# Robust Measurements for RF Fingerprinting with Constellation Patterns of Radiated Waveforms.

Améya S. Ramadurgakar*†, Jacob D. Rezac†, Lennart M. Heijnen†, Kate A. Remley†,
Dylan F. Williams†, Melinda Piket-May* and Robert D. Horansky†
*Department of Electrical, Computer and Energy Engineering
University of Colorado Boulder
Email: {ameya.ramadurgakar, melinda.piket-may}@colorado.edu
†Communications Technology Laboratory
National Institute of Standards and Technology
Email: {ameya.ramadurgakar, jacob.rezac, lennart.heijnen, robert.horansky, kate.remley, dylan.williams}@nist.gov

2023 IEEE Physical Assurance and Inspection of Electronics (PAINE) | 979-8-3503-3931-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/PAINE58317.2023.10318021

***Abstract*—We introduce an RF fingerprint for non-destructive cellular device identification. The new proposed fingerprinting algorithm is a data-driven technique based on a singular value decomposition of a user equipment's symbol-constellation points. We explore the effectiveness of the fingerprint technique with a test set of real devices and show experimentally that this fingerprint is robust to device positioning errors and measurement noise.**

***Index Terms*—RF Fingerprinting, Over the Air Measurements, Supply Chain Security**

## I. Introduction

Radio frequency (RF) fingerprints are features that consistently and uniquely serve to identify a wireless device such as a cellular user equipment (UE). They hold promise for a number of applications in hardware security and quality assurance. Reviews by authors in [1]–[4] show recent advancements made in this area and survey various approaches and open challenges for practical implementation of RF fingerprints. In this work, we provide a non-destructive fingerprinting method based on over-the-air RF measurements. Traditional device authentication is done with cryptographic methods which can be manipulated and copied [1]; RF fingerprints go beyond these methods with techniques that depend directly on hardware characteristics of devices, such as unique manufacturing imperfections and tolerances. Our work's focus is on an acceptance test scenario whose goal is to detect compromised or counterfeit cellular devices.

An extensive literature exists describing RF fingerprinting techniques for devices with different radio networks e.g., IEEE 802.11, IEEE 802.15, RFID, and cellular radio access networks. In this work, we focus primarily on data-driven fingerprinting algorithms, meaning that fingerprints are determined purely from mathematical transformations of measured data, rather than being based on hypotheses about the physical nature of hardware components in the devices. Data-driven techniques use large datasets of measurements to identify subtle differences between devices that would not be seen with traditional metrics.

In [5], we used a measurement setup identical to the one used below to differentiate between devices with a fingerprint related to the observed error-vector-magnitude (EVM) of each device. The EVM is a standard metric to assess a device's performance. We demonstrated in [5] that there is a consistent difference between symbol streams of different UEs and describe this difference in a metric called deviation EVM. In this work, we use tools from statistical learning theory to show that these differences can reliably classify different phones.

Most data-driven fingerprinting algorithms involve a dimensionality reduction step, which transforms measured data from millions of points to a fingerprint of much lower dimension (often 10 or fewer). The fingerprinting algorithm we propose in Section III uses a singular value decomposition (SVD) to perform this step. The SVD is a commonly used technique in the implementation of dimension reduction schemes, and other works use SVD for this purpose when building fingerprints; see [6] in the context of RFID fingerprinting and [7] in determining if a cellular device's camera is on, for two examples. Unlike those works, the novelty of our approach involves in applying the SVD directly to normalized symbol-constellation measurements of commercial 4G cellular devices.

In addition to the effectiveness of the proposed technique, we also explore its robustness to experimental variability. Some work has been done on fingerprinting technique sensitivity, such as evaluating the difference between high-end receivers and low-cost receivers when developing fingerprints [8]. A number of researchers have studied the performance of fingerprints with different wireless channels ( [9]–[13]) or different distances between device and receiver for training and testing [14]. We designed the testbed used in this paper to specifically explore algorithm robustness to experimental variability to ultimately ensure reproducible fingerprint measurements from one lab to another.

After introducing our test setup in Section II and proposing a new fingerprinting algorithm in Section III, we evaluated our new RF fingerprint on an example test case. We first built a database of RF fingerprints from measurements of three UEs,



Lennart M. Heijnen participated in this work while affiliated with the Eindhoven University of Technology.

each from a different manufacturer. We then compared this database to the RF fingerprints of the same UEs measured with different setup conditions from what was used to build the database. For the test UEs considered in this work, the fingerprints identified each device over 90% of the time, as long as the orientation of the UE was held within roll angles of $\pm 15°$. The fingerprints were also shown to be robust to modest levels of added measurement noise.

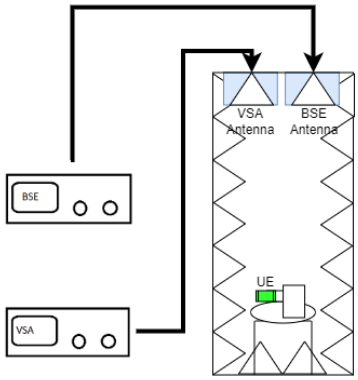


Fig. 1: Test device setup in an anechoic chamber on positioner

## II. Experiment Design

The measurement setup consists of three pieces of hardware: a base station emulator (BSE), a vector signal analyzer (VSA), and an anechoic chamber. The BSE establishes a link with the UE inside the anechoic chamber and controls the UE's power and transmitted data. The VSA is based on a real-time oscilloscope. It samples time-domain data at a high rate and uses internal procedures to align and demodulate the measured signal. The VSA only monitors the uplink signal transmitted from the UE which is at a different frequency than the downlink signal received by the UE. The measured data presented in the next section were taken at LTE band 1 with an uplink center frequency of 1950 MHz and a downlink frequency of 2140 MHz. The BSE and VSA are connected to their respective antennas inside the chamber seen in Fig. 1. The VSA and BSE each are attached to antennas having a similar radiation pattern and gain performance. Table I lists further details of the setup.

TABLE I: A listing of conditions held constant throughout all experiments.

| | |
|---|---|
| Uplink center frequency | 1950 MHz |
| Downlink center frequency | 2140 MHz |
| Radio frame duration | 10 ms |
| Uplink bandwidth | 10 MHz |
| Modulation depth | 16 QAM |

The BSE was set to configure the UE to repeatedly transmit a given sequence of symbols with 16QAM modulation depth. For the experiments shown in this paper, the symbol stream from each UE was the same length, but one manufacturer's device transmitted a different sequence of symbols than the other two. The sequence of these symbols was not used in the proposed algorithm to generate fingerprints as the transmissions from each UE's observations were uniformly sampled for each constellation point associated to a symbol.

After measuring the resulting signal and converting to frequency domain, the VSA software demodulates the signal into symbol-constellation (IQ-domain) points. Further information of this process can be found in [18]. In a post-processing step, we removed the points due to the demodulation reference signal (DMRS), leaving only the sequence of symbols each device was instructed to transmit.

In this paper we test the robustness of the proposed algorithm against two parameters: the geometry of the the measurement setup and the addition of simulated system noise. Inside the anechoic chamber is a custom UE positioner capable of movement multiple axes. We refer to the axis we study in this work as the roll angle, which is indicated in Fig. 2. We focus exclusively on this angle because auxiliary measurements have shown that changes in roll angle cause the largest variations in measured waveforms. A photograph of the inside of the chamber is additionally shown in Fig. 2. The positioner is constructed primarily of acrylic and is covered with RF absorber to reduce reflections.

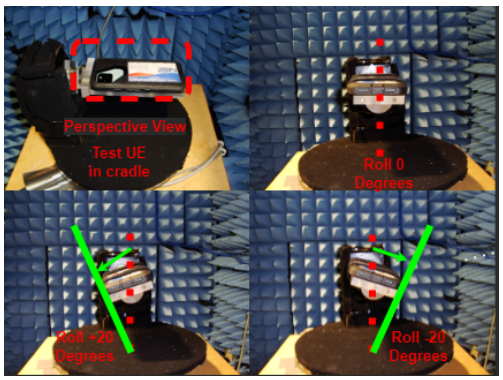


Fig. 2: Four images showing, (Top left) the top view of the UE in the positioner, (Top Right) the front view at roll angle 0°, (Bottom Left) -20° roll angle, and (Bottom Right) +20° roll angle.

Once a connection to a UE is established with the BSE, we ensured that the uplink symbol stream waveform remained constant over time and the link had a 0% block error rate (BLER), as defined in [19]. We then used the VSA to collect waveforms from three UEs, each from a different manufacturer. We took the data as a function of roll angle from 0° to $\pm$ 20° in 5° increments. At each angular position, 30 measurements were made of the symbol stream with 5 seconds between each measurement. We performed 30 measurements as a trade-off between measurement time and training set size. Furthermore, the whole experiment was repeated three times to estimate experimental uncertainty and provide training and testing datasets. Table II shows a summary of each of three datasets and how each was used to develop and evaluate RF fingerprints with the proposed algorithm.

TABLE II: Measurement data set used for testing and training the proposed algorithm.

| Measurement set | Use | Roll angles | Number of observations |
|---|---|---|---|
| Set 1 | Training | 0° | 30 |
| Set 2 | Testing | -20° to 20° in steps of 5° | 30 per step |
| Set 3 | Testing | -20° to 20° in steps of 5° | 30 per step |

## III. Description of Proposed Algorithm

We hypothesize that hardware differences in different UEs result in radiated IQ values that differ from their ideal. These differences can be summarized with a small number of principle components. If these differences can be shown to be characteristic of the UE model then they might be used as a fingerprint for supply chain security purposes. We measure a UE's emissions for one radio frame, resulting in 64,000 relevant IQ values per observation. Our proposed algorithm creates a fingerprint for each UE from unique characteristics of those IQ values.

The proposed algorithm recasts data into a few basis vectors on which the measured IQ value data is best approximated with the fewest coordinates. We perform dimension reduction with an SVD applied to the difference between observations of a device's symbol-constellation points and an estimate of each ideal symbol-constellation point. This difference is related to EVM, which we found was a characteristic unique to different UEs in [5]. In the experiments described in Section IV, we find that only two dimensions are needed when fingerprinting our dataset. In the statistical literature, similar dimension-reduction procedures are sometimes referred to as principal component analysis. We were inspired to use these lower-dimensional representations as UE fingerprints by a similar approach introduced in the context of image classification [15].

Our proposed algorithm is a three-step process: 1. data normalization, 2. dimension reduction, and 3. distance-based classification. A top level process diagram of the algorithm is shown in Fig. 3, which shows both measured IQ values and low-dimensional fingerprints. After an initial standardization step, the proposed algorithm uses the SVD described above to project each observation to a low-dimensional space on which classification is done with the $k$-nearest neighbors algorithm. The colored circles in Fig. 3 show that each UE clusters to a unique location in this low-dimensional space.

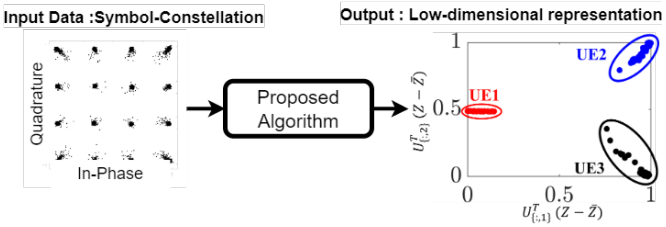


Fig. 3: Algorithm process diagram for UE identification. The left figure shows measured IQ values that are normalized and dimension reduced to the points shown on the right figure.

To describe the algorithm mathematically, we denote the $J$ observations of symbol-constellation points by $\mathbf{q}_j$, $j = 1, \ldots, J$. We use bold lower-case letters to indicate column vectors and bold upper-case letters to indicate matrices. For measurement set 1 described in Table II, we take $J = 90$ observations ((30 observations per UE) $\times$ 3 UEs), and similarly for the other measurement sets. Each observation $\mathbf{q}_j \in \mathbb{C}^{SN}$ is a vector with $64,000$ entries, consisting of $N = 4000$ points per symbol and $S = 16$ symbols due to the 16-QAM modulation scheme. The normalization step will result in a matrix on which we perform dimension reduction, $\mathbf{Z} \in \mathbb{R}^{2SN \times J}$, whose columns are the real and imaginary parts of the normalized $\mathbf{q}_j$ vectors.

For each observed vector of IQ values, $\mathbf{q}_j$, we perform the normalization separately on the $S$ subsets of $\mathbf{q}_j$ corresponding to which symbol which was transmitted. Denote these $N$-dimensional vectors of transmissions of symbol $s$ by $\mathbf{q}_j^{(s)}$. The data normalization step consists of transforming each $\mathbf{q}_j^{(s)}$ into a new vector $\mathbf{z}_j^{(s)}$ which has mean zero and unit variance[1]. We collect normalized data from each observation into the matrix $\mathbf{Z}$ whose $j$th column is

$$\mathbf{Z}_{:,j} = [\mathrm{Re}(\mathbf{z}_j^{(1)}), \ldots, \mathrm{Re}(\mathbf{z}_j^{(16)}), \mathrm{Im}(\mathbf{z}_j^{(1)}), \ldots, \mathrm{Im}(\mathbf{z}_j^{(16)})]^T,$$

where $\mathrm{Re}(\cdot)$ and $\mathrm{Im}(\cdot)$ indicate the real and imaginary part of a vector, respectively. For measurement set 1, this is a $128,000 \times 90$ dimensional matrix, and similarly for other measurement sets.

The algorithm next projects the normalized data to a lower-dimensional subspace with the SVD, as described above. The dimension of this subspace, denoted $k_{\mathrm{SVD}}$, is chosen by the user; we have found that $k_{\mathrm{SVD}} = 2$ to be effective in the experiments in Section IV. We calculate the SVD $\mathbf{USV}^T = (\mathbf{Z} - \overline{\mathbf{Z}})$, where the first $k_{\mathrm{SVD}}$ columns of matrices on the left are the new basis set and $\overline{\mathbf{Z}}$ is an average of the columns of $\mathbf{Z}$. We remove $\overline{\mathbf{Z}}$ to further normalize the information on which we apply the SVD. The normalized data are then projected onto the new coordinates with $[\mathbf{U}_{:,1:k_{\mathrm{SVD}}}]^T(\mathbf{Z} - \overline{\mathbf{Z}})$, where the subscript on $\mathbf{U}$ indicates that only the first $k_{\mathrm{SVD}}$ columns of $\mathbf{U}$ are used. The projected matrix does not necessarily have a physical meaning; it is the nearest matrix to $\mathbf{Z} - \overline{\mathbf{Z}}$ in a $k_{\mathrm{SVD}}$-dimensional subspace. The cluster of these coordinates for each UE defines locations in the new coordinate space that are assigned to that device. Details of the algorithm which results in fingerprints are provided in Algorithm 1.

Finally, with the training data clustered as described above, we use the $k$-nearest neighbor ($k$-NN) algorithm [16] to determine the probability that data from an unknown device is assigned to each UE manufacturer. In particular, let $\mathbf{z}^{(\mathrm{new})}$ be a new measurement of an unknown device that has been normalized and reordered in the same way as $\mathbf{Z}$. Then,

[1]In practice, normalize variance by treating each $\mathbf{q}_j^{(s)}$ as an $N \times 2$ matrix whose first column consists of the real part of $\mathbf{q}_j^{(s)}$ and second column the imaginary part. We multiply these reshaped IQ values by a matrix $\mathbf{L}$ chosen so that the sample covariance matrix of the resulting matrix is the identity. We reshape the result into an $N \times 1$ vector of complex values, $\mathbf{z}_j^{(s)}$.

**Algorithm 1** Training Algorithm for UE Identification

**Input:**

- Symbol-constellation vectors for each symbol $s$ and observation $j$: $\mathbf{q}_j^{(s)}, j = 1, \ldots, J,\ s = 1, \ldots, S$
- UE labels: $u_j, j = 1, \ldots, J$
- SVD-reduced dimension: $k_{\text{SVD}}$
- $k$-Nearest Neighbor parameter: $k_{\text{NN}}$

1: **for** $j = 1 \ldots J$ **do**
2: $\quad \mathbf{Z}_{:,j} \leftarrow$ standardization and reordering of $\mathbf{q}_j$
3: **end for**
4: $(\mathbf{U}, \mathbf{S}, \mathbf{V}) \leftarrow \text{SVD}(\mathbf{Z} - \overline{\mathbf{Z}})$
5: $\mathbf{D} \leftarrow [\mathbf{U}_{:,1:k_{\text{SVD}}}]^T(\mathbf{Z} - \overline{\mathbf{Z}})$

**Output:** Predicted probability of any vector $\in \mathbb{R}^{k_{\text{SVD}}}$ having each class label $\leftarrow$ k-NN$(\mathbf{D}, u_j)$

$[\mathbf{U}_{:,1:k_{\text{SVD}}}]^T(\mathbf{z}^{(\text{new})} - \overline{\mathbf{Z}})$ represents the fingerprint of the new measurement. The $k$-NN classifier determines the device to which this measurement corresponds by finding the distance between the new measurement and each measurement in the training dataset, each projected into the SVD-informed low-dimensional space. The new measurement is classified as whichever device from the training dataset makes up the plurality of the new measurement's $k_{\text{NN}}$ nearest neighbors. In other words, the classification is deployed onto an unknown UE by applying steps 1. and 2. to a measurement and using the $k$-NN classifier to determine which UE in the training dataset is closest to the new measured data.

## IV. Results and Analysis

We are interested in how well the above algorithm classifies a new observation of a UE. To this end, we take a number of repeat observations of each UE and determine how often each of these observations is correctly identified. We report true-positive rates (TPRs) and accuracy rates to summarize the algorithm's effectiveness. The TPR of each UE is the percentage of times that the proposed algorithm identifies a measurement as that UE, compared to the total number of measurements of that UE. The accuracy rate is the percentage of total classifications that were correct across all UEs.

The algorithm has two free parameters which must be selected before application to measurements: the number of dimensions onto which the data is projected, $k_{\text{SVD}}$, and $k_{\text{NN}}$, the number of nearest neighbors to which each datapoint is compared in the $k$-NN classification. We choose these by maximizing true positive and accuracy rates on a randomly split subset of measurement Set 1. Specifically, we randomly split measurement Set 1 into a subset of 20 training points and 10 validation points. We train the proposed algorithm on the 20 training points and evaluate its performance on the remaining 10 validation points for different values of $k_{\text{SVD}}$ and $k_{\text{NN}}$. Selecting $k_{\text{SVD}} = 2$ and $k_{\text{NN}} = 3$ gives perfect true positive and accuracy rates on this subset of data, so we continue with those parameters throughout.

To further assess the limits of UE identification, the constellation data was digitally altered with additive white Gaussian noise (AWGN). The distribution of measured constellation points was expanded with added noise for the testing data sets. We quantify this added noise through the EVM [17] of the newly created data as

$$\text{EVM}(S_{\text{ideal}}, S_{\text{meas}}) = \left( \frac{\frac{1}{N}\sum_{n=1}^{N} |S_{\text{ideal,n}} - S_{\text{meas,n}}|^2}{\frac{1}{N}\sum_{n=1}^{N} |S_{\text{ideal,n}}|^2} \right)^{1/2}. \tag{1}$$

Here, $S_{\text{ideal}}$ and $S_{\text{meas}}$ are ideal and measured constellation points in the complex plane for N measured symbols. The measured symbol stream is passed through a simulated AWGN channel with varying signal-to-noise ratios (SNR) from 20 to 40 dB in increments of 10 dB. As EVM is a good measure of noise in an IQ value measurement, these noise levels are represented in EVM values in percentages. The constellation diagrams and calculated EVM values are shown in Fig. 4 where each EVM value corresponds to $S_{\text{meas}}$ with a different AWGN level in Eq. (1). The EVM values shown in plots of Fig. 4, are a representation of just one measured observation.

Fig. 5 shows the TPR for two sets of test data for each device. The algorithm was trained using data set 1 which was taken at 0° roll angle. After training, it was used to classify UE measurements from sets 2 and 3 as a function of roll angle. Here, the TPR for each UE model is plotted against roll angle. We see that the proposed algorithm predicts with high accuracy the correct UE models and is robust to UE orientation.

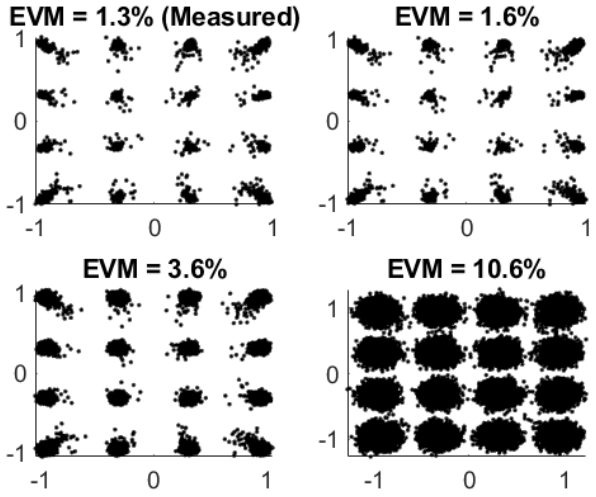


Fig. 4: Constellation with different EVMs. (Top Left) EVM of 1.3% has no added noise i.e. 0 dB, (Top Right) EVM of 1.6% is 40 dB SNR, (Bottom Left) EVM of 3.6% is 30 dB SNR and (Bottom Right) EVM of 10.6% is 20 dB SNR.

Fig. 6 shows how adding varying levels of simulated measurement noise have an effect on the performance of the proposed algorithm. The data set that was used to generate the curves is the same that was used for Fig. 5, but with added noise on the testing data. The same level of noise was added to all the 30 observations of angular measurements. We obtain near perfect classification when EVM is less than 1.6%. As

more noise is added the classification accuracy decreases. As Fig. 5 shows, accuracy is low (below 40%) for all angles when EVM is increased to 10.6%. These experiments show that our proposed algorithm is robust against some signal degradation with AWGN.

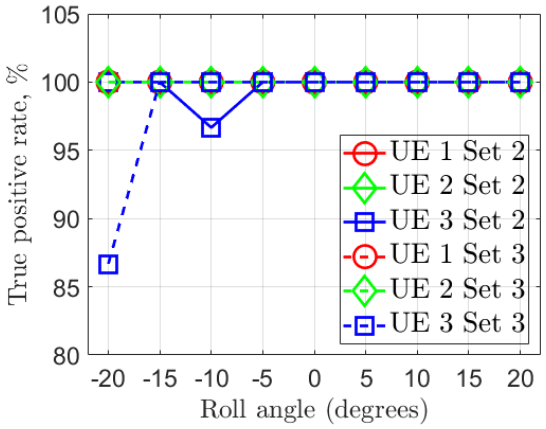


Fig. 5: True positive rates of the three UEs as a function of different roll angles. These are the result of training the proposed algorithm on 0° data from measurement set 1 and applying it on measurement sets 2 and 3. Each measurement set was comprised of 30 observations.

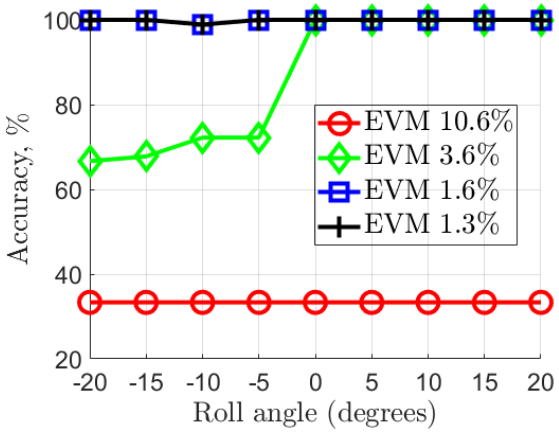


Fig. 6: Accuracy rates (combining the true positive rates of all UEs) as a function of each roll angle for varying AWGN levels as testing data. The training was at the zero degree angular position and no added noise. An EVM of 1.3% corresponds to the original data with no added noise.

## V. Conclusions

Communication devices require non-destructive tests to determine aberrations in their construction. These aberrations could be due to errors in integration of the whole system, or due to hardware security issues such as attempting counterfeit or espionage. RF fingerprinting may be used to address this need. In this paper, we have shown a method to identify different UEs with over-the-air RF signatures.

The algorithm differentiates between devices based on the individual error vectors of the symbols radiated by each UE. Since OTA measurements can be sensitive to the experimental setup, we investigated the proposed algorithm as a function of device orientation and system noise. We have shown this new algorithm is robust to device orientation as well as additive noise. This is important for its use in varying test setups across different labs.

Further verification of our findings will require a larger set of UEs for classification and therefore acquisition of additional UEs for further investigation at serial number variation level. Understanding the fingerprinting variability is key to the real-world use of RF fingerprinting techniques. To this end, our future direction involves studying the impact of additional measurement variability on wireless device fingerprinting, such as modulation scheme and transmission frequency.

## References


[1] G. Baldini and G. Steri, 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), pp. 1761-1789 (2017).

[2] X. Guo, Z. Zhang, and J. Chang, Survey of Mobile Device Authentication Methods Based on RF Fingerprint. IEEE INFOCOM 2019, pp 1-6 (2019).

[3] N. Soltanieh, Y. Norouzi, Y. Yang, and N. C. Karmakar, A Review of Radio Frequency Fingerprinting Techniques. IEEE J. Radio Freq. Identif. **4** (3), pp. 222–233 (2020).

[4] Q. Xu, R. Zheng, W. Saad and Z. Han, "Device Fingerprinting in Wireless Networks: Challenges and Opportunities," in IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 94-104, Firstquarter 2016, doi: 10.1109/COMST.2015.2476338.

[5] A.S. Ramadurgakar, K.A. Remley, D.F. Williams, J.D. Rezac, M. Piket-May, and R. Horansky, A Measurement-Referenced Error Vector Magnitude for Counterfeit Cellular Device Detection. 2023 101st ARFTG Microwave Measurement Conference (ARFTG) (2023). In Press.

[6] B. Danev, T.S. Heydt-Benjamin, S. Capkun, Physical-layer Identification of RFID Devices. USENIX Security Symposium, pp. 199-214 (2009).

[7] B.B. Yilmaz, E.M. Ugurlu, A. Zajić and M. Prvulovic, "Detecting Cellphone Camera Status at Distance by Exploiting Electromagnetic Emanations," MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM), 2019, doi: 10.1109/MILCOM47813.2019.9021060

[8] S. Rehman, K. Sowerby, and C. Coghill, Analysis of receiver front end on the performance of RF fingerprinting. 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications pp. 2494-2499 (2012).

[9] A. Al-Shawabka, F. Restuccia, S. D'Oro, T. Jian, B.C. Rendon, N. Soltani, J. Dy, S. Ioannidis, K. Chowdhury, and T. Melodia, Exposing the fingerprint: Dissecting the impact of the wireless channel on radio fingerprinting. IEEE INFOCOM, pp. 646-655 (2020).

[10] H. Patel H, M.A. Temple, B.W. Ramsey, Comparison of high-end and low-end receivers for RF-DNA fingerprinting. 2014 IEEE Military Communications Conference, pp 24-29 (2014).

[11] L. Peng L, A. Hu, J. Zhang, Y. Jiang, J. Yu, Y. Yan, Design of a hybrid RF fingerprint extraction and device classification scheme. IEEE Internet of Things Journal **6**(1), pp. 349-360 (2018).

[12] K. Sankhe, M .Belgiovine, F. Zhou F, L. Angioloni, F. Restuccia, S. D'Oro, T. Melodia, S. Ioannidis, K Chowdhury, No radio left behind: Radio fingerprinting through deep learning of physical-layer hardware impairments. IEEE Transactions on Cognitive Communications and Networking **6**(1), pp. 165-78 (2019).

[13] J. Lu, A. Hu, G. Li, and L. Peng, A robust RF fingerprinting approach using multisampling convolutional neural network. IEEE Internet of Things Journal **6** (4), 6786 - 6799 (2019).

[14] G. Li, J. Yu, Y, Xing, and A. Hu, Location-invariant physical layer identification approach for WiFi devices. IEEE Access textbf7, pp. 106974 - 106986 (2019).
[15] M. A. Turk and A. P. Pentland, "Face recognition using eigenfaces," Proceedings. 1991 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 1991, pp. 586-591, doi: 10.1109/CVPR.1991.139758.
[16] T. Hastie, R. Tibshirani, & J. Friedman, *The Elements of Statistical Learning: Data Mining, Inference, and Prediction*, vol. 2. New York: Springer (2009).
[17] S. Forestier, P. Bouysse, R. Quere, A. Mallet, J. . -M. Nebus and L. Lapierre, "Joint optimization of the power-added efficiency and the error-vector measurement of 20-GHz pHEMT amplifier through a new dynamic bias-control method," in IEEE Transactions on Microwave Theory and Techniques, vol. 52, no. 4, pp. 1132-1141, April 2004, doi: 10.1109/TMTT.2004.825745.
[18] Keysight Technologies, "Vector Signal Analysis Basics." Accessed: Jul. 06, 2023. [Online]. Available: https://www.keysight.com/us/en/assets/7018-02891/application-notes/5990-7451.pdf
[19] ETSI 3GPP, "Universal Mobile Telecommunications System (UMTS); Base Station (BS) conformance testing (FDD) 3GPP TS 25.141 version 8.14.0 Release 8." Accessed: Jul. 06, 2023. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/125100_125199/125141/08.14.00_60/ts_125141v081400p.pdf