ISBN: 978-981-94-4198-3
2025 the 15th International Workshop on Computer Science and Engineering (WCSE 2025)
doi: 10.18178/wcse.2025.06.037

A large-scale LPWAN Architecture for Multimedia Data Collection in High-security Challenge Areas

OUATTARA Yacouba [1], TRAORE Mamoutou [2,3] + and PODA Pasteur [2]

[1] Universite Joseph KI-ZERBO, Ouagadougou, BURKINA FASO
[2] Universite Nazi BONI, Bobo-Dioulasso, BURKINA FASO
[3] Centre d'Excellence Interdisciplinaire en Intelligence Artificielle pour le Développement (CITADEL), BURKINA FASO

Abstract. The Internet of Things (IoT) is rapidly expanding, including in conflict zones where security is critical. Sound signals used for intelligence in the Middle East, combined with Sahel challenges from poor infrastructure, emphasize the need for better data collection. This paper proposes a secure IoT architecture using Low Power Wide Area Network (LPWAN) technology and steganography to efficiently optimize sharing of critical information and enhance military operational efficiency. Based on surveys with military personnel and reviews of existing IoT methods, our solution leverages LPWAN's range, low energy, and cost benefits to address security and resilience challenges in high-risk regions globally.

Keywords: LPWAN, LoRaWAN, Architecture, Design, Terrorism, Steganography, Military.

1. Introduction

The Internet of Things (IoT) has garnered significant research interest due to challenges in its design and architecture, notably the diverse languages, protocols, and standards, and the lack of a unified standardization platform [1]. Foundational studies propose a four-layer IoT architecture and highlight that Layer 2, the Gateway and Network Layer requires a robust network, yet specific solutions remain elusive, as noted by CISCO and Edge [2]. Connectivity and network security are crucial for handling critical data [3,4].

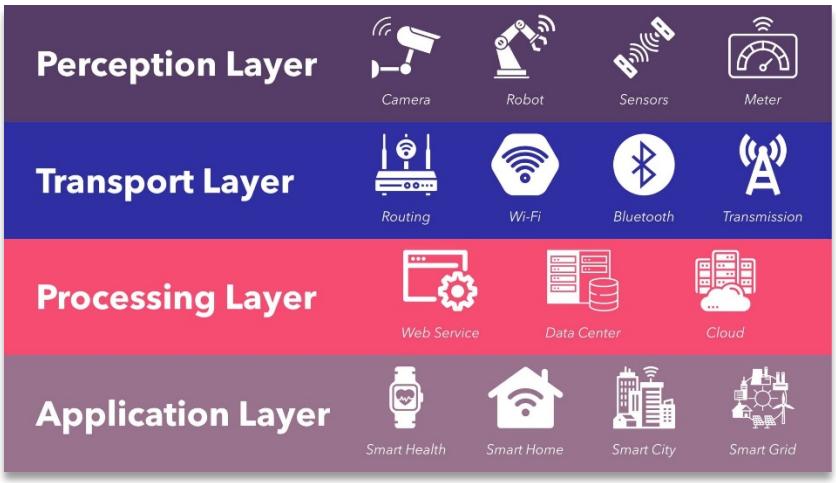

Fig. 1: Architecture of an IoT solution [2]

In the Sahel, where combating terrorism is a priority, reliable real-time information is hampered by logistical challenges. Here, a large-scale, secure IoT network using LPWAN technologies (e.g., Sigfox, LoRaWAN, Nb-IoT, LTE-M) offers promising opportunities to enhance surveillance and counter-terrorism efforts [5].

Corresponding author. Tel.: + (226) 66 12 98 24.
E-mail address: mamoutoutraore.sa@gmail.com.yacouattt@yahoo.fr, mamoutoutraore.sa@gmail.com, pasteurpoda@yahoo.fr

2. Materials and Methods

2.1. Study of Some Concepts

Here are some key concepts for the rest of our study:

- LPWAN Technologies: Low-power wide-area networks connect IoT devices over large areas with minimal energy use, ideal for low-data-rate environments with extended battery life [6].
- LoRaWAN: An LPWAN protocol based on LoRa, enabling long-distance, low-power data transmission and efficient management of numerous devices [6].
- Steganography: A method of concealing information within media (images, videos, audio) to discreetly enhance data security.
- IoT (Internet of Things): Encompasses connected devices that collect, share, and analyze data, improving real-time decision-making across industries [7].
- Gateway: A device that connects IoT sensors to larger networks by translating various IoT protocols (e.g., LoRa, ZigBee, Bluetooth) into IP protocols [8].
- SenseCAP A1101 LoRaWAN Vision AI Sensor: A smart sensor using LoRaWAN for AI-driven data transmission, suitable for environmental monitoring, security, and automation.
- Network Server: Central to IoT architecture, it receives, authenticates, processes, and routes data from devices through gateways, ensuring effective communication with higher-level systems [10].

These concepts are critical for establishing secure, optimized infrastructures where long-distance connectivity, security, and energy efficiency are essential [9].

2.2. Survey

Designing an LPWAN network for information gathering in terrorism-prone Sahel regions requires a systematic approach, starting with a detailed military survey. This step gathers precise data on the operational needs and environmental constraints specific to these sensitive areas, as identified during military meetings (see Figs. 2 and 3).

- **Identify Terrorist Groups.**
- **Spoken Language:** Serve as a cultural marker.
- **Dress Style:** Indicate group affiliation.
- **Communication Frequency:** Analyse habits.
- **Movement Radius:** Define monitoring zones.
- **Travel Time:** Assess speed.
- **Alert Signs:** Detect indicators like donkey debris in deserted areas or ground marks after explosive burial.

Fig. 2: Classification of Survey Elements by Category (source military)

Fig. 3: Data on image collection for our study (Military source)

Based on the survey, deploying a large-scale IoT network with carefully chosen sensors is essential to gather critical information for these scenarios:

- **Identifying Suspicious Individuals:** The network should capture data on dress style, equipment (with registration details), and the presence of individuals with livestock or weapons [11].
- **Scanning Communication Frequencies:** IoT devices can periodically transmit data, enabling analysis of communication patterns to infer activities and intentions [12].
- **Monitoring Movements and Hazardous Activities:** The network must track movements in sensitive areas, detecting suspicious gatherings or behaviours for prompt intervention [13].

2.3. Design Objectives

LPWAN architectures target energy efficiency, extended range, scalability, cost-effectiveness, interference management, and integration key factors for evaluating their suitability [14]. Selection criteria include power consumption, range, location, data throughput, installation, bandwidth, cost (including free or low-cost private/operated options), bidirectionality, and geolocation.

In addition to these, this work pursues two main goals:

- **Enhancing Data Confidentiality:** employ steganography to hide messages a resource-efficient alternative to cryptography that optimises sensor performance [55].
- **Ensuring Sensor Physical Security:** protect sensors from intrusion and extreme weather using IP67/IP68 enclosures and concealed deployment to minimise sabotage risk [56].

2.4. Related Works

Mattia Ragnoli et al. [15] propose a multi-technology LoRaWAN architecture for real-time monitoring of worker safety and structural integrity on construction sites, integrating sensors, RFID, solar-powered nodes, and an IoT platform.

Mehmet Ali Ertürk et al. [16] review LoRaWAN's architecture, protocols, and use cases while highlighting research opportunities in deployment optimisation, network management, and interoperability.

Gaia Codeluppi et al. [17] introduce LoRaFarM, a modular IoT architecture for sustainable agricultural management, validated on an Italian farm via environmental data collection and web visualisation.

Kun-Lin Tsai et al. [18] present the Low-Power AES Data Encryption Architecture (LPADA) for LoRaWAN, reducing dynamic and leakage power by 62% and 88.5% respectively, while enhancing security through key updates.

Jhonattan J. Barriga et al. [19] propose a smart parking solution using LoRaWAN sensors and a Kubernetes cluster, integrated with REST APIs and web/mobile applications for real-time management.

Antonio Cilfone et al. [20] propose a container-based architecture to virtualise LoRaWAN end nodes into IP-compatible networks via CoAP, ensuring seamless communication.

Massimiliano Gaffurini et al. [21] develop an emulation platform using container-based virtualisation to assess LoRaWAN's scalability and performance in smart cities.

Maram Alkhayyal and Almetwally Mostafa [22] review AI and ML advancements to optimise energy efficiency and performance in LoRaWAN networks, while **Hyungsub Kim et al.** [23] propose a hybrid architecture that switches between LoRaWAN and LoRa mesh modes based on conditions.

Pietro Spadaccino et al. [24] examine AI and ML integration in LoRaWAN to enhance energy efficiency and resource utilisation. **Ramakant Kumar** [25] integrates LoRaWAN with MANET networks to improve campus communication, focusing on range, energy efficiency, and adaptability.

André Proto et al. [26] introduce a lightweight intrusion detection system based on sensor energy consumption for LoRaWAN. **Min Chen et al.** [27] propose a cognitive architecture for stable and efficient communications in heterogeneous IoT environments.

Hatem A. Alharbi et al. [28] explore UAV drones for optimising unloading decisions. **Mr Djibrilla Incha Adamou** [29] studies the physarum fungus, inspiring simplified data collection methods that consider

collection point capacity and reduce collection times. **Ben Buurman and Gour Karmakar** [14] analyse methods for designing context-specific architectures.

The reviewed studies collectively address data collection and transmission challenges through innovative architectures, efficient mobility models, drone integration, and structured design approaches. Building on these insights, the proposed architecture integrates AI sensors for multimedia collection secured by steganography, uses drones as gateways for wide-area transmission, and optimises energy consumption and mobility management to offer a comprehensive solution.

2.5. Comparative Analysis

The comparison table is separated into comparison of licensed spectrum (Table 1) and unlicensed (Table 2) spectrum.

Table 1: Detailed comparison of licensed spectrum LPWAN technologies [30–37]

LPWAN	3GPP Energy-Saving Techniques	NB-IoT	LTE-M	EC-GSM
Description	Energy saving techniques used in 3GPP LPWAN protocols	3GPP cellular standard offering low data transmission speed, long range and low power consumption	3GPP standard providing high-performance networks to a limited number of devices, with broadband capabilities	Uses existing GSM and GPRS infrastructure for IoT, enhancing coverage, security and energy efficiency
Business model	Subscriber-driven	Subscriber-driven	Subscriber-driven	Subscriber-driven
Urban scope	1 to 5 km (700 MHz)	1 to 2 km	1 to 10 km	3 to 5 km
Rural scope	5 to 15 km (700 MHz)	Less than 100 km	Up to 100 kilometers	Up to 35 km
Topology	Star	Star	Mainly star and sometimes mesh	Star
Data rate	Data Rate and Throughput Limitations	Up to 250 kbps	High speed (1 Mbps)	Bitrates from 350 bps to 240 kbps
Access method	Temporal diversity to improve reach	Narrow spectrum, OFDMA, Random access, Power control, Power control	OFDMA	ALOHA
Security	AES	AES & MAC	AES & HMAC	A5 encryption
Features	Periodic transceiver deactivation, information caching	UNB modulation, LTE-based architecture, various deployment modes	LTE-based architecture, improvements for version 14	Use of existing GSM and GPRS infrastructure, high potential presence

Table 2: Detailed comparison of unlicensed spectrum LPWAN technologies [35], [38–44]

LPWAN	SigFox	LoRaWAN	Weightless-IoT	NB-Fi	DASH7 (D7AP)
Description	French subscriber-focused organization	Open standard focused on manufacturing	Family of standards with different penetration attempts	Standard developed by the NB-Fi and WAVIoT alliance	Protocol developed by the DASH7 Alliance (D7AP)
Business model	Subscriber-driven	Manufacturing Focused	Flexible deployment approach tailored to specific needs	Public, private and enterprise networks managed by WAVIoT	User-managed private networks
Urban scope	5 km	5 km	2-5 km	16.6 km (estimate)	500 m to 2 km
Rural scope	Several dozen kilometers	15-25 km	About 25 km	Greater than 10km	Up to 5 km
Topology	Star	Star	Flexibility in network design	Star	Star
Data rate	Variable (usually 100 bps)	Up to 50 kbps	Variable (typically 11 bps)	Minimum: 11 bps, Accepted: 50-25600 bps	Variable to a few hundred kbps
Access method	Strict message transmission policies	Mechanisms to avoid congestion and interference	TDMA	Random access with narrow modulation	Different methods of communication
Security	Optional AES-128 encryption	Mechanisms to ensure data security	AES	AES-128	AES
Features	Using compatible radio transceivers	Classification of devices into three categories according to their ability to receive downlink messages	Using different standards for different bands	Adjustable transmit power, 30 seconds uplink and 60 seconds downlink latency	Using D7AP protocol, BLAST concepts, variable size data frames, API simplifying network addressing

Given the requirements, LoRaWAN is the optimal connectivity choice for our case study [45] because it offers an affordable total cost of ownership, resilient end-to-end security, two-way communication, up to 15 years of battery life, ensured standards compliance and interoperability, robust coverage, and flexible deployment models.

However, technologies using licensed spectrum face major challenges, particularly due to their complexity and high total cost of ownership.

2.6. Optimal Technical Choices

For a large-scale LoRaWAN architecture with the Sense-CAP A1101 LoRaWAN Vision AI sensor, it is recommended to use multi-channel gateways such as the **RAK7249 WisGate Edge Pro** [46] for a cost-effective solution or the **Kerlink Wirnet iStation** [47] for enhanced robustness and range. The network server can be based on an open-source solution like **ChirpStack** [48], ideal for low-cost local deployments, or a cloud platform such as The Things Stack for greater simplicity and scalability. Lastly, for processing steganographed data, a local solution such as a **Raspberry Pi 4 paired with a Coral AI module** [49] is suitable for light workloads, while a cloud service like **AWS IoT Core with SageMaker** [50] is more appropriate for advanced large-scale analyses. This configuration ensures a balance between cost, performance, and scalability for the network.

3. Results

In a country at war, combat zones extend over several kilometres. Certain areas lack the essential equipment needed for loyalist fighters to use advanced technologies against enemy offensives. Moreover, communication between these zones is nearly non-existent, hampering both humanitarian aid efforts and troop coordination. To address these challenges, we propose deploying a LoRaWAN architecture designed to efficiently manage these combat zones. This infrastructure will be reinforced by aerial vehicles equipped with LoRaWAN mini-receivers, which will collect and transmit data to a central server for thorough analysis and processing.

3.1.Proposed LoRaWAN Architecture

In this section, we will present in detail the LoRaWAN architecture of our network, developed following an in-depth survey conducted with the military. This architecture is the result of a careful analysis of the specific operational needs identified during the survey, thus ensuring a solution perfectly adapted to the requirements of the field in areas at risk of terrorism (Fig. 4.) [51] [52].

3.2.Process of Collecting Information by Sensors

In our approach, we have designed an architecture covering a wide range of zones, from area A to area n (where n represents the total number of monitored area), using zones A and B as examples. As shown in the diagram, we employ AI-enabled SenseCAP A1101 LoRaWAN Vision sensors, which incorporate artificial intelligence to enhance network efficiency. [9].

The nodes of these sensors collect key data, such as images and audio recordings. When an image is captured, it is first processed using steganography before being sent to the gateway, which then transmits it to the network server. The server directs the image to the processing centre, where an inverse algorithm is applied to restore the image to its clear form, enabling analysis and interpretation.

Furthermore, it will be possible to track the movements of soldiers in real time, thanks to sensors that record events and transmit data to the gateways following the same transmission process. Additionally, patrol drones deployed in the monitored zones will be able to connect to the sensors and exchange information in real time, thereby optimising surveillance (see Fig. 4.).

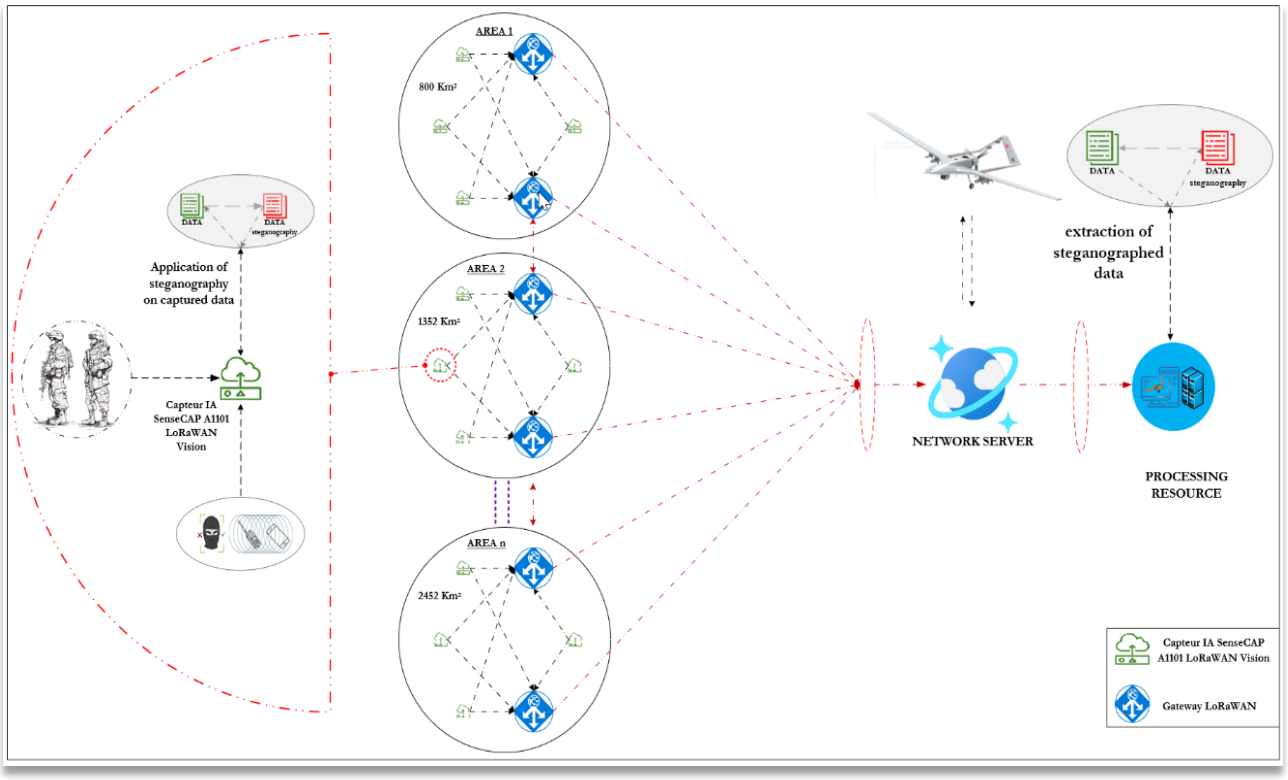

Fig. 4: Architecture design seen from the plan in our LoRaWAN network

4. Discussion

The basic LoRaWAN architecture reliably transmits data over long distances with minimal energy consumption, making it ideal for remote or low-infrastructure areas. It comprises sensors (nodes), gateways, a network server, and data processing applications to collect and send simple data (e.g., temperature, humidity, location) to a central server [53].

The SenseCAP A1101 LoRaWAN Vision AI sensor advances traditional sensors by integrating AI to capture and process complex data (e.g., images, audio) at the source, reducing transmission volume, optimising bandwidth, and lowering latency [9]. Integrating steganography further compresses and secures data before transmission, enhancing confidentiality in high-risk environments.

In areas 1 and 2 facing terrorist threats, the SenseCAP A1101 offers significant benefits [54]:

- **Enhanced accuracy:** Visual and audio capabilities deliver detailed situational data.
- **Optimised resources:** Local AI processing reduces bandwidth usage and boosts efficiency.
- **Improved security:** Steganography ensures secure data transmission.
- **Energy efficiency:** Low power consumption ensures extended autonomy.

Integrating AI-enabled sensors within a broader architecture is innovative. Using drones as gateways ensures extensive coverage and reliable transmission, even in isolated areas. Key elements include:

- **Secure multimedia collection:** AI sensors gather rich data while steganography protects its confidentiality.
- **Energy optimisation:** Reduced energy consumption in isolated nodes promotes extended autonomy.
- **Advanced mobility management:** Mobile drones optimise connection management in high-mobility areas.

Additionally, integrating LoRaWAN receivers on fighter jets and ground units offers dual functionality real-time surveillance and enhanced strategic analysis. This unified approach overcomes traditional LoRaWAN limitations, delivering a comprehensive, resilient solution tailored to current security and data management needs.

5. Conclusion

The fight against terrorism in the Sahel demands real-time, accurate data despite significant logistical and technological challenges. In this paper, we have detailed these issues and proposed an LPWAN network design. Our rigorous methodology allowed us to identify military needs in these sensitive areas and develop a large-scale IoT architecture, optimised and secured with steganography algorithms.

After reviewing related work and comparing LPWAN technologies, we concluded that LoRaWAN is the optimal choice for our case study, given its cost-effectiveness, security, battery life, and deployment flexibility. We also explore the potential of the SenseCAP A1101 LoRaWAN Vision AI sensor to address resource challenges, thereby providing a robust, scalable solution.

Our proposed LoRaWAN architecture, tailored to military requirements in the Sahel, offers an efficient solution for information gathering, enhancing terrorism surveillance and prevention. Future work will involve simulating the architecture to assess its real-world feasibility in terms of coverage, capacity, energy consumption, throughput, latency, reliability, and scalability.

6. Acknowledgements

This work was partially supported by the IDRC, AI4D and SIDA through their funding of the activities of the “Centre d’Excellence Interdisciplinaire en Intelligence Artificielle pour le Développement” (**CITADEL)**.

7. References

[1] Nahit Pawar. Conception d’une architecture complète pour l’inter-operabilité des objets connectés hétérogènes et des services de l’Internet des Objets. *PhD thesis, Institut Polytechnique de Paris, 2021.*

[2] Adam Simmons *covers Towers for Dgtl Infra, including American Tower (NYSE: AMT).* Technology: Internet of Things (IoT) Architecture: Layers Explained. *November 13, 2022*

[3] Iheb HAFDALLAH. Un modèle décentralisé basé sur la Blockchain pour les environnements IoT sécurisés. *PhD thesis, Université Echahid Chikh Larbi Tébessi-Tébessa, 2023.*

[4] Yousra Mahmoudi. Optimisation avancée des réseaux de capteurs intelligents dans les technologies d’Internet des objets. *PhD thesis, Universite´ du Québec à Trois-Rivières, 2024.*

[5] Silvio Gerard. How LPWAN technologies empower the future of IoT connectivity, 2023-06-29. Section: LoRa Basic.

[6] Juan Pablo Becona, Marcel Grané, Matias Miguez, and Alfredo Arnaud. Lora, Sigfox, and NB-IoT: An empirical comparison for IoT LPWAN technologies in the agribusiness. IEEE Embedded Systems Letters, 2024.

[7] Abdennabi Morchid, Rachid El Alami, Aeshah A Raezah, and Yassine Sabbar. Applications of internet of things (iot) and sensors technology to increase food security and agricultural sustainability: Benefits and challenges. *Ain Shams Engineering Journal, 15(3):102509, 2024.*

[8] Noelia Caballero-Casero, Ana M Ballesteros-Gomez, and Soledad Ru-bio. Supramolecular solvents: a gateway to all-in-one extractions in chemical exposomics. *Analytical and Bioanalytical Chemistry, pages 1–9, 2024.*

[9] William Fabre, Karim Haroun, Vincent Lorrain, Maria Lepecq, and Gilles Sicard. From near-sensor to in-sensor: *A state-of-the-art review of embedded ai vision systems. Sensors, 24(16):5446, 2024.*

[10] Bindu Bala and Sunny Behal. Ai techniques for IoT-based DDOS attack detection: *Taxonomies, comprehensive review and research challenges. Computer science review, 52:100631, 2024.*

[11] Hoe Tung Yew, Frederick Siong Chang, Keh Nguang Png, Teck Sian Chan, Choon Wei Wong, Lumbanon Yu Peng Lim, and Vincent Hung Jie Tiew. *Internet of things: Applications, challenges, and future trends. In Internet of Things and Artificial Intelligence for Smart Environments,* pages 1–18. Springer, 2024.

[12] Sonile K Musonda, Musa Ndiaye, Hastings M Libati, and Adnan M Abu-Mahfouz. Reliability of LoRaWAN communications in mining environments: *A survey on challenges and design requirements.* Journal of Sensor and Actuator Networks, 13(1):16, 2024.

[13] N Shivaanivarsha, AG Vijayendiran, and A Sriram. LoRaWAN based smart safety helmet with protection mask for miners. *In 2024 International Conference on Communication, Computing and Internet of Things (IC3IoT),*

pages 1–6. IEEE, 2024.

[14] Gour C. Karmakar Syed Muhayminul Islam Ben Buurman, Joarder Kamruzzaman. (PDF) low-power wide-area networks: Design goals, architecture, suitability to use cases and research challenges.

[15] Ragnoli Mattia, Davide Colaiuda, Alfiero Leoni, Giuseppe Ferri, Gian-luca Barile, Marianna Rotilio, Eleonora Laurini, Pierluigi De Berardinis, and Vincenzo Stornelli. A LoRaWAN multi-technological architecture for construction site monitoring. Sensors, 22(22):8685, 2022.

[16] Mehmet Ali Ertürk, Muhammed Ali Aydın, Muhammet Talha Buyükakkaslar, and Hayrettin Evirgen. *A survey on LoRaWAN architecture, protocol and technologies.* Future internet, 11(10):216, 2019.

[17] Gaia Codeluppi, Antonio Cilfone, Luca Davoli, and Gianluigi Ferrari. *Lorafarm: A LoRaWAN based smart farming modular iot architecture*. Sensors, 20(7):2028, 2020.

[18] *Kun-Lin Tsai, Fang-Yie Leu, Ilsun You, Shuo-Wen Chang, Shiung-Jie Hu, and Hoonyong Park. Low-power AES data encryption architecture for a LoRaWAN.* IEEE Access, 7:146348–146357, 2019.

[19] Jhonattan J Barriga, Juan Sulca, José Léon, Alejandro Ulloa, Diego Portero, José Garcia, and Sang Guun Yoo. A smart parking solution architecture based on LoRaWAN and kubernetes. Applied Sciences, 10(13):4674, 2020.

[20] Antonio Cilfone, Luca Davoli, and Gianluigi Ferrari. Lora meets IP: a container-based architecture to virtualize LoRaWAN end nodes. *IEEE Transactions on Mobile Computing, 2024*.

[21] Massimiliano Gaffurini, Alessandra Flammini, Paolo Ferrari, Dhiego Fernandes Carvalho, Eduardo Paciencia Godoy, and Emiliano Sisinni. *End-to-end emulation of LoRaWAN architecture and infrastructure in complex smart city scenarios exploiting containers.* Sensors, 24(7):2024, 2024.

[22] Maram Alkhayyal and Almetwally Mostafa. Recent developments in ai and ml for IoT: *A systematic literature review on LoRaWAN energy efficiency and performance optimization*. Sensors, 24(14):4482, 2024.

[23] Hyungsub Kim, Hayoung Kim, Somi Baek, Ryan Melenchuk, Jaden Soroka, and Anthony Smith. Hybrid lora network architecture: Automatic switching between LoRaWAN and lora mesh network in environments with dynamic obstacle variations. *In 2024 33rd International Conference on Computer Communications and Networks (ICCCN), pages 1–6. IEEE, 2024*.

[24] Pietro Spadaccino, Domenico Garlisi, Andrea Franceschi, Ilenia Tinnirello, and Francesca Cuomo. Accelerating network resource allocation in LoRaWAN via distributed big data computing. *IEEE Access, 2024.*

[25] Ramakant Kumar. Integrating LoRaWAN with mobile ad-hoc networks for enhanced campus communication. *arXiv preprint arXiv:2410.19708, 2024*.

[26] André Proto, Charles Christian Miers, and Tereza Cristina MB Carvalho. An intrusion detection architecture based on the energy consumption of sensors against energy depletion attacks in LoRaWAN. *In IoTBDS, pages 268–275, 2024.*

[27] Min Chen, Yiming Miao, Xin Jian, Xiaofei Wang, and Iztok Humar. Cognitive-LPWAN: *Towards intelligent wireless services in hybrid low power wide area networks, 2018-09-30.*

[28] Hatem A Alharbi Barzan Yosuf Jaber Almutairi, Mohammad Aldos-sary. (PDF) delay-optimal task offloading *for UAV-enabled edge-cloud computing systems. 2024-10-22.*

[29] Djibrilla Incha Adamou. Data collection networks for extended white zones, 2019-11-29.

[30] Marceau Coupechoux and Philippe Martins. Evolution et standardisation des infrastructures radiomobiles cellulaires du 3GPP: du GMS à l'umts. *In Vers les systèmes radiomobiles de 4e génération, pages 1–21. Springer, 2013.*

[31] Tifrani Fawzi and Toumert Said. Etude et dimensionnnement d'un réseau multiservices 3GPP (UMTS). PhD thesis, *Université Mouloud Mammeri, 2015*.

[32] Romain Barbau. Performances des réseaux NB-IoT terrestres et satellites. *PhD thesis, Institut National Polytechnique de Toulouse-INPT, 2022*.

[33] Bachir HAIL, Encadré par MOUSSA, and Mohamed Amine. Station de Mesure IoT pour la Surveillance des Données d'un Parc Photovoltaïque. *PhD thesis, UNIVERSITE DE ECHAHID CHEIKH LARBI TEBESSI, 2024.*

[34] Hugo Raps, Nathan Cornelie, Thom Guillot, Eddy Bajic, and Kais Mekki. Etude expérimentale des performances

de communication LTE-M pour l'internet des objets industriels. *In Colloque sur les Objets et Systèmes Connectés, COC'2023, 2023.*

[35] Sébastien Maudet. Analyse et modélisation énergétiques des réseaux de communications pour l'IoT. *PhD thesis, Nantes Université, 2024.*

[36] Alexis Bitaillou, Benoît Parrein, and Guillaume Andrieux. Synthèse sur les protocoles de communication pour l'Internet des objets de l'industrie 4.0. *PhD thesis, LS2N, Université de Nantes; IETR, Université de Nantes, 2019.*

[37] Anthony JUTON. Réseaux très basse consommation, longue portée, bas débit, *l'exemple de LoRaWAN. Revue 3EI, 2019.*

[38] Rejané Dalcé, Imen Megdiche, Thierry Val, and Khawla Ltifi. Une canne connectée LoRaWAN, wifi et ble pour le suivi des personnes âgées. *In JETSAN 2021-Colloque en Télésanté et dispositifs biomédicaux-8ème édition, 2021.*

[39] Norhane Benkahla. Gestion de la qualité de service (QoS) dans un réseau LoRaWAN avec mobilité. *PhD thesis, Ecole Supérieure des Communications de Tunis, 2021.*

[40] Daniele Christiane Kedy Koum, Charlotte Eposse, Ritha Mbono Betoko, Zeinabou Ismaila, Loick Pradel Kojom Foko, Carine Laure Njanseb Nembot, and Calixte Ida Penda. Compte rendu des 4èmes journées scientifiques de la société camerounaise de médecine périnatale, février 2023. *African Journal Perinatology Vol, 1(1):80–89, 2024.*

[41] Daniel N do Nascimento and Felipe MG França. Object modelling through weightless tracking. *Neural Computing and Applications, 36(17):10257–10278, 2024.*

[42] Natalia Gorodnova and Yelena Shablova. Development of the industrial internet of things in Russia and China: Economic and legal aspects. *In BIO Web of Conferences, volume 138, page 02018. EDP Sciences, 2024.*

[43] Wael Ayoub, Abed Ellatif Samhat, Fabienne Nouvel, Mohamad Mroue, and Jean-Christophe Prévotet. Internet of mobile things: Overview of LoRaWAN, dash7, and NB-IoT in LPWANs standards and supported mobility. *IEEE Communications Surveys & Tutorials, 21(2):1561–1581, 2018.*

[44] Wael Ayoub, Fabienne Nouvel, Abed Ellatif Samhat, Jean-Christophe Prevotet, and Mohamad Mroue. Overview and measurement of mobility in dash7. *In 2018 25th International Conference on Telecommunications (ICT), pages 532–536. IEEE, 2018.*

[45] Arnaud Delprat (Managing Director). *LoRaWAN France, 2022.*

[46] Francesco Pirotti, Marco Piragnolo, Marika D'Agostini, and Raffaele Cavalli. Information technologies for real-time mapping of human well-being indicators in an urban historical garden. *Future Internet, 14(10):280, 2022.*

[47] Joao Pinelo, André Dionisio Rocha, Miguel Arvana, Joao Gonc¸alves, Nuno Cota, and Pedro Silva. Unveiling lora's oceanic reach: *Assessing the coverage of the azores LoRaWAN network from an island. Sensors, 23(17):7394, 2023.*

[48] Sergio H Silva, Guilherme P Koslovski, Maur´ıcio A Pillon, and Charles Christian Miers. Credential lifecycle analysis in private LoRaWAN networks for industrial iot (iiot). *In IoTBDS, pages 157–165, 2024.*

[49] George Routis, Marios Michailidis, and Ioanna Roussaki. *Plant dis-ease identification using machine learning algorithms on single-board computers in IoT environments. Electronics, 13(6):1010, 2024.*

[50] Nikhil S Chougule, Chetan J Awati, and Rashmi Deshmukh. Using AWS sagemaker to deploy ml credit card fraud detection model. In 2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI), *pages 150–156. IEEE, 2024.*

[51] Nadjeh CHAOUA Bouthaina, DEFFAF. Routage en temps réel dans les réseaux de capteurs sans fil avec prolongation de la durée de vie du réseau dans le cadre de l'internet des objets. *2024-09-17.*

[52] BENOUDNINE SALAH. Intelligent system based on the internet of things for the fight against covid-19. *2022-11-08.*

[53] Axel von Arnim. Visual sensor for identification and optical communication between moving objects: from images to events. *Theses, University of the Côte d'Azur, March 2024.*

[54] Seeed Studio. Sensecap a1101 LoRaWAN vision ai sensor user guide. *2024. Version v1. 0.5.*

[55] H. K. Channi, « Real-Time Applications of Deep Learning-Based Steganography in IoT Networks », *in Enhancing*

Steganography Through Deep Learning Approaches, IGI Global Scientific Publishing, 2025, p. 331-360. doi: 10.4018/979-8-3693-2223-9.ch015.

[56] T. Tamilselvi; G. T. Bharathy; S. A. Saranya. « IoT based smart agricultural monitoring system ». AIP Conf. Proc. 3162, 020068 (2025) *https://doi.org/10.1063/5.0241516.*