Symmetric keys should be refreshed automatically, based on pre-shared keys and dynamic parameters. While encryption prevents plaintext access, interception may still lead to message loss or failed decryption. Persistent update issues, caused by interference or attacks, may require manual recovery. To reduce targeted disruption, key updates should occur at randomized times, even if their average frequency stays fixed [17].

V. PRACTICAL STUDY OF ENCRYPTED MESSAGE COMMUNICATION AT DIFFERENT DISTANCES

A. COMMUNICATION SETUP AND ENCRYPTION MECHANISM

A study measured the data transmission speed under different message sending parameters. Each message requires a delay for separation, reducing the overall data rate. A custom delimiter was used to separate messages while working with LoRa devices (E32-433T30D) connected to a Raspberry Pi 4 Model B single-board computer [18]. This improved speed by using a delimiter byte instead of a delay.

To establish communication between devices, the Python programming language and a library were used. The library's default configuration for LoRa devices called Ebyte LoRa E32. The LoRa modules were connected to the Raspberry Pi via GPIO pins [19].

The Ebyte LoRa E32 library allows configuration of module parameters (frequency, data rate, transmission power, channels, etc.), management of device modes, checking of device status and configuration, and sending of data. Using this library, a client application was written to send messages and a server application to receive them.

The AES encryption algorithm in CTR mode was applied in this study. We recommend this type of encryption, as AES is approved by the U. S. National Institute of Standards and Technology as one of the most effective encryption methods for securing data. CTR-mode encryption does not change the length of the original text after encryption – the ciphertext has the same length as the original message, and each block is processed independently without additional overhead [20].

B. MESSAGE STRUCTURE AND TRANSMISSION STRATEGY

When a message is transmitted in encrypted form rather than plaintext, there is a high probability that the encrypted message may contain at least one newline character "*n*", which is commonly used as a delimiter. This can cause incorrect message splitting by the receiver. This issue can be resolved by using a longer delimiter. Using a delimiter consisting of two or more characters greatly reduce the chance of accidental matches. For instance, we can define "END" as a delimiter – these three characters signal to the receiver that the message has ended. Although there is still a chance that the message could accidentally contain this exact sequence, increasing the number of bytes in the delimiter reduces this probability exponentially.

Another approach is to add the message length at the beginning, allowing the receiver to detect where it ends. This is most effective when the maximum message size is known. For instance, if messages are under 256 bytes, one byte (0–255) can indicate length, including itself. If messages exceed 256 bytes (e. g., 1000), two bytes can be used to specify length and mark message boundaries.

In this study, UTF-8 encoding was used for communication between LoRa devices. UTF-8 supports 256 different characters, which are used to construct the messages. Each character requires one byte, i. e., 8 bits [21].

Thus, the sender creates a message, encrypts it using AES in Counter mode, appends the "END" delimiter (three bytes) to the encrypted message, and sends the complete message to the receiver.

Tests showed that LoRa message segments are limited to 55 bytes. Therefore, the client application (transmitter) was configured to limit each data segment to a maximum of 55 bytes. Any message exceeding this limit is split into parts and sent over multiple segments of 55 bytes each. Fig. 1 shows the message structure.

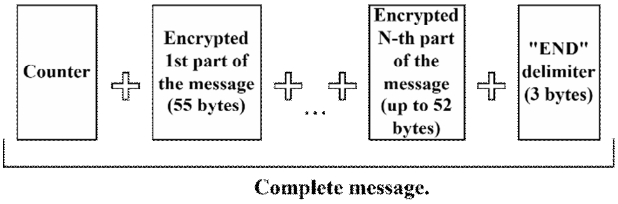
Counter
Encrypted 1st part of the message (55 bytes)
...
Encrypted N-th part of the message (up to 52 bytes)
"END" delimiter (3 bytes)
Complete message.

Fig. 1. Structure of created messages

It was also established that the required delay for successful reception depends on message segment size. Sending a 55-byte segment takes 0.8 seconds. Therefore, this duration was used in the transmitter program as the delay necessary for successful message delivery. Messages may arrive corrupted when this delay is reduced (theoretically increasing the transmission speed). However, excessive delay reduction prevents successful reception or decryption due to reflections or noise. If a device receives a new signal before the previous one has completed, the receiver will end up with corrupted data.

Additionally, during fast transmissions, the sender may unintentionally interfere with its own previous segment that has not yet reached the receiver. Therefore, a delay of precisely 0.8 seconds before sending each message segment was used. This delay may be adjusted for different conditions or devices.

The following formula (1) is used to calculate the data transmission rate DTR.

$$DTR = \frac{P}{60} \times N, \quad (1)$$

where P is the number of successfully received messages per minute, and N is the number of bytes in each transmitted message.

During testing of the maximum data transmission speed, results showed that the number of messages sent per minute did not vary with different message segment sizes. For example, 29 messages of 145 bytes each were successfully transmitted within one minute (each message was divided into segments, with a maximum segment size of 55 bytes). Under different conditions, where each message contained 115 bytes (also divided into segments of no more than 55 bytes), the same number of messages – 29 per minute – was transmitted. Using formula (1), the data transmission speed was calculated for different message sizes.

In the first case, the data transmission speed is:

$$DTR_1 = \frac{29}{60} \times 145 = 70.08 \; (bytes/\text{sec}),$$

In the second case, the speed is:

$$DTR_2 = \frac{29}{60} \times 115 = 55.58 \; (bytes/\text{sec}),$$

Although the number of messages remains the same, the data transmission speed noticeably decreases. This occurs because each message is split into 3 segments (e. g., 145 bytes → 55+55+35; 115 bytes → 55+55+5). Thus, speed drops since the last segment isn't fully packed but still delayed by 0.8 seconds. In such cases, this speed loss can be offset by computing the minimum time for the final segment.

After many attempts, a peak of 77 bytes/s was reached using the default Ebyte LoRa E32 library settings. In this specific attempt, 84 messages of 55 bytes each were successfully transmitted, with a delay of 0.71 seconds between segments. To calculate the time required to receive a data segment, we can use a speed of 70 bytes / second, as under such conditions, messages are almost guaranteed to be successfully delivered. To calculate the time t (in seconds) for a message segment that is smaller than 55 bytes, we use formula (2):

$$t = \frac{1}{70} \times N, \quad (2)$$

where N is the number of bytes in the packet, and 70 represents the data transmission speed in bytes per second. Using the formula (2), we can determine the time required to send each packet that is smaller than the default 55 bytes. This allows us to approach the maximum possible speed for sending smaller packets. The value 70, representing the transmission rate, may be adjusted if other configurations of LoRa devices result in different speeds.

To increase the amount of transmitted information, it is also possible to use basic data encoding. This is useful for custom LoRa networks transmitting various decodable data types. E. g., one device sends humidity, another sends temperature at different times on the same frequency (or even at the same time but on a different frequency – in which case the receiver must be properly tuned to the second device's frequency). To avoid using several bytes to explain the message, a single-character identifier (e. g., at the start) can replace longer message descriptions. This helps the receiver decode different message types.

C. FIELD TEST RESULTS

After implementing the measures described above, an experimental field test was conducted to evaluate the device's performance at different distances. The test used a 433MHz Long Range Directional Antenna 2-unit Yagi Antenna 6dBi antenna for the receiver and a 1x118in 433MHz SMA Male Plug Horn 5dBi antenna for the transmitter. The receiver remained stationary throughout the test, while the transmitter moved continuously to assess communication capability in various terrains and at varying distances.

In an urban area with residential buildings and dense construction – where the receiver was located immediately behind one of the buildings (which significantly impairs signal reception due to the obstruction) – the maximum transmission distance achieved was 320 meters. Under line-of-sight conditions, successful message transmission was achieved at approximately 70 bytes/s over a distance of 5 km. The longest distance at which a single encrypted message was successfully transmitted and decrypted was 11.36 km. The transmitter's path is shown in Fig. 2.

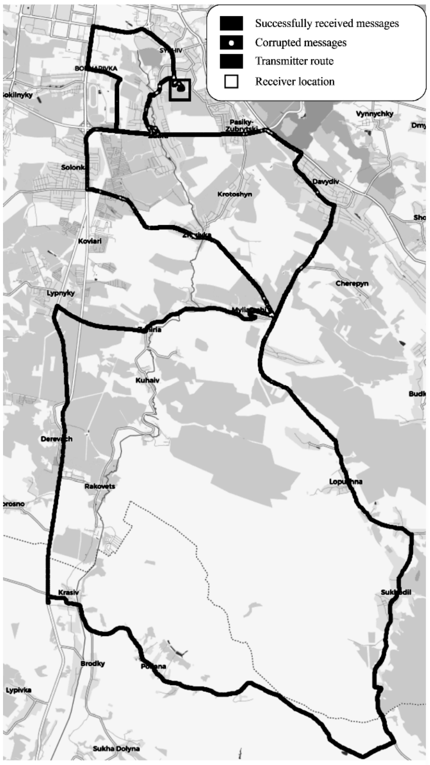

Fig. 2. The movement path of the transmitter

After completing the experiment, an elevation profile of the longest successful transmission segment (11.36 km) was generated, during which an encrypted message was successfully delivered. This transmission segment is marked in Fig. 3.

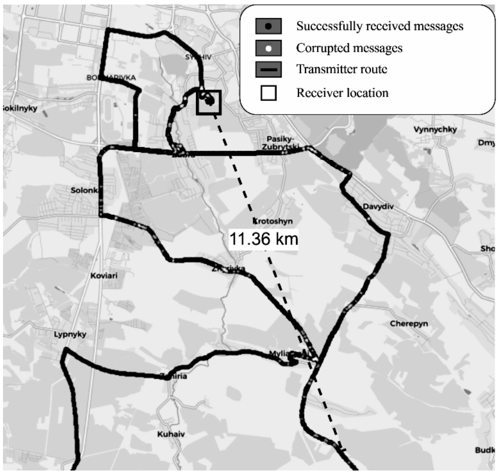

Fig. 3. The longest distance of a successfully transmitted message

Landscape features greatly impact radio wave propagation. Terrain obstacles (e. g., hills) cause attenuation, blockage, diffraction, and multipath effects. Additionally, complex landforms contribute to diffraction and multipath propagation, resulting in changes to the signal's phase and amplitude [22].

The elevation profile is shown in Fig. 4. From this figure, it can be seen that there were no significant terrain obstacles higher than either the receiver or the transmitter – between the two points (with the receiver on the left side of the graph and the transmitter on the right), which likely enabled the successful transmission of the message.

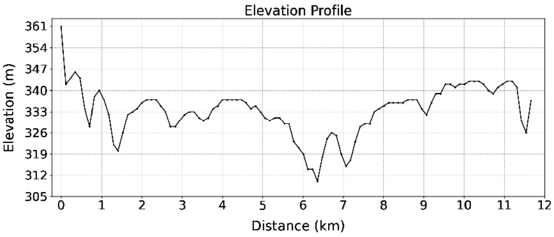

Fig. 4. Elevation profile of the longest successfully transmitted message path

The receiver was positioned on the roof of a residential building at an elevation of 361 meters above sea level, which is shown by the sharp elevation increase at the beginning of the graph.

The theoretical Fresnel zone for this transmission scenario (at a distance of 11.36 km) is illustrated in Fig. 5.

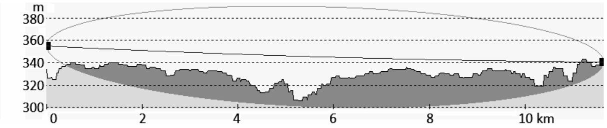

Fig. 5. Fresnel zone during message transmission from the longest distance

It is important to note that even when there is no direct line of sight between the transmitter and the receiver, successful radio transmission can still occur if the Fresnel zone is at least partially clear. Radio waves are capable of bending around obstacles or reflecting off surfaces. In such cases, successful communication is unlikely, but still possible. This highlights the resilience of low-frequency, long-range communication technologies like LoRa, especially in complex or obstructed environments.

Fig. 6 shows the theoretical coverage area of the stationary antenna.

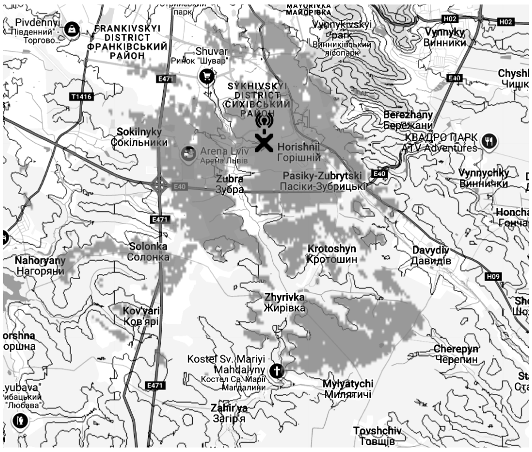

Fig. 6. Coverage area of the stationary antenna

Although this antenna serves as the receiver in this experiment, the coverage zone demonstrates not only where the antenna is able to transmit a radio signal, but also where it can receive one. This is because the Fresnel zone remains the same regardless of which antenna is the transmitter, and which is the receiver. In practice, this means that optimizing antenna placement for either direction improves overall system performance and coverage reliability.

The maximum distance at which the receiver was able to decode some part of the message (but not decrypt) part of the transmitted message was 18.86 km (Fig. 7).

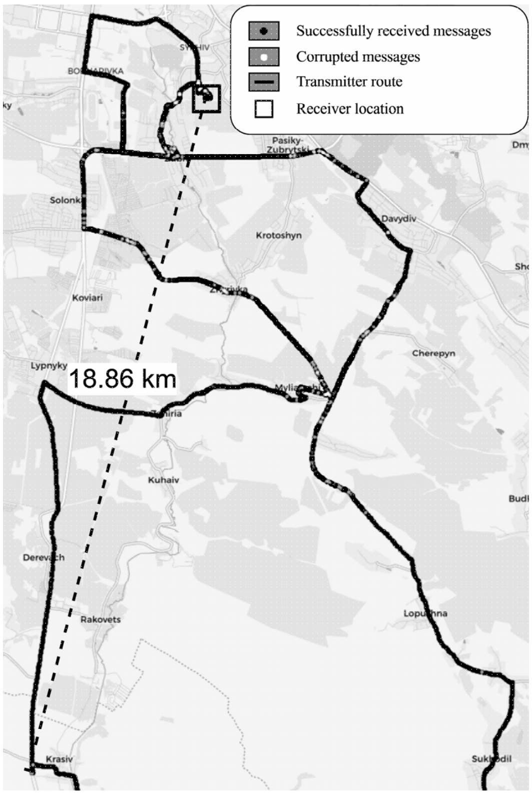

Fig. 7. Maximum distance of received damaged message

VI. DISCUSSION

The transmission coverage was expected to be consistent across the region, but even slight terrain variations, such as buildings or hills, caused complete signal loss in some areas. Still, LoRa achieved 11.36 km – farther than commonly reported.

Analysis of the Fresnel zone confirmed that antenna height is critical for signal quality and range. Elevated antennas reduce interference and boost signal, confirming Fresnel theory.

Surprisingly the longest successfully received message was captured despite the absence of direct line-of-sight between the transmitter and the receiver. In a previous test, the farthest received message still had a clear line-of-sight. This confirms the physical principles of wave propagation, where signals can still be transmitted without direct line-of-sight through reflection, diffraction, or bending around obstacles.

Another critical aspect to consider in secure communication is the proper use of encryption. When using AES in CTR mode, it is essential to use a unique IV for each encryption and add message authentication, since reusing IVs or omitting integrity checks can lead to plaintext recovery or message tampering.

VII. CONCLUSION

This scientific study examined the problem of secure data transmission using LoRa technology without the LoRaWAN protocol. Modern encryption algorithms that can be used to secure messages without adding redundant information were investigated. Furthermore, approaches to protecting transmitted data were proposed, considering the specific characteristics of LoRa, particularly its low data rate. Methods for optimizing message formats were also considered to minimize data overhead and improve communication efficiency.

Following the theoretical analysis, experimental tests were conducted to evaluate the maximum achievable data rate under standard device settings (77 bytes / second) and the maximum distance for transmitting encrypted information in a suburban environment (measured at 11.36 km).

This research can serve as a foundation for building custom long-range communication systems using LoRa devices in areas where other wireless technologies are not available.

References

[1] Foubert, B., & Mitton, N. (2020). Long-Range Wireless Radio Technologies: A Survey. *Future Internet, 12(1)*, 13. DOI: https://doi.org/10.3390/fi12010013.

[2] Tataria, H., Haneda, K., Molisch, A. F., et al. (2021). Standardization of propagation models for terrestrial cellular systems: A historical perspective. *International Journal of Wireless Information Networks,* 28, 20–44. DOI: https://doi.org/10.1007/s10776-020-00500-9.

[3] Natgunanathan, I., Fernando, N., Loke, S. W., & Weerasuriya, C. (2023). Bluetooth Low Energy Mesh: Applications, Considerations and Current State-of-the-Art. *Sensors, 23(4),* 1826. DOI: https://doi.org/10.3390/s23041826.

[4] Jouhari, M., Saeed, N., Alouini, M., & Amhoud, E. M. (2023). A survey on scalable LORAWAN for massive IoT: recent advances, potentials, and challenges. *IEEE Communications Surveys & Tutorials, 25(3),* 1841–1876. DOI: https://doi.org/10.1109/comst.2023.3274934.

[5] Bonilla, V., Campoverde, B., & Yoo, S. G. (2023). A Systematic Literature Review of LoRaWAN: Sensors and Applications. *Sensors, 23(20),* 8440. DOI: https://doi.org/10.3390/s23208440.

[6] Ertürk, M. A., Aydın, M. A., Büyükakkaşlar, M. T., & Evirgen, H. (2019). A Survey on LoRaWAN Architecture, Protocol and Technologies. *Future Internet, 11(10),* 216. DOI: https://doi.org/10.3390/fi11100216.

[7] Azevedo, J. A., & Mendonça, F. (2024). A critical review of the propagation models employed in LoRa systems. *Sensors, 24(12),* 3877. DOI: https://doi.org/10.3390/s24123877.

[8] Azim, A. W., Bazzi, A., Bomfin, R., Shubair, R., & Chafii, M. (2023). Layered Chirp Spread Spectrum Modulations for LP-WANs. *IEEE Transactions on Communications, 72(3),* 1671–1687. DOI: https://doi.org/10.1109/tcomm.2023.3331019.

[9] Mayer, K. M., Cottatellucci, L., & Schober, R. (2023). Optimal antenna placement for two-antenna near-field wireless power transfer. *ICC 2023 – IEEE International Conference on Communications, Rome, Italy,* 2135–2140. DOI: https://doi.org/10.1109/ICC45041.2023.10278773.

[10] Hikmaturokhman, A., Ramadhani, E., & Wulandari, A. (2025). Designing Data Communication Security System on LoRA Network Using PRESENT Algorithm. *Jurnal Telematika, 19,* 72–81. DOI: https://doi.org/10.61769/telematika.v19i2.674.

[11] Chi, D. V., Nguyen, K. D., Nguyen, L. T., Le, D. N., Luu, Q. H., & Huynh, S. T. (2022). Applying AES algorithm for secure data transmission between Sensor node and LoRa Gateway to Web Server. *Journal of Mining and Earth Sciences, 63(1),* 105–114. DOI: https://doi.org/10.46326/JMES.2022.63(1).10

[12] Sanchez-Iborra, R., Sánchez-Gómez, J., Pérez, S., Fernández, P. J., Santa, J., Hernández-Ramos, J. L., & Skarmeta, A. F. (2018). Enhancing LoRaWAN Security through a Lightweight and Authenticated Key Management Approach. *Sensors, 18(6),* 1833. DOI: https://doi.org/10.3390/s18061833.

[13] Mekki, K., Bajic, E., Chaxel, F., & Meyer, F. (2018). A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT Express, 5(1),* 1–7. DOI: https://doi.org/10.1016/j.icte.2017.12.005.

[14] Elshabrawy, T., & Robert, J. (2018). The Impact of ISM Interference on LoRa BER Performance. *IEEE Global Conference on Internet of Things (GCIoT),* 1–5. DOI: https://doi.org/10.1109/GCIoT.2018.8620142.

[15] Wiyadi, E., Setiadi, R. N., & Umar, L. (2020). Effect of vegetation profile and air data rate on packet loss performance of LORA E32-30 DBm 433 MHz as a wireless data transmission. *Journal of Physics Conference Series, 1655(1),* 012015. DOI: https://doi.org/10.1088/1742-6596/1655/1/012015.

[16] Thaenkaew, P., Quoitin, B., & Meddahi, A. (2023). Leveraging Larger AES Keys in LoRaWAN: A Practical Evaluation of Energy and Time Costs. *Sensors, 23(22),* 9172. DOI: https://doi.org/10.3390/s23229172.

[17] Cheng, Y., Saputra, H., Goh, L. M., & Wu, Y. (2018). Secure smart metering based on LoRa technology. *IEEE International Conference on Identity, Security, and Behavior Analysis (ISBA),* 1–8. DOI: https://doi.org/10.1109/ISBA.2018.8311466.

[18] Mathe, S. E., Kondaveeti, H. K., Vappangi, S., Vanambathina, S. D., & Kumaravelu, N. K. (2024). A comprehensive review on applications of Raspberry Pi. *Computer Science Review, 52,* 100636. DOI: https://doi.org/10.1016/j.cosrev.2024.100636.

[19] Smith, S. (2024). Programming GPIO PINs. *Apress eBooks* 163–187. DOI: https://doi.org/10.1007/979-8-8688-0137-2_8.

[20] Lata, K., Chhabra, S., & Saini, S. (2021). Hardware–Software Co-Design framework for data encryption in image processing systems for the Internet of things environment. *IEEE Consumer Electronics Magazine, 11(4),* 92–97. DOI: https://doi.org/10.1109/mce.2021.3115999.

[21] Lemire, D. (2021, September). Unicode at Gigabytes per Second. In *International Symposium on String Processing and Information Retrieval* (pp. 13–18). Cham: Springer International Publishing. DOI: https://doi.org/10.1007/978-3-030-86692-1_2.

[22] Celaya-Echarri, M., Azpilicueta, L., Lopez-Iturri, P., Picallo, I., Aguirre, E., Astrain, J. J., Villadangos, J., & Falcone, F. (2020). Radio wave propagation and WSN deployment in complex utility tunnel environments. *Sensors, 20(23),* 6710. DOI: https://doi.org/10.3390/s20236710.

Nazarii Yuzvak is a student at Lviv Polytechnic National University, enrolled in the Cybersecurity program since 2021. His academic and professional interests lie in the fields of software development and cybersecurity. He is particularly passionate about Python programming and is actively involved in projects related to secure communication and applied cryptography.

Roman Banakh, the author, was born in Lviv, Ukraine, in 1992. He received his B. S. and M. S. degrees in information security at Lviv Polytechnic National University in 2014 and his Ph.D. in cybersecurity at Lviv Polytechnic National University in 2024. From 2020 to 2023, he was an assistant professor at the Security of Informational Technologies department of Lviv Polytechnic National University. Starting in 2024, he became a senior lecturer at Lviv Polytechnic National University. His research interests include cloud computing, informational and communication systems on high load, security of IoT, and computer system architecture.

Abdallah Ibrahim earned a B. Sc. in Computer Engineering from Suez Canal University in 2010, followed by two M. Sc. degrees in Computer Sciences–one in 2012 from Suez Canal University and another in 2015 from the University of Luxembourg. During his studies, he collaborated onses for undergraduate students. Research interests: physics and astronomy, international projects at prominent research centers like Luxembourg's SnT and Poland's PSNC. Since 2015, he has been with the University of Luxembourg's SnT, focusing on Cloud Computing, SLA, QoS, and SaaS performance. In 2019, he completed a Smart ICT diploma in collaboration with ILNAS, Dell EMC, and the University of Luxembourg. His research interests include Cloud and Edge Computing, QoS, Industry 4.0, smart mobility, optimization, and machine learning. He also represents Luxembourg in ISO technical committees on Cloud and IoT standards and is engaged in tech start-up formation and validation.