Research Article

An Ensemble Learning Method for Wireless Multimedia Device Identification

Zhen Zhang,¹ Yibing Li,¹ Chao Wang,¹ Meiyu Wang,¹ Ya Tu,¹ and Jin Wang^{1,2}

¹College of Information and Communication Engineering, Harbin Engineering University, Harbin, 150001, China

²School of Computer & Communication Engineering, Changsha University of Science & Technology, Changsha 410114, China

Correspondence should be addressed to Jin Wang; jinwang@csust.edu.cn

Received 27 May 2018; Revised 9 August 2018; Accepted 27 September 2018; Published 15 October 2018

Guest Editor: Weizhi Meng

Copyright © 2018 Zhen Zhang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In the last decade, wireless multimedia device is widely used in many fields, which leads to efficiency improvement, reliability, security, and economic benefits in our daily life. However, with the rapid development of new technologies, the wireless multimedia data transmission security is confronted with a series of new threats and challenges. In physical layer, Radio Frequency Fingerprinting (RFF) is a unique characteristic of IoT devices themselves, which can difficultly be tampered. The wireless multimedia device identification via Radio Frequency Fingerprinting (RFF) extracted from radio signals is a physical-layer method for data transmission security. Just as people's unique fingerprinting, different Internet of Things (IoT) devices exhibit different RFF which can be used for identification and authentication. In this paper, a wireless multimedia device identification system based on Ensemble Learning is proposed. The key technologies such as signal detection, RFF extraction, and classification model are discussed. According to the theoretical modeling and experiment validation, the reliability and the differentiability of the RFFs are evaluated and the classification results are shown under the real wireless multimedia device environments.

1. Introduction

With the rapid development of the wireless multimedia technologies, the security of wireless multimedia data transmission becomes increasingly more and more important. The design of efficient identification and authentication algorithms among different wireless multimedia devices has become an urgent subject.

As is well known, the Internet of Things [1] and the wireless sensor network (WSN) [2–4] are important carriers of multimedia data transmission; they will lead to improved efficiency, reliability, security, and economic benefits in our daily life [5]. At the same time, wireless multimedia technology and application have been widely studied by the researchers all over the world [6, 7]. However, because of the opening of transmitting channels, compared with the traditional wired network, the wireless network is more vulnerable to large-scale malicious attacks. Now, many existing networks are unprotected against a lot of different malicious attacks [8–10]; meanwhile the security of them is confronted with a series of new threats and challenges [11–13]. Traditional

methods for protecting the security of wireless network are usually based on bit-level security protocol. However, there are usually loopholes in the actual wireless network security protocols [14]. For example, the IEEE 802.11 Wireless LAN's (WLAN) wired equivalent encryption protocol (WEP) is easily attacked by statistical analysis of [15]; although it has been upgraded to WPA and WPA2, its password can be restored, and there are still a variety of security problems [16]. The Radio Frequency Fingerprinting (RFF) is an inherent characteristic of wireless multimedia devices, which can hardly be tampered. In recent years, RFF extraction and identification methods for wireless multimedia devices have been widely studied [17–20].

The identification and authentication wireless multimedia device based on RFF is an important physical-layer method for wireless multimedia security [21–23], which has been widely used in intrusion detection [24], access control [25], wormhole detection [26], and cloning detection [27]. RFF is extracted from radio signals from wireless multimedia devices, which is a unique characteristic of wireless multimedia devices themselves and can difficultly be tampered. In

FIGURE 1: Wireless multimedia device identification process.

physical layer, RFF is just as people's unique fingerprinting; different wireless multimedia devices exhibit different RFF which can be used for identification and authentication. As is well known, RFF is derived hardware imperfection of wireless multimedia device, which can be observed and extracted. With the development of machine learning and the emergence of a large number of new technologies [28], new methods about RFF have been put forward continuously in recent years. Han J et al. [29] propose a physical-layer identification and authentication system for ultrahigh frequency (UHF) passive tags, which is called GenePrint. The classification accuracy of the passive tags is higher than 99.68 %. Furthermore, GenePrint can effectively defend against the replay attack. Huang G et al. [30] propose a novel Specific Emitter Identification (SEI) method based on nonlinear characteristics. The permutation entropy is calculated as the radio signal fingerprint for identifying the unique transmitter. Furthermore, the technology of bispectrum and stray parameter are used for the comparison with the new method, which indicates that the proposed method has a better performance in the classification of the wireless network cards. The PHY-based security based on Time Domain (TD) is also studied extensively in the recent years. Donald R et al. [31] demonstrate the performance of Dimensional Reduction Analysis (DRA) using discrete Gabor-Transform features, which are extracted from the Wi-Fi and WiMAX signals. Jia Y et al. [32] attempt to simultaneously find a low-rank representation matrix of original data and the optimal classifier parameter, which can be used to improve the performance of radiometric identification. Experiments indicate that the new method not only has a higher accurate classification and identification rate, but also has better robustness against noise.

In this paper, the structure of wireless multimedia device identification is proposed. Firstly, the main components of this structure are presented. Secondly, the key technologies such as signal collection, RFF generation, and classification model are discussed. Thirdly, according to the theoretical modeling and experiment validation, the differentiability of the RFFs is extracted. The classification result is shown under

the real wireless multimedia device environments. Finally, the advantages and disadvantages of the proposed algorithm and its future prospects are described.

2. General View

In physical layer, the classification and identification of wireless multimedia device include four entities, which are shown in Figure 1: Acquisition Signal Module: acquiring the radio signals from wireless multimedia devices; Burst Extraction Module: detecting and intercepting the start of the turn-on transient; Signal Analysis Module: obtaining identification-relevant information from the radio signals; Fingerprint Generation Module: reducing assist information and generating the RFF; Classifier Module: a classifier for comparing RFF and requesting the identification of the comparison results [33, 34]. Furthermore, in order to better verify the identification performance of wireless multimedia device under different signals to noise ratio (SNR), the Additive White Gaussian Noise (AWGN) module and the data condition module are used in the experiments.

2.1. Data Set Definitions. As shown in Figure 2, the signals in this paper are mainly collected by Agilent oscilloscope, and 10 wireless multimedia devices of the same model and manufacturer are used for this research. In order to dislodge the influence of channel environment, wireless multimedia devices and receiving devices are connected directly with a cable (that is to say, ignoring the influence of multipath, time delay, and clutter in signal transmission process).

The sampling rate of the receiver is 40 MHz; each of the turn-on transients contains 159901 sampling points. For obtaining the complete turn-on transients, the Variance Trajectory (VT) [35] algorithm and Bayesian Change Detection (BCD) [36] are used for transient point detection and interception. The original dataset contains 500 transients from 10 devices, each of which contain 50 samples. According to the ratio of 2:3, the 500 signals are divided into training samples and test samples. At the same time, in order to

FIGURE 2: Schematic diagram of the experimental devices.

FIGURE 3: Four-stage (five-level) dual-tree complex wavelet transform (DT-CWT).

compare the performance of identification system under different SNR, the AWGN generation module, in Figure 1, is used in this paper. The noise is added with the simulation software (the range of SNR is 0~35dB, and the step is 1 dB).

2.2. Signal Analysis

2.2.1. Time Domain RF-DNA Fingerprinting. For TD fingerprinting, Radio Frequency-Distinct Native Attribute (RF-DNA) can be generated by the instantaneous amplitude, frequency, and phase response of radio signal's subsequence [37]. The unique features are obtained by the standard deviation (δ), variance (δ^2), skewness (γ), and kurtosis (κ) from $N_R + 1$ subsequence of the original signal, where N_R represents the number of the subsequence. The statistics can be arranged as follows:

$$F_{R_i} = [\delta_{R_i}, \delta_{R_i}^2, \gamma_{R_i}, \kappa_{R_i}]_{1 \times 4} \quad (1)$$

Where $i = 1, 2, \dots, N_R + 1$. Then, F_{R_i} can be used to generate the final TD fingerprint:

$$F^C = [F_{R_1} \ F_{R_2} \ F_{R_3} \ \dots \ F_{R_{N_R+1}}]_{1 \times 4(N_R+1)} \quad (2)$$

Where C refers to the signal's instantaneous parameter, including $\{a(n)\}$, $\{\varphi(n)\}$ and $\{f(n)\}$.

2.2.2. Wavelet Domain (WD) RF-DNA Fingerprinting. For signal analysis, the Discrete Wavelet Transform (DWT) is a

very effective tool. But there are still some disadvantages. One distinct disadvantage of DWT is that it is not shift invariant. The DT-CWT is an improved method of DWT, which is used to overcome the disadvantage of DWT. The DT-CWT is commonly implemented by two real-valued filter banks, which is shown in Figure 3.

In Figure 3, the two filter banks represent two branches of Tree1 and Tree2, respectively, where the filter coefficients $h_1(t)$, $h_0(t)$, $h'_1(t)$, and $h'_0(t)$ are implemented directly as the Analysis Filters (AF) given in [38].

For real-valued input radio signals, the WD coefficients I_{WD}^L and Q_{WD}^L of Tree1 and Tree2 represent the real and imaginary components of complex coefficients [39]:

$$S_{WD}^L(n) = I_{WD}^L(n) + jQ_{WD}^L(n) \quad (3)$$

Then the WD fingerprints can be generated using the similar method [40] in Section 2.2.1.

2.3. Fingerprint Generation. The Robust Principle Component Analysis (RPCA) is an improved algorithm for traditional Principal Component Analysis (PCA). Because of the serious robustness problem of traditional PCA technology, the theoretical framework of RPCA was put forward to solve this problem.

Assuming that the observation matrix $\mathbf{D} = R^{(M \times N)}$ is originally a low-rank matrix $\mathbf{A} = R^{(M \times N)}$, it is polluted by matrix $\mathbf{E} = R^{(M \times N)}$ which has sparse distribution and

arbitrarily large amplitude. The RPCA tries to separate the low-rank part from the sparse part of the observation matrix $\mathbf{D}$ and obtains the low-rank distribution matrix $\mathbf{A}$ and the sparse distribution matrix $\mathbf{E}$, respectively. By increasing the constraints of low rank and sparsity of matrix $\mathbf{A}$ and matrix $\mathbf{E}$, the sparse matrices can be computed by calculating the following convex optimization [41, 42]:

$$\begin{aligned} \min_{\mathbf{A}, \mathbf{E}} \quad & \|\mathbf{A}\| + \lambda \|\mathbf{E}\| \\ \text{s.t.} \quad & \mathbf{D} = \mathbf{A} + \mathbf{E} \end{aligned} \quad (4)$$

Where $\|\cdot\|_*$ is the kernel norm of matrix; it can also be understood as the sum of singular values in a matrix. $\lambda > 0$ is the tuning parameter [43] to balance the low-rank matrix and the sparse matrix.

In order to verify the performance, the dataset in Section 2.1 is used for simulation and evaluation. The dimensions are decreased based on RPCA analysis method. According to the contribution rate of main components, the first two principal components are selected for visualization.

3. Designed Classifier

3.1. Adaboost Algorithm. Adaboost algorithm is an iterative algorithm. It does not need to know the prior knowledge of weak classifiers. Instead, it changes the distribution of data and combines weak classifiers to achieve classification. This method has achieved good results in practical applications.

The specific description of the Adaboost algorithm is as follows.

Input: N labeled training samples $\{(1, c(1)), \dots, (N, c(N))\}$, where $1, \dots, N$ are serial numbers; $c(N)$ characterizes the different sample categories with a range of $(0, 1)$; the training sample has a D distribution space and uses a weak learning algorithm; the number of iterations is set to T .

Initialization: if the sample $y_i = 0$, then make $w_{1,i} = 1/2m$; if the sample $y_i = 1$, then $w_{1,i} = 1/2l$;

Execution: the number of iterations is T , and each iteration performs the following steps.

(1) Normalized weights:

$$\frac{w_{t,i}}{\sum_{j=1}^n w_{t,j}} \rightarrow w_{t,i} \quad (5)$$

(2) Calculate the current error of weight:

$$\varepsilon_j = \sum_i w_{t,j} |h_j(x_i) - y_i| \quad (6)$$

Among them, h_j is a weak classifier generated by the feature j .

(3) Screening: the screening process is to add the smallest weak classifier in the previous step to the strong classifier we need.

(4) Update: regenerate each weight:

$$w_{t+1,i} = w_{t,i} \beta_t^{1-e_i} \quad (7)$$

Where $\beta_t = \varepsilon_t / (1 - \varepsilon_t)$, and if the i^{th} sample x_i is correctly classified, then $e_i = 0$; otherwise $e_i = 1$.

FIGURE 4: Schematic diagram of GBDT algorithm.

FIGURE 5: Binary classification.

(5) The resulting strong classifier is

$$h_j(x) = \begin{cases} 1, & \sum_{t=1}^r a_t h_t(x) \geq \frac{1}{2} \sum_{t=1}^r \alpha_t \\ 0, & \text{else} \end{cases} \quad (8)$$

In the above formula, $\alpha_i = \log(1/\beta_i)$.

3.2. Gradient Boosting Decision Tree. Gradient Boosting Decision Tree (GBDT) is a combination of decision tree and Boosting method. It is also one of the integrated learning Boosting algorithms [44]. In the GBDT algorithm, the decision tree training object is not a tree but an error in the classification of the previous decision tree. This is the Boosting concept. The principle of the gradient-based decision tree algorithm is shown in Figure 4.

As can be seen from Figure 4, GBDT is a kind of linear training, so it cannot be trained in parallel. In training, the difference between the training and the actual value is the target of the second tree optimization, as shown in formula T_2 :

$$T = T_1 + T_2 + T_3 \quad (9)$$

From the idea of the algorithm shown in Figure 4, we can see that there is a difference between GBDT and traditional boosting. That is, the GBDT iteration is the residual or gradient descent value, and boosting is the sample data. Figure 5 is an example of using GBDT for binary classification.

The node R , which is about to be divided into two categories, can get μ on an average of several different y , and then use it as the output value of the node, as shown in equation ((3)-(4)):

$$\mu = \frac{\sum_{i=1}^n y_i}{n} \quad (10)$$

From this, the resulting optimization goal is the node error, which is shown in Equation ((3)-(5)):

$$\text{Error} = \sum (y_i - \mu)^2 \quad (11)$$

FIGURE 6: The energy ratio of original feature curves changing with dimensions. (a) Time domain RF-DNA fingerprinting. (b) Wavelet domain RF-DNA fingerprinting.

In the process of binary classification of decision trees, the criteria for classification are to select the attribute that maximizes the classification gain, and the calculation method for split gain is as follows:

$$G = S - S_j \quad (12)$$

In the above equation, to obtain the S_j , the loss function can be replaced by a variance, as follows:

$$S_j = \sum_{m \in L} (y_m - \mu_L)^2 + \sum_{n \in R} (y_n - \mu_R)^2 \quad (13)$$

After S_j is obtained, S and S_j are sequentially expanded, respectively, as in equation (12); then the split gain G can be obtained:

$$G = \left(\frac{Sum_L^2}{\|L\|} + \frac{Sum_R^2}{\|R\|} \right) - \frac{Sum^2}{\|Total\|} \quad (14)$$

In the above equations, Sum_L^2 and Sum_R^2 represent the square sum of samples on the left and right subtrees, while Sum^2 is used to represent the sum of the squares of all the samples. Therefore, to make the classification work best, G gets the maximum in each iteration. It should be noted that, in the GBDT algorithm, the purpose of each decision tree training is to optimize the residual of the previous item.

4. Simulation Result

4.1. Dimension Reduction Algorithm. In general, the features extracted by the feature extraction method have certain redundancy and noise. If the identification is performed

TABLE 1: The relationship between the energy ratio and the dimensionality reduction.

Energy ratio	85%	90%	95%
TD	-	-	3
WAV	6	13	24

directly, it will not only increase the computational complexity of the subsequent process and the requirements for computer memory, but also affect the final classification identification effect. Therefore, it is necessary to reduce the dimensionality of original feature set. Section 2.3 introduces the dimensionality reduction algorithms for PCA and RPCA, where RPCA is an improved algorithm for PCA. In Figure 6, when SNR=20dB, the energy ratio curves of the time domain and wavelet domain characteristics were obtained by using PCA and RPCA methods, respectively.

The energy ratio refers to the ratio of feature vector information after dimension reduction to the feature vector information without dimension reduction. It can be seen from Figure 6 that RPCA has a better dimensionality reduction effect. Under these two feature extraction methods, a higher proportion of energy can be achieved in the same dimension. Considering these advantages of RPCA, the RPCA method is chosen in this paper to reduce the original features.

Table 1 shows the reduced dimension of several typical energy ratios in the use of time and wavelet domain feature extraction methods and the use of RPCA.

4.2. Classification and Identification. Experiments mainly selected the two ensemble learning classifiers described in

FIGURE 7: The identification rate of the authorized devices with 3-dimensional features based on (TD) RF-DNA fingerprint.

Section 3, Adaboost and GBDT. In order to verify the performance of classifier, k-Nearest Neighbor (KNN) and Grey relational analysis (GRA) classifier are used for comparison. The ensemble classifier depth is 5, learning rate is 0.3, and number is 50. Before classification and identification, it is necessary to determine the specific feature dimensions. According to the results in Table 1, we selected the dimensions corresponding to the energy proportions of 85%, 90%, and 95% compared with the original features, respectively. Among them, for the time domain feature set, since the energy proportion has exceeded 95% when it falls to three dimensions, the experiment is selected in 3 dimensions; for the feature set of the wavelet domain, 6, 13, 24, and 200 dimensional features are selected for testing.

From Figure 7, in the range of 0~35dB SNR, the identification rate increases with SNR. The four classifiers have the same performance; meanwhile the identification rate of different signals is basically stable at 10 dB; the identification rate is up to 95% in this condition.

We can obtain the same results as above for the classification and identification results of wavelet domain RF-DNA Fingerprinting in high SNR in Figure 8. However, the performance of time domain RF-DNA Fingerprinting is better in low SNR. Meanwhile, the performance of GBDT and Adaboost can achieve a higher identification rate compared with KNN and GRA, especially when the dimension of feature is high. At the same time, compared with the experimental results in Figure 7, it can be seen that time domain RF-DNA fingerprint features have better performance at low SNR. This is mainly because the data set in this paper is formed by the turn-on transient signal of wireless devices. It has a distinct envelope feature, and the time domain RF-DNA fingerprint is mainly based on the instantaneous amplitude phase and frequency characteristics, so it is easier to distinguish different devices. In order to verify the effect

of dimension reduction after RPCA dimension reduction on overall identification rate, this article compares the overall identification rate of signals in the range of 0~35dB SNR in different dimensions, as shown in Figure 9.

As can be seen from Figure 9, with the increase of feature dimensions, the average identification rate of the signal shows a trend of increasing first and then decreasing. This is because when the input dimension is too low, the information carried by the feature is too small, and when the input dimension is too high, although there is more comprehensive original feature information, it will also increase noise and redundancy, which will lead to a reduction of identification rate.

5. Conclusion

With the popularity and development of wireless networks, the security of wireless networks has gradually become a research hotspot. Radio frequency fingerprinting technology is a kind of wireless network security technology based on the characteristics of physical layer. It can be used for the identification of most existing wireless multimedia devices, and it has a wide range of application scenarios. RF-DNA Fingerprinting technology is a brand-new RF Fingerprinting method developed in recent years, and it has good device classification identification effect. This paper proposes an RF-DNA Fingerprinting system based on ensemble learning and uses the RF-DNA Fingerprint feature based on time domain and wavelet domain to verify the classification and identification performance. In order to reduce the computational overhead and redundant information of the original features, in this paper, RPCA is introduced to reduce the dimensionality of original features. The experimental results show that it has good classification and identification performance. When the SNR is greater than 10 dB, the GBDT classifier is used to

FIGURE 8: The identification rate of authorized devices under different dimensions. (a) 6-dimensional features, (b) 13-dimensional features, (c) 24-dimensional features, (d) 200-dimensional features.

FIGURE 9: The identification results of four classifiers with SNR = 0 dB~20dB.

classify the RF-DNA features in the time domain and wavelet domain, and the identification rate can reach over 95%, which can realize the effective identification of different equipment types.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

- [1] S. Li, L. D. Xu, and S. Zhao, "The internet of things: a survey," *Information Systems Frontiers*, vol. 17, no. 2, pp. 243–259, 2015.
- [2] F. Yunus, N. N. Ismail, S. H. Ariffin, A. A. Shahidan, N. Fisal, and S. K. Syed-Yusof, "Proposed transport protocol for reliable data transfer in wireless sensor network (WSN)," in *Proceedings of the 2011 Fourth International Conference on Modeling, Simulation and Applied Optimization (ICMSAO)*, pp. 1–7, Kuala Lumpur, Malaysia, April 2011.
- [3] J. Wang, J. Cao, R. S. Sherratt, and J. H. Park, "An improved ant colony optimization-based approach with mobile sink for wireless sensor networks," *The Journal of Supercomputing*, pp. 1–13, 2017.
- [4] J. Wang, J. Cao, S. Ji, and J. H. Park, "Energy-efficient cluster-based dynamic routes adjustment approach for wireless sensor networks with mobile sinks," *The Journal of Supercomputing*, vol. 73, no. 7, pp. 3277–3290, 2017.
- [5] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," *Business Horizons*, vol. 58, no. 4, pp. 431–440, 2015.
- [6] Z. Pan, J. Lei, Y. Zhang, and F. L. Wang, "Adaptive fractional-Pixel motion estimation skipped algorithm for efficient HEVC motion estimation," *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, vol. 14, no. 1, pp. 1–19, 2018.
- [7] J. Han, R. Quan, D. Zhang, and F. Nie, "Robust object co-segmentation using background prior," *IEEE Transactions on Image Processing*, vol. 27, no. 4, pp. 1639–1651, 2018.
- [8] H. Wu and W. Wang, "A Game Theory Based Collaborative Security Detection Method for Internet of Things Systems," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 6, pp. 1432–1445, 2018.
- [9] X. Cao, D. M. Shila, Y. Cheng, Z. Yang, Y. Zhou, and J. Chen, "Ghost-in-ZigBee: Energy Depletion Attack on ZigBee-Based Wireless Networks," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 816–829, 2016.
- [10] E. Y. Vasserman and N. Hopper, "Vampire attacks: Draining life from wireless ad Hoc sensor networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 2, pp. 318–332, 2013.
- [11] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.
- [12] A. Mpitiopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 4, pp. 42–56, 2009.
- [13] Y. Liu, M. Dong, K. Ota, and A. Liu, "ActiveTrust: secure and trustable routing in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 2013–2027, 2016.
- [14] D. Macedonio and M. Merro, "A Semantic Analysis of Wireless Network Security Protocols," in *NASA Formal Methods*, vol. 7226 of *Lecture Notes in Computer Science*, pp. 403–417, Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.
- [15] R. Chaabouni, "Break WEP Faster with Statistical Analysis," *Break WEP Faster with Statistical Analysis*, 2006.
- [16] I. P. Mavridis, A.-I. E. Androulakis, A. B. Halkias, and P. Mylonas, "Real-life paradigms of wireless network security attacks," in *Proceedings of the 15th Panhellenic Conference on Informatics, PCI 2011*, pp. 112–116, Greece, October 2011.
- [17] G. Baldini, G. Steri, and R. Giuliani, "Identification of Wireless Devices From Their Physical Layer Radio-Frequency Fingerprints," 2018.
- [18] A. Mahmood and M. A. Jensen, "Data-dependent transmitter fingerprints for radio authentication," in *Proceedings of the 2014 IEEE Radio and Wireless Symposium, RWS 2014*, pp. 265–267, USA, January 2014.
- [19] T. J. Bihl, K. W. Bauer, and M. A. Temple, "Feature selection for RF fingerprinting with multiple discriminant analysis and using ZigBee device emissions," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1862–1874, 2016.
- [20] J. Lopez, N. C. Liefer, C. R. Busho, and M. A. Temple, "Enhancing Critical Infrastructure and Key Resources (CIKR) Level-0 Physical Process Security Using Field Device Distinct Native Attribute Features," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 5, pp. 1215–1229, 2018.
- [21] B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices," *ACM Computing Surveys*, vol. 45, no. 1, article 6, 2012.
- [22] O. Gungor and C. E. Koksak, "On the basic limits of RF-fingerprint-based authentication," *Institute of Electrical and Electronics Engineers Transactions on Information Theory*, vol. 62, no. 8, pp. 4523–4543, 2016.
- [23] W. Wang, Z. Sun, S. Piao, B. Zhu, and K. Ren, "Wireless physical-layer identification: modeling and validation," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 2091–2106, 2016.
- [24] J. Hall, M. Barbeau, and E. Kranakis, "Enhancing intrusion detection in wireless networks using radio frequency fingerprinting," in *Proceedings of the Third IASTED International Conference on Communications, Internet, and Information Technology*, pp. 201–206, USA, November 2004.
- [25] O. Ureten and N. Serinken, "Wireless security through RF fingerprinting," *Canadian Journal of Electrical and Computer Engineering*, vol. 32, no. 1, pp. 27–33, 2007.
- [26] K. B. Rasmussen and S. Capkun, "Implications of radio fingerprinting on the security of sensor networks," in *Proceedings of the Security and Privacy in Communications Networks and the Workshops (SecureComm)*, 2007.
- [27] B. Danev, T. S. Heydt-Benjamin, and S. Capkun, "Physical-layer identification of RFID devices," in *Usenix Security Symposium*, pp. 199–214, Montreal, Canada, 2009.
- [28] Y. Zheng, B. Jeon, L. Sun, J. Zhang, and H. Zhang, "Student's t-Hidden Markov Model for Unsupervised Learning Using Localized Feature Selection," *IEEE Transactions on Circuits & Systems for Video Technology*, no. 99, p. 1, 2017.

- [29] J. Han, C. Qian, P. Yang et al., "GenePrint: generic and accurate physical-layer identification for UHF RFID tags," *IEEE/ACM Transactions on Networking*, no. 99, p. 1, 2015.
- [30] T. Anderson, L. Peterson, S. Shenker, and J. Turner, "Overcoming the internet impasse through virtualization," *The Computer Journal*, vol. 38, no. 4, pp. 34–41, 2005.
- [31] D. R. Reising, M. A. Temple, and J. A. Jackson, "Authorized and Rogue Device Discrimination Using Dimensionally Reduced RF-DNA Fingerprints," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 6, pp. 1180–1192, 2015.
- [32] Y. Jia, J. H. Ma, and L. Gan, "Radiometric Identification Based on Low-Rank Representation and Minimum Prediction Error Regularization," *IEEE Communications Letters*, vol. 21, no. 8, pp. 1847–1850, 2017.
- [33] H. J. Patel, M. A. Temple, and R. O. Baldwin, "Improving ZigBee device network authentication using ensemble decision tree classifiers with radio frequency distinct native attribute fingerprinting," *IEEE Transactions on Reliability*, vol. 64, no. 1, pp. 221–233, 2015.
- [34] R. Klein, M. A. Temple, M. J. Mendenhall, and D. R. Reising, "Sensitivity Analysis of Burst Detection and RF Fingerprinting Classification Performance," in *Proceedings of the ICC 2009 - 2009 IEEE International Conference on Communications*, pp. 1–5, Dresden, Germany, June 2009.
- [35] W. C. Suski II, M. A. Temple, M. J. Mendenhall, and R. F. Mills, "Using spectral fingerprints to improve wireless network security," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '08)*, pp. 2185–2189, December 2008.
- [36] O. Ureten and N. Serinken, "Bayesian detection of Wi-Fi transmitter RF fingerprints," *IEEE Electronics Letters*, vol. 41, no. 6, pp. 373–374, 2005.
- [37] D. R. Reising, M. A. Temple, and M. E. Oxley, "Gabor-based RF-DNA fingerprinting for classifying 802.16e WiMAX mobile subscribers," in *Proceedings of the 2012 International Conference on Computing, Networking and Communications, ICNC'12*, pp. 7–13, USA, February 2012.
- [38] D. Sun and X. P. University, "Application of Wavelet Transform on Speech Signal Noise Reduction," *Information & Communications*, 2017.
- [39] I. W. Selesnick, R. G. Baraniuk, and N. G. Kingsbury, "The dual-tree complex wavelet transform," *IEEE Signal Processing Magazine*, vol. 22, no. 6, pp. 123–151, 2005.
- [40] R. W. Klein, M. A. Temple, and M. J. Mendenhall, "Application of wavelet-based RF fingerprinting to enhance wireless network security," *Journal of Communications and Networks*, vol. 11, no. 6, pp. 544–555, 2009.
- [41] H. L. Van Trees and K. L. Bell, *Bayesian Bounds for Parameter Estimation and Nonlinear Filtering/Tracking*, IEEE, 2007.
- [42] Y. Lin, X. Zhu, Z. Zheng, Z. Dou, and R. Zhou, "The individual identification method of wireless device based on dimensionality reduction and machine learning," *The Journal of Supercomputing*, pp. 1–18, 2017.
- [43] C. Lu, J. Feng, Y. Chen, W. Liu, Z. Lin, and S. Yan, "Tensor Robust Principal Component Analysis: Exact Recovery of Corrupted Low-Rank Tensors via Convex Optimization," in *Proceedings of the 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 5249–5257, Las Vegas, NV, USA, June 2016.
- [44] I. Omerhodzic, S. Avdakovic, A. Nuhanovic, and K. Dizdarevic, "Energy distribution of EEG signals: EEG signal wavelet-neural network classifier," *World Academy of Science, Engineering and Technology*, vol. 37, pp. 1240–1245, 2010.