2020

# Physical-Layer Authentication Using Channel State Information and Machine Learning

St. Germain, Ken; Kragh, Frank

ArXiv

Germain, Ken St, and Frank Kragh. "Physical-Layer Authentication Using Channel State Information and Machine Learning." arXiv preprint arXiv:2006.03695 (2020).
http://hdl.handle.net/10945/65606

# Physical-Layer Authentication Using Channel State Information and Machine Learning

Ken St. Germain
*Department of Electrical and Computer Engineering*
*Naval Postgraduate School*
Monterey, CA
kenneth.stgermain@nps.edu

Frank Kragh
*Department of Electrical and Computer Engineering*
*Naval Postgraduate School*
Monterey, CA
fekragh@nps.edu



***Abstract*—Strong authentication in an interconnected wireless environment continues to be an important, but sometimes elusive goal. Research in physical-layer authentication using channel features holds promise as a technique to improve network security for a variety of devices. We propose the use of machine learning and measured multiple-input multiple-output communications channel information to make a decision on whether or not to authenticate a particular device. Our approach uses received channel state information to train a neural network in an adversarial setting. These characteristics are then used to maintain authentication in subsequent communication sessions. This work analyzes the use of information from the wireless environment for the purpose of authentication and demonstrates the employment of a generative adversarial neural network trained with received channel data to authenticate a transmitting device without prior knowledge of receiver noise.**

***Index Terms*—Physical-layer security, authentication, MIMO, CSI, machine learning, generative adversarial network**

## I. Introduction

The protection of integrity, confidentiality, and availability is a challenge in wireless networks. Unlike networks with wired point-to-point connections, the broadcast nature of the wireless domain grants bona fide users and malicious actors the same access to the communication channel. As the 3rd Generation Partnership Project and 5th generation mobile networks bring the promise of very high data rate mobile communications, they must also be secure. Without appropriate security, there will be intrusions and attacks, countering the networks' benefits.

The literature proposes two broad categories to distinguish legitimate from illegitimate devices at the physical-layer. The first relies on unique imperfections of the transmitter hardware that manifest as radio frequency (RF) fingerprints or signatures [1]–[3]. The second method leverages the stochastic nature of the wireless channel to take advantage of multi-path fading environments. The temporally and spatially-unique impulse or frequency response can be used to identify the transmitter [4]–[6].

Our proposed method is based on research using the second category. The effects of the multipath channel can be described in the channel state information (CSI) matrix. The focus of this paper is on the static case, and using a technique as described by [7] can be adopted to account for scenarios where motion is expected to change the CSI.

In this paper we use a generative adversarial network (GAN) to determine if a transmitter should be authenticated or denied access.

The contributions of this paper are:

- We introduce analysis and simulation illustrating how the received CSI matrix elements and measurement error can be used for physical-layer authentication.
- There are two novel contributions in this work:
  (1) In Section III, a hypothesis test for physical-layer authentication using all elements in a CSI matrix and the respective receiver measurement error on those elements.
  (2) In Section V, the use of a GAN model to accurately use MIMO CSI as a basis of authentication at the physical-layer.
- Distinguishing from previous research, our proposal discards the generative model at the conclusion of training and retains the discriminative model. The fully-trained discriminative model, having learned from a generative model that creates indistinguishably realistic CSI samples, is particularly suited to make authentication decisions.

This paper discusses previous work in physical-layer authentication using machine learning in Section II. Section III provides the concept for authentication using CSI and introduces a method to accomplish this. Next we present the system model for the GAN in Section IV. The development of the GAN and simulation results is shown in Section V. Finally, we summarize our observations and discuss future work in Section VI. With respect to notation, unless otherwise addressed, vectors are indicated with bold lower-case letters, and matrices are bold upper-case letters.

## II. Background and Related Work

The nature of the wireless medium affects the transmitted signal as it propagates to the receiver. The narrowband model of the wireless channel is given by

$$\boldsymbol{y} = \boldsymbol{H}\boldsymbol{x} + \boldsymbol{n} \tag{1}$$

where $\boldsymbol{y}$ is the received signal, $\boldsymbol{x}$ is the transmitted signal, $\boldsymbol{H}$ is the time-varying CSI or channel response, and $\boldsymbol{n}$ is the noise vector. $\boldsymbol{H}$ is an $N \times M$ matrix of circularly symmetric complex-valued Gaussian random variables representing

multiple channel conditions such as multi-path fading and the use of multiple antennas [8]. The number of transmitter antennas is $M$ and the number of receiver antennas is $N$. There are several examples in the literature where authors mapped collected CSI to the a priori known position of legitimate transmitters, trained machine learning systems to recognize those signatures, then accurately determined the position of the transmitter [9]–[11]. Taking this a step further, much research has been conducted with machine learning and location information to make an authentication decision based on CSI [12]–[15].

In 2014, Goodfellow et al. [16] proposed the novel concept of a GAN. Composed of two artificial neural network models called the discriminator and the generator, the GAN framework trains these models as they compete against each other in an adversarial competition. While GANs have successfully contributed to many areas that rely on image processing such as single image super-resolution [17], medical radiology [18], facial recognition [19], etc., there have been breakthroughs by applying GANs to investigations in the RF field as well.

O'Shea et al. [20] used a GAN to determine the optimal modulation scheme in a given channel, showing how GANs can allow for adaptation to the RF environment. In an adversarial situation such as jamming and spoofing, Roy [21] proposed the use of GANs for building a robust system that can determine legitimate transmitters from illegitimate ones based on the imbalance of in-phase and quadrature components of a symbol constellation. The amplitude-feature deep convolutional GAN was used by Li et al. [22] to reduce the effort and increase the accuracy in creating a MIMO CSI-based fingerprint database for a Wi-Fi localization system. By combining samples created from collected CSI and samples created with generated CSI data, the error distance was reduced compared to only using processed collected CSI data. The results improved the accuracy of locating the position of transmitters in an indoor, classroom setting.

## III. Authentication with CSI

A receiver continues to authenticate a transmitter if the received CSI varies less than a threshold applied to the received CSI from previous transmissions. During initial authentication, by such means as cryptography or RF fingerprinting, the receiver makes CSI measurements of the channel and stores that information for future authentication.

During channel measurement, the receiver imparts noise to the received signal, resulting in variation to the measured CSI elements. This error, $\boldsymbol{\epsilon}$, is modeled as an additive complex zero-mean Gaussian process, $\mathcal{CN}(0, \boldsymbol{\Sigma}_\epsilon)$, where the covariance of the sample mean is $\boldsymbol{\Sigma}_{\bar{\epsilon}} = \boldsymbol{\Sigma}_\epsilon / s$ for $s$ samples during the measurement. Therefore, the $k$th CSI measured by the receiver, $\hat{\boldsymbol{H}}_k$, is given as

$$\hat{\boldsymbol{H}}_k = \boldsymbol{H} + \boldsymbol{\epsilon}_k \qquad k = 1, 2, \ldots, s \tag{2}$$

where $\boldsymbol{H}$ is the true CSI from (1) and $\boldsymbol{\epsilon}_k$ is a complex $N \times M$ matrix with independent identically distributed elements.

A threshold is then applied to each CSI element, $h_{n,m}$, where the transmitter is authenticated if the distance from every received element, $\hat{h}_{n,m,k}$ from $\hat{\boldsymbol{H}}_k$ for $k > s$, to the estimated element, $h_{n,m}$ from $\boldsymbol{H}$, is less than or equal to a threshold, $z_{n,m}$, based on the average eigenvalue, $\lambda_{ave}$, from the covariance matrix $\boldsymbol{\Sigma}_{\bar{\epsilon}_{n,m}}$. To simplify the notation, we will consider $z_{n,m}$ the same value $z$ for all $n$ and $m$ terms, however in practice, $z$ could vary among CSI elements. The numbered sequential transmission count is represented by $k$. Following the hypothesis testing in [23], we have the null hypothesis, $\mathcal{H}_0$, to authenticate, and the alternative hypothesis, $\mathcal{H}_1$, to deny authentication

$$\begin{aligned}\mathcal{H}_0 :&(\mathrm{Re}(\hat{h}_{n,m,k}) - \mathrm{Re}(h_{n,m}))^2 \\ &+ (\mathrm{Im}(\hat{h}_{n,m,k}) - \mathrm{Im}(h_{n,m}))^2 \leq z^2 \quad \forall n, m \\ \mathcal{H}_1 :&(\mathrm{Re}(\hat{h}_{n,m,k}) - \mathrm{Re}(h_{n,m}))^2 \\ &+ (\mathrm{Im}(\hat{h}_{n,m,k}) - \mathrm{Im}(h_{n,m}))^2 > z^2 \quad \exists n, m\end{aligned} \tag{3}$$

where $\mathrm{Re}(\cdot)$ and $\mathrm{Im}(\cdot)$ return the real and imaginary parts of the CSI matrix elements, respectively and $z$, is a tunable parameter that can be adjusted to suit the requirements of the system. To minimize false positives, $z$ can be set to a relatively small value such as $\lambda_{ave}^{\frac{1}{2}}$, and to minimize false negatives, $z$ can be expanded to a greater value, such as $6\lambda_{ave}^{\frac{1}{2}}$. In order to successfully authenticate, all elements in $\boldsymbol{H}$ and $z$ must jointly achieve the $\mathcal{H}_0$ result. We can determine the probability of one transmitter being accidentally authenticated as another based on the error tolerance for the first transmitter, $z$. Let $a_{n,m}$ be the real part and $b_{n,m}$ be the imaginary part of the complex value for the true CSI element, $h_{n,m} = a_{n,m} + jb_{n,m}$. Both $a_{n,m}$ and $b_{n,m}$ are independent Gaussian random variables with variance $\sigma^2/2$. To this variable, we add the result of the receiver noise, $\boldsymbol{\epsilon}$. The real and imaginary parts of $\epsilon_{n,m}$ are zero-mean independent Gaussian distributed random variables each with sample mean covariance $\Sigma_{\bar{\epsilon}_{n,m}}$.

For a transmitter to be authenticated, $\mathcal{H}_0$ must be satisfied for every CSI element, $h_{n,m}$. Given $h_{n,m} = a_{n,m} + jb_{n,m}$, we can determine the probability that another transmitter will be authenticated. Let $z = 5\lambda_{ave}^{\frac{1}{2}}$ where $\lambda_{ave}$ is the average eigenvalue from the receiver noise covariance matrix, $\boldsymbol{\Sigma}_{\bar{\epsilon}_{n,m}}$ and $u$ and $v$ be the respective real and imaginary parts of the CSI from another transmitter. The probability of $u + jv$ resulting in $\mathcal{H}_0$ for $h_{n,m}$ is

$$\begin{aligned}P([u + jv] \in \mathcal{D}_{n,m}) &= \iint_{\mathcal{D}_{n,m}} \frac{\exp\left(-\frac{u^2+v^2}{\sigma^2}\right)}{2\pi\sqrt{|\boldsymbol{\Sigma}_{u,v}|}}\, du\, dv \\ \text{where,}& \\ \mathcal{D}_{n,m} &= \{(u, v) \mid (u - a_{n,m})^2 + (v - b_{n,m})^2 \leq z^2\}\end{aligned} \tag{4}$$

$$\boldsymbol{\mu}_{u,v} = \begin{pmatrix}0\\0\end{pmatrix}, \qquad \boldsymbol{\Sigma}_{u,v} = \begin{pmatrix}\sigma^2/2 & 0\\ 0 & \sigma^2/2\end{pmatrix}$$

With independent $u$ and $v$, (4) can be evaluated using $P(X \cap Y) = P(Y|X) \cdot P(X)$, where $P(X)$

is the probability that $a_{n,m} - z \leq u \leq a_{n,m} + z$, and $P(Y|X)$ is the probability that $b_{n,m} - \sqrt{z^2 - (u - a_{n,m})^2} \leq v \leq b_{n,m} + \sqrt{z^2 - (u - a_{n,m})^2}$. Therefore,

$$P([u + jv] \in \mathcal{D}_{n,m}) = (Q(A) - Q(B)) \cdot (Q(C) - Q(D))$$

where,

$$\begin{aligned} A &= \frac{a_{n,m} - z}{\sigma} \quad B = \frac{a_{n,m} + z}{\sigma} \\ C &= \frac{b_{n,m} - \sqrt{z^2 - (u - a_{n,m})^2}}{\sigma} \\ D &= \frac{b_{n,m} + \sqrt{z^2 - (u - a_{n,m})^2}}{\sigma} \end{aligned} \tag{5}$$

and the $Q(\cdot)$ function is

$$Q(x) = \int_x^{+\infty} \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{t^2}{2}\right) dt$$

The transmitter must satisfy $\mathcal{H}_0$ for every CSI element. The probability for authentication in a MIMO channel with $M$ transmit antennas and $N$ receive antennas is then

$$\begin{aligned} &\prod_{m=1}^{M} \prod_{n=1}^{N} P([u_{n,m} + jv_{n,m}] \in \mathcal{D}_{n,m}) \\ &\mathcal{D}_{n,m} = \{(u_{n,m}, v_{n,m}) \mid (u_{n,m} - a_{n,m})^2 \\ &\qquad + (v_{n,m} - b_{n,m})^2 \leq z^2\} \end{aligned} \tag{6}$$

Simulating (5) and (6) with $a_{n,m}, b_{n,m}, u$, and $v$ all distributed as $\mathcal{N}(0, 0.5)$, Fig. 1 illustrates how unlikely an accidental authentication will be as the antenna elements of the receiver and transmitter are increased and the threshold is reduced.

To implement this authentication scheme and determine which hypothesis $\hat{h}_{n,m,k}$ satisfies, we require advance knowledge of the noise power our receiver imparts to $\boldsymbol{H}$ to determine $z$ and that may change over time and be different among devices. Instead, we will allow a neural network to implicitly determine the threshold and perform the authentication decision. We created a GAN that is trained on authentic samples from

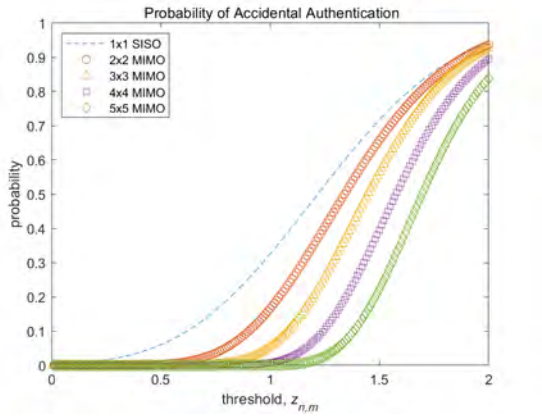



Fig. 1: Probability of authentication for various MIMO configurations and thresholds

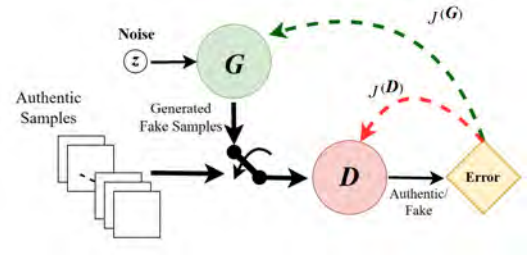



Fig. 2: Training a generative adversarial network

a dataset and samples produced by a generative model. The discriminative model then learned the characteristics of $h_{n,m}$ and $\boldsymbol{\Sigma}_{\bar{\epsilon}_{n,m}}$. Following training, two testing datasets validated the performance of the discriminative model to accurately distinguish $\boldsymbol{H}$ between trusted and untrusted transmitters.

## IV. System Model

We consider a wireless MIMO communications channel with trusted users and untrusted users, some of the latter group who are malicious adversaries. The adversaries have resources available to change their antenna characteristics, transmitter RF path timing, output power, and/or present reflectors between themselves and the receiver. Thus, they are able to change their CSI as measured by the receiver. To defeat this scenario, the discriminative model at the receiver is adversarially trained by a generative model that creates authentic looking CSI samples.

During training, the discriminative model, $\mathcal{D}$, receives authentic samples from the training data or fake samples generated by the generative model, $\mathcal{G}$. The generative model creates fake samples based on a function from random variable input, $z$, and the parameters in $\mathcal{G}$. The discriminative model then assigns a probability from zero to one based on whether the sample is fake (0.0) or authentic (1.0). Fig. 2 shows a functional depiction of a GAN in training, where $J^{(D)}$ and $J^{(G)}$ are the loss functions for the discriminative model and the generative model, respectively.

The adversarial competition in the GAN is a minimax game where the discriminative model attempts to correctly label training samples from a distribution produced by CSI matrix elements, $p_{data}(h_{n,m})$, and fake training samples created by the generator. The discriminative model is trained to maximize the probability of assigning the correct label, while the generative model is trained to minimize the same probability.

## V. Simulation

The GAN processed a single subcarrier in a MIMO $4 \times 4$ configuration. Therefore, the discriminative model has 16 complex inputs and 1 real output, while the generative model has 1 real input and 16 complex outputs. The inputs for the discriminative model and the outputs for the generative model represent the complex elements in the CSI matrix. A dataset of 3,000 authentic training samples were created, where each sample is a $4 \times 4$ complex matrix.

TABLE I: GAN architecture

Discriminator:

| Layer | output size | activation |
|---|---|---|
| Input 1: $x \sim p_{data}(x_{1,1})$ | 2 | |
| Input 2: $x \sim p_{data}(x_{1,2})$ | 2 | |
| ⋮ | ⋮ | |
| Input 16: $x \sim p_{data}(x_{4,4})$ | 2 | |
| Concatenated | 32 | |
| Fully connected | 64 | LeakyReLU (alpha = 0.3) |
| Dropout = 0.2 | | |
| Fully connected | 32 | LeakyReLU (alpha = 0.3) |
| Dropout = 0.2 | | |
| Output | 1 | Sigmoid |

Generator:

| Layer | output size | activation |
|---|---|---|
| Input: $z \sim p_z(z)$ | 5 | |
| Fully connected | 16 | LeakyReLU (alpha = 0.3) |
| Fully connected | 32 | LeakyReLU (alpha = 0.3) |
| Fully connected | 64 | tanh |
| Output 1 | 2 | linear |
| Output 2 | 2 | linear |
| ⋮ | ⋮ | ⋮ |
| Output 16 | 2 | linear |

### A. GAN development

The GAN is implemented using the Python programming language, Keras [24] front-end, and Tensorflow [25] back-end. Additionally, Numpy, Pandas, and Matplotlib Python libraries were used. The overall GAN design is summarized in Table I, with a total of 9,057 parameters. The file size of the discriminator network was 98.8 KB.

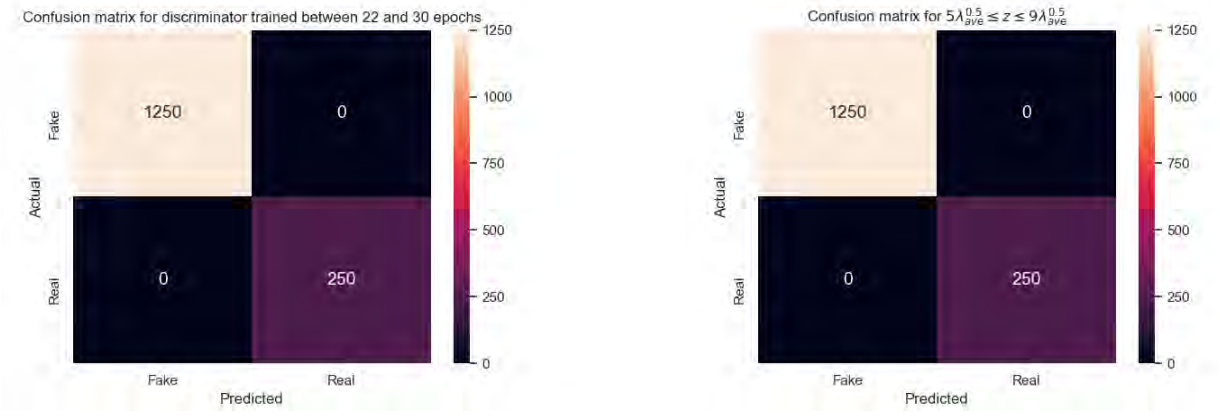
### B. Datasets

The training dataset consists of 3,000 samples. Each sample is created by adding measurement error in the form of AWGN to a single CSI matrix composed of 16 circularly symmetric Gaussian complex values with zero mean, and unit variance, $\mathcal{CN}(0,1)$. The GAN was trained using mini-batches of 64.

Two testing datasets were created, each consisting of 1,500 samples. The first testing dataset replicated the accidental authentication case. There are two transmitters, one of which should be authenticated. For the transmitter that should be authenticated, the same random number generator seed from the training dataset was used and a single CSI matrix was created, while another CSI matrix for the other transmitter was generated using a different seed. To both of these, the same AWGN distribution was added to simulate CSI measurement error, resulting in 250 legitimate samples, and 1,250 illegitimate samples. The second testing dataset emulated five nefarious users attempting to authenticate by matching the CSI matrix of a single legitimate transmitter. If by some unlikely method, an adversary were able to know the channel characteristics between two legitimately authenticated transmitters, the adversary may also have the resources necessary to spoof their transmitted CSI to appear as another transmitter's received CSI. As before, an AWGN distribution was added to simulate CSI measurement error, resulting in 250 legitimate samples. To complete this dataset, five different offsets were added to the CSI measurement error real and imaginary components from the legitimate transmitter, resulting in five subsets of 250 samples each.

### C. Results

The performance of the discriminative model indicates the viability of using a GAN for physical-layer authentication using CSI. The results for the five nefarious user testing dataset is shown using the confusion matrix in Fig. 3a. The same test dataset used on the discriminator was applied to the hypothesis test in (3) where the test was 100% accurate when $z$ ranged from $5\lambda_{ave}^{\frac{1}{2}}$ to $9\lambda_{ave}^{\frac{1}{2}}$ as shown in Fig. 3b. When $z$ was less than $5\lambda_{ave}^{\frac{1}{2}}$, legitimate samples were misidentified, and when $z$ was greater than $9\lambda_{ave}^{\frac{1}{2}}$, illegitimate samples were then misidentified. The advantage to using the GAN is that $z$ doesn't need to be determined in advance. To obtain 100% accuracy with the accidental authentication testing dataset, the discriminator needed to be trained at least 19 epochs, and using the hypothesis test, $z$ ranged from $5\lambda_{ave}^{\frac{1}{2}}$ to $20\lambda_{ave}^{\frac{1}{2}}$.




(a) GAN confusion matrix

(b) Hyptothesis test confusion matrix

Fig. 3: Confusion matrices for five adversaries and one legitimate transmitter test dataset for (a) GAN and (b) hypothesis test

To compare the relative performance of the GAN-trained discriminator and the hypothesis test in (3) for noisy receivers, AWGN was increased by an order of magnitude to the received samples in the training and nefarious adversaries testing datasets. The hypothesis test resulted in 97.4% accuracy with $z = 3\lambda_{ave}^{\frac{1}{2}}$, while the discriminator was 99.07% accurate after 28 training epochs. The hypothesis test authenticated 212 out of 250 legitimate samples, and denied authentication to 1250 illegitimate samples. The discriminator authenticated 236 legitimate samples, and like the hypothesis test, it denied authentication to 1250 samples. Further increasing the receiver noise diminished the performance of both authentication methods using the original testing datasets.

## VI. Conclusion and Future Work

We showed how CSI could be used as a method to provide physical-layer authentication. Our analysis illustrated that the probability of accidentally authenticating other transmitters decreases as receive and transmit antennas are increased and a threshold value is judiciously applied. We then developed a GAN trained on a dataset of CSI matrices to perform physical-layer authentication in an adversarial environment. After training less than 30 epochs, the discriminator was 100% accurate, implicitly determining appropriate thresholds for received CSI matrix elements without information regarding receiver noise. The discriminator performance was superior to the hypothesis method when receiver noise was increased by an order of magnitude.

This paper demonstrated how physical-layer authentication can be accomplished in a flat fading single subchannel environment. By applying this concept to multiple subchannels, there is an opportunity for obtaining robust multi-channel characteristics that can be used to identify a transmitter for authentication. Furthermore, the GAN should be evaluated on additional training and test datasets to demonstrate effectiveness in a variety of wireless environments.

## References


[1] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proceedings of the 14th ACM international conference on Mobile computing and networking - MobiCom '08*. San Francisco, California, USA: ACM Press, 2008, p. 116.

[2] O. Gungor and C. E. Koksal, "On the Basic Limits of RF-Fingerprint-Based Authentication," *IEEE Transactions on Information Theory*, vol. 62, no. 8, pp. 4523–4543, Aug. 2016.

[3] A. C. Polak, S. Dolatshahi, and D. L. Goeckel, "Identifying Wireless Users via Transmitter Imperfections," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 7, pp. 1469–1479, Aug. 2011.

[4] J. K. Tugnait, "Wireless User Authentication via Comparison of Power Spectral Densities," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1791–1802, Sep. 2013.

[5] Yingbin Liang, H. Poor, and S. Shamai, "Secure Communication Over Fading Channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[6] N. Al Khanbashi, N. Al Sindi, S. Al-Araji, N. Ali, Z. Chaloupka, V. Yenamandra, and J. Aweya, "Real time evaluation of RF fingerprints in wireless LAN localization systems," in *2013 10th Workshop on Positioning, Navigation and Communication (WPNC)*, Mar. 2013, pp. 1–6.

[7] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "A Physical-Layer Technique to Enhance Authentication for Mobile Terminals," in *2008 IEEE International Conference on Communications*, May 2008, pp. 1520–1524, iSSN: 1550-3607, 1938-1883.

[8] "Models for MIMO propagation channels: a review," vol. 2, no. 7.

[9] C. Nerguizian, C. Despins, and S. Affes, "Geolocation in mines with an impulse response fingerprinting technique and neural networks," in *IEEE 60th Vehicular Technology Conference, 2004. VTC2004-Fall. 2004*, vol. 5, Sep. 2004, pp. 3589–3594 Vol. 5, iSSN: 1090-3038.

[10] J. Xiao, K. Wu, Y. Yi, and L. M. Ni, "FIFS: Fine-Grained Indoor Fingerprinting System," in *2012 21st International Conference on Computer Communications and Networks (ICCCN)*, Jul. 2012, pp. 1–7, iSSN: 1095-2055.

[11] X. Wang, L. Gao, S. Mao, and S. Pandey, "CSI-Based Fingerprinting for Indoor Localization: A Deep Learning Approach," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 1, pp. 763–776, Jan. 2017.

[12] R.-F. Liao, H. Wen, J. Wu, F. Pan, A. Xu, Y. Jiang, F. Xie, and M. Cao, "Deep-Learning-Based Physical Layer Authentication for Industrial Wireless Sensor Networks," *Sensors (Basel, Switzerland)*, vol. 19, no. 11, May 2019. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6603790/

[13] R. Liao, H. Wen, J. Wu, F. Pan, A. Xu, H. Song, F. Xie, Y. Jiang, and M. Cao, "Security Enhancement for Mobile Edge Computing Through Physical Layer Authentication," *IEEE Access*, vol. 7, pp. 116 390–116 401, 2019.

[14] F. Pan, H. Wen, R. Liao, Y. Jiang, A. Xu, K. Ouyang, and X. Zhu, "Physical layer authentication based on channel information and machine learning," in *2017 IEEE Conference on Communications and Network Security (CNS)*, Oct. 2017, pp. 364–365.

[15] F. Pan, Z. Pang, M. Luvisotto, X. Jiang, R. N. Jansson, M. Xiao, and H. Wen, "Authentication Based on Channel State Information for Industrial Wireless Communications," in *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, Oct. 2018, pp. 4125–4130.

[16] I. J. Goodfellow, J. Pouget-Abadie, M. Mirza, B. Xu, D. Warde-Farley, S. Ozair, A. Courville, and Y. Bengio, "Generative Adversarial Nets," in *Proceedings of the 27th International Conference on Neural Information Processing Systems - Volume 2*, ser. NIPS'14. Cambridge, MA, USA: MIT Press, 2014, pp. 2672–2680, event-place: Montreal, Canada.

[17] C. Ledig, L. Theis, F. Huszr, J. Caballero, A. Cunningham, A. Acosta, A. Aitken, A. Tejani, J. Totz, Z. Wang, and W. Shi, "Photo-Realistic Single Image Super-Resolution Using a Generative Adversarial Network," in *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Jul. 2017, pp. 105–114, iSSN: 1063-6919.

[18] K. Armanious, C. Jiang, M. Fischer, T. Kstner, T. Hepp, K. Nikolaou, S. Gatidis, and B. Yang, "MedGAN: Medical Image Translation using GANs," *Computerized Medical Imaging and Graphics*, p. 101684, Nov. 2019.

[19] J. Bao, D. Chen, F. Wen, H. Li, and G. Hua, "CVAE-GAN: Fine-Grained Image Generation through Asymmetric Training," in *2017 IEEE International Conference on Computer Vision (ICCV)*, Oct. 2017, pp. 2764–2773, iSSN: 2380-7504.

[20] T. J. O'Shea, T. Roy, N. West, and B. C. Hilburn, "Physical Layer Communications System Design Over-the-Air Using Adversarial Networks," in *2018 26th European Signal Processing Conference (EUSIPCO)*, Sep. 2018, pp. 529–532.

[21] D. Roy, T. Mukherjee, M. Chatterjee, E. Blasch, and E. Pasiliao, "RFAL: Adversarial Learning for RF Transmitter Identification and Classification," *IEEE Transactions on Cognitive Communications and Networking*, pp. 1–1, 2019.

[22] Q. Li, H. Qu, Z. Liu, N. Zhou, W. Sun, S. Sigg, and J. Li, "AF-DCGAN: Amplitude Feature Deep Convolutional GAN for Fingerprint Construction in Indoor Localization Systems," *IEEE Transactions on Emerging Topics in Computational Intelligence*, pp. 1–13, 2019.

[23] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Transactions on Wireless Communications*, vol. 7, no. 7, pp. 2571–2579, Jul. 2008.

[24] F. Chollet, et al., *Keras*, 2015. [Online]. Available: https://keras.io

[25] M. Abadi, et al., "TensorFlow: Large-Scale Machine Learning on Heterogeneous Systems," 2015. [Online]. Available: https://www.tensorflow.org/