Radio Frequency Fingerprinting and its Challenges

Saeed Ur Rehman[*], Kevin W. Sowerby[τ], Shafiq Alam[ϒ], Iman Ardekani[*]
[*]Department of Computing, Unitec Institute of Technology, Auckland, New Zealand
[τ]Department of Electrical and Computer Engineering, The University of Auckland, New Zealand
[ϒ]Department of Computer Science, The University of Auckland, New Zealand
Email: {srehman, iardekani}@unitec.ac.nz, {kw.sowerby,sala038}@aucklanduni.ac.nz

***Abstract*—RF fingerprinting aims to develop a unique RF fingerprint for a wireless device that can be used as an identity, in the same way a biological fingerprint operates, to improve the security and privacy of wireless communication. This is in contrast to the traditional bit-level algorithmic approaches to securing transmissions. In this work, we present a comprehensive overview of challenges in the deployment of RF fingerprinting in low-cost portable mobile devices including: the preliminary results showing the effect of channel impairments on RF fingerprinting accuracy and open research challenges associated with the deployment of RF fingerprinting.**

***Index Terms*—Physical Layer Security, Radio Fingerprinting, USRP, Radiometric signature**

I. Introduction

Physical layer security is a new paradigm for securing the identity of wireless devices by extracting the unique features embedded in the electromagnetic waves emitted by transmitters, called RF fingerprinting. These unique features arise from inherent randomness in the manufacturing process, particularly the presence of analog components (digital-to-analog converters, band-pass filters, frequency mixers and power amplifiers) in the radio transmission chain. RF fingerprinting has been evaluated for a number of wireless devices operating on different standards, including CRN, Universal Mobile Telecommunications System (UMTS), Wi-Fi, push-to-talk transmitters, Bluetooth and Radio-Frequency Identification (RFID). It has been found that every transmitter has a unique RF fingerprint and has also been shown that the likelihood of two transmitters having the same RF features is very low. Therefore, a unique RF fingerprint can be used to authenticate the identity of a specific wireless transmitter and provide confidentiality of the transmitted messages. Although many researchers have explored RF fingerprinting techniques, the feasibility of RF fingerprinting using today's typical portable mobile devices has not yet been successful. Researchers have not considered the limitations of the normal receiver which is built with low-cost components and has hardware imperfections embedded during the manufacturing phase. Our research work on a small number of devices has found that RF fingerprinting can be achieved with low-cost receivers for a specific transmitter-receiver pair [1], and that it is hard to reproduce an RF fingerprint from any other device that will deceive the RF fingerprinting system [2]. The dependency of RF fingerprinting on different parameters such as change in device temperature, components aging and wireless channel impairments are open research questions, which need to be addressed.

Contributions: : The main contribution of this preliminary work is an assessment of the performance of RF fingerprinting under realistic operating conditions. This paper will also discuss the open research challenges in deployment of RF fingerprinting using today's low-cost devices.

II. Performance evaluation for time-varying wireless channel

The wireless channel changes owing to movement of the objects surrounding the transceiver or owing to the transceiver itself. Therefore, a wireless channel is a continuous, time-varying process. In this work, RF fingerprint analysis was performed for three types of indoor channel: a) low multipath fading, b) medium multipath fading, and c) high multipath fading. These three channel types correspond to the situations in which the channel characteristics vary over time from low fading to high fading or vice versa. Table 1 shows the range of values a parameter can take in the simulated multipath fading channels. The range of values represents the channel characteristics in a typical indoor environment [3, 4]. All the values are assigned randomly using a uniform distribution from the given range.

Table I: The attributes of different multipath fading channels

		Multipath Fading Channel Type		
		Low	Medium	High
Attributes	Number of paths (K)	4 to 8	8 to 16	16 to 26
	Path delays (T_k) in ns	1 to 20	1 to 50	1 to 100
	Path gains (a_k) in dB	-40 to -20	-40 to -10	-20 to 0
	Doppler shifts (f_d)	4	4	4

The collected signals from our previous work [5] were passed through a simulated multipath channel and its effect on the performance of RF fingerprinting was analyzed. We have used seven similar transmitter and receivers for collecting the signals but results are shown for one receiver only [1]. Figure 1 show the classification process, where Multi-Layer Perceptron neural network is used for training and testing.

Figure 2(a-c) shows the True Acceptance (TA) Rate for the three channel models for signals captured with receiver Rx1. The simulation results show that the channel has limited effect on the classification accuracy of the RF fingerprinting. In a low-fading channel, there is almost no variation in the RF fingerprinting results. However, the classification results show that the RF fingerprinting accuracy is less in the medium-fading and high-fading channels, compared with the low-fading channel. The frequency responses of the medium and high-fading channels show that fading affects some parts of the frequency spectrum (frequency selective fading). This causes the RF fingerprint [2] of a specific transmitter to vary from signal to signal in medium and high-fading channels, and as a result the accuracy is less. However, our simulated medium and high-fading channel represents the worst case scenarios and is not typical in an indoor environment. Figure 2(d) compares the high-fading channel with the results obtained without fading. The legend "No-fad" is used for the results, when the collected signals are not passed through any faded channels described above. The "No-fad" signals represent Line-Of-Sight (LOS) signals that were captured with the transmitter and receivers in a lab environment. There is almost 5 to 10% decrease

[1] Details of equipment and data collection can be found in [5]

[2] The RF fingerprint of a transmitter is formed with Power Spectral Density coefficients of signal [5]

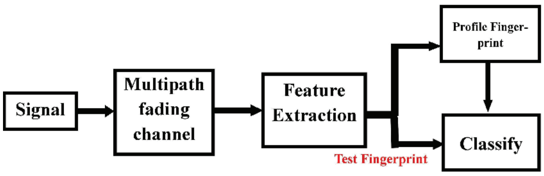


Figure 1: Classification process of RF fingerprinting

in the accuracy compared to the channel with no fading. The same trend is observed across all the seven receivers.

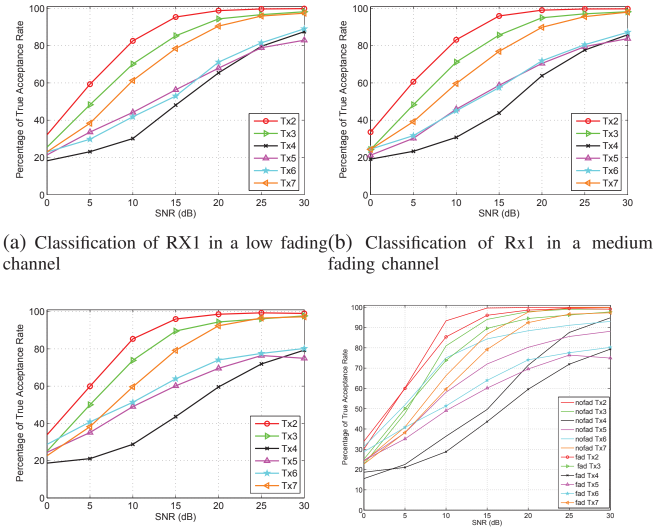
III. Conclusion and Open Research Challenges

Our preliminary simulation results show that channel impairments have limited effect on the performance of RF fingerprinting. However, our work on a real test-bed is still in progress as we are performing experiments to validate our simulation results. Furthermore, the classification results reported in this working paper were obtained when training and testing were performed with the same channel conditions, i.e. a profile RF fingerprint was created in low-fading channel conditions then the testing was performed in the same low-fading channel conditions. However, in reality, the channel characteristics change over time owing to the mobility of the transmitter and receiver or because of the movement of objects surrounding the transceivers. A profile RF fingerprint generated in one channel condition might be different from the testing fingerprint in different channel conditions. Therefore, the results might vary when classification is performed with training and testing data under different channel conditions. This will be explored in the future work.

A. Open Research Challenges

Modeling the impairments of transceivers: Majority of the previous research into RF fingerprinting has experimentally evaluated the effect of impairments present in the front end of low-end devices. Our experimental testbed consists of seven low-end transceivers, which were made of similar components. Performing experiments with a large number of receivers and transmitters would further validate our results. However, it is quite difficult to perform experiments on a large test bed owing to the cost of the equipment and the experimental time involved. Therefore, a novel theoretical framework is required, which should model the imperfections arising due to modulation errors at the modulator, phase noise at oscillators, spurious tones from mixers and Power Amplifiers (PA), nonlinearity distortion at PAs, power ramp distortions (which are associated with the transients), and distortion of the equivalent filter in the path from the digital module to the antenna (including the analog Intermediate Frequency (IF) filters and RF filters) and from various analog components in the transmission and reception chains. The theoretical model will enable the researchers to investigate the likelihood of two receivers forming the same fingerprint of a single transmitter in order to analyze the reliability and robustness of RF fingerprinting. Theoretical work should be complemented with extensive experiments involving a higher number of transmitters and receivers to validate the theoretical model.

Effect of mobility and device aging: Majority of the RF fingerprinting experiments have deployed the transmitter and receiver at a fixed location during the measurements. Therefore, variations in channel characteristics were limited. Measurements should be performed for a moveable transmitter and receiver, and data captured over many days to further investigate the effect of channel impairments. This would give an insight into any variation that can occur in an RF fingerprint over time.



(a) Classification of RX1 in a low fading channel

(b) Classification of Rx1 in a medium fading channel

(c) Classification of Rx1 in a high fading channel

(d) Comparison of classification of a high-fading channel with a no-fading channel.

Figure 2: RF fingerprinting classification accuracy for Rx1 in different fading channel.

Device aging would change the RF fingerprint, and variation in the temperature of the device and environment will also have some effects on an RF fingerprint. However, to the best knowledge of the authors, there is no research article available to support this argument. Therefore, the effect of device aging and temperature variations require further research.

To compensate for changes in the RF fingerprint that could arise over time as transmitters' age, an unsupervised fast, reliable, and computationally less expensive incremental machine-learning algorithm should be developed. The learning algorithm should be developed for portable, resource-constrained mobile devices, in contrast to existing algorithms mainly developed for computer systems. The unsupervised machine-learning algorithm should enable a wireless device to autonomously create an RF fingerprint and provide a new framework for the secrecy and privacy of the wireless device.

References

[1] S. Rehman, K. Sowerby, and C. Coghill, "Analysis of receiver front end on the performance of rf fingerprinting," in *Personal Indoor and Mobile Radio Communications (PIMRC), 2012 IEEE 23rd International Symposium on*. IEEE, 2012, pp. 2494–2499.

[2] ——, "Analysis of impersonation attacks on systems using rf fingerprinting and low-end receivers," *Journal of Computer and System Sciences*, vol. 80, no. 3, pp. 591–601, 2014.

[3] C.-D. Iskander and H.-T. Multisystems, "A matlab-based object-oriented approach to multipath fading channel simulation," *a MATLAB Central submission available in www. mathworks. com*, 2008.

[4] M. C. Jeruchim, P. Balaban, and K. S. Shanmugan, *Simulation of communication systems: modeling, methodology and techniques*. Springer, 2000.

[5] S. U. Rehman, K. W. Sowerby, and C. Coghill, "Radio-frequency fingerprinting for mitigating primary user emulation attack in low-end cognitive radios," *IET Communications*, vol. 8, no. 8, pp. 1274–1284, 2014.