American Journal of Interdisciplinary Research and Development
ISSN Online: 2771-8948
Website: www.ajird.journalspark.org
Volume 23, December, 2023

AI-BASED RF FINGERPRINTING DEVICE IDENTIFICATION AND WIRELESS SECURITY

Bekhzod Sulaymonov,
PhD in Technical Sciences
Senior Lecturer at Department of IT and Cybersecurity,
Armed Forces Academy, Tashkent, Uzbekistan
bbsulaymonov@gmail.com

Adiba Sulaymonova,
Student, TUIT named after Muhammad Khwarezmi,
Tashkent Uzbekistan
sulaymonovs@gmail.com

Abstract:
AI-powered RF fingerprinting contributes to the security of emerging networks, authenticating received signal characteristics through an artificial intelligence mechanism. This method is rooted in an AI-based approach. The RF fingerprinting technique is adept at identifying distinctive RF features, which is crucial for optimizing security in wireless networks. Our investigation delves into AI-based RF fingerprinting, employing recurrent neural networks coupled with long short-term memory to classify and analyze signals. We address challenges arising from signal variability, environmental factors, and device introductions. The primary focus is on the efficacy of RF fingerprints for authentication across diverse communication technologies. The methodology encompasses data collection training, showcasing a high accuracy rate in transmitter classification. This study emphasizes the considerable potential of AI-based RF fingerprinting in mitigating security and identification challenges in the era of the Internet of Things (IoT).

Keywords: artificial intelligence, identification, security, RF fingerprinting, wireless security, IoT.

Introduction

RF fingerprinting is used to identify distinct radio frequency characteristics, i.e., frequency response, signal strength, and modulation patterns. AI-based RF fingerprinting consists of machine learning algorithms that are trained to recognize RF signals with related specific devices. These AI algorithms are used to analyze large datasets of RF signals for pattern identification that are difficult for humans to discern. Trained AI models classify RF signals for identification of device transmitting signals. It helps in Real-time analysis in each network. AI-based RF fingerprinting is used for security and detection. For IoT, it assists in managing a multitude of connected devices by tracking and identifying them, along with contributing to optimization by source identification, enhancing overall network performance. Despite its applications, it faced various challenges, such as variability of RF signals due to environmental factors, the introduction of a new device that can impact the effectiveness of RF fingerprinting, and RF characteristics that raise privacy concerns. DL DL-based RF fingerprinting is a valid solution for physical layer security [1]. Automated identification and authentication from device-specific fingerprints collected by received RF signal samples. These signals exist due to device circuitry components in the RF signal path [2]. With AI power, fingerprinting technology enables network security services that protect against unauthorized access malicious activities cyber-physical infrastructure security [3]. There has been a rapid increase in Internet of Things devices and data. RF figure printing is a technique that provides the solution to various security issues, authentication, and identification. It utilizes frequency variations, small amplitudes, and phase for each device for RF integrated circuits that use antenna elements for connections [4]. AI algorithms detect these signatures. The traditional methods achieved 63% roundabout accuracy using small signatures in 250 devices [1].

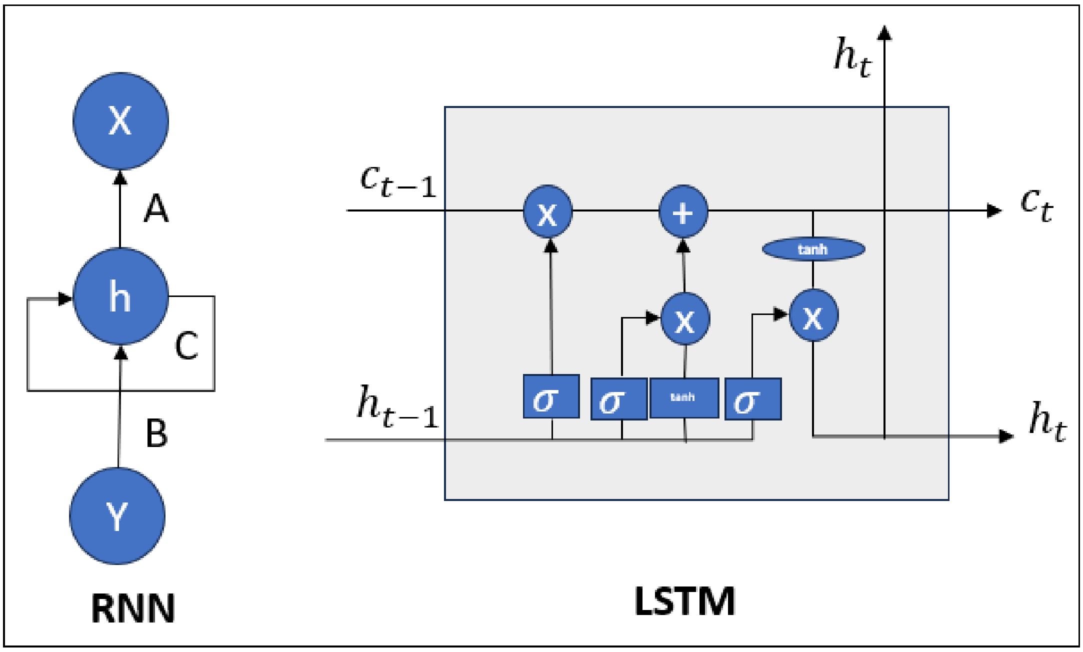

Figure 1. Component of RNN LSTM neural Network

Literature Review

RFFs are effective authenticated sources of transmission for devices at risk and exposure to attacks. There is no additional computation at the transmitter and the receiver, authentication is offloaded completely. The AI-trained model extracts patterns from the receiver so that the source can be authenticated. These patterns are unique in their characteristics. Radio signals are affected by small differences that combine the capabilities of Artificial Intelligence and RF signal tools. These are based on Deep learning as well as

Machine learning algorithms [5]. Many studies show work on RFF-based fingerprinting, while some of them focus on Bluetooth, LTE, Wi-Fi, Zigbee, and ADS-B. Other work focused on AI algorithms with RF-based fingerprinting problems using ad hoc and Neural network solutions. Previous work focused on their reliability issues, reliable training, and prevention for such technique deployment [6]. Nonlinear characteristics making fingerprints dependent on power transmitters unpredictably [7], heat dissipation, and device aging are recent contributions like training of RF models their testing produced unsatisfactory performance along with a drop of 0.5 in accuracy.

The process of RF fingerprinting identifies transmitter unique characters on transmitter signals for the prevention of node impersonation where security credentials are obtained [8]. Many features are dependent on hardware that exist due to manufacture process variations of hardware process in wireless transmitters, which meets requirements even though they are small enough for coming up with standards allowing unique feature identification, i.e., signals transient phase, power amplifier imperfections, errors in phase and magnitude, frequency differences, clock offset. Existing algorithms based on unsupervised learning. They require device registration and training before setting up the database. Which is useful for spoofing identification RF fingerprinting AI-based work is dependent upon human-engineered features stack protocol layers. We have evaluated a deep neural network that could be applied for efficient identification of the device by automatic learning of RF fingerprints dependent on the device. It does not need humans to define features to be used in the RF fingerprinting process.

Recurrent neural networks (RNNs) for RF Fingerprinting:

RNN neural network gave a sequence of dynamics using network cycles that maintain a state randomly selected long context window, making it applicable for data in sequence. Trillions of parameters were difficult to train on RNN; therefore, LSTM long short-term memory for solving vanishing gradient problems was developed. RNNs slowly change during training, so they have LSTM in the form of weights for data that act as activations from node to node. It captures features, i.e., frequency drift and ramp-up trend during the initial sequence. The Architecture had recurrently connected units as memory blocks. Each block contains a memory cell and three multiplicative units (input, output and forget gate). That performs operations such as writing, reading, and resetting cells. The gate allows information retention to solve vanishing issues during the training phase, such as activation rewriting, which is prevented until the input gate remains closed. Memory cells contain self-connected recurrent edge offset weight that passes along multiple steps. Based on these features, LSTM-based RNN is a good choice for RF fingerprinting applications. Like other techniques, it does not involve human-engineered features.

American Journal of Interdisciplinary Research and Development
ISSN Online: 2771-8948
Website: www.ajird.journalspark.org
Volume 23, December, 2023

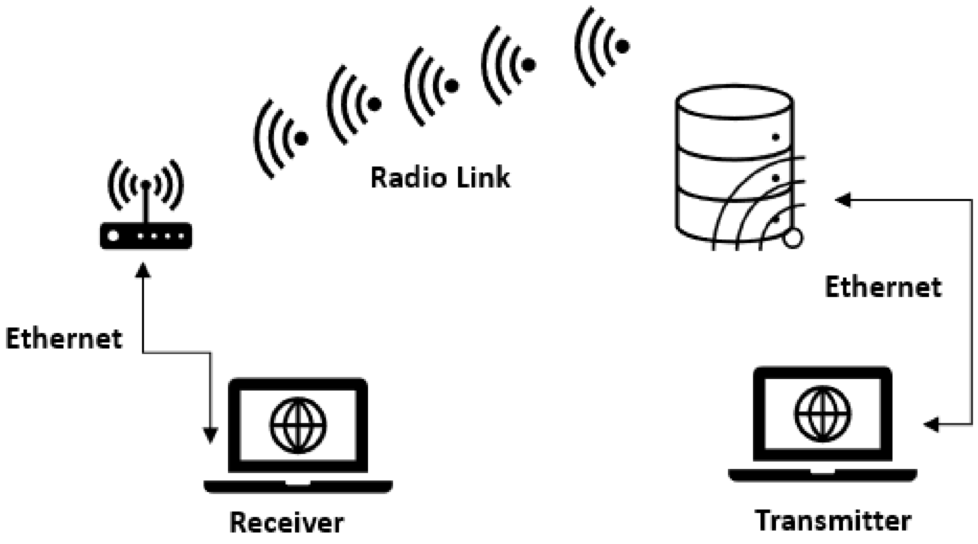

Figure 2. Working of Receiver and transmitter over AI-based RF fingerprinting Network

Data Collection:

Transmission experiments for training and testing were carried out using software defined radio modules. It had six transmitters and one receiver. The receiver and transmitter were connected using an RF test cable to control the SNR signal-to-noise ratio. Random data is generated, packed, and transmitted to the transmitter. 925 MHz carrier of signals was used. SNR is added with Gaussian noise for degradation due to loss channel and external noise. A total of 6000 data units were transmitted and each of them had 500 bits of data. The receiver converted analog signals into digital signals by ADC converter, resulting in about 6000 samples per packet.

Training:

The hidden layer of the LSTM block was implemented where logistic sigmoid function input, output and forget gates, and activation vectors were used, all of them having the same size. The weight matrix from cell to vector was diagonal. Each vector input is obtained from the cell element of the vector. To enhance clarity, bias was eliminated, and samples were segmented into per-sequence packets. A testing subset comprised 20% of the dataset, leaving the remaining 80% for training purposes. The Recurrent Neural Network (RNN) was trained using Long Short-Term Memory (LSTM) cells, with the output layer configured as a SoftMax layer.

Evaluation:

The RNN model classifies transmitters even in strong noise interference, which is surprisingly high and effective. Training data was increased to get better-trained model accuracy. It achieved a probability of detection of 0.99. There was no distinguishable difference between both data. Degradation in SNR gave degradation in the probability of detection. Inaccuracy was managed by training steps increment. At the 4000 steps of training, it performed accurately with a 95% probability of distribution, for further training, increment overfitting of the model was observed. Interference effects were emulated by adding sequences in which the scaling factor varied from 3 to 17 dB SIR.

Conclusion:

In our exploration of AI-based RF fingerprinting, we presented a comprehensive overview of its utilization, employing RNN-based solutions for device identification and security applications. This innovative approach facilitates the identification and authentication of devices based on their distinctive radio frequency signatures. The RNN model, specifically based on Long Short-Term Memory (LSTM), exhibited exceptional performance, effectively capturing hardware-specific features in wireless transmitters and showcasing robust results even in the presence of interference and noise.

A noteworthy aspect of the AI algorithm is its capability to analyze extensive datasets in real time, demonstrating versatility across diverse network environments. Despite challenges posed by environmental factors and the introduction of new devices, AI-based RF fingerprinting emerges as a valuable tool for addressing security concerns, facilitating detection, and optimizing performance, particularly within the dynamic landscape of the Internet of Things (IoT). The evaluation process underscored a high probability of detection at 0.99, highlighting the model's resilience and significant potential for elevating security, authentication, and identification in wireless communication networks, especially within the evolving realm of IoT.

References:

1. T. Jian et al., "Deep learning for RF fingerprinting: A massive experimental study," IEEE Internet of Things Magazine, vol. 3, no. 1, pp. 50-57, 2020.
2. S. Rajendran and Z. Sun, "Rf impairment model-based iot physical-layer identification for enhanced domain generalization," IEEE Transactions on Information Forensics and Security, vol. 17, pp. 1285-1299, 2022.
3. A. Jagannath, J. Jagannath, and P. S. P. V. Kumar, "A comprehensive survey on radio frequency (rf) fingerprinting: Traditional approaches, deep learning, and open challenges," Computer Networks, vol. 219, p. 109455, 2022.
4. A. Saeif, S. Savio, and O. Gabriele, "The day-after-tomorrow: On the performance of radio fingerprinting over time," in Proceedings of the 39th Annual Computer Security Applications Conference, 2023, pp. 439-450.

American Journal of Interdisciplinary Research and Development
ISSN Online: 2771-8948
Website: www.ajird.journalspark.org
Volume 23, December, 2023

5. K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]," IEEE Wireless Communications, vol. 17, no. 5, pp. 56-62, 2010.
6. Y. Huang, "Radio frequency fingerprint extraction of radio emitter based on I/Q imbalance," Procedia computer science, vol. 107, pp. 472-477, 2017.
7. N. Soltani, G. Reus-Muns, B. Salehi, J. Dy, S. Ioannidis, and K. Chowdhury, "RF fingerprinting unmanned Aerial vehicles with non-standard transmitter Waveforms," IEEE Transactions on vehicular technology, vol. 69, no. 12, pp. 15518-15531, 2020.
8. Q. Xu, R. Zheng, W. Saad, and Z. Han, "Device fingerprinting in wireless networks: Challenges and opportunities," IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 94-104, 2015.