Physical Communication 70 (2025) 102626

Contents lists available at ScienceDirect

Physical Communication

journal homepage: www.elsevier.com/locate/phycom

Full length article

Autoencoder-based physical layer authentication in a real indoor environment

Linda Senigagliesi *, Gianluca Ciattaglia, Ennio Gambi

Department of Information Engineering, Università Politecnica delle Marche, via Brecce Bianche 12, Ancona, 60131, Italy

ARTICLE INFO

Keywords:
Machine learning
Autoencoder
Physical layer authentication
Channel measurements
Universal Software Radio Peripherals

ABSTRACT

Authentication of wireless nodes, as in fifth-generation (5G) and Internet of Things (IoT) networks, is an increasingly pressing issue, in order to limit the required computational effort and the necessary overhead. A simplification of the authentication process may therefore be of interest to achieve the satisfaction of stringent performance requirements, such as those envisaged for sixth-generation (6G) networks. This paper provides a study on the feasibility of physical layer authentication (PLA) in a real indoor environment, as an alternative solution to the traditional authentication schemes. To ensure the reliability of the proposed approach a simulated scenario is firstly tested. Subsequently, real-world data are collected through a laboratory setup using a Vectorial Signal Transceiver (VST) and two Universal Software Radio Peripherals (USRPs) to emulate the behavior of the receiver, the legitimate transmitter, and the potential adversary. A machine learning (ML) algorithm is then exploited to act as authenticator. This means that channel fingerprint is extracted from signals to create a dataset used to train a sparse autoencoder. To emulate a real authentication scenario, the autoencoder is trained only on the class of the legitimate user. Once a new message arrives, the autoencoder task is to discern authentic signals from those forged by the adversary. It is shown that a geometric mean of accuracy of more than 90%, with corresponding low levels of false alarm and missed detection, is achievable irrespective of the nodes location, underlining the robustness and versatility of the proposed ML-based PLA approach.

1. Introduction

The proliferation of 5G networks and the Internet of Things (IoT) has presented new difficulties for security and authentication systems. At present, a large number of distributed devices, often non-static and with limited memory and computing capacity, require network authentication [1]. Beyond 5G systems will face a wide range of constraints, including the need to meet aggressive latency requirements [2], establish extensive connectivity, minimize energy consumption, and reduce computational complexity, all while ensuring explicit security assurances. Notably, the widespread deployment of low-end IoT devices, which are often produced using diverse manufacturing processes, raises significant concerns regarding the long-term security of the IoT [3], motivating the need for intelligent and adaptive security schemes at all layers [4] and to identify suitable alternatives, such as lightweight blockchain schemes [5], that can complement conventional upper-layer security cryptographic systems.

Among possible solutions, physical layer security (PLS) is emerging as an attractive alternative [6]. Authentication schemes at the physical layer, in particular, has some main benefits [7]: first, they are keyless and do not require users to exchange secret keys or any other trusted party to provide the necessary credentials; second, the level of security that can be achieved is independent of the computational power of the attacker, because it only depends on the distinctive properties of the communication channels.

Physical layer authentication (PLA) provides mechanisms for message authentication based on hardware fingerprint or imperfections of the wireless transceivers [8], or on the distinctive characteristics of the communication medium, such as the channel state information (CSI), the received signal strength indicator (RSSI), the channel frequency response (CFR) and the angle-of-arrival (AoA) [9]. In the last years, several papers have proposed the use of PLA schemes in combination with machine learning (ML) techniques [10–12] to enhance the level of security. In these works, channel characteristics are taken as features to feed the algorithm and to facilitate the distinction between different users.

ML and deep learning (DL) algorithms are often trained supposing to know something about the adversarial channel [13]. However, this is an unrealistic assumption in a real scenario. Binary classification is

* Corresponding author.
E-mail address: l.senigagliesi@staff.univpm.it (L. Senigagliesi).

https://doi.org/10.1016/j.phycom.2025.102626
Received 30 July 2024; Received in revised form 30 September 2024; Accepted 12 February 2025
Available online 28 February 2025

usually considered, where the initial training phase includes several examples of legitimate and illegitimate CSI [14]. Knowing some information about the attacker gives an indisputable advantage, since algorithms can more easily recognize the presence of possible opponents by being aware of their peculiar characteristics. In order to provide a real evaluation of the security level that PLA can achieve in practice, one-class classification (OCC) [15] represents a more appropriate solution. These ML techniques, in fact, learn from a training set containing samples from a single class, which, in an authentication scenario, is that of the legitimate transmitter. Among possible approaches, this paper focuses specifically on autoencoders working in anomaly detection mode [16], where eventual anomalies indicate that forged messages have been detected. Autoencoders have been recently successfully applied to PLA in different contexts which have different characteristics and issues from those considered in this paper, including underwater acoustic networks [17], Industrial Internet of Things (IIoT) [18] and satellite communications [19]. All of these works, however, consider synthetic datasets to test the proposed methodology, and the same happens frequently with several PLA approaches [20–23]. Real datasets are usually built by using GNURadio [24,25] or, more often, Universal Software Radio Peripherals (USRPs) to simulate the behavior of nodes within the network.

1.1. Related work

USRPs have been extensively used in the literature to generate real datasets for testing PLA protocols. In [26], the researchers used the Carrier Frequency Offset (CFO) as a device-specific fingerprint to authenticate static nodes. In a subsequent study [27], they expanded on this by utilizing time-varying CFO as a unique identifier to detect spoofing attacks. The experimental setup involved USRP nodes representing the authentication characters, i.e., legitimate transmitter and receiver, and adversary. The unique properties of time-varying CFO, influenced by randomly varying Doppler shifts, were leveraged for authentication purposes. None of these works, however, employed ML to improve authentication, but a Kalman filter was applied at the receiver to predict CFO variations.

USRP-based generated datasets are often used in conjunction with ML algorithm to enhance authentication performance. Already in 2017, a dataset obtained with USRP N210 SDR has served to experimentally validate a Gaussian Mixture Model (GMM) based clustering algorithm to authenticate users in mission critical machine type communications [28].

Adaptive neural networks have been suggested as a method of achieving adaptive authentication in [29], along with a prototype implementation on a platform for USRP in the presence of multipath fading. It is also assumed that a pre-shared secret key is accessible during the training stage.

Authors of [30] proposed a physical layer channel information approach combined with machine learning (specifically, a support vector machine (SVM) algorithm) for detecting clone and Sybil attacks in industrial edge networks, using six USRP platforms, where each one represents an industrial edge computing node. In [13] a physical layer spoofing detector in multiple input multiple output (MIMO) systems over USRPs is implemented, using AdaBoost algorithm.

In [31] a DL-based PLA framework is proposed to enhance the security of industrial wireless sensor networks (IWSNs). Three algorithms, the deep neural network (DNN)-based sensor nodes' authentication method, the convolutional neural network (CNN)-based sensor nodes' authentication method, and the convolution preprocessing neural network (CPNN)-based sensor nodes' authentication method, have been adopted to implement PLA in IWSN. The experiments have been performed with USRPs to evaluate the authentication performance of the proposed algorithms.

An approach for PLA in industrial wireless cyber–physical systems has been proposed in [14], conducting simulations on a real industrial dataset. A long term evolution (LTE) stack is implemented on the USRP platforms, using orthogonal frequency division multiplexing (OFDM) and time-division duplexing. Decision trees, SVMs, k-nearest neighbors (k-NN) and ensemble learning are considered. Reinforcement learning is applied in [32] for PLA in a dynamic wireless environment with a receiver and possible spoofers. Experimental results over USRPs in an indoor environment are carried out to test the proposed spoofing detection scheme.

In [33], the goal was to use CFO as a device fingerprint to distinguish long-range (LoRa) devices via a USRP (acting as the authenticator) and to compensate for the frequency drift in received signals. Using received LoRa IQ samples, FFT, and spectrogram analysis, the results demonstrated that CFO estimation and compensation effectively reduced device misclassification rates. A hybrid DL classifier was employed to adjust for each transmitter's inherent CFO. The research was further extended in [34], considering long-term CFO measurements over several months. Additionally, multilayer perceptron (MLP) and long short-term memory (LSTM) network classifiers were implemented and evaluated, along with the previously used CNN. Since this paper is not focused on authentication but on identification, no attack is considered and all the employed neural networks are trained on multiple classes. USRPs are exploited for physical layer identification also in [35,36]. In [37] experiments were conducted using 50 off-the-shelf Wi-Fi devices. Different fusion strategies were implemented and six deep neural networks were used, including fully connected neural network (FNN), CNN and recursive neural network (RNN).

Recently, authors of [38] developed an experimental analysis based on the use of USRPs to evaluate a multi-frequency band PLA protocol. The dataset was built in an indoor environment and a data-driven method based on binary SVM was employed.

The literature reviewed highlights a significant gap in the current body of work: the absence of a clearly defined and practically applicable attacking model. More specifically, there is a lack of research that focuses on implementing such models in real-world scenarios, where practical challenges and unpredictability are factors. Additionally, many of the existing studies predominantly rely on binary classification methods to address the problem. However, these approaches fall short when applied to PLA techniques. This is because binary classification assumes that the authenticator possesses a certain level of knowledge—either complete or partial—about both the attacker and the adversarial communication channel. In reality, this assumption is often unrealistic, as real-world adversaries and channels can be much more dynamic and unpredictable. Therefore, more sophisticated models and techniques are needed to address the complexities of real-world PLA systems.

1.2. Contribution

In this paper, an approach is proposed to overcome the existing gaps highlighted in the literature reviewed above, with particular reference to the lack of a well-defined attacking model, especially its implementation in a real world scenario, and the use of binary classification methods, which are not realistic for a PLA approach.

An assessment of the authentication performance achievable by implementing a PLA scheme in a real indoor environment is provided. First, the proposed method is tested on a simulated scenario to prove its validity. A wireless OFDM transmission is then realized to implement a communication between two nodes, in the presence of an adversary who aims to impersonate the legitimate transmitter. An attacking model which can be implemented through USRP is then defined, allowing the adversary to sense the legitimate transmitter power level and adjusting itself as a consequence. Finally, a sparse autoencoder working in anomaly detection mode and trained only on the legitimate user's channel fingerprint is exploited to distinguish the legitimate channel from the adversary's one. Autoencoder capability to keep up with channel variation over time is proven through the

comparison with other simpler OCC algorithms.

The rest of the paper is organized as follows. Section 2 outlines the considered authentication setup is provided, along with the adversarial model. In Section 3 a description of the proposed ML methodology is provided. Section 4 illustrates the setting used to generate the simulated dataset, which is necessary to test the proposed approach. The setup for experimental measurements is detailed in Section 5. Numerical results and discussion are reported in Section 6. Finally, Section 7 concludes the paper.

2. System model

To take into account the most widely adopted transmission scheme, in this paper an OFDM transmission is modeled, where communications occur over a series of N subcarriers. In order to apply PLA, the receiver estimates the time-variant channel response of each subcarrier and exploits this information to discriminate the legitimate transmitters from possible adversaries in the network.

Channel frequency response (CFR) samples generally consist of three parts: a fixed part representing the channel's average response over time (and containing information on spatial variability), a variable part with zero mean, and receiver additive white Gaussian noise (AWGN) noise. The vector collecting the CFRs estimated on the N subcarriers at time kT [39] is represented by

$$\hat{\mathbf{h}}^{(\mathrm{XY})}[k] = \mathbf{h}^{(\mathrm{XY})} + \boldsymbol{\epsilon}[k] + \mathbf{w}[k], \tag{1}$$

where X and Y represent a general couple of transmitter and receiver, respectively, $\boldsymbol{\epsilon}[k]$ is the zero-mean variable part at time kT, $\mathbf{w} \sim \mathcal{CN}(\mathbf{0}_{N\times 1}, \sigma^2\mathbf{I}_N)$ represents the vector of AWGN samples at time kT, where $\mathcal{CN}(\mathbf{0}, \mathbf{R})$ denotes the distribution of circularly symmetric complex Gaussian random vectors (with zero mean) having covariance matrix $\mathbf{R}$. It is assumed that $\boldsymbol{\epsilon}[k]$ is independent of $\mathbf{w}[k]$.

The temporal dispersion of a time-variant wireless channel $c(t, \tau)$ is described according to a discrete tapped-delay-line with L taps model [40], given by

$$c(\tau, t) = \sum_{l=1}^{L} A_l(t)\delta(t - \tau_l), \tag{2}$$

where t corresponds to the observation time and τ_l and $A_l(t)$ are, respectively, the delay and complex amplitude of the lth multipath component, being $A_l(t)$ a time-variant uncorrelated Gaussian random process with zero mean and Doppler power spectrum $S_l(f)$. The Doppler power spectrum considers the mobility of nodes within the network. Two cases are usually considered, the flat Doppler spectrum for static nodes and the Jakes spectrum for moving nodes. The term $\boldsymbol{\epsilon}[k]$ in (1), which represents the frequency response of the variable part, is the Fourier transform of $c(\tau, t)$ in terms of τ [39].

2.1. Authentication protocol

Authentication processes are usually based on two steps. During the first step, or *training phase*, an authenticator, named Bob, collects K samples $\hat{\mathbf{h}}^{(\mathrm{AB})}$ that he knows for sure are coming from the legitimate transmitter, Alice. These K samples constitute the channel profile that Bob associates to Alice. At the end of the training phase, Bob receives additional messages without being certain of their origin. Bob estimates the channel through which these new packets arrive and uses this estimate $\hat{\mathbf{h}}^{(\mathrm{XB})}$ (where X represents the unknown sender) to determine the source of the new messages. During this authentication phase, in fact, an adversary, named Eve, tries to impersonate Alice and to be authenticated by Bob. During both phases, the receiver is assumed to be in a fixed position, while the transmitter and attacker may move with different velocities.

Since the channel is time-varying, the channel profile evaluated by Bob during the authentication phase may differ from the one evaluated previously. Besides taking into account this variability without accidentally rejecting messages from Alice (thus incurring in a *false alarm*), Bob must be able also to correctly identify messages coming from possible attackers in the network (who are trying to impersonate Alice and induce a *missed detection*). In order to solve both these problems, autoencoders are considered, as will be explained in the following section.

2.2. Attacker's model

An active attacker (Eve) is considered, with no limitations on her computational power and no assumptions about her position. This scenario emphasizes the need for robust security measures to protect against the worst-case scenario. This kind of analysis is essential for designing robust and resilient authentication solutions. Moreover, in order to make the attacker as powerful as possible, some further preliminary assumptions are considered:

- The attacker knows Alice's and Bob's location.
- Based on this location and eavesdropping the messages sent during the training phase, Eve estimates the power level transmitted by Alice and extracts useful channel statistics. However, she is unable to know the exact statistics of the main channel.
- The attacker adjusts her power level to have an average power value equal to that of Alice.

On the basis of this information, Eve then generates a counterfeit vector $\mathbf{f}$ to best replicate that of the legitimate transmitter. What Bob receives is therefore a noisy version of the vector

$$\hat{\mathbf{h}}^{(\mathrm{E})} = \mathbf{f} + \mathbf{w}_E. \tag{3}$$

During authentication phase, he compares $\hat{\mathbf{h}}^{(\mathrm{E})}$ and (1) to decide who the sender of the new message is on the basis of some predefined metric. In the approach proposed in this paper, this metric corresponds to the reconstruction error produced by a sparse autoencoder, as explained in the next section.

3. Autoencoders for anomaly detection

Bob most likely only receives signals from the authorized transmitter during the training period because the attacker's location and statistics are unknown. Given that Alice's samples represent the target class and Eve's samples are considered outliers, one-class classifiers are the appropriate choice to correctly represent the authentication task in this situation. However, one-class classification in combination with a dimensionality reduction tool, such as principal component analysis (PCA), results ineffective to take into account the temporal evolution of the channels, especially when the channel exhibits rapid time variation. For this purpose, this paper considers the use of autoencoders, a special class of neural networks.

The goal of the family of algorithms known as autoencoders for unsupervised learning is to encode the input into a compressed and meaningful representation before decoding it so that the reconstructed input is as close to the original as possible [41]. An autoencoder consists of an encoder and a decoder, with functions $A : \mathbb{R}^n \to \mathbb{R}^p$, respectively, where n is the dimension of the original data $\mathbf{x}$ and p the dimension of the compressed data $\hat{\mathbf{x}}$, being $n < p$. The two encoding and decoding functions A and B must be designed in order to minimize the loss function

$$\mathcal{L} = \arg\min_{A,B} E[\Delta(\mathbf{x}, \hat{\mathbf{x}})], \tag{4}$$

where E is the expectation over the distribution of x and Δ is the reconstruction loss function, which measures the mean squared error between the output of the decoder and the input.

Here, the focus is on sparse autoencoders [42], as shown by the example in Fig. 1. The key benefits of sparse autoencoders are their

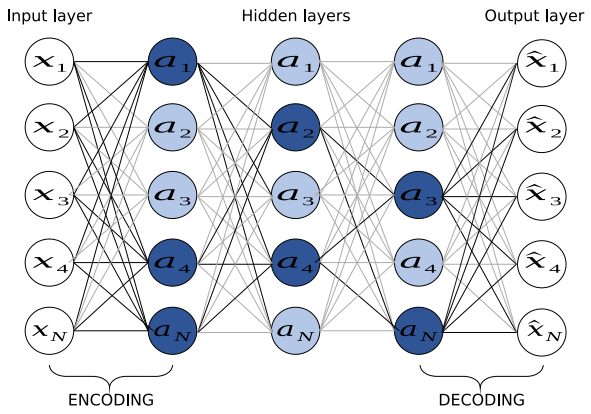


Fig. 1. Sparse autoencoder. Dark blue nodes represent the activated nodes. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

resistance to noise and ability to achieve a decent trade-off between bias and variance. An autoencoder that uses a sparsity penalty as part of its training criteria is known as a *sparse autoencoder*. By penalizing hidden layer activations, which would only encourage a few nodes to activate when a single sample is input into the network, the loss function is typically developed. L1 regularization and KL-divergence are usually the two methods that are taken into consideration while creating a sparsity penalty. In the first case (4) for sparse autoencoders becomes

$$\mathcal{L}_s = \arg\min_{A,B} E[\Delta(\mathbf{x}, \hat{\mathbf{x}})] + \lambda \sum_i a_i, \tag{5}$$

where a_i is the activation at the ith hidden layer and i iterates over all the hidden activations, while λ represents the parameter for L1 regularization.

In the second case the loss function assumes the form

$$\mathcal{L}_s = \arg\min_{A,B} E[\Delta(\mathbf{x}, \hat{\mathbf{x}})] + \sum_j KL(p\|\hat{p}_j), \tag{6}$$

where the regularization term aims at matching p to $\hat{p}$, being p represents the probability of activation of each neuron and $\hat{p}_j = \frac{1}{m}\sum_i a_i(x)$ is the empirical probability calculated for each neuron j.

Assuming that a single class of data is available for training, autoencoder for anomaly detection purpose is applied. The objective of anomaly detection is to learn the "normal behavior" of data when only normal data examples are known (in this case, Alice's channel varying over time), and then to recognize and report the samples not compliant with the normal behavior as anomalies (i.e., Eve's channel estimate). Since a trained autoencoder would be able to learn the latent subspace of typical samples, autoencoders are used for this task. Once trained, it would produce low reconstruction error for typical samples and high reconstruction error for abnormal samples [43–45]. The reconstruction error is defined as

$$Err = \sum_{n=0}^{N-1} \sqrt{(\hat{y}_n - \hat{h}_n)^2}, \tag{7}$$

where $\hat{y}$ is the CFR reconstructed by the autoencoder on each subcarrier and $\hat{h}$ is the actual CFR that Bob is trying to associate to Alice or Eve. The average reconstruction error over a certain interval of time $\Delta\tau$ is the compared with a threshold θ and a decision on the source of the new message is made as follows

$$\begin{cases} \mathbb{E}[Err(\Delta\tau)] \leq \theta : & \text{assign to Alice,} \\ \mathbb{E}[Err(\Delta\tau)] > \theta : & \text{assign to Eve.} \end{cases} \tag{8}$$

The value of θ is chosen to balance the probability of false alarm (FA) and missed detection (MD), as will be explained in more detail in Section 6.

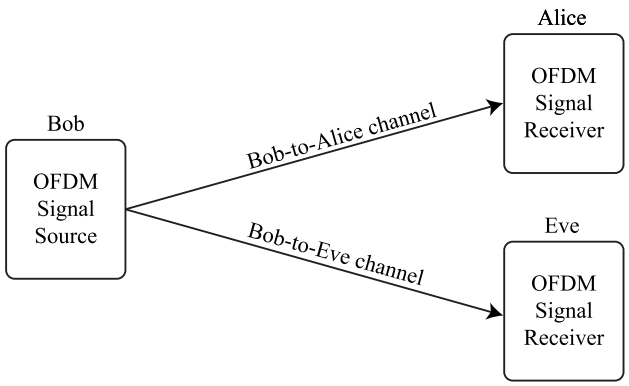


Fig. 2. Scheme of the implemented methodology during simulations and experimental tests.

4. Preliminary simulations

Before validating the proposed method with experimental data, the simulation model was tested considering realistic channel parameters to verify the feasibility of the considered approach. Since in a real scenario the channel characteristics change depending on the positions of transmitters and/or receivers, simultaneous acquisitions by Eve and Alice of the signal transmitted by Bob are performed. With this choice of the test setup, that is the same for simulated and experimental evaluations, the channel responses are evaluated from the spectrum of the signals received by Alice and Eve, considering a constant-in-frequency transmitted signal by Bob. A scheme of the test methodology is depicted in Fig. 2. The simulation was implemented using Matlab2023/Simulink.

4.1. Indoor simulations

To evaluate the effect of time-varying fading channels on the authentication performance, a fixed sequence of complex symbols is sent in input to the OFDM modulation block of a properly designed Simulink model. A flat spectrum of the transmitted signal is then generated, where the number of OFDM subcarriers is 8192. Not the cyclic prefix, neither the guard bands nor the pilot carriers are considered, because they are not of interest for the simulation purposes. The signal generated by the OFDM transmitter, simulating Bob, is organized in a matrix of [8192×k] elements, where 8192 is the number of subcarriers for each OFDM symbol, and k is the number of transmitted symbols. To define the simulation parameters, the bandwidth B of the modulated signal is chosen equal to 40 MHz accordingly with the USRP 2974 capabilities, which will be used in the laboratory setup. The sampling time $t_{sampling}$ can be then derived considering the total number of subcarriers as

$$t_{sampling} = \frac{8192}{40\ \text{MHz}} = 204.8\ [\mu\text{s}]. \tag{9}$$

A simulation time of 20 s is chosen so that, considering the sampling time derived in Eq. (9), the number of transmitted symbols is about 97657. Alice's and Eve's channels are simulated through different blocks which include free space loss, AWGN and fading. The free space loss is computed by considering the transmitted power and the distance of the receiver, where the transmitted power is set to 10 mW and the transmitter–receiver distance varies from 1 m to 5 m, with a step of 1 m. For each value, a simulation is performed. The signal power strength obtained is used to calculate the signal-to-noise Ratio (SNR) to be introduced into the Simulink AWGN block. The noise power N is calculated from the noise figure parameter (NF) of the USRP 2974, which is about 7 dB [46], according to $N = 10\log_{10}(K_B T_e B)$ [dB], where K_B, B and T_e are the Boltzmann's constant, the bandwidth and the equivalent noise temperature, respectively.

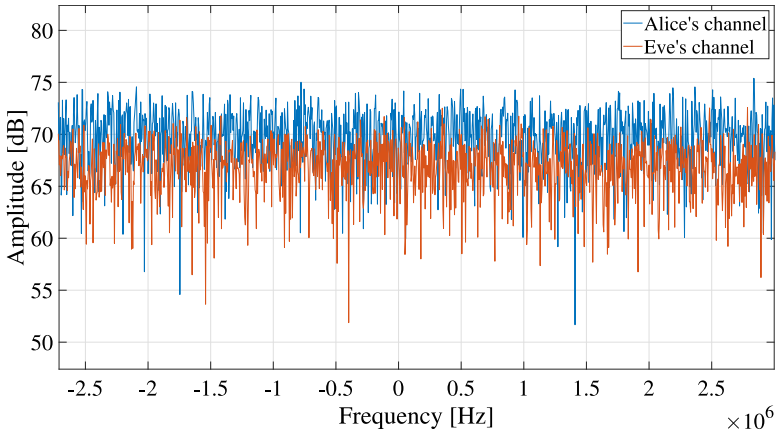


Fig. 3. Example of the fading channel effect on the OFDM transmitted signal. The case is when Alice and Eve are placed at one meter distance from Bob.

Table 1
Simulation parameters.

Parameter name	Value
Number OFDM FFT points	8192
$t_{sampling}$	204.9 μs
Bandwidth (B)	40 MHz
Transmitted power	−20 dBW
Noise Figure (NF)	7 dB
Simulation length	20 s
Alice's and Eve's distances	1, 2, …, 5 m

Fading is simulated using the SISO block, that requires to define the number of received repetitions of the transmitted signal, along with the relative delay and attenuation. These values are obtained through proper ray tracing simulations of the experimental environment, as shown in Fig. 4.

In Fig. 4 a graphical representation of the simulated environment is reported. It depicts a classic indoor situation, with a meeting table surrounded by chairs and other furniture and a wooden wall dividing the room into two separate compartments. The transmitter carrier frequency is 2 GHz and transmitter power is 0.01 W. In the first considered scenario (see Fig. 4(a)), Alice and Bob are in the same compartment, while Eve is in the other one. Alice-Bob distance and Eve-Bob distance are approximately 4.27 m and 7.38 m, respectively, and the height of the three antennas is 1 m. Alice and Eve are approximately 5 m apart. In the second scenario (see Fig. 4(b)), Alice and Eve are in the same compartment, 1.22 m apart. Their distances from Bob are 3.78 m and 5 m, respectively. The obtained fading values, in terms of attenuation and delays of different generated rays, can be introduced within the simulation model and complete the OFDM signal distortion with the fading effect. As mentioned before, a simulation is performed for each value of the distance between Alice and Eve from Bob's position, leading to a total number of twenty-five cases. All the parameters used are summarized in Table 1. An example of the resulting simulated channels is depicted in Fig. 3.

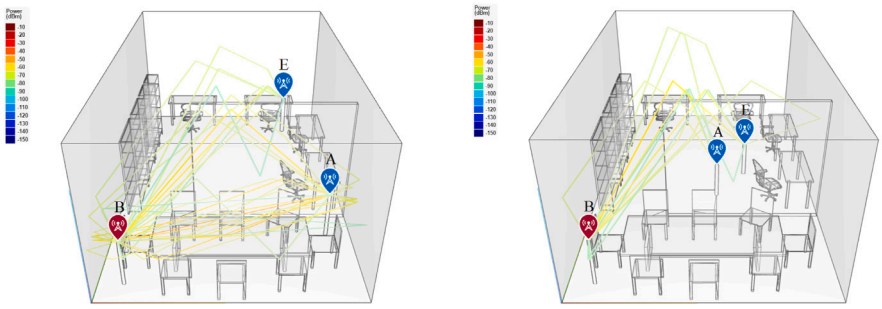
5. Experimental data

For the experimental tests, an indoor environment is considered, namely the Information Engineering Department at Università Politecnica delle Marche in Italy. The setup involves different instrumentation for Bob, Alice and Eve's implementation. To transmit the signal and implement Bob, a Vectorial Signal Transceiver (VST) from National Instruments is used. Thanks to its vectorial features, such a system can generate an arbitrary user defined waveform in baseband that can be moved to a specific radio frequency carrier. The generation is performed by a specific module: the PXIe-5841 is able to allocate signals in the radio frequency range 9 kHz to 6000 kHz. It exploits also 1 GHz of real-time bandwidth [47] for the baseband signal generation. The same features are available at the receiver side of the instrument. The VST can downconvert signals from the radio frequency range 9 kHz to 6000 kHz to baseband with a real-time bandwidth of 1 GHz. Such features make the VST an instrument able to implement Bob's side of the communication system with high performance. The PXIe-5841 has two SMA connectors, one for the transmission and one for the reception. In this work only the transmission is used and a "VERT 2450" antenna was connected, operating in the following frequency ranges: [2.4–2.5], [5.15–5.35], [5.725–5.85] GHz. The same antenna model was then also used for reception, at the two receiver stages of the two USRP-2974s from National Instruments. This second type of instrument is used to implement Eve's and Alice's side of the communication system. Such devices are designed for prototyping and work in the same fashion as the VST. In the experimental setup, they are used to downconvert the radio frequency signal and acquire the complex samples transmitted by the VST. The USRPs have a radio frequency range slightly different than the VST (i.e., 10 kHz to 6000 kHz) and a real-time bandwidth of 160 MHz. As these devices have fewer capabilities than the VST, the limits of the implementation are set by the USRPs. The picture of the described instrumentation is reported in Figs. 5(a) and 5(b).

Owing to channel reciprocity, it is assumed that the estimated channel on the downlink is the same as on the uplink. Therefore, reversed roles for the transmitter and receiver can be considered and these experimental channel measurements to test PLA can be used in the examined setting.

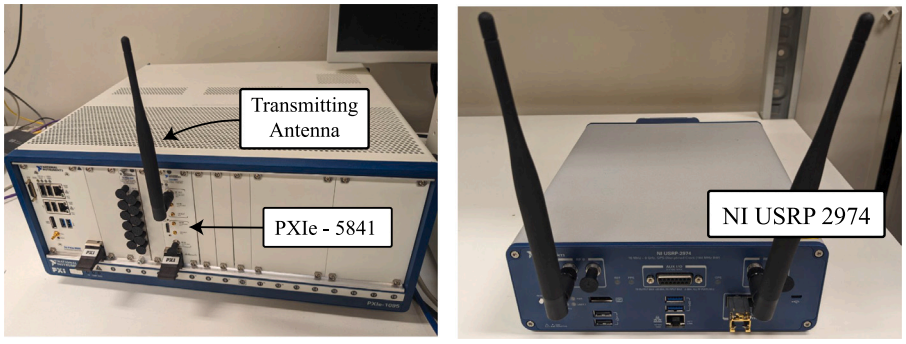
To perform the experimental tests, a different signal is used compared to the one employed for the simulations. In the experimental part it is not necessary to generate a complete OFDM signal, so only the pilot tones are sent. The VST is configured to generate 40 harmonics centered on the 2 GHz carrier, spaced by 1 MHz with a transmitting power of 0 dBm. The power is higher than that of simulations, and the reason lies in the sensibility of the USRP receivers. To obtain a satisfying level of the received signal more power must be transmitted. The harmonic on the central carrier was removed to avoid problems in reception related to the USRP hardware. The signal generated by the VST is depicted in Fig. 6.

Correspondingly, the two USRPs are configured with a center frequency of 2 GHz, a baseband sampling rate of 60 MS/s and a reference level of −20 dBm. The reference level parameter is used to control the gain of the amplifier at the receiver side. Both USRPs are equipped with two channels, and each one can be used for transmitting or receiving purposes. The receiver channels, namely RF0 and RF1, are both used to acquire the radio frequency signals. The two USRPs are named "Alice" and "Eve" and represent an authorized and an unauthorized user, respectively, in a classic wireless transmission security problem.



(a) Alice and Eve distant from each other. (b) Alice and Eve close together.

Fig. 4. Simulated indoor environment.



(a) (b)

Fig. 5. Instrumentation used in the experimental setup: (a) the VST chassis and the PXIe - 5841 module, (b) the NI USRP-2974.

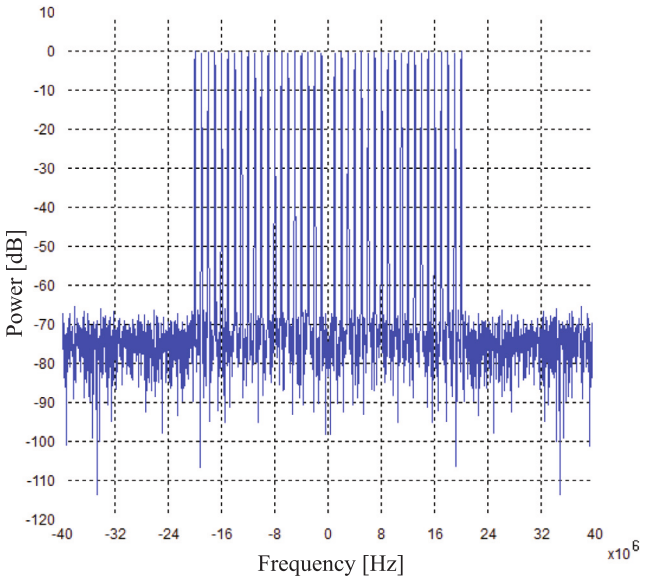


Fig. 6. Signal generated by the VST. The representation is in baseband form.

The tests were carried out at different locations in the Information Engineering Department of Università Politecnica delle Marche by placing Alice and Eve on top of metal at the positions highlighted in Fig. 7. 'B' indicates Bob's position, while couples 'A-E' represent different locations for Alice and Eve. At each location, a signal of 20 s duration was acquired from both USRPs simultaneously and with the same orientation of the antennas (in all possible combinations, i.e., vertical-vertical, vertical-horizontal, horizontal-vertical, horizontal-horizontal). It was chosen to change the orientation of the antennas at each measurement location to evaluate the correlation between the transmitting channels and the orientation of the antennas themselves.

6. Numerical results and discussion

In this section numerical results obtained through simulated and experimental data are shown. In both cases, the absolute values of the CFR measured on each subcarrier represent the feature of the dataset used as input to the DL algorithm. After several tests, it turns out that the CFR phase provides no benefit to the classification results on both simulated and real data. Classification is performed by computing the average error value on 100 successive samples and comparing it with a threshold. Authentication performance is measured in terms of the geometric mean of the accuracy, the probability of false alarm (P_{FA}) and the probability of missed detection (P_{MD}). The geometric mean is defined as $g_{\text{MEAN}} = \sqrt{(1 - P_{\text{FA}})(1 - P_{\text{MD}})}$. Threshold is chosen in order to find a balance between the probabilities of FA and MD by minimizing g_{MEAN}.

First, an example of the application of the sparse autoencoder on the simulated data of distant Alice and Eve is reported in Fig. 8. In this figure, data are alternated, considering 100 samples from Alice and 100 from Eve, and the CFR over time on a single subcarrier is shown. Results obtained on simulated data are shown in Figs. 9(a) and 9(b), both for the case where Alice and Eve are close together and for the case where they are more distant. For the simulations, 10 subcarriers are randomly selected. Both scenarios show an excellent authentication performance, even with a small training set (larger than 20), proving the feasibility

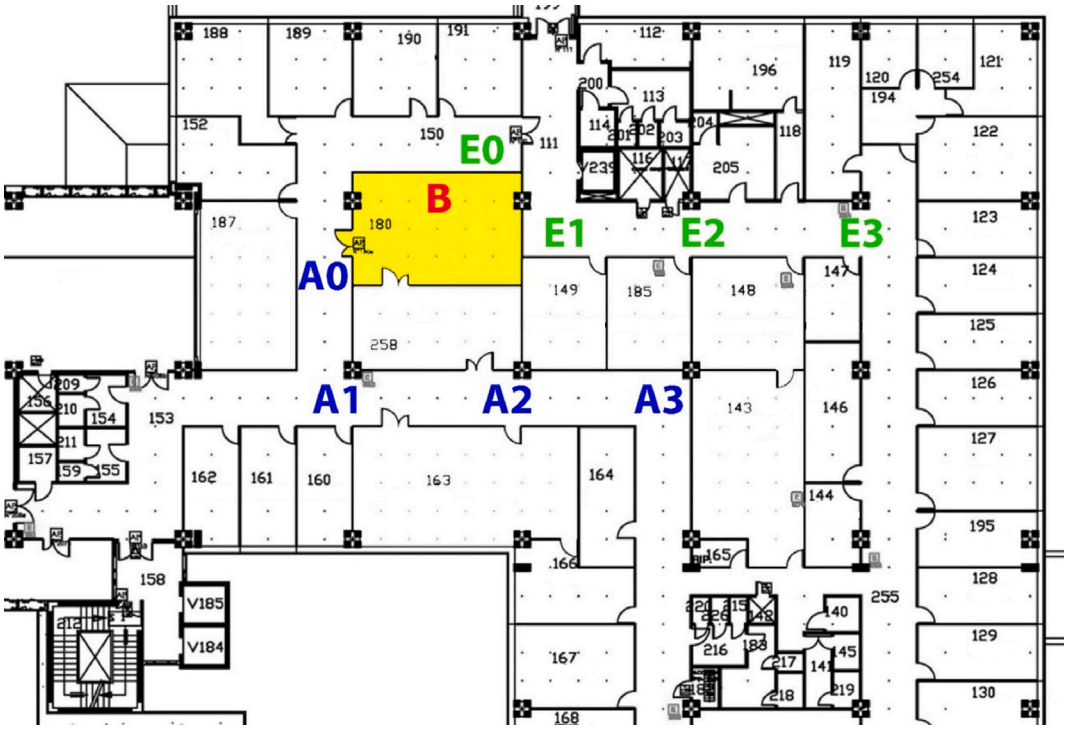


Fig. 7. Measuring stations: B denotes Bob's position, and A and E denote Alice's and Eve's positions, respectively.

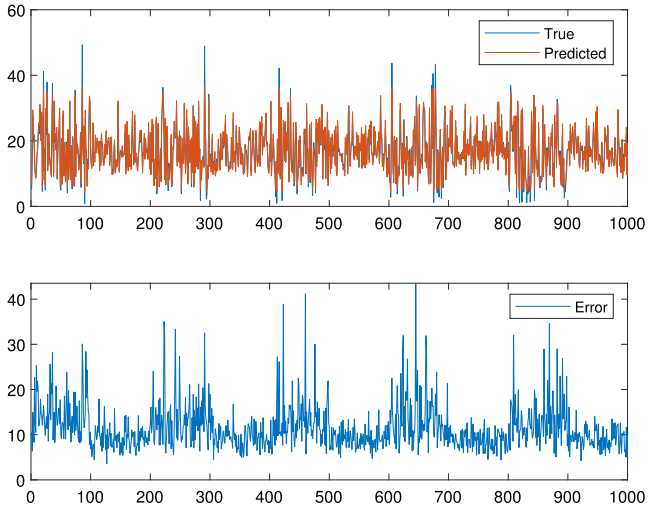


Fig. 8. Example of autoencoder application on a single channel subcarrier.

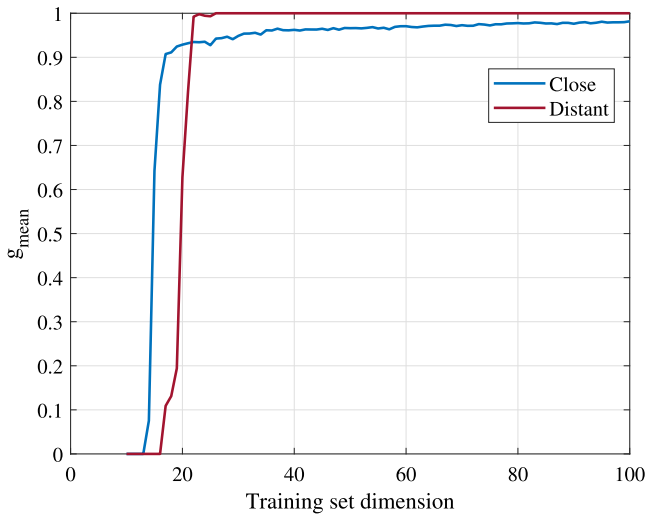
of the proposed approach in an indoor environment. As predictable, it is easier for the autoencoder to distinguish Alice from Eve when they are further apart, although a g_{mean} of 98% is achieved even when they are close, with almost null probability of FA and 1.6% probability of MD. There is no significant improvement with a training set of more than 100 samples. Results have been averaged over 30 trials. After an initial peak of 0.086 (with a training set of 15 samples), variance on results remains below $2 \cdot 10^{-4}$.

After verifying that the proposed approach works well in the case of simulated transmission, the achievable performance in the case of real communication is analyzed. The first thing to note is that, unlike the simulated scenario, the channel is time-varying, being subject to the movement of people and objects within the considered environment. Figs. 10(a) and 10(b) show the g_{mean} and the probabilities of FA and MD achieved by applying the sparse autoencoder on the real data, considering Alice and Eve located in different positions, as illustrated in Fig. 7. The following parameter setting for the sparse autoencoder has been considered:

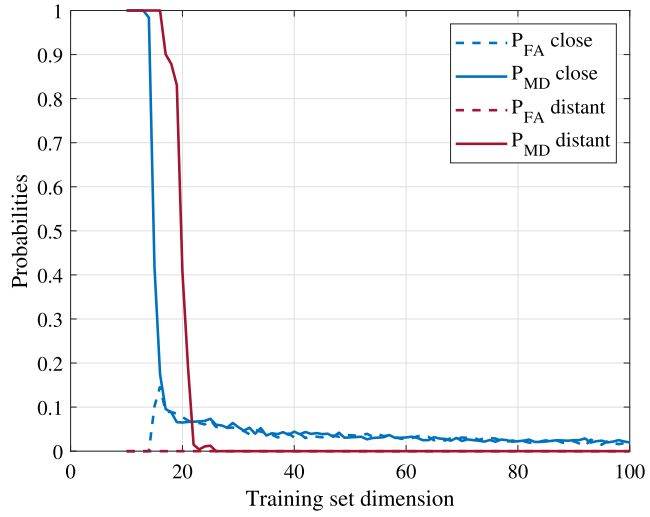
- 600 epochs;
- coefficient for the L2 weight regularizer $2 \cdot 10^{-10}$;
- sparsity regularization 10^{-10};
- sparsity proportion 0.7.

In this case, results have been averaged over 50 trials. Since the receivers have two antennas, equal gain combining (EGC) is applied to the received data and 39 real subcarriers are considered. Compared with results obtained on synthetic data, it can be immediately observed that the size of the training set necessary to have good authentication performance is higher, due to the channel variability introduced. The autoencoder, in fact, needs more data over time to learn the characteristics of Alice's channel. However, as is also the case with simulations, but with due proportion, after a certain value the size of the training set stops having an impact on the results. Also, results prove that the classification accuracy is independent of the distance between the USRPs and the VST. Only the results for Position 1 show some difference from the others, probably caused by a greater channel variability at the initial stage of data collection.

Finally, the proposed approach is compared with other existing OCC algorithms, namely OC-SVM [48] and OC-forest, also known as *isolation forest* [49]. Both these algorithms correspond to the one-class version of the well-known SVM and random forest, and can be used in anomaly detection mode. Differently from autoencoders, these techniques are not designed to properly take into account the time variation of the samples, i.e., in the case here considered, the variation of the channel response over time, as evident from Fig. 11. Starting from the same dataset of real data collected in different positions, it can seen from Figs. 11(a) and 11(b) that OC-SVM and OC-forest are much less effective than autoencoder, leading to worst probabilities of FA and MD. Regarding Fig. 11(a), probability of FA decreases as the size of the training set increases, while MD exhibits the opposite behavior. The results also show lower stability and higher variance than those obtained using the autoencoder, although they were averaged over 150

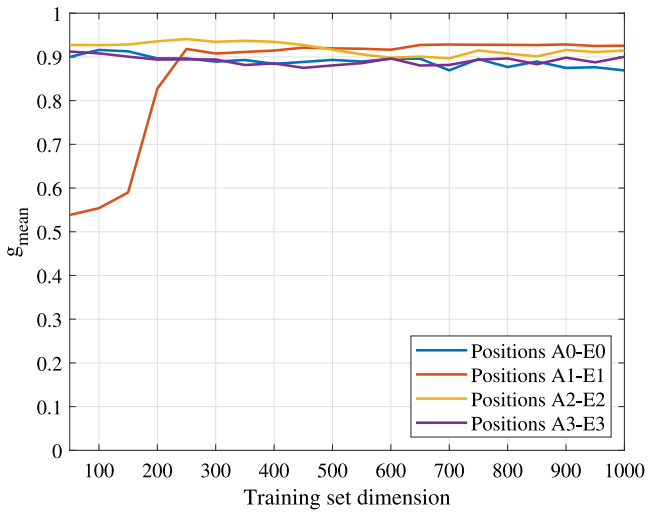


(a) g_{mean}

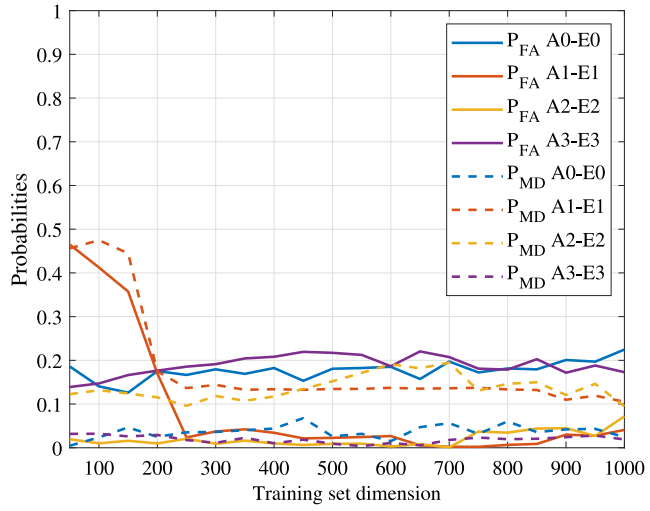


(b) Probabilities of FA and MD

Fig. 9. Authentication performance measured on simulated data by varying the training set dimension.



(a) g_{mean}



(b) Probabilities of FA and MD

Fig. 10. Authentication performance measured on real data by varying the training set dimension, with horizontal antennas, using the sparse autoencoder.

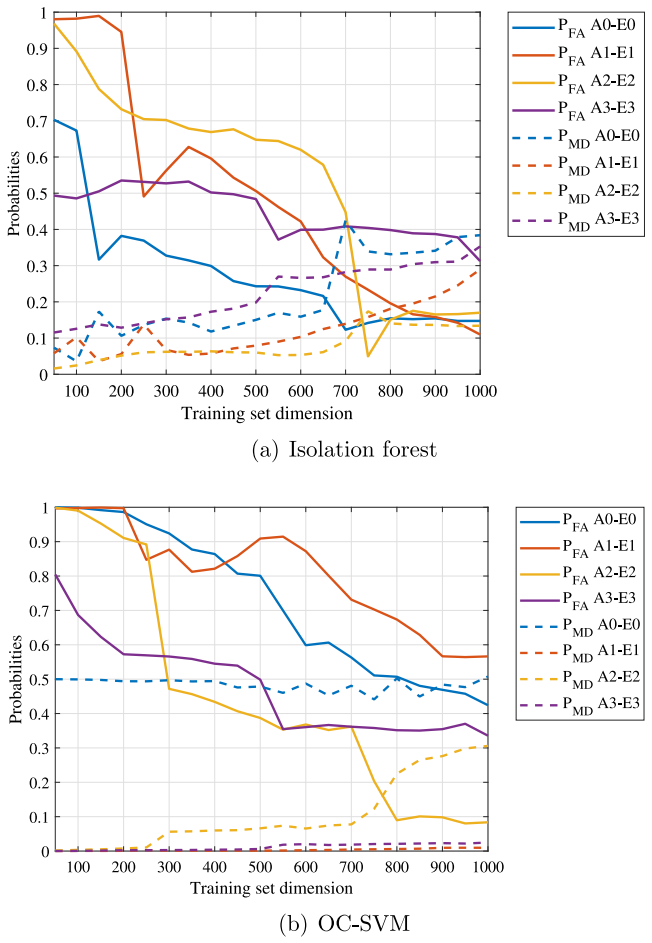
trials.

It is evident from the above results that a machine learning algorithm capable of taking into account the time variability of the channel is necessary to achieve a decent authentication level when considering an indoor scenario characterized by a changing environment, with people moving around and changing multipath components. In particular, the chosen autoencoder presents multiple advantages: it can be trained on a single class, that of the legitimate transmitter, and the training set dimension has a negligible impact in most of the examined cases. More importantly, it enables to obtain very low values of missed detection probability, which means that the adversary is correctly identified in most of the cases. When different algorithms are applied, such as isolation forest and OC-SVM, a marked deterioration in performance becomes visible, since the channel variations are not properly considered.

Despite the good results obtained by means of the sparse autoencoder, one of the key limitations of the paper is the absence of consideration for moving nodes, which are common in real-world network scenarios, especially in mobile and wireless environments. By focusing only on static nodes, the results may not fully capture the dynamic nature of real-world attacks. Moving nodes involve a more rapidly varying channel, which the autoencoder alone cannot keep up with. In this case, machine learning-based classification should be supported by tracking algorithms to enhance the authentication performance. Additionally, the paper employs a relatively simple attack model, which may not adequately represent the complexity and sophistication of real-world adversarial strategies. A more advanced attack model is needed to better simulate realistic adversarial behaviors and evaluate the robustness of the proposed methods under more challenging conditions. Future works will consider these further steps towards a fully realistic scenario.

7. Conclusions

In this paper an approach based on a sparse autoencoder to assess the level of authentication achievable in a real indoor changing environment has been proposed. A real dataset was created by leveraging a Vectorial Signal Transceiver (VST), playing the role of the receiver, and two Universal Software Radio Peripherals (USRPs), emulating the behavior of the legitimate transmitter and the potential adversary.



(a) Isolation forest

(b) OC-SVM

Fig. 11. Probabilities of FA and MD measured on real data by varying the training set dimension, horizontal antennas, using (a) isolation forest and (b) OC-SVM.

The proposed deep learning algorithm has been trained only on data coming from the legitimate user in a short interval of time. Before applying it to real-world data, the autoencoder has been tested with simulated data, proving its effectiveness even when the adversary is less than 1.5 meters away from Alice. Next, the same technique has been applied to real data, collected at different locations within a time-varying indoor environment. Results show that a geometric mean of accuracy higher than 90% is achieved with a small training set, regardless of nodes location, demonstrating the validity and robustness of the proposed approach. Nevertheless, the validity of this paper is limited to a scenario involving only static nodes. Future works will involve a more complicated scenario with moving nodes along with more sophisticated attack models.

CRediT authorship contribution statement

Linda Senigagliesi: Writing – review & editing, Writing – original draft, Methodology, Investigation, Formal analysis. **Gianluca Ciattaglia:** Writing – original draft, Software, Data curation. **Ennio Gambi:** Supervision, Funding acquisition.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This research was supported by the Italian National Project "Programma Operativo Nazionale (PON) Ricerca e Innovazione 2014-2020" (risorse FSE REACT-EU, Azione IV.4 - Contratti di ricerca su tematiche dell'innovazione, CUP CCI2014IT16M2OP005).

Data availability

Data will be made available on request.

References

[1] M.K. Hasan, Z. Weichen, N. Safie, F.R.A. Ahmed, T.M. Ghazal, A survey on key agreement and authentication protocol for Internet of Things application, IEEE Access (2024).
[2] L. Balraj, A. Prasanth, An energy-aware software fault detection system based on hierarchical rule approach for enhancing quality of service in internet of things-enabled wireless sensor network, Trans. Emerg. Telecommun. Technol. 35 (4) (2024) e4971.
[3] A. Munir, I.A. Sumra, R. Naveed, M.A. Javed, Techniques for authentication and defense strategies to mitigate IoT security risks, J. Comput. Biomed. Informatics 7 (01) (2024).
[4] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, M. Ylianttila, Security for 5G and beyond, IEEE Commun. Surv. & Tutorials 21 (4) (2019) 3682–3722, http://dx.doi.org/10.1109/COMST.2019.2916180.
[5] L. Balraj, A. Prasanth, K.D. Sowndarya, T. Kuntavai, A lightweight blockchain scheme for secure data communication in internet of things-enabled wireless sensor network, in: 2024 International Conference on Smart Systems for Applications in Electrical Sciences, ICSSES, IEEE, 2024, pp. 1–6.
[6] L. Mucchi, S. Jayousi, S. Caputo, E. Panayirci, S. Shahabuddin, J. Bechtold, I. Morales, R.-A. Stoica, G. Abreu, H. Haas, Physical-layer security in 6G networks, IEEE Open J. Commun. Soc. 2 (2021) 1901–1914, http://dx.doi.org/10.1109/OJCOMS.2021.3103735.
[7] A. Mukherjee, Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints, Proc. IEEE (ISSN: 0018-9219) 103 (10) (2015) 1747–1761, http://dx.doi.org/10.1109/JPROC.2015.2466548.
[8] A.C. Polak, S. Dolatshahi, D.L. Goeckel, Identifying wireless users via transmitter imperfections, IEEE J. Sel. Areas Commun. (ISSN: 0733-8716) 29 (7) (2011) 1469–1479, http://dx.doi.org/10.1109/JSAC.2011.110812.
[9] T.M. Pham, L. Senigagliesi, M. Baldi, G.P. Fettweis, A. Chorti, Machine learning-based robust physical layer authentication using angle of arrival estimation, in: GLOBECOM 2023-2023 IEEE Global Communications Conference, IEEE, 2023, pp. 13–18.
[10] H. Fang, X. Wang, S. Tomasin, Machine learning for intelligent authentication in 5G and beyond wireless networks, IEEE Wirel. Commun. 26 (5) (2019) 55–61, http://dx.doi.org/10.1109/MWC.001.1900054.
[11] L. Senigagliesi, M. Baldi, E. Gambi, Comparison of statistical and machine learning techniques for physical layer authentication, IEEE Trans. Inf. Forensics Secur. 16 (2021) 1506–1521, http://dx.doi.org/10.1109/TIFS.2020.3033454.
[12] L. Alhoraibi, D. Alghazzawi, R. Alhebshi, O.B.J. Rabie, Physical layer authentication in wireless networks-based machine learning approaches, Sensors 23 (4) (2023) 1814.
[13] S. Chen, H. Wen, J. Wu, J. Chen, W. Liu, L. Hu, Y. Chen, Physical-layer channel authentication for 5G via machine learning algorithm, Wirel. Commun. Mob. Comput. (2018).
[14] F. Pan, Z. Pang, H. Wen, M. Luvisotto, M. Xiao, R.-F. Liao, J. Chen, Threshold-free physical layer authentication based on machine learning for industrial wireless CPS, IEEE Trans. Ind. Informatics 15 (12) (2019) 6481–6491.
[15] M.M. Moya, D.R. Hush, Network constraints and multi-objective optimization for one-class classification, Neural Netw. 9 (3) (1996) 463–474.
[16] L. Senigagliesi, G. Ciattaglia, E. Gambi, Autoencoder based physical layer authentication for UAV communications, in: 2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring), 2023, pp. 1–6, http://dx.doi.org/10.1109/VTC2023-Spring57618.2023.10200623.
[17] P. Casari, F. Ardizzon, S. Tomasin, Physical layer authentication in underwater acoustic networks with mobile devices, in: Proceedings of the 16th International Conference on Underwater Networks & Systems, 2022, pp. 1–8.
[18] R. Meng, X. Xu, B. Wang, H. Sun, S. Xia, S. Han, P. Zhang, Physical-layer authentication based on hierarchical variational autoencoder for industrial Internet of Things, IEEE Internet Things J. 10 (3) (2023) 2528–2544, http://dx.doi.org/10.1109/JIOT.2022.3213593.
[19] G. Oligeri, S. Sciancalepore, S. Raponi, R.D. Pietro, PAST-AI: Physical-layer authentication of satellite transmitters via deep learning, IEEE Trans. Inf. Forensics Secur. 18 (2023) 274–289, http://dx.doi.org/10.1109/TIFS.2022.3219287.

[20] H. Wang, X. Wang, H. Fang, L. Hanzo, GALAMC: Guaranteed authentication level at minimized complexity relying on intelligent collaboration, IEEE Trans. Commun. 71 (5) (2023) 2916–2930, http://dx.doi.org/10.1109/TCOMM.2023.3255245.
[21] M. Abdrabou, T.A. Gulliver, Adaptive physical layer authentication using machine learning with antenna diversity, IEEE Trans. Commun. 70 (10) (2022) 6604–6614, http://dx.doi.org/10.1109/TCOMM.2022.3196648.
[22] K. St. Germain, F. Kragh, Physical-layer authentication using channel state information and machine learning, in: 2020 14th International Conference on Signal Processing and Communication Systems, ICSPCS, 2020, pp. 1–8, http://dx.doi.org/10.1109/ICSPCS50536.2020.9310070.
[23] H. Fang, X. Wang, L. Hanzo, Learning-aided physical layer authentication as an intelligent process, IEEE Trans. Commun. (ISSN: 0090-6778) 67 (3) (2019) 2260–2273, http://dx.doi.org/10.1109/TCOMM.2018.2881117.
[24] W. Lee, S.Y. Baek, S.H. Kim, Deep-learning-aided RF fingerprinting for NFC security, IEEE Commun. Mag. 59 (5) (2021) 96–101, http://dx.doi.org/10.1109/MCOM.001.2000912.
[25] D. Roy, T. Mukherjee, M. Chatterjee, E. Blasch, E. Pasiliao, RFAL: Adversarial learning for RF transmitter identification and classification, IEEE Trans. Cogn. Commun. Netw. 6 (2) (2020) 783–801, http://dx.doi.org/10.1109/TCCN.2019.2948919.
[26] W. Hou, X. Wang, J. Chouinard, Physical layer authentication in OFDM systems based on hypothesis testing of CFO estimates, in: 2012 IEEE International Conference on Communications, ICC, 2012, pp. 3559–3563, http://dx.doi.org/10.1109/ICC.2012.6364429.
[27] W. Hou, X. Wang, J.-Y. Chouinard, A. Refaey, Physical layer authentication for mobile systems with time-varying carrier frequency offsets, IEEE Trans. Commun. 62 (5) (2014) 1658–1667, http://dx.doi.org/10.1109/TCOMM.2014.032914.120921.
[28] A. Weinand, M. Karrenbauer, R. Sattiraju, H. Schotten, Application of machine learning for channel based message authentication in mission critical machine type communication, in: European Wireless 2017; 23th European Wireless Conference, 2017, pp. 1–5.
[29] X. Qiu, J. Dai, M. Hayes, A learning approach for physical layer authentication using adaptive neural network, IEEE Access 8 (2020) 26139–26149.
[30] S. Chen, Z. Pang, H. Wen, K. Yu, T. Zhang, Y. Lu, Automated labeling and learning for physical layer authentication against clone node and sybil attacks in industrial wireless edge networks, IEEE Trans. Ind. Informatics 17 (3) (2021) 2041–2051, http://dx.doi.org/10.1109/TII.2020.2963962.
[31] R.-F. Liao, H. Wen, J. Wu, F. Pan, A. Xu, Y. Jiang, F. Xie, M. Cao, Deep-learning-based physical layer authentication for industrial wireless sensor networks, Sensors 19 (11) (2019) 2440.
[32] L. Xiao, Y. Li, G. Han, G. Liu, W. Zhuang, PHY-layer spoofing detection with reinforcement learning in wireless networks, IEEE Trans. Veh. Technol. 65 (12) (2016) 10037–10047, http://dx.doi.org/10.1109/TVT.2016.2524258.
[33] G. Shen, J. Zhang, A. Marshall, L. Peng, X. Wang, Radio frequency fingerprint identification for LoRa using spectrogram and CNN, in: IEEE INFOCOM 2021 - IEEE Conference on Computer Communications, 2021, pp. 1–10, http://dx.doi.org/10.1109/INFOCOM42981.2021.9488793.
[34] G. Shen, J. Zhang, A. Marshall, L. Peng, X. Wang, Radio frequency fingerprint identification for LoRa using deep learning, IEEE J. Sel. Areas Commun. 39 (8) (2021) 2604–2616, http://dx.doi.org/10.1109/JSAC.2021.3087250.
[35] S. Riyaz, K. Sankhe, S. Ioannidis, K. Chowdhury, Deep learning convolutional neural networks for radio identification, IEEE Commun. Mag. 56 (9) (2018) 146–152, http://dx.doi.org/10.1109/MCOM.2018.1800153.
[36] K. Sankhe, M. Belgiovine, F. Zhou, S. Riyaz, S. Ioannidis, K. Chowdhury, ORACLE: Optimized radio classification through convolutional neural networks, in: IEEE INFOCOM 2019 - IEEE Conference on Computer Communications, 2019, pp. 370–378, http://dx.doi.org/10.1109/INFOCOM.2019.8737463.
[37] S. Zeng, Y. Chen, X. Li, J. Zhu, Y. Shen, N. Shiratori, Time–frequency fusion for enhancement of deep learning-based physical layer identification, Ad Hoc Networks 142 (2023) 103099, http://dx.doi.org/10.1016/j.adhoc.2023.103099, URL https://www.sciencedirect.com/science/article/pii/S1570870523000197.
[38] S. Han, H. Lee, J. Choi, E. Hwang, Multi-frequency band physical-layer authentication in indoor environment, in: GLOBECOM 2023 - 2023 IEEE Global Communications Conference, 2023, pp. 1741–1746, http://dx.doi.org/10.1109/GLOBECOM54140.2023.10436790.
[39] L. Xiao, L.J. Greenstein, N.B. Mandayam, W. Trappe, Using the physical layer for wireless authentication in time-variant channels, IEEE Trans. Wirel. Commun. 7 (7) (2008) 2571–2579, http://dx.doi.org/10.1109/TWC.2008.070194.
[40] P. Bello, Characterization of randomly time-variant linear channels, IEEE Trans. Commun. Syst. 11 (4) (1963) 360–393, http://dx.doi.org/10.1109/TCOM.1963.1088793.
[41] D. Bank, N. Koenigstein, R. Giryes, Autoencoders, 2020, arXiv:2003.05991.
[42] R. Shi, J. Ji, C. Zhang, Q. Miao, Boosting sparsity-induced autoencoder: A novel sparse feature ensemble learning for image classification, Int. J. Adv. Robot. Syst. 16 (3) (2019) 1729881419853471.
[43] D. Gong, L. Liu, V. Le, B. Saha, M.R. Mansour, S. Venkatesh, A.v.d. Hengel, Memorizing normality to detect anomaly: Memory-augmented deep autoencoder for unsupervised anomaly detection, in: Proceedings of the IEEE/CVF International Conference on Computer Vision, 2019, pp. 1705–1714.
[44] K. Zhang, M. Peng, P. Zhang, X. Li, Secrecy-optimized resource allocation for device-to-device communication underlaying heterogeneous networks, IEEE Trans. Veh. Technol. 66 (2) (2017) 1822–1834, http://dx.doi.org/10.1109/TVT.2016.2566298.
[45] B. Zong, Q. Song, M.R. Min, W. Cheng, C. Lumezanu, D. Cho, H. Chen, Deep autoencoding gaussian mixture model for unsupervised anomaly detection, in: International Conference on Learning Representations, 2018.
[46] USRP-2974, 2023, https://www.ni.com/it-it/shop/model/usrp-2974.html. (Accessed 22 August 2023).
[47] PXIe-5841, 2023, https://www.ni.com/it-it/shop/model/pxie-5841.html. (Accessed 22 August 2023).
[48] K.-L. Li, H.-K. Huang, S.-F. Tian, W. Xu, Improving one-class SVM for anomaly detection, in: Proceedings of the 2003 International Conference on Machine Learning and Cybernetics (IEEE Cat. No. 03EX693), vol. 5, IEEE, 2003, pp. 3077–3081.
[49] F.T. Liu, K.M. Ting, Z.-H. Zhou, Isolation forest, in: 2008 Eighth IEEE International Conference on Data Mining, 2008, pp. 413–422, http://dx.doi.org/10.1109/ICDM.2008.17.

Linda Senigagliesi received the Ph.D. degree in information engineering from the Università Politecnica delle Marche, Ancona, Italy, in 2019. During her Ph.D., she was a Visiting Student with the Department of Electrical Engineering, Chalmers University of Technology, Gothenburg, Sweden. She is currently an Assistant Professor of Telecommunications with the Information Engineering Department (DII), Università Politecnica delle Marche. Her main research interests include information-theory and physical layer security, with application to distributed storage systems and wireless communications. Her activity is focused on machine learning techniques for physical layer authentication and privacy. Dr. Senigagliesi is a member of the IEEE INGR Physical Layer Security Focus Group and Cost Action CA22168—Physical Layer Security for Trustworthy and Resilient 6G Systems (6G-PHYSEC). She has served on the Technical Program Committee of several international conferences.

Gianluca Ciattaglia received the bachelor's and master's degree in electronic engineering and the Ph.D. degree in information engineering from the Università Politecnica delle Marche, Ancona, Italy, in 2014, 2017, and 2022, respectively. In 2018, he worked at Ferrari S.p.A., Maranello (MO), Italy, as an Electronics Engineer. Since 2022, he has been a Research Fellow with the Università Politecnica delle Marche. He works on signal processing and measurements for Radar sensors.

Ennio Gambi received the Laurea degree in electronic engineering from the University of Ancona, Ancona, Italy, in 1986. In 1992, he joined the Università Politecnica delle Marche, where he is currently an Associate Professor of Telecommunications. He has authored more than 200 scientific publications, and has been a supervisor of more than 500 degree theses. His main research interests are currently focused on the applications of millimeter-wave radars and red green blue-depth (RGB-D) sensors, with particular attention to the observation of subjects for the extraction of vital parameters, through the processing of extracted data based on machine learning algorithms. He has also been dealing with home automation systems for some time and their evolution toward ambient assisted living systems, and is interested in systems for monitoring the gas composition, aimed at ensuring air quality