future internet

MDPI

Article

Machine Learning and Deep Learning-Based Multi-Attribute Physical-Layer Authentication for Spoofing Detection in LoRaWAN

Azita Pourghasem *, Raimund Kirner, Athanasios Tsokanos, Iosif Mporas * and Alexios Mylonas

Cybersecurity and Computing Systems Research Group, Department of Computer Science, University of Hertfordshire, Hatfield AL10 9AB, UK

* Correspondence: a.pourghasem@herts.ac.uk (A.P.); i.mporas@herts.ac.uk (I.M.)

Abstract: The use of wireless sensor networks (WSNs) in critical applications such as environmental monitoring, smart agriculture, and industrial automation has created significant security concerns, particularly due to the broadcasting nature of wireless communication. The absence of physical-layer authentication mechanisms exposes these networks to threats like spoofing, compromising data authenticity. This paper introduces a multi-attribute physical layer authentication (PLA) scheme to enhance WSN security by using physical attributes such as received signal strength indicator (RSSI), battery level (BL), and altitude. The LoRaWAN join procedure, a key risk due to plain text transmission without encryption during initial communication, is addressed in this study. To evaluate the proposed approach, a partially synthesized dataset was developed. Real-world RSSI values were sourced from the LoRa at the Edge Dataset, while BL and altitude columns were added to simulate realistic sensor behavior in a forest fire detection scenario. Machine learning (ML) models, including Logistic Regression (LR), Random Forest (RF), and K-Nearest Neighbors (KNN), were compared with deep learning (DL) models, such as Multi-Layer Perceptron (MLP) and Convolutional Neural Networks (CNN). The results showed that RF achieved the highest accuracy among machine learning models, while MLP and CNN delivered competitive performance with higher resource demands.

Keywords: wireless sensor networks; physical-layer authentication; deep learning; machine learning; spoofing; multi-attribute; altitude; radio frequency fingerprinting; battery level; RSSI; LoRaWAN

Academic Editors: Emanuele De Santis and Francesco Delli Priscoli

Received: 6 November 2024
Revised: 14 January 2025
Accepted: 27 January 2025
Published: 6 February 2025

Citation: Pourghasem, A.; Kirner, R.; Tsokanos, A.; Mporas, I.; Mylonas, A. Machine Learning and Deep Learning-Based Multi-Attribute Physical-Layer Authentication for Spoofing Detection in LoRaWAN. *Future Internet* **2025**, *17*, 68. https://doi.org/10.3390/fi17020068

1. Introduction

IoT has become an important technology across multiple sectors, impacting industries such as healthcare, smart cities, agriculture, environmental monitoring, and more. IoT, as defined by Ref. [1], is a complex system of entities—comprising cyber-physical devices, information resources, and people—that exchange information and interact with the physical world through sensing, processing, and actuating. In recent years, the integration of Artificial Intelligence (AI) with IoT has further accelerated technological advancements, created new use cases, and enhanced the capabilities of next-generation connected systems [2]. According to Ref. [3], combining AI and IoT will transform industries by creating smarter and more flexible networks and infrastructure. An essential component within the IoT ecosystem is WSNs, consisting of numerous sensor devices deployed to gather environmental data such as temperature and humidity [4]. Based on Ref. [5], WSNs are experiencing rapid growth, with the global market expected to expand at a Compound

Annual Growth Rate (CAGR) of 17.64%, reaching a valuation of USD 148.67 billion. WSNs play a crucial role in monitoring systems across multiple domains, such as healthcare, agriculture, and environmental protection, including forest fire detection.

However, the security challenges posed by the large-scale deployment of IoT and WSN devices are significant. The heterogeneity of IoT devices, particularly in WSNs, introduces vulnerabilities due to resource constraints such as limited battery life, processing power, and storage capacity. These constraints make it difficult to implement robust software- and hardware-based security measures, exposing the network to external attacks [6].

Security in WSNs is particularly critical given the real-time, sensitive nature of the data transmitted. Unauthorized access, data manipulation, and network breaches could have devastating consequences, especially in applications such as healthcare and environmental monitoring, where WSNs are often deployed in open, unattended environments. For instance, in healthcare, WSNs can monitor patients' vital signs, while in military operations, they can detect enemy intrusion. Both scenarios rely on the authenticity, integrity, and confidentiality of the data transmitted over the WSNs [7].

Given the broadcasting nature of LoRaWAN, networks using this protocol remain particularly susceptible to attacks like eavesdropping, data forgery, and spoofing. Spoofing occurs when a malicious actor impersonates a legitimate sensor by falsifying attributes such as MAC addresses, signal strength, or location. These attacks compromise the authenticity and reliability of transmitted data, potentially leading to unauthorized access and the disruption of critical applications [8,9]. In addition to spoofing, jamming attacks can disrupt communication by introducing intentional interference, rendering the network unusable and causing significant reliability issues [10].

LoRaWAN's OTAA join procedure aggravates these vulnerabilities by transmitting plaintext device identifiers during initial communication, making it a critical risk area for spoofing attacks. This lack of encryption enables attackers to intercept and manipulate transmitted data, highlighting the need for stronger physical-layer authentication mechanisms to secure communication. To address these security challenges, this paper presents a novel multi-attribute PLA scheme for WSNs. PLA offers a proactive approach to security by authenticating devices based on their unique physical characteristics, such as RSSI, BL, and GPS-reported altitude. Unlike traditional cryptographic techniques, which may be too resource-intensive for WSNs, PLA is better suited for low-power devices, providing an efficient means of ensuring device authenticity at the physical layer. This research focuses on applying the proposed PLA scheme in a forest fire detection scenario, where static sensors are deployed to monitor environmental conditions.

The proposed PLA approach is designed to mitigate spoofing attacks and unauthorized access by verifying sensor nodes based on their physical attributes. By combining RSSI, BL, and altitude, this method ensures the authenticity of sensor nodes during wireless communication. Integrating both machine learning (ML) models, such as LR, RF, and KNN, and deep learning (DL) models like MLP and CNN, enables the system to analyze the collected physical attributes and enhance detection accuracy for malicious nodes attempting to spoof legitimate sensors.

The key contributions of this research are as follows:

1. We introduce a multi-attribute PLA scheme for LoRaWAN-based WSNs, using RSSI, BL, and GPS-reported altitude to strengthen device authentication. This additional physical layer of security aims to reduce susceptibility to spoofing attacks in resource-constrained networks.
2. ML models, including LR, RF, and KNN, and deep learning models, including MLP and CNN, are applied to analyze physical attributes (RSSI, BL, and altitude), aiming

to improve the accuracy of detecting nonlegitimate nodes attempting to impersonate legitimate sensors.

3. The PLA scheme is tailored specifically for low-power LoRaWAN-based WSN environments, evaluated using a partially synthesized dataset that integrates real-world RSSI values from the LoRaWAN at the Edge Dataset (LoED). This ensures that the dataset reflects practical conditions, making the scheme applicable to real-world scenarios like forest fire detection, where reliable, low-energy security measures are essential.
4. We provide a detailed evaluation of our proposed scheme, assessing its effectiveness in detecting spoofing attacks by using standard classification metrics such as accuracy, precision, recall, and F1-score. Additionally, we evaluate computational efficiency in terms of training time and memory usage, ensuring suitability for low-power LoRaWAN environments.

The rest of this paper is structured as follows. Section 2 reviews related work on PLA schemes and the integration of ML and DL techniques. Section 3 outlines the methodology for developing the multi-attribute PLA scheme. Section 4 describes the implementation of the PLA scheme. Section 5 presents the evaluation of the models used for detecting spoofing attacks. Section 6 concludes the paper and discusses future work.

2. Background on Physical-Layer Security in LoRaWAN and WSNs

Physical-layer security is a critical requirement in WSNs and LoRaWAN, where vulnerabilities such as spoofing and jamming pose significant threats. These attacks exploit the open nature of wireless communication, where signals can be intercepted, manipulated, or disrupted without physical access to the network. Traditional cryptographic methods are commonly used to secure upper layers of network communication. However, these approaches impose high computational and energy costs, making them unsuitable for resource-constrained IoT environments like LoRaWAN and WSNs [11]. PLA offers a lightweight alternative by using device-specific physical-layer attributes for authentication and anomaly detection [8].

Spoofing attacks compromise network integrity by allowing malicious nodes to impersonate legitimate devices using forged attributes such as RSSI or MAC addresses. Similarly, jamming attacks disrupt communication by introducing interference, severely impacting system reliability. These threats are exacerbated by the lack of encryption at the physical (PHY) layer in LoRaWAN, as shown in Figure 1, where the red-highlighted section is labelled as the "Not Protected Layer" in the LoRaWAN communication stack.

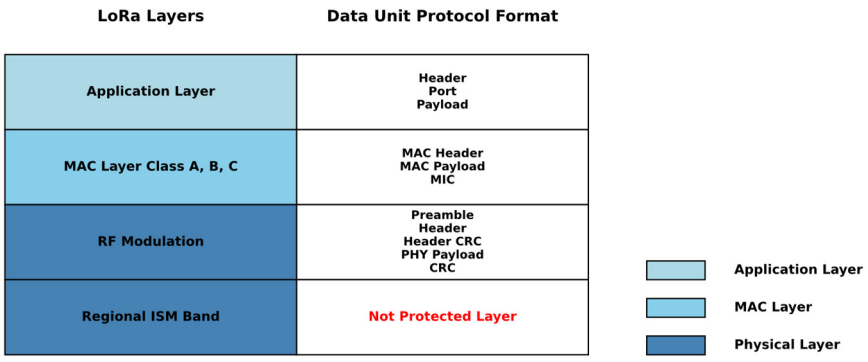

Figure 1. LoRa layer stack highlighting the "Not Protected Layer"—created based on Ref. [12].

Figure 1 visually demonstrates the vulnerabilities in the LoRaWAN communication stack, specifically in the PHY layer, due to unencrypted data transmission. This absence of encryption leaves the PHY layer highly susceptible to critical security threats, including

spoofing attacks, where malicious actors impersonate legitimate devices, and jamming attacks, which disrupt communication by introducing intentional interference. These vulnerabilities underscore the fundamental weakness of the PHY layer, as it lacks intrinsic mechanisms for data protection or authentication, making it a critical target for adversaries aiming to compromise network integrity and reliability [12].

2.1. PLA for Spoofing Mitigation

PLA schemes are particularly effective in combating spoofing attacks, which exploit the broadcast nature of wireless networks. By analyzing device-specific physical attributes, PLA offers a lightweight mechanism for detecting spoofing attempts without the overhead of traditional cryptographic solutions [13]. Early PLA methods relied heavily on single attributes, such as RSSI, due to their simplicity and low energy requirements. However, RSSI-based schemes are highly susceptible to environmental interference, including multipath fading and shadowing, which lead to increased false positives and reduced reliability [8]. To overcome these limitations, researchers have developed multi-attribute PLA schemes that integrate complementary features for improved detection accuracy. For instance, Ref. [14] demonstrated the effectiveness of combining RSSI with Radio Frequency Fingerprints (RFF), using hardware-specific imperfections that are difficult to replicate. Similarly, advanced techniques using deep learning, as proposed by Ref. [15], enable dynamic analysis of network traffic, adapting to varying environmental conditions to enhance spoofing detection. While PLA is primarily used for spoofing mitigation, its ability to detect signal anomalies also makes it applicable to jamming detection. For example, sudden drops in RSSI or consistent interference patterns may indicate jamming activity. Our study builds on these researches by integrating dynamic and static attributes like RSSI, Battery Level (BL), and altitude, enabling a multi-attribute approach that addresses spoofing threats in resource-constrained IoT environments.

2.2. Evolution of Multi-Attribute PLA Schemes

The evolution of PLA schemes reflects a significant shift from single-attribute methods to multi-attribute approaches, driven by the increasing complexity of physical-layer threats. Early PLA schemes relied on single attributes, such as RSSI, which, while lightweight, were vulnerable to environmental interference and dynamic conditions [9]. Recognizing these limitations, researchers began integrating additional attributes to enhance detection accuracy and robustness. Ref. [14] introduced a pioneering approach by combining RSSI with Radio Frequency Fingerprints (RFF) using hardware-specific imperfections for improved spoofing detection. Ref. [16] extended this concept by incorporating timing-based features, such as signal phase and delay, to address adaptability in highly dynamic environments. These studies demonstrated that multi-attribute PLA schemes could outperform single-attribute methods in both static and dynamic scenarios.

The application of machine learning models further advanced PLA schemes, enabling real-time detection of physical-layer threats. Ref. [10] proposed a supervised learning model for jamming detection in multi-hop IoT networks, combining RSSI and Signal-to-Noise Ratio (SNR). This approach achieved high detection accuracy while maintaining computational efficiency, underscoring the scalability of multi-attribute PLA for IoT systems.

Machine-learning techniques, such as LR and RF, are particularly well suited for resource-constrained sensors due to their low computational overhead compared to more complex deep-learning models. These models require minimal processing power while achieving high detection accuracy, making them effective for real-time spoofing and jamming detection in IoT environments [17]. Recent studies, such as Ref. [18], have explored

lightweight ML techniques, highlighting their computational efficiency and suitability for resource-constrained environments. Their work demonstrates the potential of models like Naïve Bayes and SVMs for achieving high accuracy in detecting physical-layer threats with minimal resource usage. Similarly, Ref. [19] presented an effective combination of CNN and LSTM models for the real-time detection of physical-layer attacks in IoT. Their approach adapts to dynamic network environments. Further, Ref. [20] compared traditional ML methods, such as decision trees and RF, with deep-learning models like CNN for RSSI-based jamming detection. Their findings highlighted trade-offs between accuracy and computational requirements, providing insights into optimizing PLA schemes for diverse IoT scenarios.

While this progress represents significant progress, they also highlight the need for novel features and enhanced adaptability, particularly in resource-constrained environments. This need motivates our work, which integrates additional dynamic and spatial attributes to extend the capabilities of existing PLA methods.

2.3. Gaps in Existing PLA Approaches

Despite advancements in PLA schemes, several challenges remain in ensuring their real-world applicability. Single-attribute methods, such as RSSI-based PLA, are prone to environmental interference and dynamic network conditions, leading to false positives and reduced reliability [15]. While multi-attribute schemes address some of these limitations, many rely on static or context-specific attributes that may not generalize well across diverse IoT environments. Dynamic environments, characterized by factors such as multipath fading and interference, significantly affect the accuracy of attributes like RFF and signal timing [14]. Moreover, existing approaches often overlook dynamic features that evolve naturally with device behaviour, such as battery usage or physical displacement. Emerging approaches aim to fill these gaps by using lightweight and hybrid models that balance computational efficiency and accuracy. For instance, Ref. [19] demonstrated the effectiveness of SVMs in constrained environments, while Ref. [20] highlighted hybrid deep-learning solutions, such as CNN–LSTM models, which adapt to dynamic IoT conditions. These advancements underline the ongoing efforts to develop scalable and robust PLA schemes for real-world deployments. Building on these insights, our proposed multi-attribute PLA scheme integrates both dynamic and static features, including RSSI, BL, and altitude. BL introduces a time-evolving attribute that reflects device behaviour, enhancing resilience against replication attacks. Altitude ensures spatial consistency, mitigating the risk of spoofing through unauthorized device relocation. By combining these attributes, our scheme adapts effectively to dynamic environments, offering a robust solution for securing LoRaWAN-based WSNs in challenging scenarios, such as forest fire detection systems.

3. Design and Implementation of the Multi-Attribute PLA Scheme for LoRaWAN

This section outlines the design, implementation, and evaluation of a multi-attribute PLA scheme for LoRaWAN-based WSNs. The proposed methodology focuses on securing communication against spoofing attacks, with a forest fire detection scenario as the primary use case.

3.1. LoRaWAN Architecture and Deployment

The LoRaWAN architecture used in this study follows a hierarchical structure involving end devices (EDs), gateways (GWs), Join Server (JS), Network Server (NS), and Application Server (AS). Figure 2 illustrates the LoRaWAN architecture for the proposed forest fire detection use case.

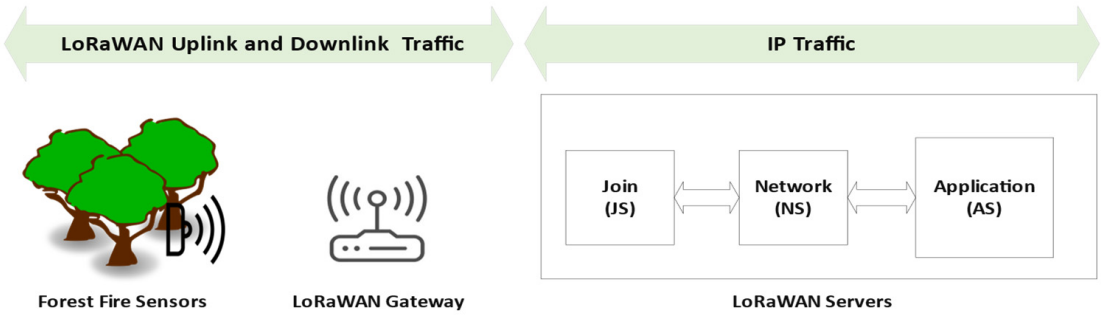

Figure 2. LoRaWAN Architecture for the proposed forest fire detection use case.

The sensors deployed across a monitored area form the ED to GW communication. The monitored sensors collect environmental data and transmit them to gateways using LoRaWAN's long-range, low-power communication protocol. These static devices represent forest fire detection sensors in this scenario.

Then, in the GW to NS section of the architecture, the GWs forward data to the JS during the Over-The-Air Activation (OTAA) process for device authentication. The NS ensures routing and data integrity while managing communication between GWs and the AS. Then, in the next section where the AS is located, the process of authentication happens, where a decision is made based on the received data and an actionable insight is generated, such as fire alerts.This deployment mimics real-world LoRaWAN use cases, addressing vulnerabilities in the OTAA process, where unencrypted join-request messages make the network susceptible to spoofing. The proposed PLA scheme targets these vulnerabilities by enhancing physical-layer security.

3.2. Dataset Description

The dataset used in this study originates from the LoRaWAN at the Edge (LoED) Dataset [18], a real-world dataset capturing network behavior under realistic conditions. It contains 155,422 entries and includes attributes such as the timestamp of the signal (Time), a unique identifier for each sensor (Device Address), the gateway receiving the signal, the RSSI, and SNR. To extend the dataset for the proposed multi-attribute PLA scheme, two additional attributes were synthesized. The BL was modeled to decrease over time, reflecting real-world sensor battery depletion, with sudden changes flagged as anomalies. The altitude attribute was simulated to represent static sensor installation heights with minor variations to account for GPS inaccuracies. These additions transformed the dataset into a multi-attribute dataset, combining real-world RSSI values with synthetic BL and altitude data, thereby simulating environmental and signal variations critical for evaluating spoofing detection mechanisms.

3.3. PLA Scheme Implementation

The proposed PLA scheme authenticates devices using three physical-layer attributes: RSSI, BL, and altitude. Each attribute serves as a unique identifier, creating a PLA mechanism that is difficult for attackers to replicate. The RSSI values are analyzed to detect deviations outside expected ranges, indicating potential spoofing. For instance, a sudden shift from weak to strong RSSI could suggest an illegitimate source. The gradual depletion of BL is expected during normal operation. Sudden drops may indicate tampering or sensor compromise. Static sensors maintain consistent altitudes, and significant deviations suggest physical relocation or replacement. If any of the attributes fall outside their defined thresholds, the authentication will fail, ensuring that only devices meeting all criteria are successfully authenticated. This multi-attribute approach ensures effective authentication against spoofing attacks, enhancing security in vulnerable environments.

3.4. Data Preprocessing and Model Development

The dataset was preprocessed and balanced to ensure effective training and evaluation of the proposed PLA scheme. RSSI, BL, and altitude values were standardized to achieve uniformity and improve model performance. To address data imbalance, legitimate entries (status = 0) and spoofed entries (status = 1) were balanced through random undersampling. The evaluation of the PLA scheme utilized a combination of ML and DL models to classify legitimate versus spoofed sensors. Standard ML models, including LR and KNN, were implemented due to their efficiency and interpretability in resource-constrained environments. These models were chosen for their ability to provide baseline comparisons in classification tasks. DL models, specifically MLP and CNN, were employed to explore the capacity of neural networks to capture non-linear relationships and complex patterns among the multi-attribute dataset. These architectures were selected for their proven effectiveness in handling multi-dimensional data while maintaining flexibility for varying input features. All models were trained and tested on the balanced dataset to ensure consistent evaluation metrics. The results were analyzed to compare the performance of traditional ML models and advanced DL techniques in detecting spoofing attacks based on the multi-attribute PLA framework.

4. Deployment and Model Training of the PLA Scheme

The proposed multi-attribute PLA scheme is implemented in three distinct phases, each addressing a specific aspect of sensor authentication. These phases ensure seamless integration with the LoRaWAN architecture and effective protection against spoofing attacks. This section elaborates on each phase, the ML and DL models used, the dataset preparation, and the deployment strategy.

4.1. Phase 0: Initial Join Procedure for LoRaWAN

Phase 0 addresses the initial registration of sensors into the LoRaWAN network, which occurs only once for each sensor. Sensors are registered using either the OTAA method or the Activation by Personalization (ABP) method. OTAA dynamically generates session keys during the join process, enhancing security, while ABP provides pre-configured keys for faster setup but with reduced flexibility. Once registered, sensors transmit encrypted data to the LoRaWAN gateway. The gateway forwards these data to the NS, where integrity checks are conducted. The AS processes and securely stores the identification of the sensors through the built-in LoRaWAN join procedure as shown in Figure 3, phase 0.

4.2. Phase 1: Multi-Attribute PLA

In phase 1, the proposed PLA authentication mechanism becomes active. Sensors transmit encrypted data containing three key physical-layer attributes of RSSI,BL, and altitude. These attributes are encrypted using the Application Session Key (AppSKey) and sent to the gateway. The NS verifies the data's integrity using the Network Session Key (NwkSKey) and forwards it to the AS. The AS decrypts the attributes and creates a database of the three attributes for each sensor. From now on, the sensors that match the database and have attributes within predefined thresholds are authenticated, allowing their payloads to be processed. Sensors failing this authentication are flagged as spoofed and denied access. This phase is also depicted in Figure 3.

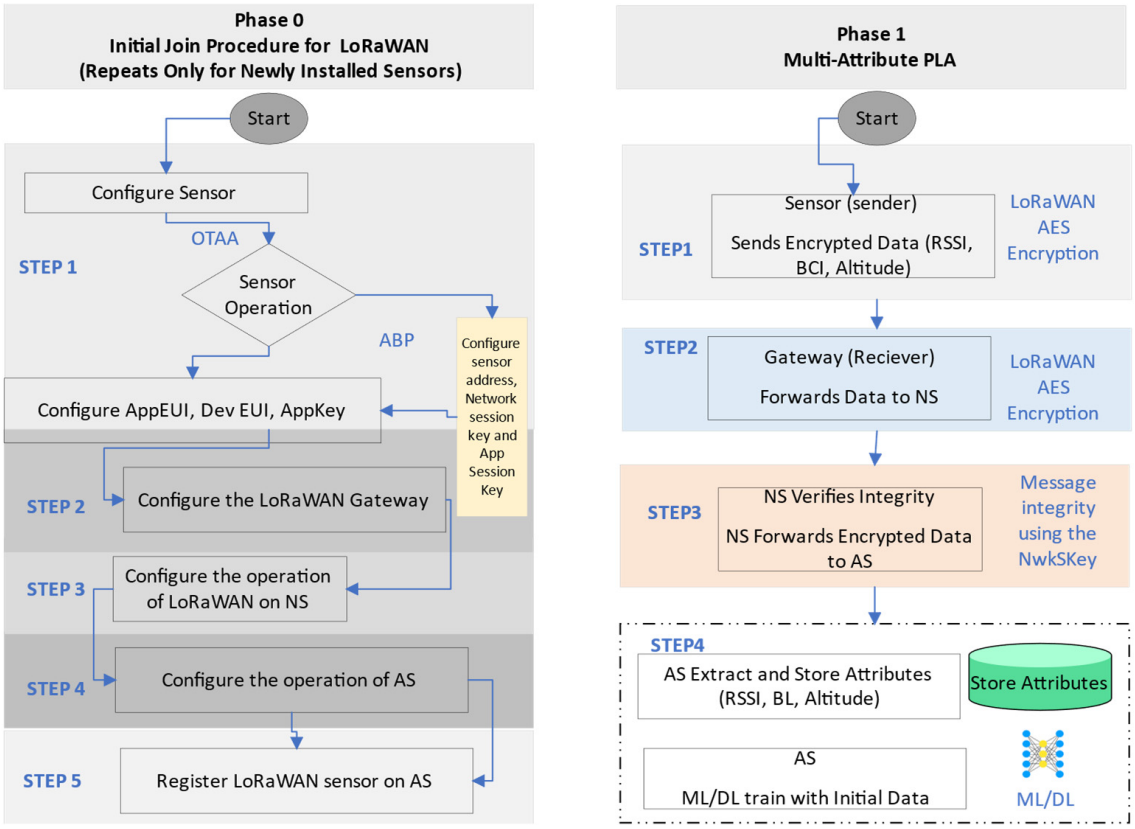

Figure 3. Phase 0, Initial Join Procedure for LoRaWAN; Phase 1, Multi-Attribute PLA.

4.3. Phase 2: Continuous Authentication and Anomaly Detection

Phase 2 introduces continuous authentication. In this stage, pre-trained machine learning (ML) and deep learning (DL) models analyze incoming sensor data in real-time. Each record is evaluated for deviations in RSSI, BL, or altitude. If any attribute falls outside acceptable thresholds, the sensor is flagged as spoofed, and its data transmission is blocked. Legitimate data are processed, ensuring uninterrupted operation. Continuous authentication also enables model retraining as new data are collected. This adaptability allows the system to respond effectively to evolving threats and dynamic environments. By continually refining the model based on real-time data, the scheme enhances its ability to differentiate between legitimate and non-legitimate sensors. Phase 2 focuses on real-time detection and prevention of spoofing attacks, as shown in Figure 4.

4.4. Machine Learning and Deep Learning Models

The success of the multi-attribute PLA scheme relies heavily on ML and DL models to classify sensors as legitimate or spoofed. LR serves as a lightweight binary classification model that evaluates the likelihood of a sensor's legitimacy based on its attributes. Its simplicity and computational efficiency make it well suited for real-time scenarios [21]. RF constructs multiple decision trees, providing robust classification performance, even in noisy data environments. It is particularly effective for handling non-linear relationships [22]. KNN is a proximity-based classification algorithm that relies on the closeness of data points. While simple, it may struggle with scalability in high-dimensional spaces [22].

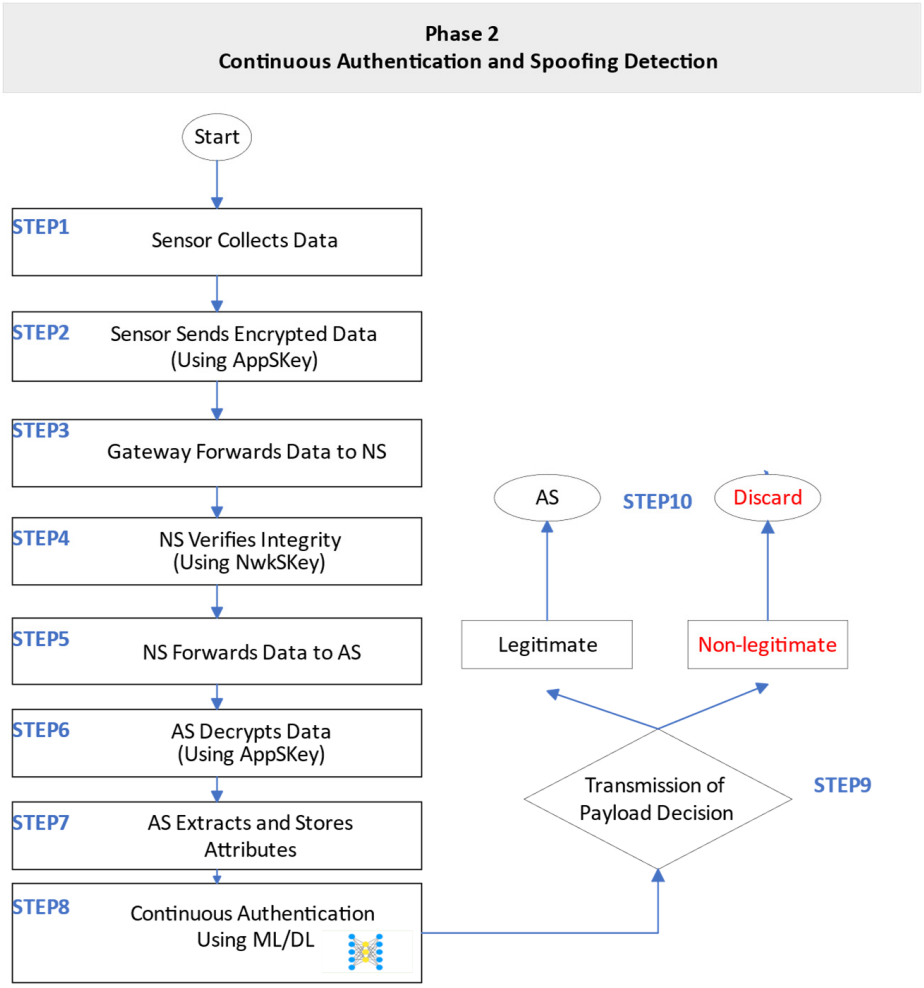

Figure 4. Phase 2, Continuous authentication and spoofing detection and model training.

DL models include the MLP, which is a fully connected network designed to capture non-linear dependencies. Its architecture incorporates dense layers and dropout mechanisms to prevent overfitting, making it effective for structured input features [23]. The CNN uses convolutional layers to extract spatial and temporal patterns from time-series data, enhancing the representation of attributes like RSSI, BL, and altitude for improved classification accuracy [24].

4.5. Dataset Preparation and Model Deployment

The dataset used for this study originates from the LoRaWAN at the Edge Dataset (LoED) [18], which contains 155,422 entries in one of their files. This dataset is part of a larger series of files collected over four months. For the purposes of this study, only this specific file was selected to ensure focused analysis while maintaining relevance to the proposed PLA scheme. While RSSI values were sourced directly from the dataset, BL and altitude were synthesized to reflect realistic sensor behavior. These attributes were preprocessed, standardized, and balanced through random under sampling to address class imbalance, ensuring fair evaluation of the models.

The ML and DL models were trained on the preprocessed dataset to classify sensors effectively. During deployment, the models continuously process incoming sensor data, analyzing any deviations in RSSI, BL, and altitude. Non-legitimate sensors are flagged as spoofed, providing real-time protection against unauthorized access.

The hybrid approach of combining lightweight ML models for resource-constrained environments with advanced DL models for high-accuracy scenarios ensures a balance between computational efficiency and detection performance. This adaptability makes the proposed scheme suitable for diverse deployment scenarios.

5. Evaluation of ML and DL Models for Spoofing Detection

This section evaluates the proposed multi-attribute PLA scheme using various ML and DL models. The evaluation metrics include accuracy, precision, recall, F1-score, training time, and memory usage. The models evaluated include LR, RF, KNN, MLP, and CNN. The dataset was balanced through random under sampling and included three critical physical layer attributes: RSSI, BL, and altitude. Standard classification metrics, including accuracy, precision, recall, and F1-score, were used to evaluate each model. Additionally, training time and memory usage were recorded to assess computational efficiency.

The key performance metrics for each model are presented in Table 1, while computational efficiency metrics are summarized in Table 2.

Table 1. Performance metrics for ML and DL models.

Model	Accuracy	Precision	Recall	F1-Score
LR	83.16%	87.27%	83.16%	83.19%
RF	83.74%	87.13%	83.74%	83.74%
KNN	80.23%	80.46%	80.23%	80.23%
MLP	83.04%	87.08%	80.04%	83.04%
CNN	83.29%	87.21%	83.27%	83.27%

Table 2. Computational efficiency metrics for ML and DL models.

Model	Training Time (s)	Memory Usage (MB)
LR	0.002	0.80
RF	0.084	0.50
KNN	0.002	0.12
MLP	1.83	26.3
CNN	4.15	6.26

Based on the results in Table 1, RF emerged as the best-performing model, achieving the highest accuracy and F1-score at 83.74%, slightly surpassing other models. LR, MLP, and CNN exhibited comparable performance, with accuracy values around 83%, while KNN lagged with an accuracy of 80.23% and corresponding lower precision, recall, and F1-scores. These findings underscore the varying capabilities of the models in handling the dataset's complexity.

LR performed as expected for a linear model, achieving an accuracy of 83.16% and precision, recall, and F1-scores of 87.27%, 83.16%, and 83.19%, respectively. These results reflect its ability to effectively handle linearly separable data. With the shortest training time of approximately 0.002 s and low memory usage of 0.80 MB (as shown in Table 2), LR demonstrated exceptional computational efficiency, making it suitable for real-time applications.

RF slightly outperformed LR, achieving an accuracy, recall, and F1-score of 83.74%. It can handle noisy data and capture non-linear relationships, contributing to its superior performance. However, the additional complexity of growing multiple decision trees increased its training time to 0.084 s. Despite this, RF demonstrated efficient memory usage at 0.50 MB, highlighting its ability to balance performance and computational efficiency.

KNN exhibited the lowest performance among the evaluated models, achieving an accuracy of 80.23% and precision, recall, and F1-scores of approximately 80.46%. The proximity-based classification approach struggled with overlapping data points in the feature space, particularly when noisy or variable attributes like RSSI, BL, and altitude were present. While its metrics were lower than other models, KNN demonstrated fast training (0.002 s) and low memory usage (0.12 MB). However, its reduced accuracy makes it less suitable for this application.

MLP achieved an accuracy of 83.04% and precision, recall, and F1-scores of 87.08%, 83.04%, and 83.04%, respectively. Its performance is comparable to LR and RF, benefiting from its ability to model non-linear patterns. However, MLP's resource demands were significantly higher, with a training time of 1.83 s and memory usage of 26.3 MB. These resource requirements stem from the iterative weight optimization and fully connected architecture, which necessitate substantial computational resources for backpropagation and gradient descent.

CNN achieved the highest performance among the deep learning models, with an accuracy of 83.29% and precision, recall, and F1-scores of 87.21%, 83.27%, and 83.27%, respectively. Its slight improvement over MLP is attributed to its ability to capture spatial relationships and complex dependencies within the feature space. However, this performance came at the cost of a longer training time (4.15 s) and higher memory usage (6.26 MB).

Figure 5 visually compares the accuracy, precision, recall, and F1-scores for each model. While the tabulated data offer detailed numerical metrics, this chart emphasizes the consistent strengths of RF and CNN across metrics and the noticeable gap in KNN's performance. The visualization highlights RF's dominance in balancing high accuracy and F1-score, solidifying its position as the best-performing model.

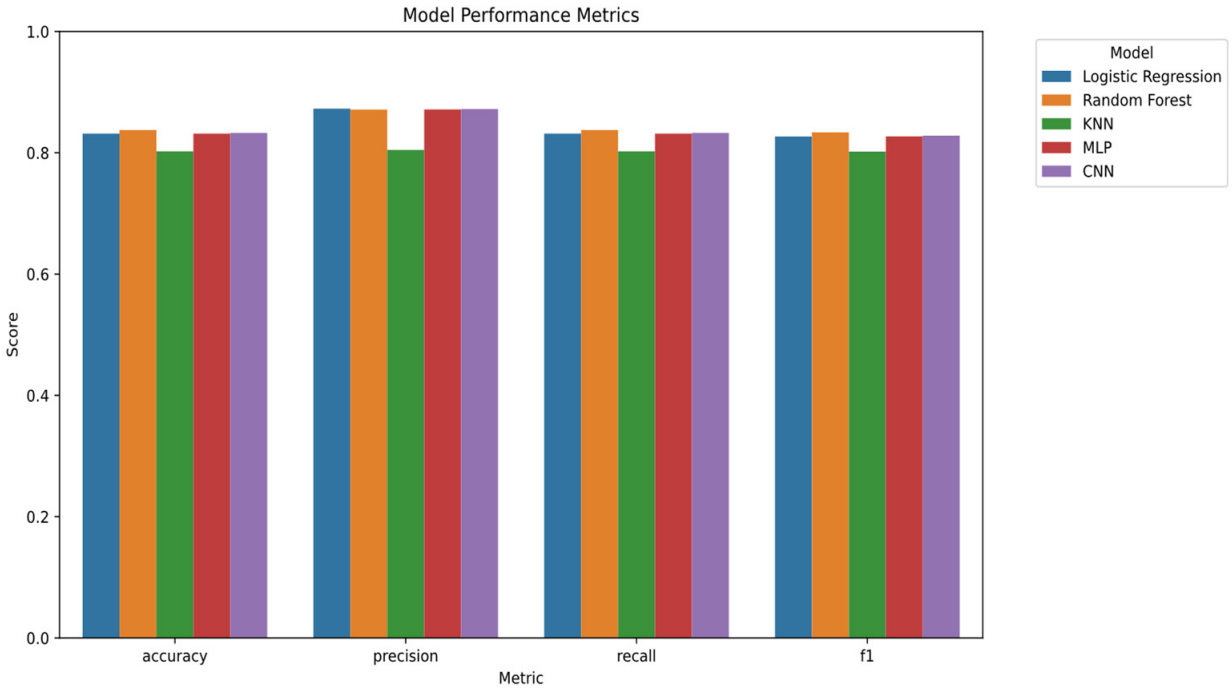

Figure 5. Visual comparison of model performance metrics across ML and DL models.

Training time analysis revealed significant variations across models. LR and KNN required the least time, making them highly suitable for real-time applications. RF achieved a balance between efficiency and accuracy with moderate training time, while deep learning

models, particularly CNN and MLP, exhibited longer training times due to their complex architectures.

Memory usage analysis underscored the resource efficiency of LR and KNN, which required minimal memory. RF consumed a modest amount of memory despite its complexity. Among the deep learning models, MLP exhibited the highest memory usage due to its fully connected architecture, while CNN demonstrated improved efficiency in memory consumption owing to its convolutional layers.

To better understand the contribution of each attribute (RSSI, BL, and altitude) to the model's decision-making, RF feature importance analysis was conducted. The results revealed the following:

Feature importance analysis, derived from RF as shown in Table 3, identified BL as the most influential attribute, contributing 44.81% to the model's decisions. Altitude followed with 32.22%, and RSSI accounted for 22.86%. These results reinforce the critical role of BL and altitude in detecting spoofing attacks, validating the multi-attribute PLA scheme's effectiveness.

Table 3. Random Forest feature importance analysis.

Feature	Importance
Battery	44.81%
Altitude	32.22%
RSSI	33.86%

6. Conclusions

This study introduced a multi-attribute PLA scheme for LoRaWAN-based WSNs using physical-layer attributes—RSSI, BL, and altitude—to enhance sensor authentication and mitigate spoofing attacks. The evaluation demonstrated that RF achieved the best overall performance, with the highest accuracy and F1-score (83.74%), while LR showed exceptional computational efficiency, making it ideal for real-time, resource-constrained environments. Among DL models, CNN achieved the highest accuracy (83.29%) and precision, but at the cost of longer training time and higher memory usage, making it suitable for applications requiring high accuracy with complex data patterns. Conversely, MLP balanced accuracy and computational efficiency, highlighting its versatility for dynamic WSN scenarios.

The analysis of training time and memory usage revealed that ML models like LR and KNN are better suited for lightweight, real-time applications, whereas DL models, particularly CNN, excel in accuracy-critical environments. RF emerged as a strong competitor for balancing accuracy, resource efficiency, and adaptability, showcasing its robustness in handling noisy and non-linear data.

Feature importance analysis using RF identified BL as the most significant attribute (44.81%), followed by altitude (32.22%) and RSSI (22.86%). This reinforces the importance of combining dynamic and static physical-layer attributes for effective spoofing detection. The proposed scheme demonstrated its capability to improve security in low-power LoRaWAN environments, especially in scenarios like forest fire detection.

For future work, we plan to include RFF as an additional attribute to compare its effectiveness with RSSI. The PLA scheme will also be improved for use in larger and more dynamic networks while maintaining efficiency. Furthermore, exploring real-world implementation scenarios will provide valuable insights into the scheme's performance and scalability in practical deployments.

Author Contributions: Data curation, A.P.; methodology, A.P.; supervision, A.M., R.K., A.T., I.M.; writing—review and editing, A.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: A sample of the dataset used can be accessed from this link Azita369/PLA-multi-attribute, accessed on 5 November 2024.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. *IEEE 2413-2019*; IEEE Standard for an Architectural Framework for the Internet of Things (IoT). IEEE: Piscataway, NJ, USA, 2020. [CrossRef]
2. Yang, Y.; Wu, L.; Yin, G.; Li, L.; Zhao, H. A survey on security and privacy issues in Internet-of-Things. *IEEE Internet Things J.* **2017**, *4*, 1250–1258. [CrossRef]
3. World Economic Forum. The Future of Jobs Report 2024. 2024. Available online: https://www.weforum.org/meetings/world-economic-forum-annual-meeting-2024/ (accessed on 5 November 2024).
4. Al-Fuqaha, A.; Guizani, M.; Mohammadi, M.; Aledhari, M.; Ayyash, M. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2347–2376. [CrossRef]
5. Mordor Intelligence. Wireless Sensor Networks (WSNs) Market—Growth, Trends, COVID-19 Impact, and Forecasts (2024–2026). *Mordor Intelligence*. 2024. Available online: https://www.mordorintelligence.com/ (accessed on 5 November 2024).
6. LoRa Alliance. LoRaWAN® 1.1 Specification. 2023. Available online: https://resources.lora-alliance.org/technical-specifications/lorawan-specification-v1-1 (accessed on 5 November 2024).
7. Rappaport, T.S. *Wireless Communications: Principles and Practice*, 2nd ed.; Prentice Hall: Upper Saddle River, NJ, USA, 2002.
8. Onyancha, B.; Kipruto, M.; Chepkemoi, N. A comprehensive review on the security challenges of wireless sensor networks. *Comput. Electr. Eng.* **2021**, *92*, 107186.
9. Bhat, N.; AlMughairi, A.; Dey, A. Securing IoT wireless networks using physical layer authentication with machine learning. *Int. J. Inf. Secur.* **2023**, *22*, 27–40.
10. de Moraes, P.; da Conceição, A.F. A Systematic Review of Security in the LoRaWAN Network Protocol. *ACM Comput. Surv.* **2021**, *30*, 102.
11. Jiang, W.; Shi, Y.; Cao, X.; Chen, H.H. A survey of security in WSNs. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2407–2433.
12. Na, S.; Hwang, D.; Shin, W.; Kim, K.H. Scenario and countermeasure for replay attack using join request messages in LoRaWAN. In Proceedings of the 2017 International Conference on Information Networking (ICOIN), Da Nang, Vietnam, 11–13 January 2017; pp. 718–720.
13. Rama Moorthy, S.; Periasamy, S.; Adhiyaman, V.; Murugan, S. A hybrid deep learning model for wireless sensor network security. *J. Intell. Fuzzy Syst.* **2020**, *39*, 5279–5289.
14. Zhang, J.; Dobre, O.; Kayhan, F. A survey on physical layer security for cognitive radio networks. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2192–2223.
15. Li, D.; Dou, W. Machine learning-based spoofing detection for wireless networks: A survey. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 91–113.
16. Gupta, K.; Shukla, S. Internet of Things: Security challenges for next generation networks. In Proceedings of the 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH), Greater Noida, India, 3–5 February 2016; pp. 315–318.
17. Bai, L.; Zhang, J.; Liu, Y. Physical-layer jammer detection in multi-hop IoT networks using machine learning. In Proceedings of the IEEE International Conference on Communications, Montreal, QC, Canada, 14–23 June 2021; pp. 4051–4056.
18. Bhatia, L.; Breza, M.; Marfievici, R.; McCann, J.A. LoED: The LoRaWAN at the Edge Dataset. In Proceedings of the 3rd International SenSys+BuildSys Workshop on Data: Acquisition to Analysis (DATA '20), Virtual Event, Japan, 16–19 November 2020. [CrossRef]
19. Gupta, R.; Li, X. Access-based Lightweight Physical Layer Authentication for the Internet of Things Devices. *IEEE Internet Things J.* **2023**, *11*, 11312–11326.
20. Kumar, V.; Singh, A. Physical-Layer Security in IoT Networks Using Feature-Based Deep Learning Approaches. *IEEE Trans. Commun.* **2024**, *23*, 1814.
21. Filippou, S.; Achilleos, A.; Zukhraf, S.Z.; Laoudias, C.; Malialis, K.; Michael, M.K. A Machine Learning Approach for Detecting GPS Location Spoofing Attacks in Autonomous Vehicles. In Proceedings of the 2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring), Florence, Italy, 20–23 June 2023; pp. 1–7. [CrossRef]

22. Pinto, E.M.d.L.; Lachowski, R.; Pellenz, M.E.; Penna, M.C.; Souza, R.D. A Machine Learning Approach for Detecting Spoofing Attacks in Wireless Sensor Networks. In Proceedings of the 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA), Krakow, Poland, 16–18 May 2018; pp. 752–758. [CrossRef]
23. Khoei, T.T.; Aissou, G.; Al Shamaileh, K.; Devabhaktuni, V.K.; Kaabouch, N. Supervised Deep Learning Models for Detecting GPS Spoofing Attacks on Unmanned Aerial Vehicles. In Proceedings of the 2023 IEEE International Conference on Electro Information Technology (eIT), Romeoville, IL, USA, 18–20 May 2023; pp. 340–346. [CrossRef]
24. Borhani-Darian, P.; Li, H.; Wu, P.; Closas, P. Detecting GNSS spoofing using deep learning. *EURASIP J. Adv. Signal Process.* **2024**, *2024*, 14. [CrossRef]