Radio Frequency Fingerprinting-Based Device Identification Using Deep Metric Learning

Dinh Tuan Anh*, Bui Tung Lam†
These authors contributed equally
Pham An Duy‡, Pham Minh Tuan*, Tran Vinh Co*, Nguyen Huu Tinh*, Huynh Cong Bang*§
* Industrial University of Hochiminh City, Vietnam
† Le Hong Phong High School for The Gifted
‡ University of Wollongong, Australia

***Abstract*—Wireless telecommunications networks are growing rapidly, and at the same time, there are increasing concerns about privacy and data security. In this context, Radio Frequency Fingerprinting (RFF) has emerged as a potential security solution at the physical layer, especially in the identification of IoT devices. RFF helps identify electronic devices based on the unique characteristics of the radio signals emitted by each device. In this study, we leverage advanced machine learning techniques, including metric learning and deep neural networks, to enhance the efficiency of mobile device identification and authentication. The identification problem is divided into two main tasks: Identifying known devices and detecting unfamiliar or unknown devices, thereby ensuring the security of wireless networks in protected areas. By combining deep neural networks with metric learning, we achieve high accuracy and effective performance in open-set recognition. This approach not only improves identification accuracy but also adds an extra layer of security against potential threats in wireless networks.**

***Index Terms*—Radio Frequency Fingerprinting, Signal Processing, RiftNet, OpenSet Problem, Metric Learning.**

I. Introduction

Nowadays, with the rapid development of telecommunication networks, network system security has become one of the major concerns, especially in protecting user privacy. Radio Frequency Fingerprint (RFF) is an emerging technology used to identify devices by analyzing the unique characteristics of the signals they transmit. This process, also known as SEI (Secure Entity Identification), involves distinguishing individual transmitting devices by comparing their RFF with the received signals [1] [2]. This method has attracted particular attention in the IoT field, where accurate device identification is important for security and management [3] [4].

RFF is derived from the hardware features inherent in different devices, allowing for efficient device identification [3]. The identification process typically involves three main steps: Feature identification, feature extraction, and device classification [5]. By collecting and processing radio signals from devices, RFF identification systems can learn and store the immutable hardware-based characteristics of each transmitter, thereby facilitating reliable authentication [6] [7].

§ Corresponding author: Huynh Cong Bang

A distinct advantage of radio frequency fingerprinting (RFF) techniques is their ability to achieve high accuracy. Furthermore, RFF identification protocols allow the device to transmit signals as usual, while the wireless waveforms are analyzed to identify a unique fingerprint [8]. This capability enhances network security by providing a robust authentication method at the physical layer, in contrast to traditional identification methods that are more susceptible to spoofing and attacks [9].

One notable advancement in this field is the use of deep neural networks such as RiftNet, which effectively capture pattern features in radio signals for accurate device identification [10]. In the original study, RiftNet was proposed to classify wireless signals such as Wi-Fi and ADS-B, focusing solely on the closed-set classification problem without addressing the challenge of identifying previously unseen or unknown devices.

In this research, we leverage machine learning and deep learning models to identify devices, and the results show remarkable effectiveness. In particular, the RiftNet model achieves the best results, with high accuracy and stability in distinguishing devices. Besides, we further extend the original RiftNet by combining it with metric learning to not only classify known devices but also detect previously unseen ones. Our approach addresses both closed-set and open-set identification problems, thereby demonstrating the great potential of this field.

II. Related Works

A. Transient Detection in Radio Signal

The radio signal is comprised of three main states: Noise, transient, and steady state, as shown in Figure 1. The signal of each device will have unique characteristics due to many differences in design and the randomness of the transmitter. The transition phase exhibits the most variation in wave energy, oscillation, and duration before entering the steady-state phase. Properly detecting and extracting features from the transient state is very important, as it can significantly affect the accuracy of machine learning classification algorithms. Two common transient detection methods that are widely used are Bayesian change point detection and Phase-Based detection [11]. The Bayesian change point detection method is based on

979-8-3315-7206-8/25/$31.00

the change of fractal (fractal dimension), which was calculated by the Higuchi method. The fractal dimension of the noisy part is higher than the transient part, so the starting point of the transient signal is determined at the highest statistical change. Besides, Phased-Based detection relies on the linear phase variation characteristic during the transition period. The Hilbert transform was used to extract the instantaneous phase and analyze the phase shift based on the window time, and then the characteristic phase region of the transient can be identified. After detecting the transient signal, we can easily separate the steady signal part.

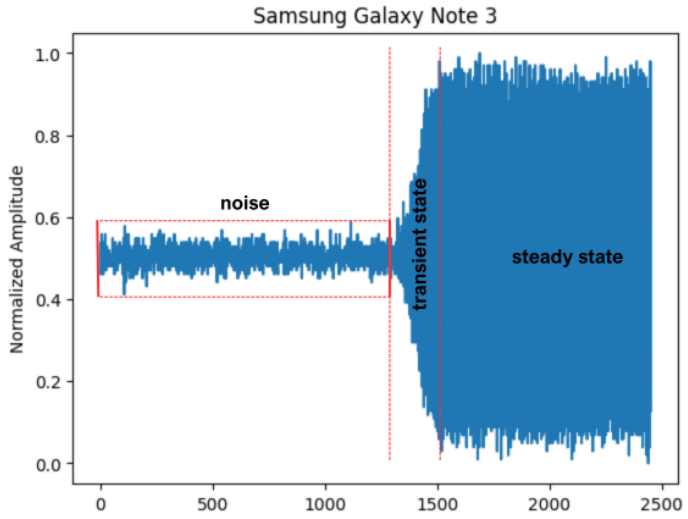

Fig. 1. Components of a radio signal

B. Signal Recognition with Machine Learning and Deep Learning

Authenticating a user in a wireless environment is challenging due to the many different factors involved, and the most reliable way to authenticate is to analyze the signals emitted by the devices. Some machine learning approaches, such as support vector machines (SVM), k-nearest neighbor (KNN), and multiple discriminant analysis (MDA), utilize statistical features extracted from the transient phase and steady phase to classify users [12]. This approach requires the transient detection technique to be very exact to separate the transient and steady state accurately.

On the other hand, a deep learning approach such as RiftNet takes the whole signal as input and tries to learn the signal pattern to classify it [10]. This approach is especially convenient because it does not require us to detect the transient properly, less complicated.

However, the original RiftNet model has not been explored in the context of identifying previously unseen or unknown devices. This remains a crucial challenge in real-world scenarios where new devices can dynamically join the network. Addressing this open-set recognition problem is essential for improving the robustness and practical applicability of RFF-based identification systems.

III. Method

A. RFF with Machine Learning

No.	Feature Name	Feature Group
1	Duration of the transient signal	Transient Signal
2	Total energy of the transient signal	
3	Standard deviation of the instantaneous phase of the transient signal	
4	Entropy of the instantaneous phase of the transient signal	
5	Total energy of the transient signal envelope	Envelope
6	Variance of the transient signal envelope	
7	Length of the transition energy distribution	TFED-Time
8	Slope of the transition energy distribution	
9	Variance of the total transition energy distribution	
10	Maximum value of the total transition energy distribution	
11	Cubic coefficient in the polynomial approximation of the total transition energy distribution	
12	Maximum value of the total transition energy distribution	TFED-Frequency
13	Variance of the total transition energy distribution	

TABLE I
TFED FEATURES EXTRACTED FROM THE SIGNAL

1) Utilize TFED characteristics of Signal: TFED (Time-Frequency Energy Distribution) utilizes the Hilbert-Huang transform to analyze the signal in the frequency and time domains to extract the characteristic energy distribution of transient components. The difference in the transient characteristics of signals of different devices was mined to extract input features. These features, which fall into groups such as Transient Signal, Envelope, TFED-Time, and TFED-Frequency, are detailed in Table I.

However, the most challenging aspect of this method is extracting the features manually. This process relies heavily on detecting transients of the signal accurately, and this is not easy in practice, especially when a low sampling frequency results in very few data points in the transient can lead to missing important information.

2) Utilize Instantaneous Phase Characteristics of Signal: RF Fingerprinting based on the transient signal utilizes a high level of statistical features, including skewness, kurtosis, and variance were extracted from three instantaneous components of the signal: Instantaneous amplitude, instantaneous frequency, and instantaneous phase. These features reflect the asymmetry, sharpness, and dispersion, which are directly affected by micro-hardware distortions during the broadcast, creating unique identification marks for each device.

B. RFF with RiftNet

Deep learning has shown its potential with recent advances and various amazing results. In the RF Fingerprinting field, the RiftNet model, which was proposed by J Robinson and his colleagues, has shown that deep learning can perform well and point out its potential [10]. RiftNet consists of two main branches: The left branch (A) and the right branch (B), as shown in Figure 2. The left branch processes the long

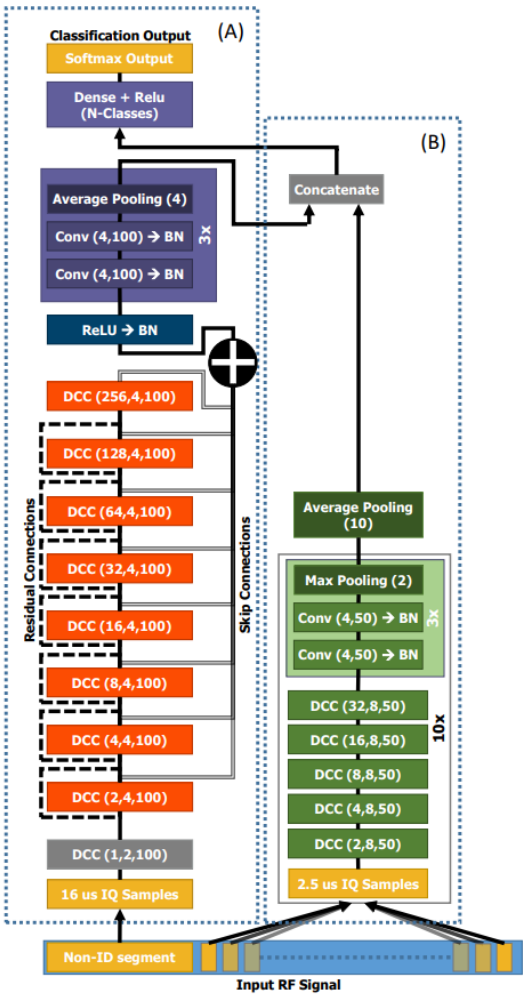

Fig. 2. RiftNet architecture. *We get this figure from: RiftNet: Radio Frequency Classification for Large Populations, Josh Robinson, Scott Kuzdeba, BAE Systems.*

input signal $16\,\mu s$, while the right branch processes shorter input signals, only $2.5\,\mu s$. Two branches utilize DCC (Dilated Convolutional Cells) blocks with different dilated ratios to extract information at different times, which helps the model learn the RF signal pattern better. The intermediate results are combined through skip connections and then fed into the classification layer.

C. Metric Learning and Open Set Problem

While closed-set RF fingerprint requires the model to classify exactly the class of the device that is known in the training set, open-set recognition poses a new difficult challenge: The System not only must recognize known devices but also recognize unknown devices that it has never seen before. This is an important demand for security systems or radio spectrum monitoring, where a new or fake device that has not been registered could be detected.

To address this, we extend RiftNet by removing the softmax classification layer and applying metric learning. Instead of training the model to predict specific classes, we train it to learn a latent space where samples of the same class are pulled closer together, and samples of different classes are pushed apart. This enables the model to capture deeper patterns independent of fixed classes.

Specifically, after training, the softmax layer is removed and the model is used as a feature extractor, generating 128-dimensional latent vectors from the training set. To simulate an open-set scenario, three classes are excluded from training and only appear in testing as unknown devices. The latent vectors are then stored on the vector database FAISS (Facebook AI Similarity Search) [13]. For recognition, we leverage discriminative methods for open-set recognition [14], which focus on decision boundaries between known classes and identify unknown classes by assigning low confidence or using a threshold. When encountering a new device, the system determines it as unknown based on its distance to known devices in the latent space.

IV. Experiment

Brand	Device Model
LG	G4
Xiaomi	Mi 6
Samsung	S3
Samsung	J7
Samsung	Note 2
Samsung	Note 3
Apple	iPhone 4s
Apple	iPhone 5
Apple	iPhone 5s
Apple	iPhone 6
Apple	iPhone 6s
Apple	iPhone 7
Apple	iPhone 7 Plus

TABLE II
List of Bluetooth devices in the 250 Msps dataset

In this research, we leverage the Bluetooth dataset in the work of Emre Uzundurukan et al. [12]. This dataset was recorded from Bluetooth signals with a sampling rate of 250 Msps from mobile phone devices of 5 branches. Each device accounted for 150 samples, which created 1950 records in total from 33 different devices. This dataset was used for the research and development of the RFF methodology for Bluetooth devices. Notably, the original study used machine learning to classify devices by brand, not individual devices. It also did not consider identifying new, unseen devices, which is important for real applications. The dataset was split into two portions: 80% for the train set and 20% for the test set.

1) RFF with Machine Learning: We used some common and popular classification machine learning models to identify users, such as Support Vector Machine (SVM), Linear Discriminant Analysis (LDA), Decision Tree, Random Forest, XGBoost, CatBoost, and Gradient Boosting. We implement them by using library `scikit-learn`, `XGBoost`, and `CatBoost` with default hyperparameters to ensure objectivity in comparison. The training and testing were performed on the same dataset for the unified.

2) RFF with RiftNet: In this experiment, we trained the RiftNet model in 100 epochs. The optimization algorithm used is `Adam` with a learning rate is 1e-4. The loss function chosen is `cross-entropy`, which is suitable for classification problems.

3) Metric Learning and Open Set Problem: After training RiftNet, we removed the softmax classification layer and applied metric learning with contrastive loss, training the model for an additional 20 epochs. We then extracted latent vectors of known users and indexed them using FAISS for querying and evaluation. A threshold of 1.0 on the Euclidean distance in the embedding space was set to distinguish known from unknown users.

V. Result

Model	Training Set Accuracy	Test Set Accuracy
Support Vector Machine	67.42%	42.22%

TABLE III
PERFORMANCE TABLE OF MACHINE LEARNING MODELS USING THE INSTANTANEOUS PHASE FEATURES OF THE SIGNAL

Model	Training Set Accuracy	Test Set Accuracy
Linear Discriminant Analysis	73.64%	72.93%
Decision Tree	100%	56.57%
Random Forest	100%	69.19%
XGBoost	100%	70.61%
CatBoost Tree	99.12%	72.12%
Gradient Boosting	99.55%	65.35%

TABLE IV
PERFORMANCE TABLE OF MACHINE LEARNING MODELS USING THE TFED FEATURES OF THE SIGNAL

1) RFF with Machine Learning: The tables III and IV have shown that machine learning models have reached absolute results in the trainset but significant degradation on the test set. This reflects overfitting-when the model memorizes the training data but does not generalize well to new data. One important reason is the difficulty in extracting features from the transient state, especially in determining exactly *endpoint*, which leads to noisy features and decreases classification performance. This also pointed out that manual features like instantaneous phase or TFED are not enough for complex signal situations, and switching to a deep learning model like RiftNet is necessary to extract hidden information in the radio signal.

2) RFF with RiftNet: The RiftNet training result shows that the model converges quickly and stably, with the loss function dropping quickly in a few beginning epochs and slowly stable (Figure 3), reflecting the ability of efficient learning of signal feature in the beginning.

Classification performance on trainset (Figure 4) and testset (Figure 5) has gradually increased through epochs, reflecting the learning ability of deep learning and generalization of the model. The best result has been reached at **epoch 96**, with accuracy on the trainset reached **99.4%** and test set reached **96.57%**.

However, performance on the test set has a slight fluctuation between epochs. The reason is test set is quite small and not diverse, which has led to the model being influenced by data distribution shift.

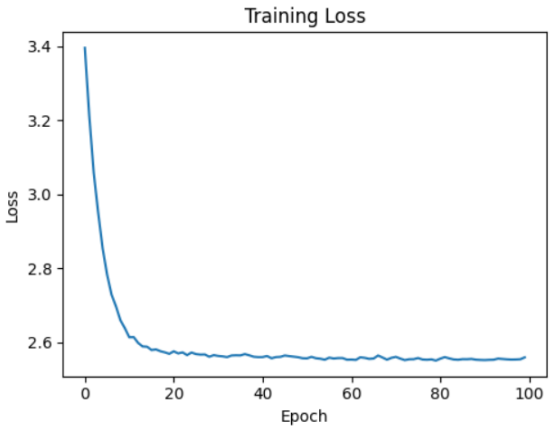

Fig. 3. Loss function over training epochs of RiftNet

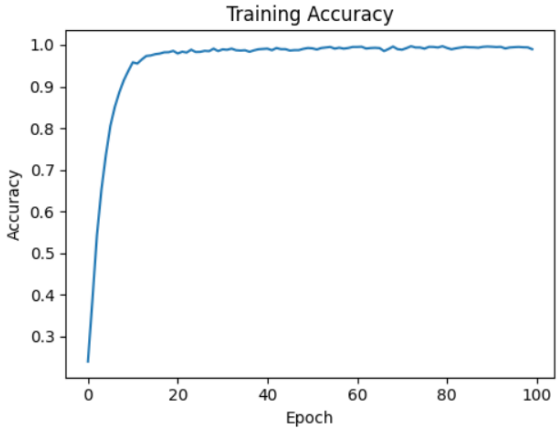

Fig. 4. Training accuracy over epochs of RiftNet

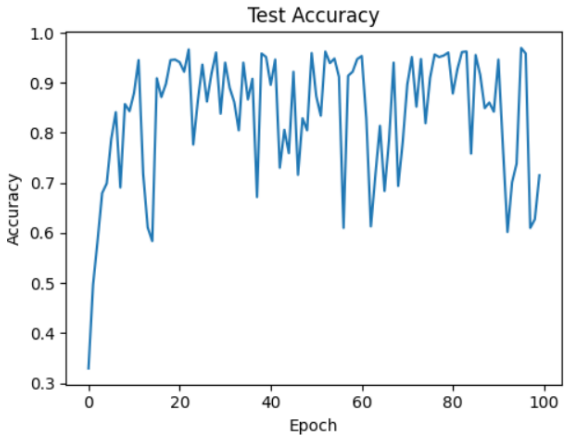

Fig. 5. Test accuracy over epochs of RiftNet

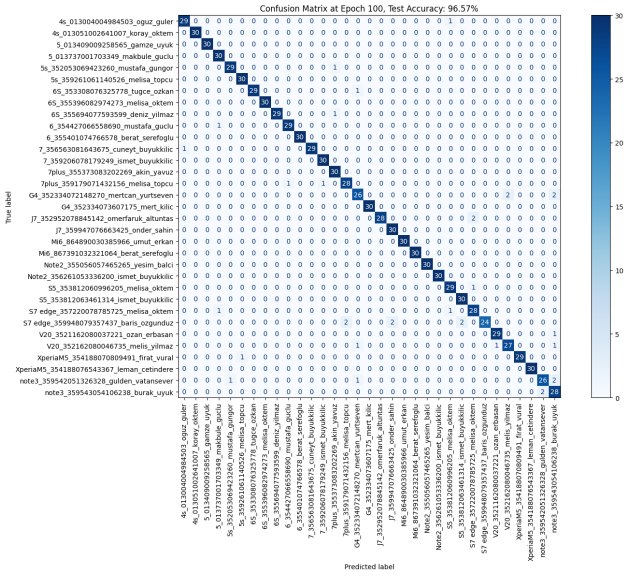

Fig. 6. Confusion matrix on the test set of the best RiftNet model

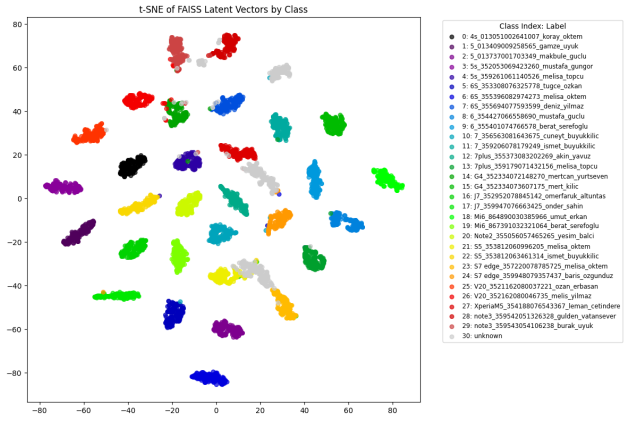

Fig. 7. t-SNE visualization of the feature vectors in FAISS.

3) Metric Learning and Open Set Problem: After applying metric learning, the latent space shows clear clusters corresponding to known users, as illustrated in Figure 7. Specifically, devices belonging to the same class are grouped into neat clusters and clearly separated from other classes. This cluster structure emphasizes the discriminative ability of the extended RiftNet model and shows that previously unseen devices are easily identified as outliers in the latent space.

The model is further tested on a mixed test set consisting of both known and unknown devices. As illustrated in Figure 8, the confusion matrix exhibits a clear cross-sectional pattern, indicating high and stable prediction accuracy for known classes. Some misclassifications mainly occur in the "unknown" class, which is expected in challenging open-set scenarios. Overall, with a threshold of 1.0, the system achieves **97.05%** accuracy in distinguishing between known and unknown users.

This result demonstrates the strong generalization ability and high potential of RiftNet combined with metric learning

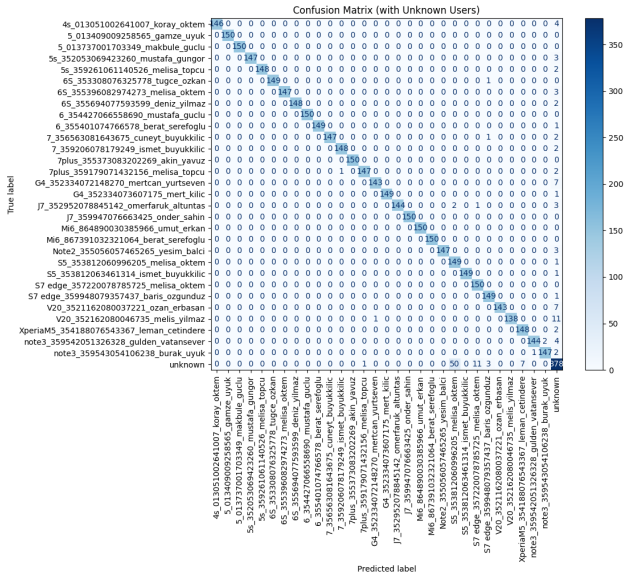

Fig. 8. Confusion matrix on the test set (including unknown users)

for device authentication based on radio signals in a practical open-set scenario.

VI. Conclusion

This research has shown the potential of applied machine learning and deep learning in RF fingerprinting. The RiftNet model achieved promising results in signal classification and device identification. However, improving the diversity of the test set is still a challenge.

In the future, we plan to experiment with our methods on larger and more diverse datasets, including the Bluetooth dataset used in RiftNet, to improve the detection of unknown devices. We will then continue to develop methods to detect anomalies or unknown devices in protected areas with high accuracy and generalize to meet the increasing security demands in wireless networks.

References

[1] Y. Lin, J. Jia, S. Wang, B. Ge, and S. Mao, "Wireless device identification based on radio frequency fingerprint features," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1–6. DOI: 10.1109/ICC40277.2020.9149226.

[2] T. Jian, Y. Gong, Z. Zhan, *et al.*, "Radio frequency fingerprinting on the edge," *IEEE Transactions on Mobile Computing*, vol. 21, no. 11, pp. 4078–4093, 2022. DOI: 10.1109/TMC.2021.3064466.

[3] Z. Shao, Z. Lv, W. Wang, and T. Zhang, "Research on illegal mobile device identification based on radio frequency fingerprint feature," *Electronics*, vol. 12, no. 14, p. 3144, 2023. DOI: 10.3390/electronics12143144. [Online]. Available: https://www.mdpi.com/2079-9292/12/14/3144.

[4] L. Xie, L. Peng, J. Zhang, and A. Hu, "Radio frequency fingerprint identification for internet of things: A survey," *Security and Safety*, vol. 3, no. 1, 2024. DOI: 10.1051/sands/20230017. [Online]. Available: https://sands.edpsciences.org/articles/sands/full_html/2024/01/sands20230017/sands20230017.html.

[5] A. Jagannath, J. Jagannath, and P. S. Pattanshetty Vasanth Kumar, "A comprehensive survey on radio frequency (rf) fingerprinting: Traditional approaches, deep learning, and open challenges," *Computer Networks*, vol. 213, p. 109 100, 2022. DOI: 10.1016/j.comnet.2022.109100. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1389128622004893.

[6] N. specified, "Radio frequency fingerprinting techniques for device identification: A survey," *International Journal of Information Security*, vol. 23, pp. 1389–1427, 2024. DOI: 10.1007/s10207-023-00801-z. [Online]. Available: https://link.springer.com/article/10.1007/s10207-02.

[7] T. Jian, B. C. Rendon, E. Ojuba, *et al.*, "Deep learning for rf fingerprinting: A massive experimental study," in *Proceedings of the IEEE International Conference on Internet of Things (iThings)*, 2020. [Online]. Available: https://ece.northeastern.edu/fac-ece/ioannidis/static/pdf/2020/J_Jian_RFDeepLearning_IoT_2020.pdf.

[8] J. Zhang, G. Shen, W. Saad, and K. Chowdhury, "Radio frequency fingerprint identification for device authentication in the internet of things," *IEEE Communications Magazine*, 2023, Early Access. [Online]. Available: https://livrepository.liverpool.ac.uk/3171530/1/manuscript%20-%20CM%202023%20RFFI.pdf.

[9] S. Al-Hazbi, A. Hussain, S. Sciancalepore, G. Oligeri, and P. Papadimitratos, "Radio frequency fingerprinting via deep learning: Challenges and opportunities," *arXiv preprint arXiv:2310.16406*, 2024. [Online]. Available: https://arxiv.org/pdf/2310.16406.

[10] J. Robinson and S. Kuzdeba, "Riftnet: Radio frequency classification for large populations," in *2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC)*, IEEE, 2021, pp. 1–6. DOI: 10.1109/CCNC49032.2021.9369492.

[11] A. M. Ali, E. Uzundurukan, and A. Kara, "Improvements on transient signal detection for rf fingerprinting," in *2017 25th Signal Processing and Communications Applications Conference (SIU)*, Zonguldak, Turkey: IEEE, May 2017, pp. 1–4. DOI: 10.1109/SIU.2017.7960507. [Online]. Available: https://ieeexplore.ieee.org/document/7960507.

[12] E. Uzundurukan, Y. Dalveren, and A. Kara, "A database for the radio frequency fingerprinting of bluetooth devices," *Data*, vol. 5, no. 2, p. 55, 2020. DOI: 10.3390/data5020055. [Online]. Available: https://www.mdpi.com/2306-5729/5/2/55.

[13] M. Douze, A. Guzhva, C. Deng, *et al.*, *The faiss library*, 2025. arXiv: 2401.08281 [cs.LG]. [Online]. Available: https://arxiv.org/abs/2401.08281.

[14] C. Geng, S.-J. Huang, and S. Chen, "Recent advances in open set recognition: A survey," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 43, no. 10, pp. 3614–3631, Oct. 2021, ISSN: 1939-3539. DOI: 10.1109/tpami.2020.2981604. [Online]. Available: http://dx.doi.org/10.1109/TPAMI.2020.2981604.