AI-based RF-Fingerprinting Framework and Implementation using Software-Defined Radios

Hovannes Kulhandjian[†], Elizabeth Batz[†], Eduardo Garcia[†], Selena Vega[†], Sanjana Velma[†], Michel Kulhandjian[‡], Claude D'Amours[‡], Burak Kantarci[‡], and Tathagata Mukherjee[††]

[†]Department of Electrical and Computer Engineering, California State University, Fresno, Fresno, CA 93740, U.S.A.
E-mail: {hkulhandjian,ebatz32,tona,selenav17,sanjanavelma}@mail.fresnostate.edu
[‡]School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, Ontario, K1N 6N5, Canada
E-mail: mkk6@buffalo.edu,{cdamours,burak.kantarci}@uottawa.ca
[††]Department of Computer Science, The University of Alabama in Huntsville, AL 35899, U.S.A.
E-mail: tathagata.mukherjee@uah.edu

***Abstract*—Radio frequency (RF) fingerprinting is considered to be a promising security solution for wireless communications at the physical layer. RF fingerprinting is still in its infancy, and much research is needed to further improve the detection capabilities. To address this problem, in this paper, we propose utilizing software-defined radios (SDRs), which have proven to be extremely beneficial to the RF research community. We demonstrate the capability of RF fingerprinting by identifying the transmit radios that are in the pre-selected whitelist (authorized) and reject any other transmit radios not found in the whitelist. We have experimented with four different universal software-radio peripherals (USRPs) models with a total of fourteen USRPs for our RF fingerprinting solution. Deep learning models and transfer learning are used to train the RF fingerprinting models. Experimental results reveal that the ability of RF fingerprinting the USRPs drops as the hardware quality of USRPs improves. For low-end USRPs an accuracy of 99% is achieved; however, for high-end radios, the accuracy decreased to as low as 43%. This is due to the difficulty of finding anomalies with high-quality hardware, which is essential for successful RF fingerprinting.**

***Index Terms*—RF-Fingerprinting, machine learning, and software-defined radios.**

I. Introduction

In recent years, radio frequency (RF) fingerprinting has gained a lot of attention from the research community. RF fingerprinting is a technique for identifying a radio transmitter based on the "fingerprint" of its signal transmission, which is difficult to duplicate. This is due to the inherent variations embedded in its hardware during the manufacturing process. For this reason, RF fingerprinting can be utilized for security purposes. Research so far has shown success using rise-time signatures, power densities, and transient signal characteristics as the defining features to classify devices [1]. An electronic fingerprint allows a wireless device to be identified based on its radio transmission characteristics [2]. Cellular providers routinely utilize RF fingerprinting to prevent mobile phone cloning; a cloned device will have the same numeric equipment identity but a distinct radio fingerprint. When a transmitter (e.g., cell phones, or any other form of radio transmitter) is first turned on, it has a rise time signature that is generated by minor differences in component values during manufacturing. The use of a separate transmitter with the same callsign is easily detected after the rising time signature is captured and matched to that callsign. Military signals intelligence and radio regulatory organizations such as the US Federal Communications Commission (FCC) employ such techniques to locate unauthorized transmitters. They are also utilized in subscriber mobile radio (SMR) systems to assess consumption for billing purposes [3], [4]. The RF fingerprinting technique offers a "physical layer" authentication solution providing substantially superior performance than typical higher-layer encryption techniques [4], [5].

RF fingerprinting is still in its infancy; more research needs to be done to further improve the detection capabilities as outlined in [6]. Even though progress in this area has been achieved more recently, the importance of this topic can date back to the Vietnam War era when the first radiometric identification systems were developed to distinguish between friendly and enemy radars [3]. In 2008, a team from the University of Wisconsin and Rutgers University explored using radiometric signatures from signals to identify wireless devices. They came up with the passive radiometric device identification system (PARADIS) that utilized the modulation domain to manipulate and classify the signals which they found to produce a high accuracy [3]. Since then, more research has been done using deep learning methods for classification. Variations of convolutional neural networks (CNNs) have been the most popular to implement for this purpose. A team at Northeastern University experimented with a custom and modified version of a ResNet architecture in which they found some success with accuracy sitting at about 77% to 93% depending on how many devices they tested with and the environmental conditions [1].

CNN-driven RF fingerprinting-based identification of unmanned aerial vehicles (UAVs) by exploiting the transmitter constellations is proposed by S. Mohanti *et al.* in [7]. The underlying architecture is based on a one-dimensional version of the standard visual geometry group (VGG) network architecture. One of the challenges of a trained neural network is that it undergoes performance degradation if it is applied to another day that experiences a different channel. As a consequence, the study proposes a processing block to deal with this issue by arranging the in-phase and quadrature-phase (IQ) samples. To overcome this problem, G. Reus-Mun

et al. [8] study the triplet loss function. The proposed triplet network architecture-based solution is capable of successfully classifying different transmitters even when training and testing are performed on different days.

Mohanti *et al.* [7] studied RF fingerprinting with the added element of UAVs. They also used a CNN but pre-processed the transmitted signals to intentionally introduce a distinct physical layer signature – the one they "injected" would be the feature their network would identify. In the past year, researchers have tried device identification by focusing on "weight pruning" to achieve minor accuracy loss in the CNN [9] and by the use of an echo state network (ESN), which yielded an average classification accuracy of 98.11% [10].

Vo-Huu *et al.* [11] explore RF fingerprinting of Wi-Fi devices by using a software-defined radio (SDR). A set of non-AI-based techniques are developed for distinguishing different Wi-Fi cards. The authors were able to distinguish between models with a success rate of 95%. They also found that it is possible to uniquely identify a device with a 47% success rate if the samples are collected within a 10s interval.

Though the same overarching topic of RF fingerprinting is explored, there are various environmental conditions to be considered and numerous approaches that have been and can be taken. Partially for this reason, the problem of wireless security using RF fingerprinting is still very relevant today. To address this problem, we propose utilizing SDR tools and concepts, which have proven to be extremely beneficial to the RF research community. SDR has made it possible to advance research directions in wireless communications by allowing the implementation of more advanced concepts and theories using the SDR platform, without which it is very difficult to implement [12]. In addition, we explored machine learning algorithms including deep learning, which have recently gained attention from the wireless communities [12], [13].

Unlike the previous research work, in this study, we utilize an SDR to fingerprint a collection of other SDRs with different models and brands, and among the same model and brand. The main objective of this paper is to implement an autonomous system for identifying authorized and unauthorized users via RF fingerprinting. An original and complete data set of signals containing the IQ data received from SDRs is gathered and used to train a deep learning network. These received raw signals were converted to spectrogram plots. This pre-processed data is then used as the input to three different deep learning networks to train on the classification of the type of SDR and of each individual device. Experimental results reveal that the ability of RF fingerprinting the USRPs drops as the quality of USRPs improves. For low-end USRPs an accuracy of 99% is achieved; however, as the radios became more advanced, the accuracy decreased to as low as 43%. This is due to the difficulty of finding anomalies with higher-quality hardware, which is essential for successful RF fingerprinting.

The rest of the paper is organized as follows. In Section II, we present the hardware configuration and setup. In Section III, we discuss the RF fingerprinting experimental results and analysis before presenting our conclusion in Section IV.

II. Hardware and Experimental Setup

To perform the RF fingerprinting experimentation we have used four different types of USRPs, (a) NI USRP 2920, (b) NI USRP 2901, (c) Ettus Research USRP B205mini, and (d) Adalm-Pluto, which are shown in Fig. 1.

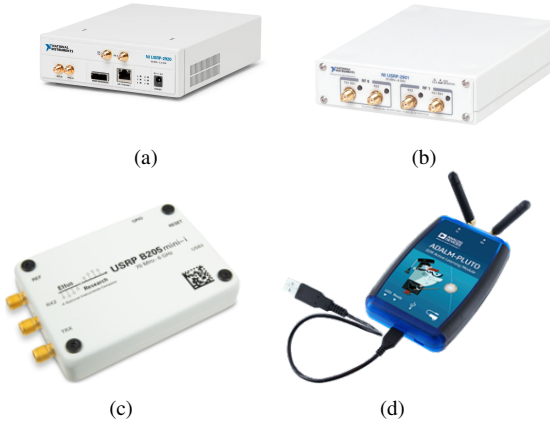

Fig. 1: (a) NI USRP 2920 (b) NI USRP 2901 (c) Ettus Research USRP B205mini (d) Adalm-Pluto.

The dataset is captured using two Dell Latitude E7420 laptops, a transmitter, a receiver, and Simulink modules. Fourteen different USRPs, i.e., two NI USRP 2920, four NI USRP 2901, four Ettus Research USRP B205min, and four Adalm-Pluto are used as transmitters and one additional NI USRP 2920 is used as a receiver during the experiments. To ensure that the data captured would only reflect the inherent characteristics of the transmitter, only one device was transmitted at a time. This prevented false positive results due to channel impairments. We have taken precautions to minimize our neural network identifying the difference in channels rather than the difference in device transmission characteristics. Each transmitter is placed about 30 cm from the receiver, as shown in Fig. 3, which is the experimental setup for Adalm-Pluto. This ensured that there would be less variation between results and established a baseline for consistency.

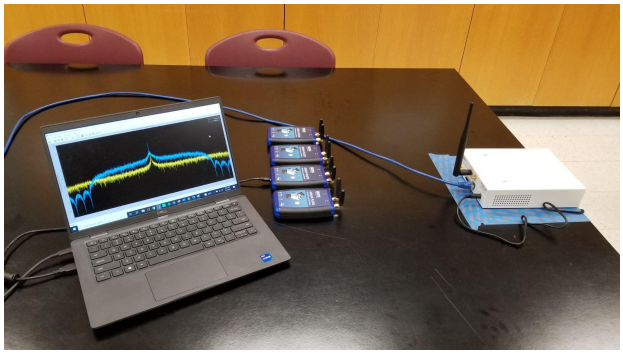

Fig. 3: Experimental setup for Adalm-Pluto SDRs.

A. SDR Configuration

We program and configure the SDRs using both MATLAB and Simulink. MATLAB is also used for frequency correction and adjustment before initiating the data acquisition process.

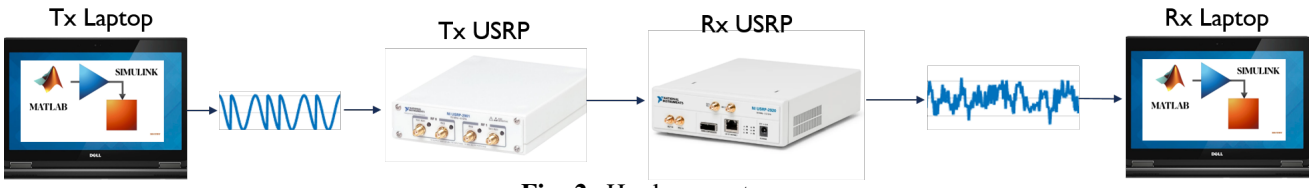

Fig. 2: Hardware setup.

This ensured that the center frequencies are aligned on the transmitter and the receiver side. Simulink modules are used to modulate the transmission message into quadrature phase-shift keying (QPSK), transmit, and then synchronize the transmitter and receiver. Figure 4 shows inside the QPSK receiver system module on Simulink. A fixed message is sent ten times over a period of eight seconds. Before each cycle, a QPSK-modulated Barker code preamble is sent to ensure synchronization and to ensure that only the message data is recorded for use in the dataset.

B. Dataset

The dataset is built using MATLAB and Simulink models, to send and receive a predetermined message modulated with QPSK at 915 MHz. The QPSK model utilized a Barker code preamble to ensure synchronization between transmitter and receiver. This signal is repeatedly recorded for each device, labeled, and processed. This message is received and recorded into a time series '.mat' file. The received data is then converted into spectrograms of 1 sec. duration each using MATLAB and is stored in predefined labeled folders. Overall, about $11,200$ spectrogram data sets are generated for deep learning training purposes and roughly 800 spectrograms from each USRPs.

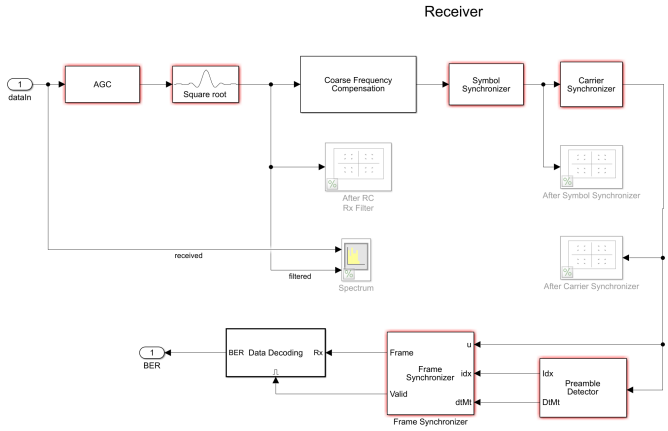

Fig. 4: Inside the QPSK receiver subsystem module.

C. Signal Post-Processing

Five types of spectrograms were generated from the signals which showed the real part, the imaginary part, the complex part, the complex-valued power density spectrum, and a three-dimensional waterfall for the complex-valued power density. After experimenting with the five different image types we concluded that complex-valued spectrograms provided the best results. Several images of real and complex spectrograms are shown in Fig. 5. The complex value images were used as the training data input for the neural network.

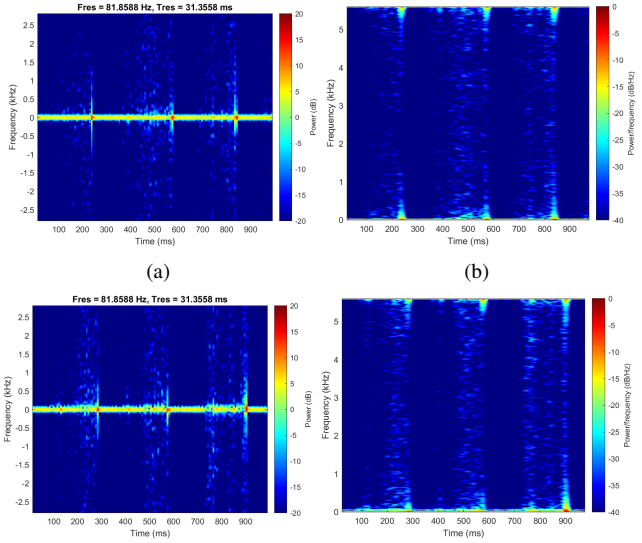

Fig. 5: (a) Real signal spectrogram for B205mini (b) Complex signal spectrogram for B205mini (c) Real signal spectrogram for Adalm-Pluto (d) Complex signal spectrogram for Adalm-Pluto.

III. RF Fingerprinting Experimental Results

In our study, we have explored different neural network architectures including the traditional CNN architecture shown in Fig. 6, as well as more popular deep convolutional neural networks including GoogLeNet, ResNet-50, and SqueezeNet. We explore the possibility of RF fingerprinting i) between the four different SDRs models (Adalm-Pluto, USRP B205min, USRP 2901, and USRP 2920), ii) among all the 14 different SDRs, and iii) within the four individual models of SDRs. The training parameters are selected using a heuristic approach. The initial learning rate is set to 0.0001, the max epochs set to 10, and the min batch size set to 20. GoogLeNet architecture provided the best results, compared to the other ones we experimented with. Therefore, we will be presenting the GoogLeNet results.

A. RF Fingerprinting Between Different SDR Brands/Models

In the first study, we explore RF fingerprinting between the four different models/brands of SDRs ranging from low-end to high-end ones (i.e., Adalm-Pluto, USRP B205min, USRP 2901, and USRP 2920). As shown in Fig. 7, the validation accuracy of 81.33% is achieved in RF fingerprinting different models/brands of SDRs.

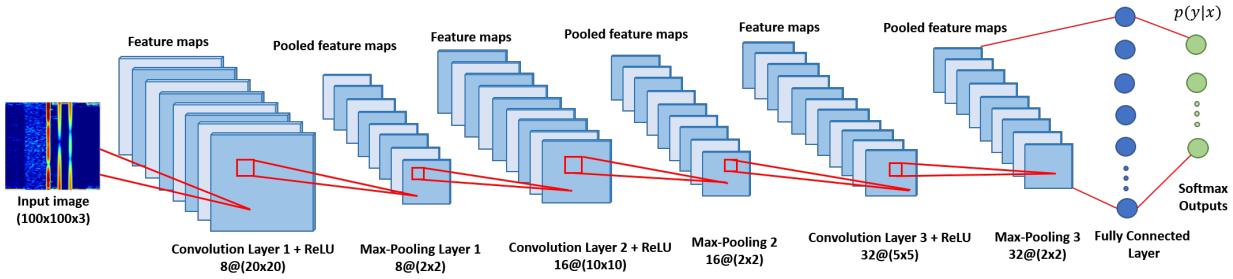

Fig. 6: Convolutional neural network architecture.

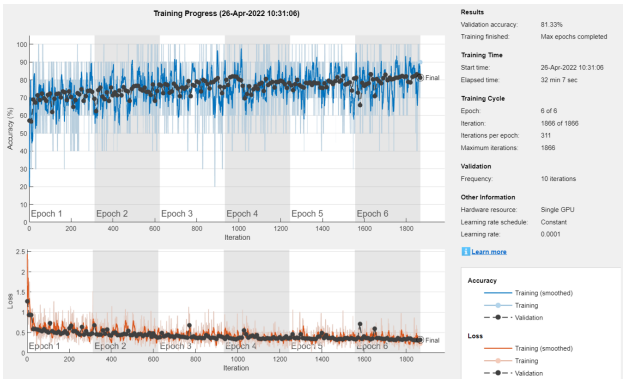

Fig. 7: Accuracy and loss training and validation results for distinguishing between different models/brands of SDR with an accuracy of 81.33%.

B. RF Fingerprinting Among All the 14 Different SDRs

In the second study, we explore RF fingerprinting among all the 14 different SDRs. In this data set, we use four Adalm-Plutos, four USRP B205min, and four USRP 2901 as well as two USRP 2920. As shown in Fig. 8, the validation accuracy drops to 75.45% in RF fingerprinting among all the 14 different SDRs. From the results, it is evident that as the number of SDRs increased it becomes more difficult to fingerprint the different SDRs.

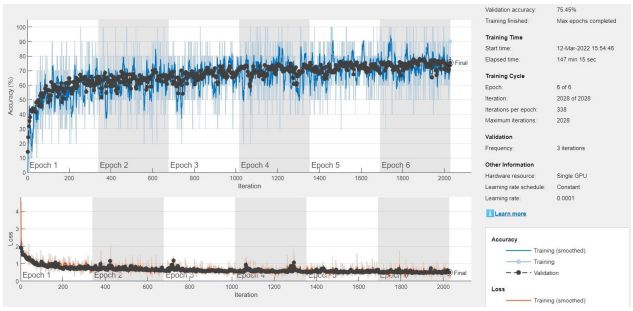

Fig. 8: Accuracy and loss training results between all 14 different SDRs with 75.45% accuracy.

C. RF Fingerprinting Within the Individual SDR Models

In the next set of studies, we explore RF fingerprinting within the four individual models of SDRs; Adalm-Plutos, USRP B205min, USRP 2901, and USRP 2920.

To gain a better understanding of the limitations of RF-fingerprinting GoogLeNet was trained on a dataset consisting of each model/brand. This was done to see if the limitations in accuracy were coming from the model having difficulty differentiating between different devices of the same make and model. So each set of spectrograms for each make and model was separated into mini-datasets. These mini-datasets were then used to train GoogLeNet to identify whether or not the decrease in accuracy was due to there being too much similarity between models of the same make and model.

1) Adalm-Pluto Results: Differentiating between Adalm-Pluto #1, #2, #3, and #4 yielded a remarkably accurate rate. GoogLeNet was able to differentiate between these devices with 99.38% validation accuracy.

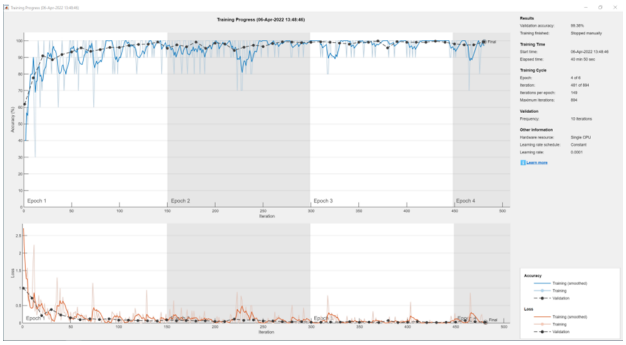

Fig. 9: Accuracy and loss training and validation results for differentiating between individual Adalm-Plutos with 99.38% accuracy.

2) USRP B205mini Results: Differentiating between USRP B205mini #1, #2, #3, and #4 yielded interesting results. GoogLeNet was able to differentiate between these devices with only 83.53% validation accuracy.

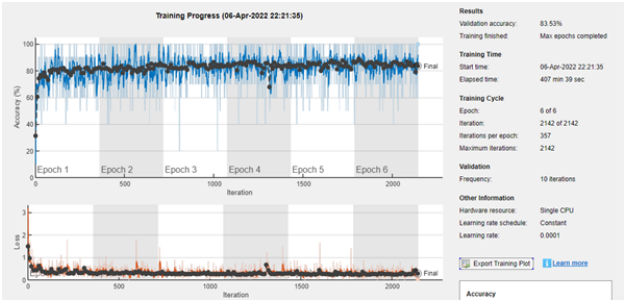

Fig. 10: Accuracy and loss training and validation results for differentiating between individual B205mini with 83.53% accuracy.

3) NI USRP 2901: Differentiating between NI USRP 2901 #1, #2, #3, and #4 yielded poor results. GoogLeNet was able to differentiate between these devices with only a 42.97% validation accuracy.

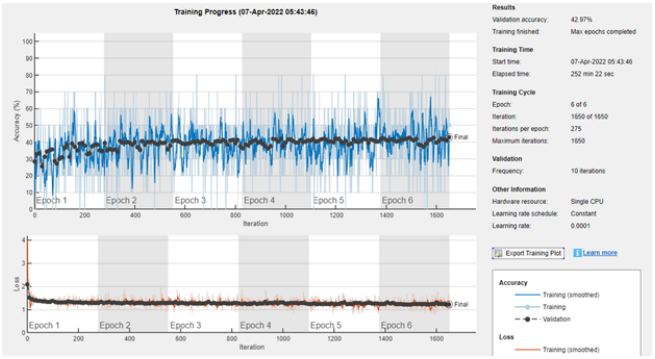

Fig. 11: Accuracy and Loss Training and Validation Results for Differentiating Between Individual USRP 2901 with 42.97% accuracy.

4) NI USRP 2920 Results: Differentiating between NI USRP 2920 #1 and #2 yielded poor results. GoogLeNet was able to differentiate between these devices with 50% accuracy. These results were somewhat expected after the running of the NI USRP 2901, as they are essentially the same base model of radio but there are only two devices in this classification as opposed to four.

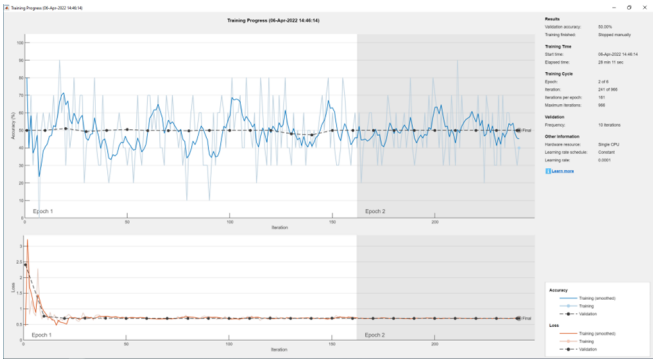

Fig. 12: Accuracy and Loss Training and Validation Results for Differentiating Between Individual USRP 2920 with 50% accuracy.

IV. Conclusion

In this paper, we developed an AI-based RF fingerprinting framework for identifying different software-defined radios (SDRs) at the physical layer. We have used a GoogLeNet-based machine learning model that could distinguish a unique authorized transmitting device with 75.45% accuracy among 14 devices which consisted of four different brands. However, the model was more accurate when models of the transmitter were differentiated from each other as it had an accuracy of 81.31%. It is reasonable to hypothesize that there are larger differences in the structure and characteristics of the transmission signal when the radio models differ. Additional classification within the individual brands resulted in an observed correlation between the sophistication of the make of SDR and the accuracy achieved. The basic Adalm-Pluto SDRs yielded a high accuracy of 99%; however, as the radios become more on higher quality, e.g., NI USRP 2920, the accuracy decreased to as low as 43%.

Acknowledgment

Special thanks to the Air Force Research Lab and Wright Brothers Institute for supporting aspects of this project in 2021/22 Beyond 5G SDR Challenge. In addition to that this work was partially supported by the Department of Defence (DOD) Instrumentation Grant Number W911NF2110210 and in part by the Natural Sciences and Engineering Research Council (NSERC) of Canada - Ontario Centre for Innovation (OCI) under the joint VIP-Alliance Program.

References

[1] T. Jian, B. C. Rendon, E. Ojuba, N. Soltani, Z. Wang, K. Sankhe, A. Gritsenko, J. Dy, K. Chowdhury, and S. Ioannidis, "Deep Learning for RF Fingerprinting: A Massive Experimental Study," *IEEE Internet of Things Mag.*, vol. 3, no. 1, pp. 50–57, Mar. 2020.

[2] C. Comert, M. Kulhandjian, O. M. Gul, A. Touazi, C. Ellement, B. Kantarci, and C. D'Amours, "Analysis of augmentation methods for RF fingerprinting under impaired channels," ser. WiseML '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 3–8. [Online]. Available: https://doi.org/10.1145/3522783.3529518

[3] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proc. of the 14th ACM Int. Conf. on Mobile Computing and Networking (MobiCom)*, San Francisco, CA, USA, Sep. 2008, pp. 116–127.

[4] L. F. Abanto-Leon, A. Bäuml, G. H. A. Sim, M. Hollick, and A. Asadi, "Stay Connected, Leave No Trace: Enhancing Security and Privacy in WiFi via Obfuscating Radiometric Fingerprints," *Proc. ACM Meas. Anal. Comput. Syst.*, vol. 4, no. 3, pp. 1115–1145, Dec. 2020.

[5] Y. Shi and M. A. Jensen, "Improved Radiometric Identification of Wireless Devices Using MIMO Transmission," *IEEE Trans. on Inf. Forensics and Security*, vol. 6, no. 4, pp. 1346–1354, Dec. 2011.

[6] C. Comert, O. M. Gul, M. Kulhandjian, A. Touazi, C. Ellement, B. Kantarci, and C. D'Amours, "Secure design of cyber-physical systems at the radio frequency level: Machine and deep learning-driven approaches, challenges and opportunities," in *Artificial Intelligence for Cyber-Physical Systems Hardening*, I. Traore, I. Woungang, and S. Saad, Eds. Springer, 2022.

[7] S. Mohanti, N. Soltani, K. Sankhe, D. Jaisinghani, M. Di Felice, and K. Chowdhury, "AirID: Injecting a Custom RF Fingerprint for Enhanced UAV Identification using Deep Learning," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Taipei, Taiwan, Dec. 2020, pp. 1–6.

[8] G. Reus-Muns, D. Jaisinghani, K. Sankhe, and K. R. Chowdhury, "Trust in 5G Open RANs through Machine Learning: RF Fingerprinting on the POWDER PAWR Platform," in *IEEE Global Commun. Conf. (GLOBECOM)*, Taipei, Taiwan, Dec. 2020, pp. 1–6.

[9] T. Jian, Y. Gong, Z. Zhan, R. Shi, N. Soltani, Z. Wang, J. G. Dy, K. R. Chowdhury, Y. Wang, and S. Ioannidis, "Radio Frequency Fingerprinting on the Edge," *IEEE Trans. on Mob. Computing*, pp. 1–1, Mar. 2021.

[10] K. Bai, C. Thiem, N. McDonald, L. Loomis, and Y. Yi, "Toward Intelligence in Communication Networks: A Deep Learning Identification Strategy for Radio Frequency Fingerprints," in *Int. Symp. on Quality Electronic Design (ISQED)*, Santa Clara, CA, USA, Apr. 2021, pp. 204–209.

[11] T. D. Vo-Huu, T. D. Vo-Huu, and G. Noubir, "Fingerprinting wi-fi devices using software defined radios," in *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, 2016, pp. 3–14.

[12] H. Kulhandjian, N. Ramachandran, M. Kulhandjian, and C. D'Amours, "Human activity classification in underwater using sonar and deep learning," in *Proc. of the Int. Conf. on Underwater Networks & Systems (WUWNet)*, Atlanta, GA, USA, Oct. 2019.

[13] H. Kulhandjian, P. Sharma, M. Kulhandjian, and C. D'Amours, "Sign Language Gesture Recognition Using Doppler Radar and Deep Learning," in *Proc. IEEE Global Commun. Conf. Workshops (GLOBECOM Wkshps)*, Waikoloa, Hawaii, U.S.A., Dec. 2019, pp. 1–6.