EAI Endorsed Transactions
on Security and Safety
Research Article EAI.EU

Device Authentication Codes based on RF Fingerprinting using Deep Learning

Joshua Bassey*, Xiangfang Li, Lijun Qian

Center of Excellence in Research and Education for Big Military Data Intelligence (CREDIT)
Department of Electrical and Computer Engineering
Prairie View A&M University, Texas A&M University System
Prairie View, TX 77446, USA.

Abstract

In this paper, we propose Device Authentication Code (DAC), a novel method for authenticating IoT devices with wireless interface, by exploiting their radio frequency (RF) signatures. The proposed DAC is based on RF fingerprinting, an information-theoretic method, feature learning, and the discriminatory power of deep learning. Specifically, an autoencoder is used to automatically extract features from the RF traces and the reconstruction error is used as the DAC, and this DAC is unique to each individual device. Then Kolmogorov-Smirnov (K-S) test is used to match the distribution of the reconstruction error generated by the receiver and the DAC in the received message, and the result will determine whether the device of interest is an intruder. We validate this concept on two experimentally collected RF traces from six ZigBee devices and five universal software defined radio peripheral devices, respectively. The traces span a range of Signal-to-Noise Ratio by varying locations, mobility of the devices, channel interference, and noise to ensure robustness of the model. Experimental results demonstrate that DAC is able to prevent device impersonation by extracting salient features that are unique to each wireless device of interest and can be used to identify radio frequency devices. Furthermore, the proposed method does not need the RF traces of the intruder during model training to be able to identify devices not seen during training, which makes it practical.

Received on 06 October 2021; accepted on 22 November 2021; published on 30 November 2021

Keywords: RF fingerprinting, Device Authentication, Deep Learning, Internet of Things, autoencoder, Kolmogorov-Smirnov (K-S) test.

doi:10.4108/eai.30-11-2021.172305

1. Introduction

Given the proliferation of complex and heterogeneous networks such as 5G, and the Internet-of-Things (IoT) paradigm, the number of deployed wireless devices are expected to grow exponentially in the near future. Furthermore, the concept of the mobile Internet of Things (MIoT) has been introduced, and is based on the integration of mobile devices and IoT. In order to provide many new services envisioned in these communication networks of the future, the security and privacy of these devices and the end users is of the utmost importance. Over the years, a huge proportion the research in wireless communication has been targeted at enhancing transmission capacity and network throughput [1–3]. However, more recently there has been a rising interest network security, and radio frequency fingerprinting (RFF) is one of the many approaches that has received a heightened interest with respect to wireless network security.

Traditionally, wireless authentication has been performed above the physical-layer with key-based cryptographic techniques. While the success of authentication techniques based on pairwise key confirmation has been demonstrated in examples such as cryptosystem, key management still faces a number of challenges when implemented in dynamic wireless communication networks. As the number of mobile and heterogeneous devices in a standardized network grows, sharing of symmetric keys in a safe and timely manner becomes

*Corresponding author. Email: joshuababbs1@gmail.com

more challenging. Also, asymmetric key algorithms are computationally demanding and incur latency which can result in undesirable delays in large-scale networks and delay-sensitive applications. Furthermore, the claim that it is computationally infeasible to crack digital keys is not yet mathematically proven [4]. Consequently, Physical-layer authentication is beginning to attract attention as a complementary approach to authentication.

RF fingerprinting (RFF) refers to the identification a wireless transmitter, by exploiting the physical-layer characteristics specific to it and the communication channel between that transmitter and a receiver [5]. RF fingerprints are typically created during the manufacturing process of the base materials of its components [6]. The creation of fingerprints are usually accidental, but it is possible to generate and insert them on purpose. In either case, they result from minute variations in the electronic components [7] and can be exploited to identify and distinguish one device from another [8], even one of the same make and model [9, 10]. This is the core concept behind RF fingerprint authentication which seeks to permit only authorized users to utilize a network. Unlike RF features, identifiers at other layers such as MAC addresses and International Mobile Subscriber Identity (IMSI) are relatively easy to impersonate [11, 12]. RFF has been used in applications such as radar, intrusion detection systems, IoT and network security in both 4G and 5G networks. RFF has also been used for tracking [7].

Deep learning is a subset of machine learning; a concept in artificial intelligence (AI) concerned with learning from data to optimize an objective. Today, AI has been integrated into almost every aspect of our daily lives, and wireless communication is no exception. Some applications of AI to wireless communication include; wireless sensor networks [13–16], modulation identification [17–19], network resource allocation [20], and abnormal information detection [21, 22]. In this paper, we consider transmitter identity authentication based on RF fingerprinting, using deep learning and information theoretic methods.

The goal of this paper is to introduce the Device Authentication Code (DAC). The process of fingerprint generation and transmitter authentication using the DAC is depicted in Figure 1. An autoencoder (AE) is trained to reconstruct the RF traces by minimizing the reconstruction error. This reconstruction error is the DAC and is used as the device's fingerprint. For authentication, the RF signal is passed through the pretrained AE at the transmitter to generate a DAC (DAC_S). The signal and DAC_S are concatenated before transmission. At the receiver, the received signal is decoupled into the original signal and DAC_S. The signal is then passed through the pretrained AE model deployed at the receiver to generate DAC_R. DAC_S and DAC_R are compared using the Kolmogorov-Smirnov statistic. A match authenticates the transmitting device, otherwise the device is deemed an intruder.

The contributions of this paper are as follows.

- We propose an unsupervised learning approach which does not require any data from the intruder during model training. This makes the proposed method practical since prior knowledge of the intruder is usually not available in reality.
- The proposed DAC is unique to each device due to manufacturing uncertainty, and at the same time it is robust to environmental uncertainties such as wireless channel variations, user mobility, and background noise. These effects are observed in form of varying signal-to-noise ratios (SNR).
- Our novel approach to authentication combines unsupervised deep generative learning and information theoretic methods. To the best of our knowledge, this is the first attempt to use this approach for device authentication.

The rest of the paper is structured in the following manner: In Section 2, we present background and related work. An explanation of the proposed approach is given in Section 3. In Section 4 information on experiments including data collection and analysis of results are presented. Discussion and futherwork are presented in Section 5 and Section 6 contains conclusions.

2. Background and Related Work

RF fingerprinting has its roots in military technologies such as radar used for enemy identification. Traditionally, detection was done by comparison of a received signal waveform with a reference waveform map obtained from the radar. However, with advent of different kinds of equipment, this approach was no longer feasible. Consequently, studies were conducted which focused on extracting characteristics of the communication signals to detect unauthorized transmitters in the VHF FM spectrum range. This gave rise to research on RF fingerprinting technologies, and subsequent design of RF fingerprint extraction and authentication methods. In this work, the focus is on two major phases of RF fingerprinting: (1) wireless transmitter RF fingerprint extraction, and (2) RF fingerprint authentication.

2.1. RF Fingerprint Feature Extraction

In RF feature extraction the features of the communication signal are extracted and transformed into an RF fingerprint suitable for identification purposes. We

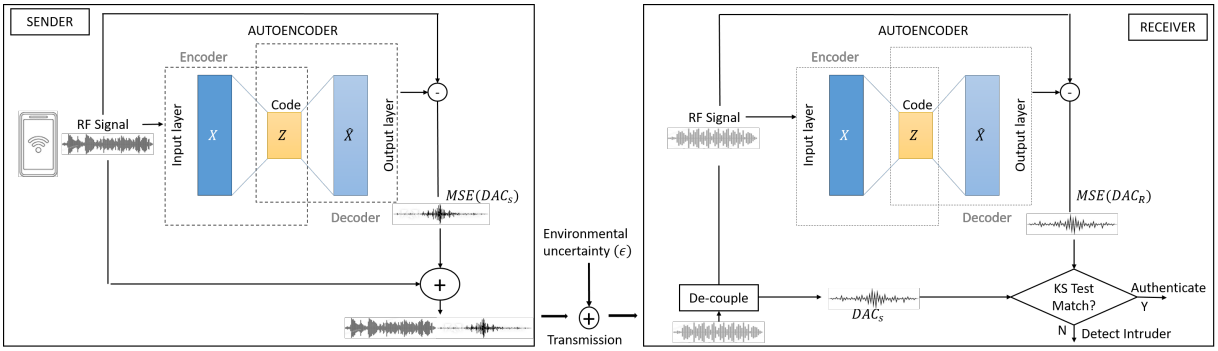

Figure 1. Authentication using the proposed Device Authentication Code

herein provide a brief background on the state-of-the art on RF fingerprint feature extraction approaches for wireless transmitters.

RF feature extraction approaches typically exploit specific constraints in the communication signal. Some approaches exploit the signal transform domain, some exploit certain nonlinear characteristics inherent to the transmitter, and others apply image processing techniques. These methods of fingerprint extraction are derived from the signal's numeric features and seek to apply linear and/or non-linear transformations to identify the inherent structure of the preprocessed communication signal. They then transform the signal to a different manifold by dimension reduction of the source signal to mitigate over fitting by classifiers. Some exploited signal parameters include higher order moments and spectral domain parameters, frequency domain and time domain parameters. For example, the I/Q imbalance in the modulation domain was used as RF fingerprint in [23]. The amplitude of transient signals were used to identify IEEE 802.11 and Bluetooth devices in [24, 25]. However, the time complexity of the approach is relatively high.

In [26] it was shown that it is possible to classify devices by exploiting the information inherent in the phase of the signal. The differences in the phase characteristics of demodulated data samples from transmitters of the same manufacturer were used as the RF fingerprint to achieve classification accuracy of up to 99.6% at short range. The accuracy decreases with distance and goes to 95.3% and 81.9% at medium and long range respectively. The entropy present in a signal has also been used as RF fingerprint. For example in [27] the authors proposed an RF fingerprint approach that exploits the multi-dimensional permutation entropy. In their work the transceivers were placed 10 meters apart so that signal propagation occurs in a short-wave line of sight (LOS).

Numerical RF feature extraction methods are limited by a number of factors. Firstly, signal modules are non-stable and are not usually Gaussian. Also, factors such as nonlinearities and noise inherent to the transmitter hardware have spurious effects on the signal when it arrives at the receiver. As a consequence the approaches based on time and frequency domain parameters have become less favored. Instead, signal processing methods such as time frequency analysis, wavelet analysis, empirical mode decomposition (EMD), fractal features, and intrinsic time decomposition have become more popular. These approaches are used to project the signals into other known domains for analysis.

In [28] intrinsic mode functions (IMF) were obtained using EMD, the entire distribution of the time-frequency was then obtained by applying the Hilbert transformation. However, obtaining the IMF from the EMD was shown to have some limitations [29] because it outputs features which are not present in the original signal. Four devices of the same model and distinct serial numbers were identified by using the dual-tree complex wavelet transform (DT-CWT). Features were obtained from the non-transient preamble response of their OFDM modulated IEEE 802.11a signal [30]. At SNR of below 20dB, the authors achieved classification accuracy as high as 80%.

In [31] the largest ZigBee tested bed containing 54 ZigBee devices, and a universal software radio peripheral (USRP) device used as receiver, was used to test an adaptive hybrid classification method that adapts to environmental conditions. In this work the classification rates were as low as 0.048 for LOS scenario, and 0.1105 when using different receivers. In [32] multiple features of RF fingerprints features were used for identifying ZigBee devices. The classification performance of five classification algorithms were compared and it was found that combining IQ offset, frequency offset, and circle offset as features for a neural network under high SNR gave a 100% classification accuracy.

Device authentication and authorization has always been an issue of concern with respect to network access, and in [33] the traditional anti-attack approaches were shown to present significant security risks where

the author used transient signals of seven authorized ZigBee devices. The Radio Frequency Distinct Native Attributes (RFDNA) fingerprints were computed and device identification was performed using multiple discriminant analysis (MDA). To verify the access rights of an authorized device, hypothetical multivariate Gaussian (MVG) likelihood test statistic was used to verify the claimed identity of a device. the detection rates were 85% and above 80% at SNR of 5 dB and 10dB respectively.

In [34] Cobb et al. proposed the passive monitoring of the salient features present in the unintentional RF transmissions of integrated circuits (IC) were exploited for device identification and verification. In the identification system, MDA was used for training and dimension reduction, and a linear Bayesian classifier was used for device ID verification. To ascertain the consistency of the identity of the device with the classification output, the Bayesian posterior probability was compared with a predetermined threshold. Their experiments involved 40 devices of a single model and the obtained average verification rates of up to 99% and test error rates of below 0.05% at 10dB.

More attention has been focused on ZigBee devices recently because of their widespread use in transportation, home automation, industrial and control systems. Consequently their security has received significant interest. The Fisher-based multi discriminant analysis and maximum likelihood (MDA-ML) approach to classification and verification was analyzed in [35]. In this study the authors assert that the performance of MDA-ML degrades when the distribution of the RF fingerprint does not satisfy the Gaussian condition. The authors also proposed a non-parametric approach to classification and authentication of devices using random forest and multi-class AdaBoost classifiers. In their experiments four ZigBee devices were used for training, and nine unauthorized devices not seen during the training were used to test the classifiers performance. The probability of classification error of their method was below 10% at 10dB.

In regards to unauthorized network access. Reising [9] proposed enhancing WAP security using RF fingerprints. In this work, dimensionality reduction analysis (DRA), combined with device ID authentication was proposed to detect unauthorized devices posing as legitimate devices. RFF techniques have been proposed in other fields [36–38] which has in turn contributed to the efficacy of RFF technology. In [39] terminal devices with constrained computational capacity in IoT were authenticated using RF fingerprint identification (RFFID). They showed that using wavelet-based features with this approach resulted in high recognition rates and better authentication.

ZigBee devices also find extensive application in IoT. As a result, the security and authentication of the decentralized architecture of ZigBee ad-hoc networks have received considerable attention. In [40], the authors applied RFDNA approach for device authentication at low signal-to-noise ratio while taking into account multi-path effects and interference from other devices. In this work the ZigBee devices were authenticated using non-parametric random forest and multi-class AdaBoost classifiers.

In our work, an autoencoder-based model is trained on RF traces collected from ZigBee devices at different SNR. The autoencoder learns the features inherent to each device's hardware and performs the process of RF feature extraction and feature dimension reduction automatically and simultaneously. During a device-to-device communication, a signal to be transmitted is input into the autoencoder, and the mean square error between the signal and its reconstruction is used as the RF fingerprint of the device and is herein referred to as the device's *Device Authentication Code (DAC)*. The authorized receiver who also possesses an identical copy of the model performs the same process. Both DACs are compared and a match authenticates the transmitter, while a mismatch signifies the an illegitimate device.

This work and others described in this section [9, 31–36] are focused on authentication of mobile devices using RFF technology. They work by comparing the claimed identity of a device with its RF fingerprint to authenticate the device. While the approach taken in this work is similar to previous work in this regard. Our approach is different in a number of respects. Previous methods are based on statistical and signal processing approaches while some combine them with machine learning. This means that the RF features are "hand engineered". In our work, feature selection is intrinsic and performed automatically using deep learning. Furthermore, a majority of the approaches considered that use supervised learning require samples and labels from all devices of interest to be present during training, and this may not be practical. Our method adopts unsupervised learning and therefore does not require labels especially from unauthorized devices. Furthermore, a majority of the methods perform each experiment using simulated RF traces or RF traces collected via cable at single SNR. Some others experiment at high SNR values. In our experiments we experiment using true over-the-air RF traces with varying received SNR in the same dataset which is more representative of real scenario. Finally, while authentication is done by comparison similar to previous methods, there is no requirement for a device to provide its claimed identity in advance.

2.2. RF Fingerprint Authentication

Device authentication and authorization has always been an issue of concern with respect to network access, and in [33] the traditional anti-attack approaches were shown to present significant security risks where the author used transient signals of seven authorized ZigBee devices. The Radio Frequency Distinct Native Attributes (RFDNA) fingerprints were computed and device identification was performed using multiple discriminant analysis (MDA). To verify the access rights of an authorized device, hypothetical multivariate Gaussian (MVG) likelihood test statistic was used to verify the claimed identity of a device. the detection rates were 85% and above 80% at SNR of 5 dB and 10dB respectively.

In [34] Cobb et al. proposed the passive monitoring of the salient features present in the unintentional RF transmissions of integrated circuits (IC) were exploited for device identification and verification. In the identification system, MDA was used for training and dimension reduction, and a linear Bayesian classifier was used for device ID verification. To ascertain the consistency of the identity of the device with the classification output, the Bayesian posterior probability was compared with a predetermined threshold. Their experiments involved 40 devices of a single model and the obtained average verification rates of up to 99% and test error rates of below 0.05% at 10dB.

More attention has been focused on ZigBee devices recently because of their widespread use in transportation, home automation, industrial and control systems. Consequently their security has received significant interest. The Fisher-based multi discriminant analysis and maximum likelihood (MDA-ML) approach to classification and verification was analyzed in [35]. In this study the authors assert that the performance of MDA-ML degrades when the distribution of the RF fingerprint does not satisfy the Gaussian condition. The authors also proposed a non-parametric approach to classification and authentication of devices using random forest and multi-class AdaBoost classifiers. In their experiments four ZigBee devices were used for training, and nine unauthorized devices not seen during the training were used to test the classifiers performance. The probability of classification error of their method was below 10% at 10dB.

In regards to unauthorized network access. Reising [9] proposed enhancing WAP security using RF fingerprints. In this work, dimensionality reduction analysis (DRA), combined with device ID authentication was proposed to detect unauthorized devices posing as legitimate devices. RFF techniques have been proposed in other fields [36–38] which has in turn contributed to the efficacy of RFF technology. In [39] terminal devices with constrained computational capacity in IoT were authenticated using RF fingerprint identification (RFFID). They showed that using wavelet-based features with this approach resulted in high recognition rates and better authentication.

ZigBee devices also find extensive application in IoT. As a result, the security and authentication of the decentralized architecture of ZigBee ad-hoc networks have received considerable attention. In [40], the authors applied RFDNA approach for device authentication at low signal-to-noise ratio while taking into account multi-path effects and interference from other devices. In this work the ZigBee devices were authenticated using non-parametric random forest and multi-class AdaBoost classifiers.

In our work, an autoencoder-based model is trained on RF traces collected from ZigBee devices at different SNR. The autoencoder learns the features inherent to each device's hardware and performs the process of RF feature extraction and feature dimension reduction automatically and simultaneously. During a device-to-device communication, a signal to be transmitted is input into the autoencoder, and the mean square error between the signal and its reconstruction is used as the RF fingerprint of the device and is herein referred to as the device's *Device Authentication Code (DAC)*. The authorized receiver who also possesses an identical copy of the model performs the same process. Both DACs are compared and a match authenticates the transmitter, while a mismatch signifies the an illegitimate device.

This work and others described in this section [9, 31–36] are focused on authentication of mobile devices using RFF technology. They work by comparing the claimed identity of a device with its RF fingerprint to authenticate the device. While the approach taken in this work is similar to previous work in this regard. Our approach is different in a number of respects. Previous methods are based on statistical and signal processing approaches while some combine them with machine learning. This means that the RF features are "hand engineered". In our work, feature selection is intrinsic and performed automatically using deep learning. Furthermore, a majority of the approaches considered that use supervised learning require samples and labels from all devices of interest to be present during training, and this may not be practical. Our method adopts unsupervised learning and therefore does not require labels especially from unauthorized devices. Furthermore, a majority of the methods perform each experiment using simulated RF traces or RF traces collected via cable at single SNR. Some others experiment at high SNR values. In our experiments we experiment using true over-the-air RF traces with varying received SNR in the same dataset which is more representative of real scenario. Finally, while authentication is done by comparison similar to

previous methods, there is no requirement for a device to provide its claimed identity in advance.

3. Proposed Method

In this work, we apply deep learning to automate the RF feature extraction and selection process, and information theoretic approach is used for feature matching. Our choice is based on the recorded success of deep learning in feature, manifold and hierarchical learning across multiple domains such as computer vision, speech, natural language and signal processing [41, 42].

In supervised deep learning, data samples and their labels from all classes of interest must be present during training. However, a test sample from a class not observed during training (an intruder in this context) will be classified as one of the already seen classes during inference. Because of this constraint we adopt unsupervised learning. Specifically, an autoencoder is trained to learn the features inherent to the transmitter hardware, and its communication with a receiving device. The error between the signal and it's reconstruction is the device's RF fingerprint and Device Authentication Code (DAC). For authentication, a two-sided Kolmogoroc-Smirnov test is used to compare the DACs generated by both transmitter and receiver. We herein provide details on the components and architecture of the DAC framework.

3.1. Autoencoders

Autoencoders (AE) are neural networks with the objective of reconstructing data input they receive (Figure 2). Mathematically given an input x, the autoencoder attempts to learn the identity function:

$$f_{W,b}(x) = x \tag{1}$$

where W and b represent the weights and bias of the network respectively. The objective is achieved by minimizing the "reconstruction error" between the input and its reconstruction:

$$L(x, \hat{x}) = \|x - \hat{x}\|^2 . \tag{2}$$

First the AE learns an "encoded" representation of the data, by extracting the inherent structure in the data [43]. Learning the encoded representation can be achieved by restricting the number of nodes in the encoding layers as done in undercomplete autoencoders [42]. Overcomplete autoencoders learn structure by imposing other regularization constraints on the encoding layer such as sparsity as in sparse autoencoders [44], or addition of noise as in denoising autoencoders [45]. Convolutional autoencoders (CAE) exploit spatial relationships in data by weight sharing [46]. AEs can be extended to make deeper networks and can be trained in a greedy layer-wise manner, where each layer is the latent representation of an already trained AE.

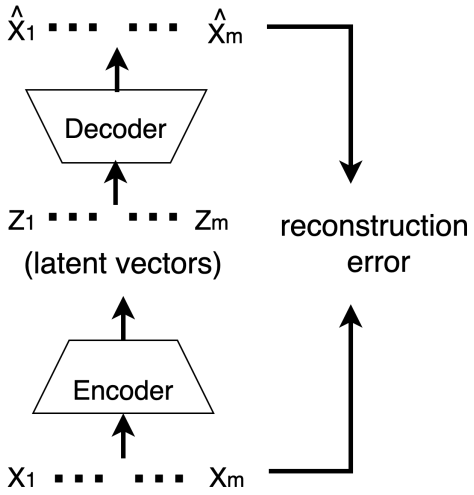

Figure 2. Architecture of an Autoencoder

3.2. Kolmogorov-Smirnov (K-S) test

The Kolmogorov-Smirnov (K-S) test is a non-parametric test used to ascertain whether a sample comes from a population whose distribution is known, or whether the distribution of two populations are the same. In the one-sample test, a one-dimensional probability distribution is compared to a reference probability distribution. In the two-sample test two samples from two distributions are compared. If we define the empirical distribution function (EDF) F_n for n independent and identically distributed (i.i.d) observations, X_i, which are ordered as:

$$F_n(x) = \frac{1}{n} \sum_{i=1}^{n} I_{[-\infty,x]}(X_i) \tag{3}$$

where $I_{[-\infty,x]}(X_i)$ is an indicator function that equals 1 when $X_i \leq x$ and 0 otherwise. Then the K-S statistic for another EDF $F(x)$ is:

$$D_n = \sup_x |F_n(x) - F(x)| \tag{4}$$

where $\sup_x$ is the supremum function of the set of distances. The K-S statistic converges to 0 as n goes to infinity if the sample is from the distribution $F(x)$. Similarly, for the two-sample test, given two empirical distributions $F_{1,n}$ and $F_{2,m}$ with sample sizes of n and m, respectively, the K-S statistic for the first and second sample is

$$D_{n,m} = \sup_x |F_{1,n}(x) - F_{2,m}(x)| \tag{5}$$

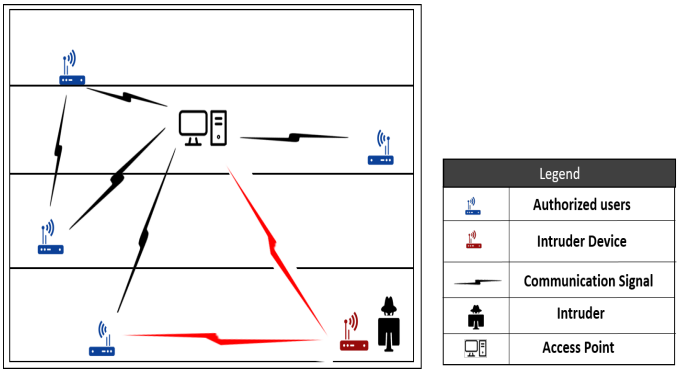

Figure 3. Threat model

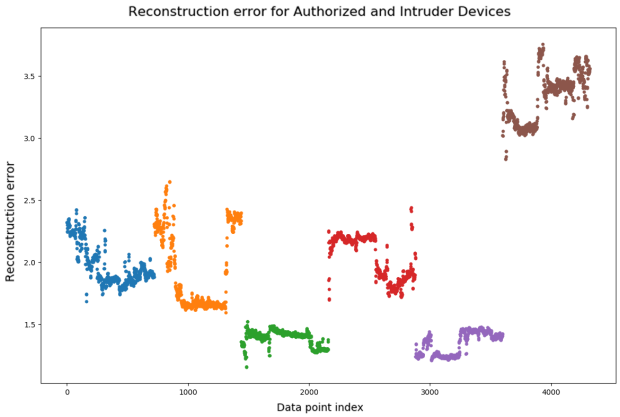

Figure 4. Reconstruction error for six identical RF devices transmitting identical signals

Given a specified level α, the null hypothesis can be rejected for large sample sizes if

$$D_{n,m} > c(\alpha)\sqrt{\frac{n+m}{nm}} \tag{6}$$

where in general

$$c(\alpha) = \sqrt{-\frac{1}{2}ln\alpha} \tag{7}$$

It is possible to set confidence limits on $F(x)$ such that for the test statistic D_α, if $P(D_n > D_\alpha) = \alpha$, then $F(x)$ will be contained in $F_n(x)$ within a tolerance of width $\pm D_\alpha$ with a probability of 1 - α. The null hypothesis is that both samples are drawn from the same distribution and the p-value is a measure of similarity. If the p-value is "small", the null hypothesis should be rejected. The K-S test measures the distance between the empirical distribution functions of both samples without any assumptions about the distribution of the data. Unlike the t-test, K-S test is robust to scale changes and it is not restricted to identifying changes only in the mean. However, because the K-S test makes no assumptions about the data distribution, the decision on what the threshold should be is data and application specific.

3.3. Problem Formulation

In this work, we consider a threat model such as shown in Figure 3. This threat model represents the extreme case where the intruder possesses a wireless device identical to an authorized device in brand, and may attempt to mimic an authorized device by transmitting an identical signal to the one transmitted by an authorized device. We assume that there are n RF devices with wireless interfaces. All devices are of the same make and model and are considered identical. All devices also transmit identical signals which are received at different SNR. It is important to note that the approach also works when the devices transmit non-identical signals. However we consider the transmission of identical signals because this depicts a situation where a malicious user attempts to claim the identity of an authorized device. Furthermore, the problem of authentication in the case where the devices are not identical and transmit non identical signals is an easier problem. It is assumed that one device is unauthorized and belongs to an intruder. Another constraint is that the RF traces from the unauthorized device are not available for the training of the model. The objective is to authenticate any authorized device of interest and identify an unauthorized device in a device-to-device communication.

We represent the features of a batch of RF devices such as wireless sensors as:

$$S = S_o + \mu_M \, , \tag{8}$$

where S_o represents the features common to every device in the batch, and is required for any device to pass quality control tests. μ_M accounts for minor differences and uncertainties due to the imperfection of the manufacturing process. An autoencoder is a mapping

$$X \rightarrow Z \rightarrow \hat{X} \, , \tag{9}$$

that encodes an input X to a latent representation Z, and decodes Z to recover X. Since there is no explicit formula for $\hat{X}$, what is done instead is to minimize:

$$min\|X - \hat{X}\|^2 \tag{10}$$

when training the model with data samples. In wireless communications there are also environmental factors ε, such as channel fading, thermal noise, and effects of device mobility, that are superimposed on the received signal. Therefore the training data can be represented as:

$$X = f(S, \varepsilon), \tag{11}$$

which is a mapping generated by the underlying stochastic process that consists of S which contains the manufacturing uncertainty μ_M, and ε which contains environmental uncertainty. Based on the premise of RF fingerprinting, μ_M is unique to every RF device. Hence, for a batch of devices:

$$S_i = S_0 + \mu_{M_i} \qquad i = 1, ...N. \tag{12}$$

it is possible to identify S_i $(\forall i \in N)$ using a method that is robust to the environmental uncertainty ε that affects the data X obtained from the batch of devices. We show experimentally that this can be achieved using an autoencoder and a two-sided K-S test. The μ learned by the autoencoder are contained in the encoded layer of the autoencoder and are unique to each device given a transmitted signal. This is why the decoder part of the autoencoder when decoding the signal will yield a unique MSE. In the context of intrusion detection, this means that the probability that an unauthorized device is able to mimic the μ_M of a legitimate device is highly unlikely.

3.4. Device Authentication with DAC

Autoencoder based models have been used for anomaly and novelty detection. For example, autoencoders were used for target recognition using radar images in [47], and outlier removal in [48]. Autoencoders were also used to detect abnormalities in machines by detecting abnormal operation sounds [49], and to detect anomalies in video frames [50]. The idea is based on the premise that a trained autoencoder will output a low reconstruction error when the data it receives belongs to the same, or a similar distribution as the data used to train the model, but a high reconstruction error otherwise. Because the distribution of the data are very different, the reconstruction error can be threshold-ed using a single value and used to identify anomalous data.

However, for the scenario considered in this paper, where the devices are of the same make and model, and may transmit identical signals (Figure 5), it is obvious that the single-valued threshold approach will not suffice. Figure 4 shows the reconstruction error during inference for a CAE trained on RF traces from from five out of six devices (one device is left out). It is observed that identifying a novel or intruder device (any one of the six devices not used in training) with a single threshold will not be possible. Instead, we require a metric that can capture and differentiate between distributions. The K-S statistic serves this purpose.

The process of feature selection and dimension reduction using the DAC framework is highlighted in Figure 6. For a device-to-device communication scenario. First, an autoencoder is trained on the RF traces from the authorized devices. During this process, the device specific imperfections are modeled. This process is akin to the RF feature selection and matching process associated with other RF fingerprinting methods. However, manual feature engineering is not required here. After model training and during inference, the distribution of the mean square error (MSE) between signals and their reconstructions will be unique to each device. This holds true for devices of the same make and model, and transmitting identical signals. The MSE are analogous to a device's RF fingerprint, and represents the Device Authentication Code in this study. It worth pointing out that the proposed DAC is unique for each individual device because of their manufacturing uncertainty μ_M, and is robust to environmental uncertainty ε. This is because the autoencoder is trained using RF traces considering different environmental conditions (different SNRs).

To perform device authentication and intrusion detection (Figure 1), we consider a device-to-device communication a between a transmitting device A, and a receiving device B. If both devices are authorized, both devices must have the same copy of the trained autoencoder model. The parameters of the model is analogous to a security key shared by both parties. The signal to be transmitted is passed through the trained autoencoder model to generate A's DAC_s. The DAC_s is then concatenated with the signal and transmitted by A. At B, the signal is decoupled into the original signal and DAC_s. B then passes the received signal through its own autoencoder model to generate another DAC_R. A two sided K-S is used to compare both DACs. If both DAC are a match (i.e., a K-S statistic of 0 and p-value of 1), then the device A is authenticated as an authorized device. If both DACs do not match, then the sending device is tagged an illegitimate device or intruder.

In the event that a malicious user tries to pose as a legitimate user, by using a device identical to a legitimate one to generate and transmit an identical signal. As long as the intruder does not have access to the key, which in this scenario is the trained autoencoder model consisting of all parameters. The probability that a DAC can be generated that would be a match with the legitimate transmitter's DAC are extremely low. The security of this approach is therefore dependent on the security and safety of the shared autoencoder parameters, and the degree of security is dependent on the complexity of the model itself. We explain with some simplistic assumptions below.

Let the possibles value for each weight in the network (key) be in the range $[0, 1]$ for up to three decimal places. This means there are 200 possible values for each network weight; 100 positive and 100 negative floating point values. If we regard only the network weights instead of all trainable parameters as the key. For a basic network with a very conservative 20000 parameters where each parameter can take any three

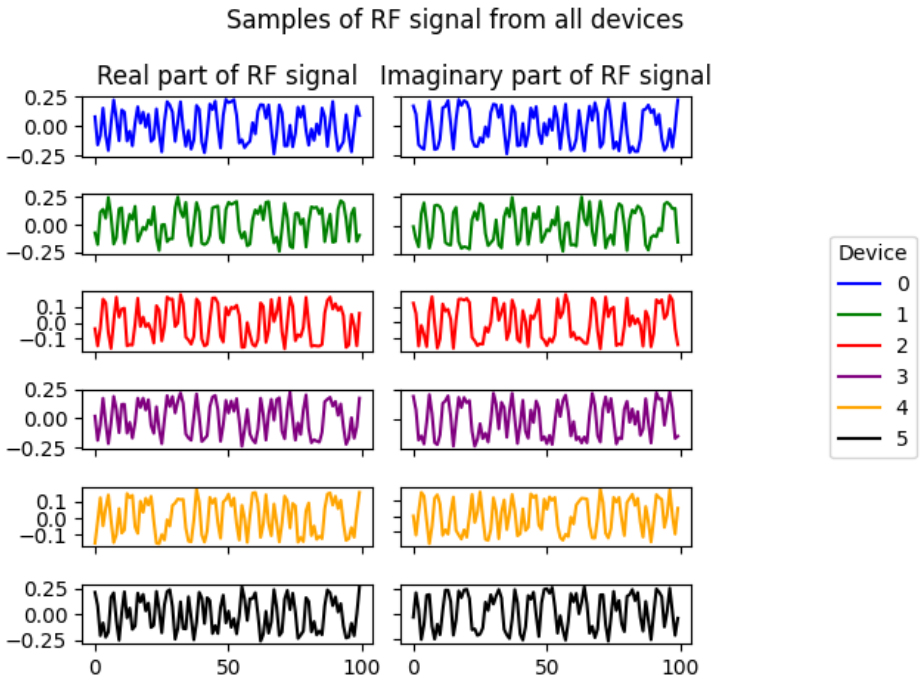

Figure 5. Sample of RF I and Q data captured from all 6 ZigBee devices

decimal floating point value in $[0, 1]$, there are 200^{20000} possible keys. It is obvious to see that the probability of an intruder obtaining the exact combination of key values that yield the right DAC is very low even for a very small network. This is the same reason why the probability of training two separate networks to converge to the exact same set of weights is almost zero. Hence, the DAC although being a MSE is a function of the autoencoder network parameters, and based on the premise of RF fingerprinting, the probability that different messages will map to the same reconstruction error using the same set of network parameters is very low.

3.5. Practical Considerations

In a real application such as device registration on a network. Every device can be required to transmit a predetermined signal upon start-up. Registration of a new device is as simple as deploying the parameters of the autoencoder model (which is the key) to that device. However, when an authorized device becomes unauthorized, the model will be fine-tuned using additional data from the current authorized devices to obtain updated model parameters and is deployed in the authorized devices. The model can also be fine-tuned when adding devices. However while best practices may require this, it is not a requirement. What is more important when adding devices is making sure only authorized devices have the current copy of the trained network parameters (or key).

The start-up signal is concatenated with the device's DAC and sent to a command or control center such as an access point (AP) or base station (BS). At the AP, the signal is decoupled and another DAC is generated. A match (i.e., a K-S statistic of 0 and p-value of 1) means that the device is an authorized (pre-registered) device, otherwise the device is flagged as a new device (possibly an intruder). In this scenario, even if an intruder knows the signal being transmitted and attempts to use an identical device to transmit the same predetermined startup signal, as long as he is not in possession of the autoencoder model (key), the probability that his DAC will be a match at the AP is extremely low. Furthermore, while it is not impossible to randomly train an arbitrary model that would be able to generate the same DAC. This is highly unlikely given that the parameters are in floating point.

The DAC is similar in concept to the idea of Message Authentication Code used for message authentication in cryptographic applications. In MAC, to transmit a message to B, A uses a key K to create a message authentication code (MAC_S), a fixed sized cryptographic checksum and function $MAC = C(K, M)$ of the message and the shared key. The MAC is appended to the message and transmitted. B applies the MAC function on the message and generates a new MAC_R using the secret key. The newly generated MAC_R is compared with the received MAC_S. If $MAC_S = MAC_R$, then:

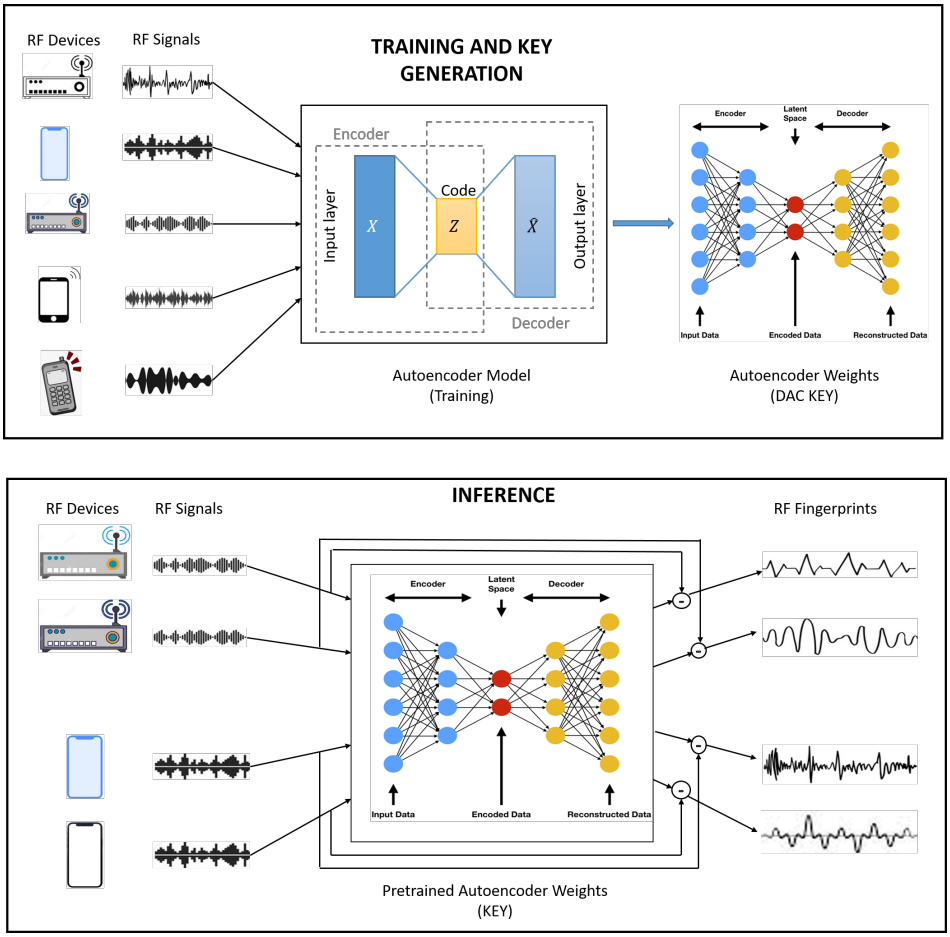

Figure 6. Training and Inference using DAC

1. B is assured that M has not been altered because if an intruder modifies M without modifying MAC_S, then MAC_R will not match MAC_S. Furthermore, the intruder cannot modify MAC_S to reflect changes in the message because he does not have K.

2. B is also assured that the message came from A because only A has K required to generate a message with the correct MAC.

However, the DAC is similar to MAC only in concept. We emphasize here that the DAC is not considered an outright replacement for MAC. MACs operate at the transport layer whereas the DAC operates at the physical layer. Rather, we consider the DAC as a complementary method to enhance the current cryptographic approaches. More discussion on this concept is provided in section 5. However, in some cases of constrained device-to-device communication, which require more lightweight approaches, the DAC may be preferred. In addition, with the MAC, one could not identify each physical device, while the proposed DAC is able to authenticate each physical radio.

4. Experimental Results

4.1. Experimental setup

Data Collection. To validate the ideas presented in this work, RF traces were collected from three types of devices: (1) six MICAz-MPR2400 sensors, (2) NI USRP-293x and (3) USRP X310 Software Defined Radio (SDR) Devices. The MICAz is a mote manufactured by Crossbow Technology. It has has on-board the IEEE 802.15.4 compliant CC2420 chip, which is a ZigBee ready transciever operating within the range [2.4000,2.4835] GHz (model MPR2400). Attached to it is a sensor board which integrates light, temperature, accelerators, microphone, and magnetometer sensors. It operates in a mesh configuration for transmission of sensor recordings to the base station node. In the MoteView Platform, the devices (MICAz) are configured to transmit data twice every second.

The USRP-293x is able to capture signals at frequencies up to 4.4GHz, with a bandwidth of up to 20MHz. The USRPs contain a Software Defined Radio Device (SDRD), and a tunable radio. The SDRD carries a high-speed analog-to-digital converter as well

Table 1. Model Parameters for Convolutional Autoencoder model

Network	Layer	Dimension	Activation
Input	Input	x (1024 x 2)	-
Encoder	2D Convolution	256 x (3 x 3)	Tanh
	Max Pooling	2 X 1	-
	2D Convolution	64 x (3 x 3)	Tanh
	Max Pooling	2 X 1	-
	2D Convolution	16 x (3 x 3)	Tanh
Decoder	Convolution Transpose	64 x (3 x 3)	Tanh
	Convolution Transpose	256 x (3 x 3)	Tanh
	2D Convolution	2 x (3x3)	Tanh

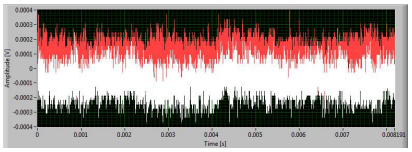

Figure 7. Captured RF IQ Data from ZigBee device (20 Frames at 2 Frame/Second)

as a digital-to-analog converter for streaming baseband IQ signals to a host PC on a 1/10 Gigabit. The data are stored in TDMS file format. The USRP-293x can implement communication applications such as broadcast FM, white space, public safety (land-mobile, and low-power unlicensed devices operating on industrial, scientific and medical (ISM) bands), cell phone, sensor networks, GPS or amateur radio.

For the ZigBee devices, six devices were configured to transmit sensor data twice every second at and the receiver to receive the signals at SNR levels of 0, -1, -5, -10, -15dB. For the USRP-293x devices, 5 devices were configured to transmit 16 QAM signals, with 4 samples per symbol. the samples had a frame length of 2044 and symbol rate of 125k symbols per second. the IQ sampling rate was set at 500k samples per second and the career frequency was set at 2GHz. Signals from all five USRPs were received at [-10dB, 10dB] in steps of 2dB using LabVIEW interface. In our experimental setup, a receiver USRP is configured with 2MHz bandwidth as required for the ZigBee protocol. To reduce the effect of interference with other devices in the 2.4gHz ISM band, channel 26 (2.48 GHz) is configured as the career frequency. The RF IQ data from both device types are captured and saved accordingly by the USRP-293x receiver. Figure 7 shows an example plot for the I and Q traces obtained from one of the ZigBee devices.

In a practical scenario, there are environmental and channel effects that impact signals transmitted over the wireless channel. Some of these phenomena include effect of degradation and distance, varying channel conditions, noise and device mobility. However, although these phenomena exhibit peculiar characteristic behavior, in terms of signal measurement; these effects are observed and find expression as varying signal strengths in the received signal. Considering this, we collect the RF traces at varying SNR, and combine them into the same dataset to simulate these effects. In other words, having one dataset contain data at different SNR levels simulates the effect of having the signal strength affected by these phenomena during transmission. This we believe is closer to reality than having multiple datasets associated with single received SNR levels as done in most previous work. In addition to this, during RF data collection, the devices were moved around by walking with the devices within a lab measuring approximately 25 x 30 ft, and outside to adjacent labs but within the same building to add some natural effect of device mobility and absence of line-of-sight. One of the plans for future work include integrating RF traces with the device mounted in high speed mobile device such as vehicles or drones in order to introduce substantial Doppler effect from high speed mobility.

For both device types, the RF traces from one of the devices (assumed to be the intruder) are not used for training the model, and 20% of the RF traces of the authorized devices were set aside for testing. For the ZigBee devices, 4435968 I and Q samples per device and a window size of 1024 was used. The training set had the dimensions (27075,1024,2) split equally among each of the five authorized devices, and the test set had dimensions (8662, 1024, 2), with half coming from the unauthorized and authorized devices respectively. Similarly, the USRP training set had the dimensions (17,280,1024,2) split equally between the authorized devices, and the test set had the dimensions (77776, 1024, 2) with approximately 55% and 45% coming from the unauthorized and authorized devices respectively. Again, for both ZigBee and USRP datasets, no RF trace from the unauthorized device was included in the training set.

Training and Authentication. The raw RF IQ traces from the authorized devices are used to train the AE-based model. Table 1 shows the parameters of the

Table 2. KS Statistic and P-value for raw data from RF Devices.

Device of interest	RF Device					
	Device 0	Device 1	Device 2	Device 3	Device 4	Device 5
Device 0	(**0.00, 1.00**)	(**0.02**, 0.00)	(**0.05**, 0.00)	(**0.03**, 0.00)	(**0.04**, 0.00)	(**0.05**, 0.00)
Device 1	(**0.02**, 0.00)	(**0.00, 1.00**)	(**0.06**, 0.00)	(**0.03**, 0.00)	(**0.05**, 0.00)	(**0.04**, 0.00)
Device 2	(**0.05**, 0.00)	(**0.06**, 0.00)	(**0.00, 1.00**)	(**0.06**, 0.00)	(**0.13**, 0.00)	(**0.08**, 0.00)
Device 3	(**0.03**, 0.00)	(**0.03**,0.00)	(**0.06**, 0.00)	(**0.00, 1.00**)	(**0.06**, 0.00)	(**0.04**,0.00)
Device 4	(**0.04**, 0.00)	(**0.05**,0.00)	(**0.13**, 0.00)	(**0.06**, 0.00)	(**0.00, 1.00**)	(**0.08**, 0.00)
Device 5	(**0.05**, 0.00)	(**0.04**, 0.00)	(**0.08**, 0.00)	(**0.04**, 0.00)	(**0.08**, 0.00)	(**0.00, 1.00**)

Table 3. KS Statistic and P-value for CAE model for all RF devices.

Device of Interest	RF Device					
	Device 0	Device 1	Device 2	Device 3	Device 4	Device 5
Device 0	(**0.000, 1.000**)	(**0.313**, 0.000)	(**0.636**, 0.000)	(**0.555**, 0.000)	(**0.771**, 0.000)	(**0.627**, 0.000)
Device 1	(**0.312**, 0.000)	(**0.000, 1.000**)	(**0.710**, 0.000)	(**0.334**, 0.000)	(**0.651**, 0.000)	(**0.380**, 0.000)
Device 2	(**0.635**, 0.000)	(**0.685**, 0.000)	(**0.000, 1.000**)	(**0.801**, 0.000)	(**0.198**, 0.000)	(**0.801**, 0.000)
Device 3	(**0.552**, 0.000)	(**0.331**,0.000)	(**0.801**, 0.000)	(**0.000, 1.000**)	(**0.979**, 0.000)	(**0.379**, 0.000)
Device 4	(**0.778**, 0.000)	(**0.653**,0.000)	(**0.236**, 0.000)	(**0.972**, 0.000)	(**0.000, 1.000**)	(**1.000**, 0.000)
Device 5	(**0.647**, 0.000)	(**0.381**, 0.000)	(**0.801**, 0.000)	(**0.384**, 0.000)	(**1.000**, 0.000)	(**0.000, 1.000**)

model. This configuration was selected from a range of configurations tested because it gave the best results in terms of the K-S Statistic. For example, while ReLU activation is popular with this model in literature and gave good results, the hyperbolic tangent activation performed better. The model performs automated feature extraction and dimension reduction on the RF data. The confidence in using deep learning for this task stems from previous work done by the authors in [51]. In this work, a convolutional neural network was used on the same dataset but for device identification using supervised classification. Classification accuracy up to 97% was obtained in those experiments, which further substantiates the claim that our model is able to perform automatic feature extraction and generate unique DAC for each device.

After training, for authentication, a sequence of RF data to be transmitted is input into the trained CAE to obtain the DAC, and the DAC is concatenated with the original signal before transmission. To authenticate a device, the DAC is also generated at the receiver, and checked to ascertain that the DAC from the transmitter matches the DAC generated at the receiver. A K-S test is used for this purpose. A match in both DACs authenticates a device, otherwise, the device is deemed illegitimate and an intruder.

The performance of the proposed approach is evaluated on the collected datasets. As previously stated, one device is considered illegitimate and its RF IQ traces are left out during training. 90% of the IQ samples from the other authorized devices at varying SNR levels are used for training. Half of the remaining 10% are used for validation and the remaining 5% of samples are mixed with IQ samples from the intruder class for testing. It is worth mentioning again that the data are collected for each device at different SNR levels and combined into one dataset in order to mimic multi-path effects, variation in channel conditions as well as noise.

4.2. Results and Analysis

Table 2 shows the KS statistic and p-values using just the raw RF traces from all the ZigBee devices. The rows of each table represent the transmitting device whose DAC is supposed to be received as the authorized device at the receiver, whereas the columns represent the device whose DAC is actually received in a device-to-device communication. For example, the cell at the intersection of the row and column both labeled "Device 0", signifies that the both the DAC transmitted and the DAC received are from Device 0. In the same vein, the entry in the last column of the first row indicates that the DAC transmitted is from device 0, but the DAC computed at the receiver belongs to device 5 (meaning this is an illegitimate transmission). The term "device of interest" signifies the authorized device in a specific communication scenario. In other words, Device 0 is the authorized transmitting device in the first row, Device 2 is the legitimate device in the second row, and so on. This means that only the entries in the diagonal represent legitimate communications. The first and second elements of the tuple in every cell of the table are the K-S statistic and p-value of the K-S test respectively.

Table 4. KS Statistic and P-value for convolutional autoencoder model for all RF devices at different SNR levels (Device of interest: 5).

SNR(dB)	RF Device					
	Device 0	Device 1	Device 2	Device 3	Device 4	Device 5
0	(**1.000**, 0.000)	(**0.999**, 0.000)	(**1.000**, 0.000)	(**1.000**, 0.000)	(**1.000**, 0.000)	(**0.000, 1.000**)
-1	(**1.000**, 0.000)	(**0.857**, 0.000)	(**1.000**, 0.000)	(**1.000**, 0.000)	(**1.000**, 0.000)	(**0.000, 1.000**)
-5	(**0.424**, 0.000)	(**0.274**, 0.000)	(**1.000**, 0.000)	(**0.589**, 0.000)	(**1.000**, 0.000)	(**0.000, 1.000**)
-10	(**0.452**, 0.000)	(**0.879**, 0.000)	(**1.000**, 0.000)	(**0.497**, 0.000)	(**0.993**, 0.000)	(**0.000, 1.000**)
-15	(**0.886**, 0.000)	(**0.932**, 0.000)	(**0.214**, 0.000)	(**0.657**, 0.000)	(**0.999**, 0.000)	(**0.000, 1.000**)
[0,-1,-5,... -10,-15]	(**0.652**, 0.000)	(**0.395**, 0.000)	(**0.820**, 0.000)	(**0.445**, 0.000)	(**0.999**, 0.000)	(**0.000, 1.000**)

As previously mentioned, the null hypothesis is that both samples are from the same distribution. The null hypothesis cannot be rejected if either the statistic is very low, or the p-value is high. On the other hand, the null hypothesis should be rejected if the K-S statistic is high and the p-value is very low. In other words, a K-S statistic in the range $[0, 0.1]$ and p-value in the range $[0.9, 1.0]$ indicates that the device of interest is an authorized device. However, a K-S statistic of greater than 0.1 and p-value less than 0.9 indicates that the DAC is from a different distribution and the device of interest is not authorized. The decision on the value of the threshold is application dependent, and in our experiments we set the threshold at 0.15 given that the highest statistic observed for any combination of transmitting and receiving device for the raw data from Table 2 is 0.13. Hence if a K-S statistic is above 1.5, the transmitter whose DAC is computed at the receiver for that communication scenario is tagged an unauthorized device.

It must be stated here, that the threshold value of 0.15 was chosen arbitrarily just for the purpose of this ZigBee experiments. In anomaly detection using autoencoders and thresholds. The problem of automatically selecting a threshold is (1) application/data specific, and (2) an active area of research. However, the value of the threshold does not have so much of an impact because in any case; only an authorized communication will have values (0.00 and 1.00), and this is akin to an assertion by the model of the statement "I am 100% certain that this transmitter is authorized". In other words, our model can be made to reject any other outcome which does not support this statement. This approach would still work.

The values of interest in Table 2 are highlighted in bold font. As stated earlier, the device of interest is the authorized transmitting device for a specific device-to-device communication. The first thing to observe is that every cell in the diagonal of the table contains $(0.00, 1.00)$. This indicates a perfect match, and is intuitive since the RF trace is from the authorized device and the DAC received matches the DAC transmitted. Secondly, for every other cell other than the diagonal cells, the first element of every tuple are very small values. This shows that the raw RF traces from all the devices according to the K-S test are considered almost identical. Hence, for an unauthorized device or intruder, the performance of the DAC approach will be based on how far away from zero the K-S statistic is, and how close to zero the p-value is. For an authorized device the KS statistic and p-values must be $(0.00, 1.00)$, signifying a match between the transmitted and received DAC.

Table 3 show a similar comparison done in Table 2. However, this time the comparison is made on the DAC obtained for every device using our approach. It can be observed that the values for the K-S statistic here are much higher than those recorded in Table 2 for the raw RF traces. In fact, only one comparison has a K-S statistic of approximately 0.2. If we consider 0.15 to be the minimum threshold below which we cannot reject the null hypothesis, then the DAC would have a discriminatory accuracy of 100%. This shows that the DAC produces very discriminatory features, even though the original data (RF traces) are almost identical. It can be seen that the DAC performs well for every possible combination of transmitter-receiver communication considering each device as an authorized device and the others as unauthorized devices. It is also worth mentioning that for each of the six scenarios which corresponds to each row in the table, data from an arbitrarily chosen device was not included in the training. However, this does not degrade the performance of our proposed approach.

Tables 4 and 5 show the performance of the CAE model trained on RF traces from ZigBee devices and USRPs, respectively. The RF traces are collected at single noise level as well as from all noise levels mixed together. These tables can be viewed as an exploded version of one row in table 3 but considering different SNR scenarios. The device of interest or authorized devices are device 5 for the ZigBee devices, and device 2 for USRP devices respectively. We mention here that similar results were obtained when running this

Table 5. KS Statistic and P-value for convolutional autoencoder model for all USRP RF devices at different SNR levels (Device of interest: 2).

Noise level	SNR (dB)	RF Device				
		Device 0	Device 1	Device 2	Device 3	Device 4
Single	-10 dB	(**0.652**, 0.000)	(**0.557**, 0.000)	(**0.000**, 1.000)	(**0.580**, 0.000)	(**0.515**, 0.000)
	-8 dB	(**0.607**, 0.000)	(**0.417**, 0.000)	(**0.000**, 1.000)	(**0.475**, 0.000)	(**0.435**, 0.000)
	-6 dB	(**0.447**, 0.000)	(**0.302**, 0.000)	(**0.000**, 1.000)	(**0.290**, 0.000)	(**0.295**, 0.000)
	-4 dB	(**0.508**, 0.000)	(**0.340**, 0.000)	(**0.000**, 1.000)	(**0.337**, 0.000)	(**0.243**, 0.00)
	-2 dB	(**0.800**, 0.000)	(**0.700**, 0.000)	(**0.000**, 1.000)	(**0.680**, 0.000)	(**0.701**, 0.000)
	0dB	(**0.587**, 0.000)	(**0.366**, 0.000)	(**0.000**, 1.000)	(**0.408**, 0.000)	(**0.209**, 0.000)
	2 dB	(**0.680**, 0.000)	(**0.605**, 0.000)	(**0.000**, 1.000)	(**0.650**, 0.000)	(**0.424**, 0.000)
	4 dB	(**0.615**, 0.000)	(**0.534**, 0.000)	(**0.000**, 1.000)	(**0.512**, 0.000)	(**0.482**, 0.000)
	6 dB	(**0.525**, 0.000)	(**0.535**, 0.000)	(**0.000**, 1.000)	(**0.520**, 0.000)	(**0.525**, 0.000)
	8 dB	(**0.487**, 0.000)	(**0.512**, 0.000)	(**0.000**, 1.000)	(**0.489**, 0.000)	(**0.457**, 0.000)
	10dB	(**0.373**, 0.000)	(**0.499**, 0.000)	(**0.000**, 1.000)	(**0.467**, 0.000)	(**0.462**, 0.000)
Combined	[-10,10]dB	(**0.319**, 0.000)	(**0.356**, 0.000)	(**0.000**, 1.000)	(**0.339**, 0.000)	(**0.411**, 0.000)

experiment with other devices considered authorized, but due to space constraints, we present only the results for one authorized device. It is observed that the proposed model performs better when tested at single noise levels, especially for the ZigBee devices, and this is expected. However, the model also performs very well on data containing RF traces from mixed noise levels by accurately authorizing an authorized device or detecting an intruder 100% of the time. This is important because in real life scenario, the wireless signals will seldom be at one noise level due to environmental factors. Hence, it is important that the model is robust to these different environmental uncertainties and potential changes.

It is obvious from tables 4 and 5 that the DAC is able to detect the unauthorized device in every instance of device-to-device communication because during training, the convolutional autoencoder acts like a denoising autoencoder. This is an improvement to the method in [9], a state-of-the-art method where 100% detection accuracy was obtained from 20dB and above, but not below 20dB. This is because the approach taken in [9] makes use of RFDNA which is based on specific statistical characteristics of the communication signals like the mean, variance, and kurtosis. While these attributes are affected by the hardware, they are more directly tied to the signal strengths, thus it performs well in high SNR regime. However, the autoencoder exploits inherent attributes of both the signal and hardware that may not be captured by the RFDNA. In addition, because the extracted features may not directly tied to the signal strengths, the proposed method works well in all SNR regimes.

In summary, it is evident that DAC approach is successful at exploiting device inherent features. In an authentication process, if the K-S statistic and the p-value between the received DAC and the DAC generated at the receiver are 0 and 1 respectively, then the transmitting device is an authorized device. Otherwise the transmitting device can be flagged as an intruder. Furthermore, it has been shown that the model is robust to varying SNR levels of the transmitted signal.

5. Discussion and Future Work

Physical-layer authentication is gaining traction in the research community for a number of reasons. First, given the rapid evolution of wireless communication towards the 5G era, communication networks are becoming more heterogeneous. Techniques such as millimeter Wave transmission and other ultra-densification methods will be the logical approach to handle the demands associated with the explosive growth of mobile data traffic. This will see a proliferation of smaller cells containing femtocells and picocells. Given the anticipated changes these future wireless systems, the functions of some layers may be modified. For example hand-offs may be eliminated from layer 3 [52]. This may present challenges in appropriately authenticating different devices that use various upper-layer protocols. However since Physical-layer features are inherent to any device, it may be beneficial to design robust physical-layer authentication approaches which are compatible but less-dependent on specific protocols

Furthermore, As the number of cells increases and the size of cells shrink, frequent and multiple authentication handover procedures are typically required because users (especially mobile users), frequently migrate from various BS/AP covered cells. Migrating context usually involves many units such as servers, APS, and BSs which all require cryptographic methods and multiple handshakes to exchange information or key pairs between each other [53]. Also additional encryption is usually implemented to ensure security of the exchange process from eavesdroppers. All these

processes contribute to the increased latency which can be to the tune of hundreds of milliseconds, and exceeds the tolerance of 5G services [54]. Exploiting Physical-layer features may be instrumental to simplifying the authentication process in future heterogeneous wireless networks.

Taking this into account, cross-layer authentication is one practical means of applying RF fingerprinting in future wireless systems. We consider two approaches to this.

Integration with existing cryptography-based Infrastructures and Protocols. The design of the key distribution and encryption algorithm of cryptographic frameworks such as the Diffie-Helmann protocol are done to ensure that the systems cannot be broken from a computational point of view. However these objectives are usually achieved by trading off computational simplicity and low latency in wireless communication systems. Given the relatively faster nature of the physical-layer process, and device-specific nature of the characteristics at the physical layer, RF fingerprinting can be employed in the design of cross-layer authentication to mitigate the constraints of delay and high computational demand associated with cryptography.

Enhancing Authentication Complexity in Heterogeneous Networks. By verifying the distinctive characteristics of the devices and the communication channel, it is possible to identify wireless transmitters at the physical layer. Unlike authentication based on digital keys, The signal propagation environment between an authorized transmitter and receiver determines the channel between both devices. Hence, there is a relationship between the environment and the physical-layer characteristics of the communicating device which are very difficult to impersonate. In other words, the key may be used to provide end-to-end authentication and not just device-to-device authentication.

For example, in an end-to-end communication scenario, it is assumed that two devices; A and B are in end-to-end communication, and the claimed identity of Device A must be authenticated by B. There is also a trusted party which could be an access point directly linked with A, and trusted by Device B.

The functions of the physical layer here is to provide the upper layers with physical layer characteristics. By virtue of its direct communication with Device A, Device C is able to analyze the physical-layer characteristics of A. Device C can then quantize and hash the characteristics specific to Device A in order to generate specific digital digits, which are appropriate for use by the authentication protocols of the upper layers. These generated digital numbers from Device A can be used to generate asymmetric key for authentication.

One of the challenges in RF fingerprinting research is the lack of widely accepted benchmark datasets by which RF fingerprinting approaches can be compared. Consequently, most proposed methods are designed and tested on only proprietary datasets generated by the researchers, and there is no means of comprehensively comparing the performance of RF fingerprinting techniques. In future work, we will generate a comprehensive RF fingerprinting dataset to further investigate the properties of the DAC, and enable parallel comparison of RF fingerprinting approaches.

6. Conclusion

In this work, we propose a novel framework for intrusion detection based on RF fingerprinting using deep learning. Specifically, the problem of identifying an authorized device or an intruder from a set of devices of the same make, model and manufacturer sending the exact same information is considered, and a novel concept of Device Authentication Code (DAC) is proposed. In the proposed framework, an autoencoder is used to automatically extract features from the RF traces, and the reconstruction error is used as the DAC. Then Kolmogorov-Smirnov (K-S) test is used to match the distribution of the reconstruction error generated by the receiver and that in the received message, and the result will determine whether the device of interest is an authorized user. We validate this concept on two experimentally collected RF traces from six ZigBee devices and five universal software defined radio peripheral (USRP) devices, respectively. Experimental results demonstrate that DAC is able to prevent device impersonation by extracting salient features that are unique to each wireless device of interest and can be used to identify RF devices. Furthermore, the proposed DAC is unique to each device due to manufacturing uncertainty, and at the same time it is robust to environmental uncertainties, such as changes in channel conditions, mobility and noise, which all are observed in terms of varying signal strength. It is worth noting that the proposed method does not need the RF traces of the intruder during model training yet be able to identify devices not seen during training, which makes it practical.

Acknowledgement

This research work is supported in part by the U.S. Dept. of Navy under agreement number N00014-17-1-3062 and the U.S. Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) under agreement number FA8750-15-2-0119. The U.S. Government is authorized to reproduce and distribute reprints for governmental purposes notwithstanding

any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the Dept. of Navy or the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) or the U.S. Government.

References

[1] Wang, J., Gu, X., Liu, W., Kumar, A. and Kim, H.J. (2019) An empower hamilton loop based data collection algorithm with mobile agent for wsns. *Human-centric Computing and Information Sciences* **9**: 18. doi:10.1186/s13673-019-0179-4.

[2] Li, W., Chen, Z., Gao, X., Liu, W. and Wang, J. (2019) Multimodel framework for indoor localization under mobile edge computing environment. *IEEE Internet of Things Journal* **6**(3): 4844–4853.

[3] Wang, J., Gao, Y., Yin, X., Li, F. and Kim, H.J. (2018) An enhanced pegasis algorithm with mobile sink support for wireless sensor networks. *Wireless Communications and Mobile Computing* **2018**: 1–9. doi:10.1155/2018/9472075.

[4] Mukherjee, A., Fakoorian, S.A.A., Huang, J. and Swindlehurst, A.L. (2014) Principles of physical layer security in multiuser wireless networks: A survey. *IEEE Communications Surveys Tutorials* **16**(3): 1550–1573.

[5] Polak, A.C. and Goeckel, D.L. (2014) Wireless device identification based on rf oscillator imperfections. In *2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*: 2679–2683.

[6] Wang, W., Sun, Z., Piao, S., Zhu, B. and Ren, K. (2016) Wireless physical-layer identification: Modeling and validation. *IEEE Transactions on Information Forensics and Security* **11**(9): 2091–2106.

[7] Baldini, G. and Steri, G. (2017) A survey of techniques for the identification of mobile phones using the physical fingerprints of the built-in components. *IEEE Communications Surveys Tutorials* **19**(3): 1761–1789. doi:10.1109/COMST.2017.2694487.

[8] Cobb, W.E., Laspe, E.D., Baldwin, R.O., Temple, M.A. and Kim, Y.C. (2012) Intrinsic physical-layer authentication of integrated circuits. *IEEE Transactions on Information Forensics and Security* **7**(1): 14–24.

[9] R. Reising, D., A. Temple, M. and A. Jackson, J. (2015) Authorized and rogue device discrimination using dimensionally reduced rf-dna fingerprints. *IEEE Transactions on Information Forensics and Security* **10**: 1–1. doi:10.1109/TIFS.2015.2400426.

[10] Gong, J., Xu, X. and Lei, Y. (2020) Unsupervised specific emitter identification method using radio-frequency fingerprint embedded infogan. *IEEE Transactions on Information Forensics and Security* **15**: 2898–2913.

[11] Tomko, A.A., Rieser, C.J. and Buell, L.H. (2006) Physical-layer intrusion detection in wireless networks. In *MILCOM 2006 - 2006 IEEE Military Communications conference*: 1–7. doi:10.1109/MILCOM.2006.302476.

[12] O'Shea, T. and Hoydis, J. (2017) An introduction to deep learning for the physical layer. *IEEE Transactions on Cognitive Communications and Networking* **PP**(99): 1–1. doi:10.1109/TCCN.2017.2758370.

[13] Wang, J., Gao, Y., Liu, W., Kumar, A. and Kim, H.J. (2019) An intelligent data gathering schema with data fusion supported for mobile sink in wireless sensor networks. *International Journal of Distributed Sensor Networks* **15**: 155014771983958. doi:10.1177/1550147719839581.

[14] Wang, J., Gao, Y., Wang, K., Sangaiah, A.K. and Lim, S.J. (2019) An affinity propagation-based self-adaptive clustering method for wireless sensor networks. *Sensors (Basel, Switzerland)* **19**.

[15] Lin, Y., Tao, H., Tu, Y. and Liu, T. (2019) A node self-localization algorithm with a mobile anchor node in underwater acoustic sensor networks. *IEEE Access* **PP**: 1–1. doi:10.1109/ACCESS.2019.2904725.

[16] Wang, J., Gao, Y., Liu, W., Kumar, A. and Kim, H.J. (2019) Energy efficient routing algorithm with mobile sink support for wireless sensor networks. *Sensors* **19**: 1494. doi:10.3390/s19071494.

[17] Tu, Y., Lin, Y., Wang, J. and Kim, J.U. (2018) Semi-supervised learning with generative adversarial networks on digital signal modulation classification. *Computers, Materials and Continua* **55**: 243–254. doi:10.3970/cmc.2018.01755.

[18] WANG, H., LI, J., GUO, L., DOU, Z., Lin, Y. and ZHOU, R. (2017) Fractal complexity-based feature extraction algorithm of communication signals. *Fractals* **25**: 1740008. doi:10.1142/S0218348X17400084.

[19] Wang, H., Guo, L., Dou, Z. and Lin, Y. (2018) A new method of cognitive signal recognition based on hybrid information entropy and d-s evidence theory. *Mobile Networks and Applications* **23**. doi:10.1007/s11036-018-1000-8.

[20] Dou, Z., Si, G., Lin, Y. and Wang, M. (2019) An adaptive resource allocation model with anti-jamming in iot network. *IEEE Access* **7**: 93250–93258.

[21] Lin, Y., Zhu, X., Zheng, Z., Dou, Z. and Zhou, R. (2017) The individual identification method of wireless device based on dimensionality reduction and machine learning. *The Journal of Supercomputing* **75**. doi:10.1007/s11227-017-2216-2.

[22] Shi, Q., Kang, J., Wang, R., Yi, H., Lin, Y. and Wang, J. (2018) A framework of intrusion detection system based on bayesian network in iot. *International Journal of Performability Engineering* **14**: 2280–2288. doi:10.23940/ijpe.18.10.p4.22802288.

[23] Hao, P., Wang, X. and Behnad, A. (2014) Relay authentication by exploiting i/q imbalance in amplify-and-forward system. In *2014 IEEE Global Communications Conference*: 613–618.

[24] Hall, J., Barbeau, M. and Kranakis, E. (2004) Enhancing intrusion detection in wireless networks using radio frequency fingerprinting. *Communications, Internet, and Information Technology* .

[25] Hall, J., Barbeau, M. and Kranakis, E. (2004) Radio frequency fingerprinting for intrusion detection in wireless networks: 201–206.

[26] Knox, D.A. and Kunz, T. (2015) Wireless fingerprints inside a wireless sensor network. *ACM Trans. Sen. Netw.* **11**(2). doi:10.1145/2658999, URL https://doi.org/10.1145/2658999.

[27] Deng, S., Huang, Z., Wang, X. and Huang, G. (2017) Radio frequency fingerprint extraction based on multidimension permutation entropy. *International Journal of Antennas and Propagation* **2017**: 1–6. doi:10.1155/2017/1538728.

[28] Huang, N., Shen, Z., Long, S., Wu, M., Shih, H., Zheng, Q., Yen, N. *et al.* (1998) The empirical mode decomposition and the hilbert spectrum for nonlinear and non-stationary time series analysis. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* **454**: 903–995. doi:10.1098/rspa.1998.0193.

[29] Feltane, A. (2016) *Time-frequency-energy analysis and real-time filtering of non-stationary signals*. Ph.D. thesis.

[30] Klein, R.W., Temple, M.A. and Mendenhall, M.J. (2009) Application of wavelet-based rf fingerprinting to enhance wireless network security. *Journal of Communications and Networks* **11**(6): 544–555.

[31] Wang, J., Zhuang, L., Cheng, W., Xu, C., Wu, X. and Zhang, Z. (2019) *Analysis of Classification Methods Based on Radio Frequency Fingerprint for Zigbee Devices*, 121–132. doi:10.1007/978-981-13-6861-5_11.

[32] Peng, L., Hu, A., Zhang, J., Jiang, Y., Yu, J. and Yan, Y. (2019) Design of a hybrid rf fingerprint extraction and device classification scheme. *IEEE Internet of Things Journal* **6**(1): 349–360.

[33] Dubendorfer, C.K., Ramsey, B.W. and Temple, M.A. (2012) An rf-dna verification process for zigbee networks. In *MILCOM 2012 - 2012 IEEE Military Communications Conference*: 1–6. doi:10.1109/MILCOM.2012.6415804.

[34] Cobb, W.E., Laspe, E.D., Baldwin, R.O., Temple, M.A. and Kim, Y.C. (2012) Intrinsic physical-layer authentication of integrated circuits. *IEEE Transactions on Information Forensics and Security* **7**(1): 14–24. doi:10.1109/TIFS.2011.2160170.

[35] Patel, H.J., Temple, M.A. and Baldwin, R.O. (2015) Improving zigbee device network authentication using ensemble decision tree classifiers with radio frequency distinct native attribute fingerprinting. *IEEE Transactions on Reliability* **64**(1): 221–233. doi:10.1109/TR.2014.2372432.

[36] Zhang, Z., Guo, X. and Lin, Y. (2018) Trust management method of d2d communication based on rf fingerprint identification. *IEEE Access* **6**.

[37] Mishra, D., De, S., Alexandropoulos, G.C. and Krishnaswamy, D. (2017) Energy-aware mode selection for throughput maximization in rf-powered d2d communications. In *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*: 1–6.

[38] Chen, Y., Wen, H., Song, H., Chen, S., Xie, F., Yang, Q. and Hu, L. (2018) Lightweight one-time password authentication scheme based on radio-frequency fingerprinting. *IET Communications* **12**(12): 1477–1484.

[39] Chen, S., Wen, H., Wu, J., Xu, A., Jiang, Y., Song, H. and Chen, Y. (2019) Radio frequency fingerprint-based intelligent mobile edge computing for internet of things authentication. *Sensors* **19**(16).

[40] Patel, H.J., Temple, M.A. and Baldwin, R.O. (2015) Improving zigbee device network authentication using ensemble decision tree classifiers with radio frequency distinct native attribute fingerprinting. *IEEE Transactions on Reliability* **64**(1): 221–233.

[41] Dhawale, C., Dhawale, K. and Dubey, R. (2020) *A Review on Deep Learning Applications*, 21–31. doi:10.4018/978-1-7998-1192-3.ch002.

[42] Goodfellow, I., Bengio, Y. and Courville, A. (2016) *Deep Learning* (MIT Press).

[43] Tschannen, M., Bachem, O. and Lucic, M. (2018) Recent advances in autoencoder-based representation learning. *ArXiv* **abs/1812.05069**.

[44] Shahin Shamsabadi, A., Babaie-Zadeh, M., Seyyedsalehi, S., Rabiee, H. and Jutten, C. (2017) A new algorithm for training sparse autoencoders. In *2017 25th European Signal Processing Conference (EUSIPCO)*: 1–8.

[45] Vincent, P., Larochelle, H., Lajoie, I., Bengio, Y. and Manzagol, P.A. (2010) Stacked denoising autoencoders: Learning useful representations in a deep network with a local denoising criterion. *J. Mach. Learn. Res.* **11**: 3371–3408. URL http://dl.acm.org/citation.cfm?id=1756006.1953039.

[46] Masci, J., Meier, U., Ciresan, D.C. and Schmidhuber, J. (2011) Stacked convolutional auto-encoders for hierarchical feature extraction. In *ICANN*.

[47] Dong, G., Liao, G., Liu, H. and Kuang, G. (2018) A review of the autoencoder and its variants: A comparative perspective from target recognition in synthetic-aperture radar images. *IEEE Geoscience and Remote Sensing Magazine* **6**(3): 44–68. doi:10.1109/MGRS.2018.2853555.

[48] Xia, Y., Cao, X., Wen, F., Hua, G. and Sun, J. (2015) Learning discriminative reconstructions for unsupervised outlier removal. In *2015 IEEE International Conference on Computer Vision (ICCV)*: 1511–1519. doi:10.1109/ICCV.2015.177.

[49] Oh, D.Y. and Yun, I.D. (2018) Residual error based anomaly detection using auto-encoder in smd machine sound. *Sensors* **18**(5). doi:10.3390/s18051308, URL https://www.mdpi.com/1424-8220/18/5/1308.

[50] Gutoski, M., Romero Aquino, N., Ribeiro, M., Lazzaretti, A. and Lopes, H. (2017) Detection of video anomalies using convolutional autoencoders and one-class support vector machines. doi:10.21528/CBIC2017-49.

[51] Bassey, J., Adesina, D., Li, X., Qian, L., Aved, A. and Kroecker, T. (2019) Intrusion detection for iot devices based on rf fingerprinting using deep learning. In *2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC)*: 98–104. doi:10.1109/FMEC.2019.8795319.

[52] Andrews, J., Buzzi, S., Choi, W., Hanly, S., Lozano, A.E., Soong, A.C.K. and Zhang, J. (2014) What will 5g be? *IEEE Journal on Selected Areas in Communications* **32**: 1065–1082.

[53] 3GPP (2012) *technical specification group service and system aspects;3GPP system architecture evolution (SAE);*. Technical Specification (TS) 33.401, 3rd Generation Partnership Project (3GPP). Version 10.3.0.

[54] He, D., Chen, C., Chan, S. and Bu, J. (2012) Secure and efficient handover authentication based on bilinear pairing functions. *IEEE Transactions on Wireless Communications* **11**(1): 48–53.