This letter addresses the problem of Internet of Things (IoT) authentication when cryptographic means are not feasible or they have limited applicability due to constraints in the context or due to the limited computing capabilities of the IoT devices. This letter presents a novel approach for the authentication of IoT wireless devices using their Radio Frequency (RF) emissions where Convolutional Neural Networks (CNN) in combination with Recurrence Plots (RP) are applied. In recent years various studies have demonstrated that wireless devices can be authenticated on the basis of their RF emissions because physical differences generate different features in the RF signal during communication. Recently Deep Learning (DL) techniques based on CNN and other algorithms have been applied to this authentication problem. In this letter we present a novel application of CNN based on the use of RP where the original time series derived from the digitized RF emissions is transformed into images on which CNN are applied. The proposed approach is applied to an experimental data set of RF emissions collected from 11 IoT devices of the same model. The results show that this technique can provide superior performance if compared to conventional machine learning algorithms based on the extraction of statistical features.

KEYWORDS
authentication, Internet of Things, machine learning, radio frequency, security, signal processing, wireless communication

1 INTRODUCTION

This letter addresses the problem of authentication of Internet of Things (IoT) devices when the authentication based on cryptographic means is difficult to achieve due to the limitations of the IoT devices or because the context does not support an efficient distribution of cryptographic materials (e.g., keys and certificates). As mentioned in Reference 1 although the design of bullet-proof authentication mechanisms is always desirable, it may be not applicable to several IoT scenarios because it may imply high computational cost and/or always connected trusted entities. For these reasons, we propose in this letter an authentication mechanism of IoT devices to be an alternative to cryptography-based authentication or to complement it (i.e., multifactor authentication).

Authentication is an important security function. Its purpose is to prove that an entity is what it claims to be. Authentication can be based on something known to the entity (e.g., a personal a password), something that is physically unique to the entity (e.g., the biometrics of a person) or something that an entity has (e.g., a smart-card). In this paper, we focus on the authentication of wireless devices. In the research literature, this is mostly based on some information known by the wireless device or owned by it (e.g., a cryptographic key or a SIM card in a wireless mobile phone). The risks associated to these two approaches are well known: cryptographic keys can be extracted from the wireless devices in the absence of adequate protection measures,
subject to social security attacks, while a Subscriber Identification Module (SIM) card can be lost or damaged. In this letter, we investigate the use of the physical properties of the wireless devices (i.e., what an entity is) to implement unique authentication.

The general idea is that specific physical features of an electronic device can appear in its outputs and they can be used to uniquely identify or authenticate the device itself. For example, a mobile phone is composed by many components (e.g., digital camera, RF front end) and the digital output of each of these components (e.g., images captured by the camera) can embed physical fingerprints, which can be used for authentication. In the case of the mobile phone, the recent survey describes the different techniques used for authentication of the mobile phone through its components. One example is the Sensor Pattern Noise (SPN) used to distinguish cameras, based on the images they produce.

The advantage of the physical properties approach is that they cannot be easily reproduced and therefore cloned. They also cannot be lost or damaged because they are physically embedded in the device. There are also potential shortcomings, which must be addressed for practical use. The main one is that this approach provides a statistical probability that the device is legitimate and it does not provide a truefalse certainty as in the case of a cryptographic key or a SIM. As a consequence, the main challenge and focus of the research community is to guarantee a high level of authentication accuracy. In this context this technique can also be used to implement multifactor authentication to augment conventional cryptographic authentication.

This approach is also called Radiometric signature identification or RF-DNA fingerprinting and it is mostly implemented by extracting statistical features or applying specific transforms (e.g., Wavelet Analysis) to the digitized samples representing RF emissions. In this letter, we use the term radiometric identification to mean physical layer authentication of wireless devices. Very recently, deep learning approaches have been applied to this context. Researchers have applied CNN to identify the RF fingerprints of wireless devices and they prove that CNN can obtain an improved identification accuracy in comparison to conventional methods based on statistical features extraction.

1.1 Our contribution
In this letter, we apply CNN in combination with the Recurrence Plots (RP) techniques to the problem of physical layer authentication, which has not been attempted in literature yet. RP are a technique to visualize the recurrences of dynamical systems and they are used, in this context, to transform the digitized RF emissions, which are then submitted to a CNN. The proposed approach is applied on an experimental data set of the RF emissions from 11 IoT wireless devices of the same model. We evaluate the impact on the classification performance of various parameters used in the generation of the RPs. The results are compared to the techniques from the literature applying the CNN and statistical feature extraction.

2 METHODOLOGY FOR DATA COLLECTION AND PROCESSING

2.1 Workflow
The overall workflow for the collection and processing of the RF emissions in the test bed is described by the Figure 1.

The methodology is composed by the following steps:

1 the RF signal in space transmitted by each device is collected using a SDR USRP type N200 receiver configured with a sampling rate of 5 MHz. The receiver clock is disciplined by a Global navigation satellite system (GNSS) device for timing...
and frequency stability and repeatability. The signal is sampled directly in In-phase and Quadrature (IQ) format and then synchronized and normalized offline to extract the bursts of traffic associated to each payload. For each wireless device, a set of 900 bursts were processed for a total of $900 \times 11 = 9900$ bursts. Each burst is represented by a complex time series.

2. The PR process can be applied both to the modulus and phase components of the complex time series representing the burst. On the other side, RP are usually applied to short time series to reduce the computational effort. Because the bursts collected by the IoT devices are quite long (7104 samples), a segmentation approach based on the mutual distance of the bursts is used to determine the most relevant segment both for the magnitude and phase components. The results show that the first segment of the magnitude component of the burst (the first 256 samples), which contains the power-up transient region of the burst, is the most relevant for classification. These results are consistent with literature, where transients are often used for RAdiometric Identification (RAI). A description of the RP technique is provided in Section 2.2.

3. Then, three different classification approaches are applied. The first is the one proposed in this letter, where RP and CNN are used in combination (it is called RP-CNN in the rest of the letter). The second is where the digital representation of the RF emissions is used directly with CNN (called T-CNN in the rest of this letter). The third approach is where statistical features are extracted from the digital representation of the RF emissions (called FEAT in the rest of this letter). In this letter, we use the same statistical features from literature: spectral entropy, variance, skewness, and kurtosis. The entire data set is split in a training set (three quarters of the entire set equal to 7425 bursts) and a testing set (one quarter of the entire set equal to 2475). The samples are shuffled 10 times using a K-fold approach. For the CNN-based approaches, 1485 bursts of the training set (one fifth) are used for validation.

4. Impact of noise. Additive White Gaussian Noise (AWGN) is added to the original data sample to simulate the presence of environmental noise as it is a common practice in the literature to evaluate the performance of the classification algorithm for different values of Signal to Noise Ratio (SNR).

5. Definition of authentication and identification metrics: two metrics are used to evaluate the performance for authentication and also identification: (a) classification accuracy and (b) confusion matrix.

### 2.2 Recurrence plots

RP is a visualization tool that aims to explore a multidimensional phase space trajectory through a 2D representation of its recurrences. The idea is to identify at which points some trajectories return to a previous state and it is a way to visualize the periodic nature of a trajectory through a phase space. RP can be formulated as:

$$R_{ij} = \theta(\epsilon - \| \vec{s}_i - \vec{s}_j \|), \quad i,j = 1, \ldots, N$$

where $N$ is the number of considered states $\vec{s}_i$, $\epsilon$ is a threshold distance, $\| \cdot \|$ is a distance measurement (i.e., Euclidean norm in this case), and $\theta$ is the Heaviside function. Beyond the threshold, two hyperparameters must be optimized for RP: the embedding dimension and the delay. The results show that the most significant parameter for RAI is the threshold, which has been optimized to $\epsilon = 0.02$. The accuracy for different values of the threshold is also provided in this letter. The embedding dimension and delay are set to 3 and 30, respectively. Figure 2 shows how the recurrence plot (amplitude component) is generated from the initial digital representation of the burst (i.e., the first segment) and the phase space.

### 2.3 Convolutional neural networks

The proposed CNN model for RAI is illustrated in Figure 3. It is made up of three convolution layers and one fully connected layer because it achieved the optimal balance between computing time and performance. The same number of layers is also
used in.\textsuperscript{6} The parameters of different layers are optimized for the problem in question and the data stream is fed to the input layer. For instance, for RP-CNN, the input size was 236*236, as exemplified in Figure 3.

3 | RESULTS AND ANALYSIS

The identification accuracy for the proposed approach and the comparison with T-CNN and FEAT is shown in Table 1, where it can be seen that the proposed approach (RP-CNN) produces a better identification accuracy in comparison to T-CNN and FEAT. In particular, the combination of CNN with RP produces more than 3% improvement in identification accuracy, as compared in comparison to the CNN applied directly to the time domain representation of the signal for the optimal value of $\epsilon = 0.02$. This result shows that CNN (or other Deep Learning algorithms) can benefit from more sophisticated 2D representations of the signal used for RAI. Table 1 also provides the accuracy for other values of $\epsilon$.

The confusion matrix obtained with RP-CNN and $\epsilon$ equal to 0.02 is shown in Figure 4.

Then, the performance of the proposed approach is evaluated for different levels of SNR as this is a common practice in RAI literature.\textsuperscript{5,6} The objective in this letter is to evaluate the impact of attenuation or the presence of obstacles for RAI performance.

We compared the impact of presence of AWGN for different values of SNR. The results are shown in Figure 5, where it can be seen that the RPs approach performs better than the other approaches for high values of SNR, but it has a worst performance for lower values of SNR. The negative impact of noise on RPs analysis is already known in literature.\textsuperscript{10} One mitigation approach is to re-evaluate the RP hyperparameters and especially the threshold as indicated in References 7 and 10.

For this reason, Figure 5 shows the identification accuracy both for $\epsilon$ equal to 0.02 and for $\epsilon$ equal to 0.06. Even if the higher value of the threshold provides a slighter lower identification accuracy at values of SNR above 40 dB, it is significantly better for lower values of SNR. We highlight the practical application of RAI is meaningful when the accuracy is above a specific threshold (eg, 80%) to support the authentication function. In this case, Figure 5 shows that the RP-CNN with $\epsilon = 0.06$ has a better performance than all the other techniques.

4 | CONCLUSIONS

This letter proposes a novel approach for the authentication of IoT devices based on CNN in combination with RP. Its performance has been evaluated in comparison to other techniques identified in literature in this domain. The proposed technique provides a significant improvement against other techniques proposed in recent literature for high values of SNR. For lower
Further research is needed to improve the performance for low values of SNR.

Rather used as a complementary authentication approach (to cryptographic authentication) rather than a principle approach.

Values of SNR, the proposed technique requires the tuning of hyperparameters to mitigate the presence of noise and it can be rather used as a complementary authentication approach (to cryptographic authentication) rather than a principle approach. Further research is needed to improve the performance for low values of SNR.

ORCID

Gianmarco Baldini http://orcid.org/0000-0003-4830-1227

REFERENCES


**How to cite this article:** Baldini G, Giuliani R, Dimc F. Physical layer authentication of Internet of Things wireless devices using convolutional neural networks and recurrence plots. *Internet Technology Letters* 2019;2:e81. [https://doi.org/10.1002/itl2.81](https://doi.org/10.1002/itl2.81)