From Isolated LPWAN Nodes to Secure IoT Data Integration: Bridging Low-Power Sensing and Network Segmentation in Agricultural Infrastructures*

Vladimír Voral[1,*,†], Pavel Ambruz[1,†], Pavel Šimek[1,†] and Jiří Vaněk[1,†]

[1] *Czech University of Life Sciences Prague, Faculty of Economics and Management, Kamýcká 129, 16500 Praha-Suchdol, Czechia*

Abstract

Internet of Things (IoT) technologies and Low-Power Wide-Area Networks (LPWAN) enable efficient data collection for environmental monitoring and precision agriculture. IoT sensors provide valuable measurements used, for example, in plant phenotyping, yet their integration into larger information infrastructures faces challenges related to heterogeneous data formats, limited standardization, and insufficient communication security. The aim of this contribution is to present an experimental model that links the transmission of sensor data via LPWAN technologies with a security architecture based on logical network segmentation and firewall routing rules. The model reflects the requirements of data standards commonly applied in plant phenotyping, particularly the Minimum Information About a Plant Phenotyping Experiment (MIAPPE) and the Breeding API (BrAPI). The results demonstrate that even basic segmentation significantly reduces unauthorized access without negatively affecting latency or the reliability of data transmission. At the same time, interoperability and the ability to share data in accordance with the FAIR principles (Findable, Accessible, Interoperable, Reusable) are preserved. The proposed approach thus provides a practical framework for the secure and standardized integration of IoT devices within agricultural and research infrastructures.

Keywords

LPWAN, IoT, segmentation, plant phenotyping, firewall, data interoperability, security

1. Introduction

Low-power wide-area network (LPWAN) technologies such as LoRaWAN and NB-IoT have become increasingly relevant for distributed sensing in agriculture, offering long-range communication and low energy consumption suitable for battery-powered field devices. These systems enable scalable monitoring of environmental parameters that influence plant growth, yet they frequently produce heterogeneous, non-standardized, and inconsistently encoded datasets. Such variability complicates their integration into established research infrastructures and data standards used in plant phenotyping. Moreover, many LPWAN sensor deployments lack essential security mechanisms, which further limits their applicability in larger multi-layer IoT architectures. Building upon previous work on LPWAN data quality and IoT network security, this paper examines how LPWAN sensing can be reliably integrated into broader IoT infrastructures while maintaining data integrity and enforcing appropriate security controls.

*ITS-2025: Information Technologies and Security, December 11, 2025, Kyiv, Ukraine

* Corresponding author.

† These authors contributed equally.

voral@pef.czu.cz (V. Voral); ambruzp@pef.czu.cz (P. Ambruz); simek@pef.czu.cz (P. Šimek); vanek@pef.czu.cz (J. Vaněk);

0009-0009-3195-189X (V. Voral); 0009-0001-6234-0620 (P. Ambruz); 0000-0001-9244-1476 (P. Šimek); 0000-0002-4573-5348 (J. Vaněk)

© 2025 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

CEUR Workshop Proceedings ceur-ws.org ISSN 1613-0073

published 2026-11-26

CEUR-WS.org/Vol-4337/paper6.pdf

1.1. Background and motivation

Low-power wide-area network (LPWAN) technologies, most notably LoRaWAN and NB-IoT, have become central to modern agricultural sensing due to their ability to support long-range communication at very low energy cost. These technologies enable battery-powered devices to operate in remote or distributed field environments without requiring continuous connectivity or mains power sources. LoRaWAN, operating in unlicensed ISM bands, provides a flexible and lightweight communication framework suited to remote sensor deployments, whereas NB-IoT leverages licensed cellular infrastructure to deliver higher reliability and more predictable quality of service. Both technologies have been widely adopted in experimental deployments aimed at monitoring environmental parameters essential to plant phenotyping and precision agriculture [8, 6].

Despite their technical advantages, LPWAN-based systems often produce measurements encoded in highly device-specific formats, ranging from raw binary payloads to compressed proprietary data structures. This lack of standardization leads to significant challenges in ensuring data interoperability, a key requirement in scientific domains where sensor outputs must be compared, integrated, or reused across platforms. In plant phenotyping, where standardized models such as MIAPPE define structured semantic descriptions of environmental conditions and plant traits, inconsistent LPWAN data formats limit automated ingestion and cross-platform analytics [1]. As a result, the value of these sensor deployments is reduced by manual preprocessing and transformation demands.

Compounding the issue of heterogeneous data formats is the limited security posture of many LPWAN deployments. While both LoRaWAN and NB-IoT offer certain built-in security mechanisms, their real-world implementations frequently lack additional layers such as network segmentation, secure routing, or end-device authentication. Especially in soil, air, and environmental monitoring, these devices often operate as unmanaged endpoints that transmit data without mutual authentication or encryption beyond the default configuration [7, 2]. This creates vulnerabilities that become critical when LPWAN sensors are integrated into larger IoT infrastructures spanning multiple users and data consumers.

Compounding the issue of heterogeneous data formats is the limited security posture of many LPWAN deployments. While both LoRaWAN and NB-IoT offer certain built-in security mechanisms, their real-world implementations frequently lack additional layers such as network segmentation, secure routing, or end-device authentication. Especially in soil, air, and environmental monitoring, these devices often operate as unmanaged endpoints that transmit data without mutual authentication or encryption beyond the default configuration [7, 2]. This creates vulnerabilities that become critical when LPWAN sensors are integrated into larger IoT infrastructures spanning multiple users and data consumers.

1.2. Problem statement

Although LPWAN technologies offer compelling advantages for agricultural sensing, their integration into complex IoT infrastructures remains challenging. The central problem addressed in this paper can be formulated as follows: How can LPWAN sensors be securely integrated into larger IoT networks composed of multiple layers, diverse user groups, and heterogeneous data services? This question reflects the growing need for interoperable and secure data acquisition pipelines as agricultural institutions increasingly adopt automated, data-driven methodologies.

Standard LPWAN architectures are generally designed as monolithic systems, where end devices communicate through gateways to a central network server without intermediate segmentation or differentiated access. While this architecture is efficient for simple deployments, it

becomes insufficient when LPWAN-generated data must coexist with other IoT components that require advanced security policies, routing rules, and role-based access. In such environments, the absence of segmentation exposes critical vulnerabilities, allowing any compromised endpoint or misconfigured sensor to potentially interfere with higher-level services [5, 3].

Moreover, LPWAN devices—often operating as unmanaged endpoints—lack robust mechanisms for authentication, key management, and controlled network entry. This is problematic for infrastructures where datasets must maintain strong integrity guarantees, especially when used in scientific contexts such as plant phenotyping or decision-support systems in precision agriculture. A single malformed or tampered payload transmitted by an unsecured LPWAN node can compromise analyses, introduce bias, or even disrupt automated control systems [4].

The goal of this paper is therefore to propose and evaluate an experimental integration model that combines LPWAN sensing with principles of network segmentation and basic firewall rules. By placing LPWAN devices into clearly defined network segments, restricting communication pathways, and enforcing structured data ingestion, the model aims to mitigate security risks while preserving the operational benefits of LPWAN communication. This approach contributes to improving data integrity, reducing attack surfaces, and facilitating the alignment of LPWAN-derived measurements with domain-specific data standards.

2. Related work

The development of modern agricultural IoT solutions highlights the growing need to connect standardized data collection with secure communication and network infrastructure. This chapter therefore provides an overview of related research in the areas of data standards, IoT network security principles, and practical approaches to low-cost segmentation [1].

2.1. Data standards and FAIR principles

In the field of plant phenotyping and environmental monitoring, several established data standards aim to ensure interoperability, long-term usability, and the sharing of scientific data. Among the most widely used are the MIAPPE, which defines the structure and metadata of phenotyping experiments, and the BrAPI, which provides an interface for unified access to phenotypic and genomic databases [9]. In medicine, a similar role is fulfilled by the Outcome Measures Framework (OMF), illustrating the broader need for data harmonization across disciplines.

A common foundation of these initiatives is the FAIR principles, designed to support efficient discovery, access, and reuse of data in automated research workflows. However, the application of FAIR principles is closely tied to data openness, which increases demands on data integrity, access control, and secure communication [10].

In the context of IoT sensors and LPWAN communication, these requirements present a significant challenge. Sensor data often use heterogeneous binary formats, vary in resolution and units, and are transmitted via communication technologies with limited bandwidth. Ensuring compliance with data standards is therefore not only a matter of format conversion but also of secure transport and protection of stored data. Consequently, openness and standardization increase the scientific value of data but also amplify security risks related to unauthorized access, manipulation, or integrity breaches during transmission and integration [11].

2.2. IoT network security and segmentation in agriculture

The security of IoT infrastructures in agriculture is often linked in the literature with network segmentation, firewall-based communication control, and endpoint protection [2, 3]. These

principles were also emphasized in previous research, which showed that a well-designed segmentation strategy and clearly defined routing policies can significantly reduce the risk of lateral movement and improve the overall clarity of the infrastructure. Essential security measures further include proper endpoint management, such as access restriction, authentication, and traffic monitoring [5].

Although these concepts form an important foundation for secure IoT communication, most existing approaches focus primarily on the macro-level of network architecture and on conventional enterprise environments. Agricultural infrastructures, however, consist of a highly heterogeneous set of components from simple sensors to gateways and cloud services—and their frequent weakness lies in the transmission of data originating from low-power LPWAN technologies [4, 8]. Current security models therefore only partially address the challenge of safely integrating sensor data that differ in payload size, granularity, and communication patterns [6].

This creates a gap in existing research, particularly regarding the relationship between network segmentation, communication security, and the characteristics of LPWAN data flows—an area that this paper aims to explore in greater detail [11].

2.3. Low-Cost segmentation in IoT infrastructure

Recent research activities indicate that even low-cost network segmentation can significantly enhance the security of IoT infrastructures, particularly in environments with limited technical resources [3]. Practical experiments with simple segmentation mechanisms show that basic logical separation of devices, complemented by minimal routing rules, can reduce attacker visibility and limit opportunities for lateral movement within the network [12]. These findings suggest that the added value of segmentation does not lie solely in advanced technologies, but rather in the thoughtful application of accessible and easily implementable mechanisms.

At the same time, most existing approaches focus primarily on access control between segments and on the behaviour of user or server devices. In environments with extensive use of IoT sensors and LPWAN communication, the integration of data flows, their protection during transmission, and the preservation of interoperability while maintaining security requirements remain less explored areas [4].

This contribution therefore builds upon the principles of low-cost segmentation but extends them towards the analysis of secure data transmission and processing, which is essential for infrastructures based on heterogeneous IoT and LPWAN devices [11].

3. Materials and methods

This section describes the experimental infrastructure that integrates data flows from IoT sensors using LPWAN communication with security mechanisms implemented through network segmentation. The chapter provides a detailed explanation of the methodology, the technologies involved, and the criteria used to evaluate the impact of the proposed approach.

3.1. Experimental setup overview

The experimental environment was designed to represent a typical low-cost IoT infrastructure using LPWAN communication for the transmission of environmental data. Two types of sensor devices were integrated into the system: the EM500-SMTC professional sensor for measuring soil moisture, temperature, and electrical conductivity [13], and the ePlant TreeTag device used for

monitoring trees, their growth, and local microclimatic conditions [14]. Both devices generate binary data packets with different levels of granularity, which are subsequently transmitted via LPWAN.

The communication layer consisted of two distinct LPWAN technologies LoRaWAN and Narrowband IoT (NB-IoT) allowing the comparison of transmission characteristics, latency, and reliability. LoRaWAN was included as a low-bandwidth long-range protocol [8], while NB-IoT provided a higher-reliability cellular alternative with different latency and payload characteristics [15]. This node then forwarded the communication to the server layer of the infrastructure.

The server layer was implemented using a local server responsible for receiving the data, decoding them into an internal representation, and storing them in a format compatible with the MIAPPE and BrAPI standards [9, 16]. The processed data were then prepared for further analysis or visualization within higher-level research or agronomic platforms [4].

From a data-flow perspective, the infrastructure can be described on Figure 1 as follows:

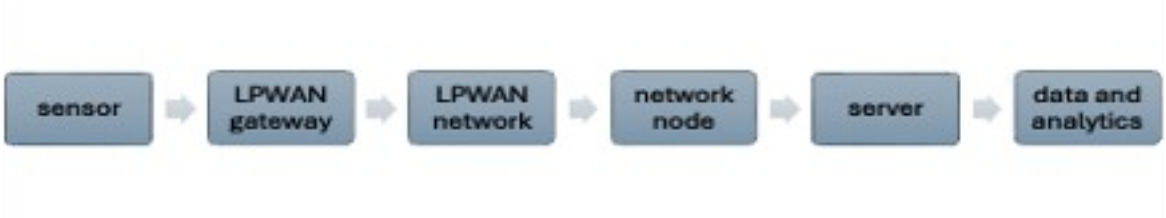


Figure 1: Data-flow of the impact of segmentation

This flow served as the foundation for subsequent experiments focused on evaluating the impact of segmentation on data security and availability [6].

3.2. Communication layer: LPWAN Integration

The communication layer of the experimental environment was based on LPWAN technologies, which enable the transmission of small data volumes over long distances with minimal energy consumption. Two technologies were used in the experiment—LoRaWAN and NB-IoT—each differing in data rate, latency, and maximum payload size. LoRaWAN typically supports transmissions in the range of several kilobits per second with a significantly limited payload [15, 17], while NB-IoT offers higher throughput and reliability, albeit at the cost of greater energy demand and reliance on mobile operator infrastructure [18].

Both technologies operate with binary data representation, which places high demands on the standardization of measured variables. In practice, different sensors vary not only in the ordering of items within the payload but also in resolution, units, and encoding schemes (e.g., 16-bit or 32-bit representations). These differences can complicate subsequent data processing, particularly when integrating measurements into higher-level data structures or when combining data from multiple device types [19].

To ensure interoperability, the study emphasized the transformation of data packets into formats compatible with the MIAPPE and BrAPI standards. This process included unit conversion, the addition of required metadata, and the mapping of individual parameters to structures defined by the corresponding ontologies [9, 16]. The resulting data layer enables secure and standardized transmission of measured values from LPWAN sensors into research and agronomic applications without loss of meaning or context.

3.3. Infrastructure Layer: Network segmentation

The infrastructure layer was designed to separate individual parts of the system according to their function and risk level. In line with principles presented in previous research, the network was divided into distinct segments comprising LPWAN sensors and gateways, the network and application server, the database layer, and the user access segment [2, 20]. This model reflects architectures commonly used in agricultural IoT systems, where it is essential to prevent direct communication between untrusted devices and critical infrastructure components [4].

Segmentation was implemented using Virtual LANs (VLANs) and complemented with Access Control Lists (ACLs) that defined specific communication paths between segments. LPWAN gateways were placed in an isolated segment with strictly limited access, allowing communication only with the server responsible for receiving incoming sensor data [3]. The application server operated within a dedicated segment that communicated solely with the database, while user workstations were fully isolated and allowed to access processed data exclusively through the application layer.

On the server layer, a set of firewall rules was defined to minimise lateral movement and permit only necessary types of communication [12]. Table 1 summarises the main rules applied in the experiment:

Table 1
Summary of the main rules

Source segment	Target segment	Allowed communication	Notes
LPWAN gateways	Application server	UDP/TC ports for data ingestion	One-way data flow
Application server	Database server	TCP 5432 (DB)	Service-level access
User segment	Application server	HTTPS	Access via application layer
User segment	LPWAN gateways	Denied	Prevents client-origin attacks
LPWAN gateways	Database	Denied	Prevents bypass of application logic
Database	User segment	Denied	Protects sensitive data

This segmentation creates a structure that significantly reduces the risk of unauthorised communication and limits the impact of potential breaches within individual network components [8]. At the same time, it does not restrict the essential data flow required for LPWAN sensor communication, which is critical for maintaining the overall functionality of the system.

3.4. Data flow and security validation

To evaluate the impact of network segmentation on the transmission of sensor data, an experiment was conducted focusing on monitoring data integrity, availability, and security throughout the entire path from LPWAN devices to the server layer. The tests were performed in

two infrastructure variants: a non-segmented topology ("flat LPWAN network") and the proposed segmented model with separated communication and application layers [6, 17]. The comparison enabled the evaluation of how segmentation influences data reliability, transmission behaviour, and system observability [4].

The key monitored metrics included packet loss rate, transmission latency between individual segments, and the detection of unauthorized access attempts. Packet loss was assessed by comparing the number of messages successfully received at the server with the number of sensor packets generated within a given time interval. Latency was measured as the difference between the moment the sensor transmitted the message and the moment it was processed by the server. The security portion of the experiment focused on probing communication paths outside the permitted routes, particularly attempts to access LPWAN gateways from the user segment or to establish direct communication between the gateway and the database [3, 12]. Such attempts were used to assess the level of lateral isolation provided by the segmentation structure.

The results showed that segmentation had no negative effect on data availability or integrity, and latency differences between the two topologies were negligible. In contrast, segmentation substantially reduced the visibility and reachability of critical components, which in the flat topology allowed potential unauthorized interactions. The segmented infrastructure therefore demonstrated higher resistance to unauthorized access while maintaining the full functionality of the LPWAN data flow [20, 8].

4. Results

4.1. Data integrity and latency impact

Across both LPWAN communication technologies (LoRaWAN and NB-IoT), the introduction of network segmentation did not negatively influence data integrity or overall transmission performance. Packet delivery rates remained stable in both configurations, with measured packet loss varying only within the normal operational range associated with the respective LPWAN technologies. The segmented topology showed no statistically significant deviations compared with the flat network, indicating that the separation of segments and the application of routing restrictions did not introduce additional communication bottlenecks.

Latency measurements confirmed this observation. The end-to-end transmission delay—measured from the sensor to the moment of successful ingestion on the server remained nearly identical in both topologies. Minor fluctuations (on the order of tens of milliseconds) were consistent with typical LPWAN network behaviour and did not correlate with the applied segmentation or firewall rules. These findings demonstrate that logical separation of the network does not compromise the timeliness of environmental monitoring data, even within energy-constrained LPWAN ecosystems.

4.2. Unauthorized access simulation

The security tests revealed clear differences between the two infrastructure variants. In the flat topology, LPWAN gateways and higher-level components were directly reachable from external segments, enabling unauthorized probing, port scanning, and attempted packet injection. The tests confirmed that, without segmentation, gateways can be targeted as potential entry points into the infrastructure.

In contrast, the segmented model effectively blocked lateral movement and prevented any unauthorized access attempts from the user segment or from misconfigured devices. ACLs and

firewall rules restricted communication strictly to defined paths, resulting in rejected connection attempts to the gateway and database segments. Furthermore, direct gateway-to-database communication was successfully blocked, ensuring that data ingestion could only occur through the application server. Visibility of critical assets was substantially reduced, demonstrating that even basic segmentation provides a robust security enhancement.

4.3. Interoperability and data reusability

The data transformation pipeline was able to process binary payloads into MIAPPE and BrAPI compliant structures without complications under both network conditions. Segmentation did not affect the formatting, annotation, or semantic integration of the data. Processed measurements remained fully compatible with FAIR principles, with metadata enrichment and standardized units preserved across the entire workflow.

The results show that communication-level restrictions do not interfere with higher-level data interoperability requirements. Instead, segmentation supports FAIR data sharing by protecting the integrity and traceability of transmitted measurements, ensuring that data entering research infrastructures remain trustworthy and reusable for scientific analysis.

5. Discussion

5.1. Interpretation of results

The findings indicate that the proposed segmentation model successfully strengthens security while preserving the functional characteristics of LPWAN communication. The negligible impact on latency and packet loss confirms that low-bandwidth technologies such as LoRaWAN and NB-IoT are compatible with more structured, security-oriented network architectures. This is particularly relevant for agricultural and research applications where data availability and reliability directly influence analytical outcomes.

At the same time, the substantial reduction in unauthorized access attempts highlights the vulnerability of flat LPWAN infrastructures. Segmentation constrains potential attack vectors and mitigates the risk associated with the deployment of heterogeneous, partially unmanaged sensor nodes. The approach therefore enhances system robustness without imposing additional communication or computational overhead.

5.2. Comparison with previous studies

Previous research in agricultural IoT security has emphasized the importance of segmentation and clear communication policies however, most studies focus on enterprise-level IT networks rather than LPWAN-based data acquisition systems. The present results expand these findings by demonstrating that even minimal segmentation measures implemented via VLANs and basic ACLs provide tangible benefits in environments that rely on long-range, low-power sensor networks.

In contrast to works primarily concerned with cryptographic mechanisms or protocol-level security, this study shows that structural network design plays an equally critical role in safeguarding data flows. Furthermore, the preservation of MIAPPE and BrAPI compatibility confirms and extends the conclusions of studies addressing interoperability challenges in plant phenotyping, reinforcing the argument that security and standardization can coexist without reducing data accessibility or performance.

5.3. Limitations and future work

This study presents an experimental integration model demonstrating that LPWAN-based sensor networks can be securely incorporated into larger IoT infrastructures through the application of basic network segmentation and firewall policies. The results confirm that such segmentation does not compromise data availability, integrity, or latency key parameters for agricultural and environmental monitoring. At the same time, segmentation substantially reduces unauthorized access and limits the exposure of critical components, thereby addressing common vulnerabilities associated with distributed LPWAN sensors.

Importantly, the proposed architecture maintains full interoperability with widely used plant phenotyping data standards, including MIAPPE and BrAPI, ensuring that sensor outputs remain FAIR-compliant and suitable for scientific reuse. The findings highlight that even low-cost, accessible security measures can meaningfully enhance the robustness of IoT infrastructures without inhibiting data sharing or the operational benefits of LPWAN communication.

The proposed model therefore offers a practical, scalable, and standards-aligned framework for deploying secure IoT infrastructures in agriculture and research environments.

Acknowledgements

The results and knowledge included herein have been obtained owing to support from the following institutional grant. Internal grant agency of the Faculty of Economics and Management, Czech University of Life Sciences Prague, grant no. IGA 2025A1012.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] Adam-Blondo, A., et al. (2024). [Details from your source — plant phenotyping data standards].

[2] Ambruz, P., Voral, V., Stočes, M., & Vaněk, J. (2024). Security aspects in the Agriculture IoT infrastructure: Network segmentation and security infrastructure perimeter. Proceedings of the 11th International Conference on ICT in Agriculture, Food & Environment (HAICTA 2024).

[3] Assistant Professor, Department of Management Studies, University of Kashmir, India, et al. (2023). Stout implementation of firewall and network segmentation for securing IoT devices. Indian Journal of Science and Technology, 16(33), 2609–2621. https://doi.org/10.17485/IJST/v16i33.1262

[4] Elijah, O., Rahman, T. A., Orikumhi, I., Leow, C. Y., & Hindia, M. N. (2018). An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges. IEEE Internet of Things Journal, 5(5), 3758–3773. https://doi.org/10.1109/JIOT.2018.2844296

[5] Mallik, A. (2019). Man-in-the-middle-attack: Understanding in simple words. Cyberspace: Jurnal Pendidikan Teknologi Informasi, 2(2), 109–134. https://doi.org/10.22373/cj.v2i2.3453

[6] Novák, V., Stočes, M., Čížková, T., Jarolímek, J., & Kánská, E. (2021). Experimental evaluation of the availability of LoRaWAN frequency channels in the Czech Republic. Sensors, 21(940). https://doi.org/10.3390/s21030940

[7] Stočes, M., Vaněk, J., Masner, J., & Pavlík, J. (2016). Internet of Things (IoT) in agriculture—Selected aspects. AGRIS on-line Papers in Economics and Informatics, 83–88. https://ageconsearch.umn.edu/record/233969/

[8] Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of Things for smart cities. IEEE Internet of Things Journal, 1(1), 22–32. https://doi.org/10.1109/JIOT.2014.2306328

[9] Pommier, C., Michotey, C., Cornut, G., Roux, C., Lopez-Mascaraque, L., Silva, V. D., … Boudiar, R. (2019). Applying FAIR principles to plant phenotypic data management in GnpIS. Database, 2019(1), baz146. https://doi.org/10.1093/database/baz146

[10] Gogna, M. L., Lorenzon, L., Ceccarelli, M., Camminatiello, S., & Manca, A. (2025). Order from entropy: Big data from FAIR data cohorts in the digital age of plant breeding. Theoretical and Applied Genetics, 138(3), 45–60. https://doi.org/10.1007/s00122-025-05040-5

[11] Roccatello, V., Giacobbe, M., Tinnirello, I., & Bianchi, G. (2021). State of the art in Internet of Things standards and interoperability. Network, 1(1), 14. https://iris.unipa.it/retrieve/aecfd0c2-eb01-488f-8199-0cb3afff51a4/network-05-00014-v2.pdf

[12] Mhaskar, N., Alabbad, M., & Khedri, R. (2021). A Formal Approach to Network Segmentation. Computers & Security, 103, 102162. https://doi.org/10.1016/j.cose.2020.102162

[13] Milesight. (2023). EM500-SMTC Soil Moisture/Temperature/EC Sensor — Datasheet. Milesight IoT Documentation.

[14] ePlant Inc. (2023). TreeTag: Wireless Tree and Vine Monitoring Device — Technical Overview. https://www.eplant.bio/how-it-works

[15] Raza, U., Kulkarni, P., & Sooriyabandara, M. (2017). Low Power Wide Area Networks: An Overview. IEEE Communications Surveys & Tutorials, 19(2), 855–873. https://doi.org/10.1109/COMST.2017.2652320

[16] Selby, P., Abbeloos, R., Backlund, J., Grimberg, Å., Jarnvall, L., Löfgren, M., … Hvidsten, T. R. (2019). BrAPI—An API for plant breeding applications. Bioinformatics, 35(20), 4147–4155. https://doi.org/10.1093/bioinformatics/btz123

[17] Adelantado, F., Vilajosana, X., Tuset-Peiro, P., Martinez, B., Melia-Segui, J., & Watteyne, T. (2017). Understanding the limits of LoRaWAN. IEEE Communications Magazine, 55(9), 34–40. https://doi.org/10.1109/MCOM.2017.1600613

[18] Mekki, K., Bajic, E., Chaxel, F., & Meyer, F. (2019). A comparative study of LPWAN technologies: LoRaWAN, Sigfox and NB-IoT. Computer Communications, 148, 1–19. https://doi.org/10.1016/j.comcom.2018.12.008

[19] IQRF Alliance. (2023). IQRF Sensor Standard – Technical Documentation. https://doc.iqrf.org/IQRF-Standards/StandardSensor/

[20] Cisco Networking Documentation. https://www.cisco.com/c/en/us/products/security/what-is-network-segmentation.html