Effect of Channel Impairments on Radiometric Fingerprinting

Saeed Ur Rehman*, Kevin W. Sowerby$^{\tau}$, Shafiq Alam$^{\Upsilon}$, Iman T Ardekani*, Dan Komosny$^{\Gamma}$
*Department of Computing, Unitec Institute of Technology, Auckland, New Zealand
$^{\tau}$Department of Electrical and Computer Engineering, The University of Auckland, New Zealand
$^{\Upsilon}$Department of Computer Science, The University of Auckland, New Zealand
$^{\Gamma}$Department of Telecommunications, Brno University of Technology, Czech Republic
Email: {srehman, iardekani}@unitec.ac.nz, {kw.sowerby,sala038}@aucklanduni.ac.nz, komosny@feec.vutbr.cz

***Abstract*—To increase network security and mitigate identity theft attacks, much of the research is focused on traditional bit-level algorithmic. In conventional wireless networks, security issues are primarily considered above the physical layer and are usually based on bit-level algorithms to establish the identity of a legitimate wireless device. Physical layer security is a new paradigm in which features extracted from an analog signal can be used to establish the unique identity of a transmitter. Our previous research work into Radiometric fingerprinting has shown that every transmitter has a unique fingerprint owing to imperfections in the analog components present in the RF front end. However, to the best of the author's knowledge, no such example is available in the literature in which the effect of radio channel on Radiometric fingerprint is evaluated. This paper presents the simulation and experimental results for radiometric fingerprinting under an indoor varying radio channel. Contrary to popular assumption, it was found that the fingerprinting accuracy is little affected in an indoor channel environment.**

***Index Terms*—Physical Layer Security, Radio Fingerprinting, Channel**

I. Introduction

Physical layer security is a new paradigm that provides an extra layer of security to wireless devices. Geographical information, channel response and transmitter radiometric information are different instances of physical layer security that are used to establish the identity of a wireless device. In the past few years, research into physical layer security has been gaining momentum. Physical layer security that is based on identifying a transmitter through the unique features extracted from its analog signal is called RF fingerprinting [1]. Transmitter imperfections that can produce RF fingerprints are originated from analogous components. The analog components (digital-to-analog converters, band-pass filters, frequency mixers and power amplifiers) present in the radio transmit chain are mainly responsible for the unique features [2].

RF fingerprinting broadly refers to the process of identifying the source of a transmission based on features extracted from its RF signal. The features of a signal can be classified as:

- Features specific to the channel, which describe the response of the wireless channel and its surrounding environment.
- Features specific to the transmitter, which characterize the wireless transmitter through the unique radiometric features caused by the transmitter hardware.

Xiao et al. used the channel frequency response to discriminate between a legitimate and a malicious user in an indoor WLAN office environment [3–5]. The results show that correct identification decreases with increases in distance. After a certain distance the channel responses for malicious and legitimate users become identical. Mathur et al. established a common cryptographic key between two communicating users using the channel response of a multipath channel [6]. They showed experimentally that the channel response between two communicating devices are unique and decorrelates rapidly in space. Similar approaches are used in [7, 8], in which different strategies are proposed to extract secret keys from channel state information, and to use the variability of the channel to disseminate secret keys.

RF fingerprinting based on features specific to a transmitter is also called radiometric identification. Radiometric identification uses only features originating from the transmitter hardware and totally ignores features of the channel, such as channel response. However, the transmitted signal passes through a wireless channel, which might change some of its attributes.

The main goal of RF fingerprinting is the detection of unique signal (transmitter) features that form a valid device RF fingerprint, based on which associations between observed signals and their senders can be made. The RF fingerprint of a transmitter should distinctly characterize it from other transmitters through its unique features present in the radio waveform. It is generally assumed that channel impairments and interference degrade the unique features embedded in the analog signal of a transmitter, which in turn decrease the RF fingerprinting accuracy. However, no evidence for this assumption is available in the literature. Most previously published studies have used either an anechoic chamber or a laboratory environment with high SNR and line-of-sight propagation in the experimental validation of RF fingerprinting techniques [9–13]. Such environments do not represent the typical conditions found in practice, in which transceivers are not of RF test laboratory specification, and channel impairments and interference degrade the unique features embedded in the analog signal of

the transmitter. The effects of realistic operating conditions on RF fingerprinting have not been assessed in the literature. This paper addresses this deficiency by analyzing the effect of channel impairments on the classification accuracy of RF fingerprinting using signals captured with low-end (i.e. low specification) receivers.

A. Contribution

The main contribution of this paper is an assessment of the performance of Radiometric fingerprinting under realistic operating conditions. The collected signals were passed through a simulated multipath channel and its effect on the performance of RF fingerprinting was analysed. Contrary to popular assumption, it was found that the fingerprinting accuracy is little affected in an indoor channel environment. The simulation analysis was complemented with experiments performed using the CORNET testbed of Virginia Polytechnic Institute and State University, Blacksburg, USA [14, 15].

II. Experimental Setup

An IEEE 802.11a/g standard preamble signal was generated in MATLAB and transmitted from the seven different USRP transmitters. The preamble signal was then captured with eight different receivers. The complex In-phase (I) and Quadrature (Q) signal components from different receivers were stored in a computer. The preambles were extracted from the I and Q components of the signals. The RF fingerprinting was analysed for varying Signal to Noise Ratios (SNR) that exists in a typical operational environment. The SNR was analysed by adding a power-scaled, random, complex Additive White Gaussian Noise (AWGN) to the preamble signal. The Power Spectral Density (PSD) coefficients were extracted from the noisy preamble signals to form the RF fingerprint for each transmitter; classification was then performed using a MultiLayer Perceptron Neural classifier. The details of the hardwares, experimental setup, preamble extraction and RF fingerprints formation can be found in our previous published works [16–19].

A. Data collection and RF Fingerprint

Each 802.11a/g RF burst starts with a preamble signal . The preamble signal is made up of a fixed training sequence, which is used for timing/ frequency acquisition, diversity selection and channel estimation. The IEEE 802.11a/g preamble signal is 16 microseconds long and consists of 10 short and 2 long training sequences [20]. Seven SBX daughter boards are used as low-end transmitter and receiver as explained in [17]. A total of 10,000 signals from each transmitter were captured and stored at each of the receivers, giving a total data set of 490,000 received signals.

In previous works, the RF fingerprint of transmitters is generated by extracting the frequency domain features from the steady-state signal [9, 13, 21, 22]. In this paper, the RF fingerprint consists of PSD coefficients and is given as:

$$\psi_X(k) = \frac{|X(k)|^2}{\sum_{k=1}^{K} |X(k)|^2} \tag{1}$$

where *X(k)* are the coefficients of discrete Fourier transform for the input signal *x(m)* given by

$$X(k) = \frac{1}{N_F} \sum_{m=1}^{N_F} x(m) e^{\left[\frac{-2\pi j}{N_F}(m-1)(k-1)\right]} \tag{2}$$

III. Fading Channel Models

In multipath fading, each path behaves as a discrete transmission path. Typically, the fading process for a non-line-of-sight path is characterized by a Rayleigh distribution, whereas a Rician distribution is used for a line-of-sight path. Rayleigh and Rician fading models represent realistic channel conditions, which include multipath scattering effects, time dispersion, and Doppler shifts arising from the mobility of the transceivers [23].

MATLAB has developed a simulator for Rayleigh and Rician fading channel models in Communication Toolbox, which is a direct implementation of a band-limited, discrete, multipath channel model of illustrated in [23]. The Doppler spectrum and the delay power profile are assumed separable in the multipath channel model, in which each path is modeled as a linear finite impulse-response (FIR) filter. The Rician fading channel model is used for evaluation in this paper.

Let $\{x_i\}$ denote the set of samples of the signal at the input of the channel. Then, $\{y_i\}$ are the set of samples of the signal after passing through a channel.

$$y_i = \sum_{n=N_1}^{N_2} x_{(i-n)} g_n \tag{3}$$

where $\{g_n\}$is the set of tap weights given as

$$g_n = \sum_{k=1}^{K} a_k sinc\left[\frac{\tau_k}{T_s} - n\right] \quad -N_1 \leq n \leq N_2 \tag{4}$$

where T_s is the input sample period of the channel, *K* denotes the total number of paths in the multipath channel, $\{\tau_k\}$ is the set of path delays, and a_k is the set of uncorrelated complex path gains in the multipath channel. Full implementation detail of the fading channel can be found in [24].

IV. Performance Analysis

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 paper, Radiometric 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 [23, 24]. 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

Doppler shifts arise owing to the relative motion of the transmitter and receiver. Doppler shifts are generally specified in terms of the speed of the transceiver [23] and are given as

$$f_d = \frac{vf}{c} \tag{5}$$

where f is the transmission frequency (ISM band), c is the speed of light ($3x10^8$) and v is the speed of the transceiver. For an indoor environment, the speed of the transceiver was assumed to be 0.5 m/s. In our simulations, the channel changes randomly for every signal passed through it.

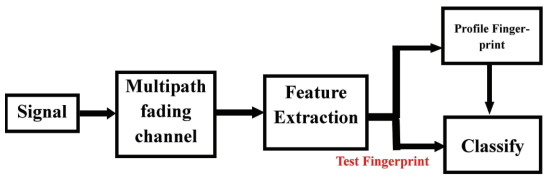

Figure 1. Signals are passed through low, medium and high multipath fading channels. Classification, training and testing are performed with signals in the same channel condition.

Figure 1 shows the simulation strategy used to analyze RF fingerprinting under different channel conditions. The collected signals were passed through the three channel models, and then the PSD features were extracted to form profile RF fingerprints of the transmitters. Classification was performed using the MLP Artificial Neural Network.

Figure 2 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 marginally 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 of a specific transmitter to vary from signal to signal in medium and high-fading channels, and as a result the accuracy is less.

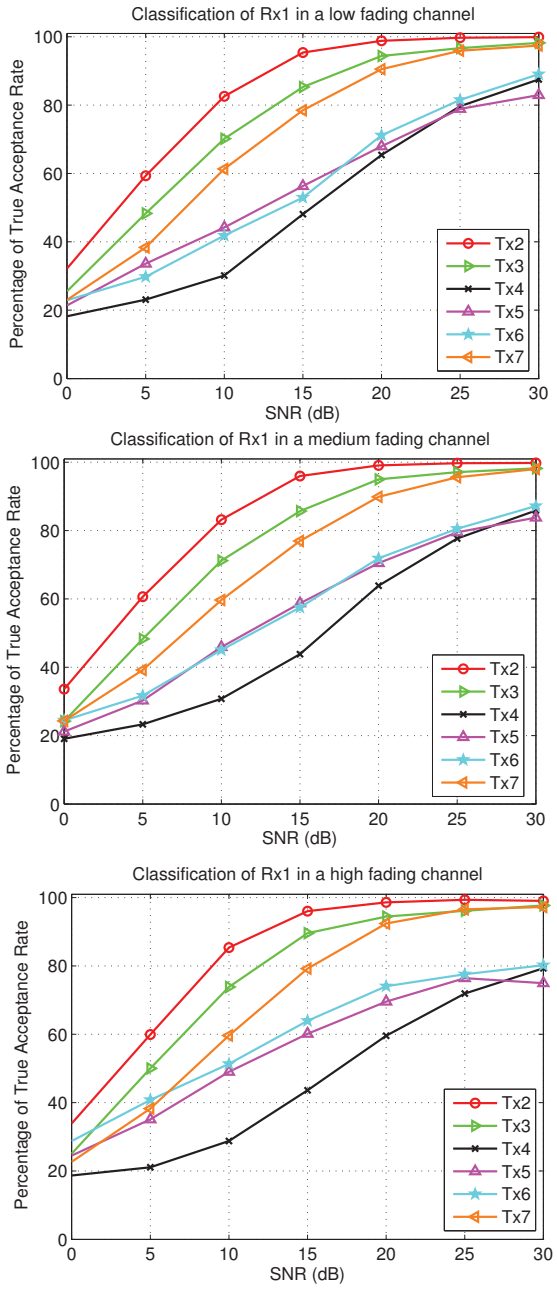

Figure 2. RF fingerprinting classification accuracy for Rx1 in different fading channel.

V. PROFILE RF FINGERPRINTS IN VARYING CHANNEL CONDITIONS

The classification results of Figure 2 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

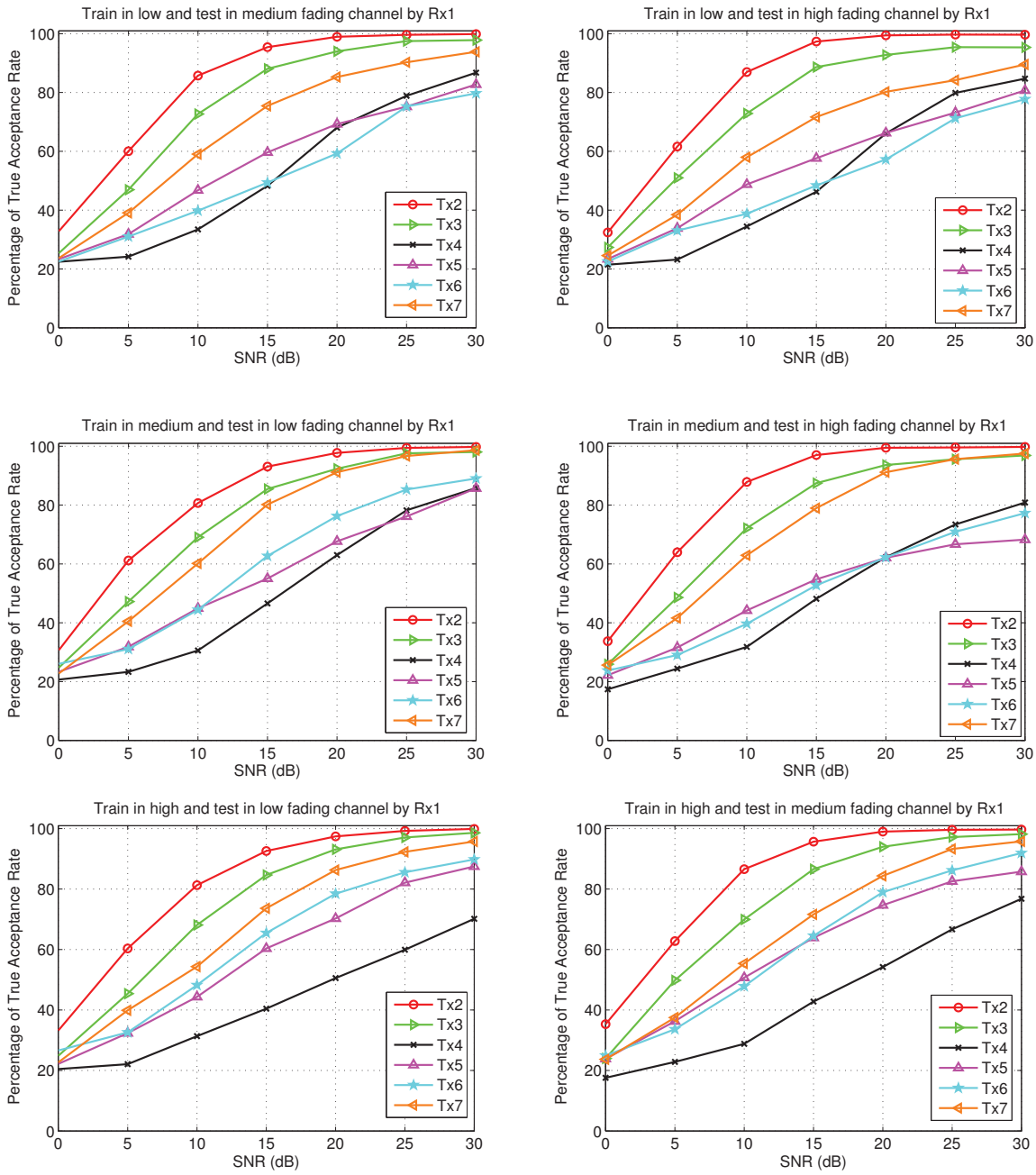

Figure 3. RF fingerprinting classification accuracy for Rx1 in different fading channel.

conditions. Therefore, a simulation was performed to analyse the accuracy of RF fingerprinting under varying channel conditions. Three scenarios were simulated, which correspond to the following situations:

1) The first scenario considered the situation in which profile RF fingerprints were generated in a low-fading environment and later, the channel environment changed from low-fading to medium or high-fading. In this scenario, the profile RF fingerprints of transmitters were generated with the signals passed through the low-fading channels. Then testing in the classifier was implemented with signals passed through medium and high-fading channels.
2) In the second scenario, profile RF fingerprints for each transmitter were generated in a medium-fading environment, and testing was carried out with signals from low and high-fading environments.
3) In the third scenario, a high-fading channel was used for creating the profile RF fingerprints, while testing was implemented for low and medium-fading environments.

Figure 3 shows the simulation results of receiver Rx1 for the three scenarios described above. The results show that the True Acceptance rates decreased slightly when the profile fingerprint was generated in a channel environment different

from the testing environment. A low-fading environment does not distort the features in the signal and thus a receiver can form a unique profile fingerprint and associate it with a specific transmitter. Later, if the channel changed from low-fading to high-fading, some of the features would be lost. However, the classifier would be able to classify the transmitter correctly owing to the availability of a unique profile fingerprint formed earlier in a low fading-channel. This is evident from the high accuracy of the results for scenario 1, in which the profile fingerprint was generated in a low-fading environment, as shown in Figure 3 (a) and (b). In both cases (Figures 3 (a) and (b)) , the accuracy of the transmitters was almost the same as compared to scenarios 2 and 3. However, the accuracy was still less than in the results plotted in Figure 2, in which training and testing were performed using the same channel. The results for scenario 2 are plotted in Figure 3 (c) and (d), and for scenario 3 in Figure 3 (e) and (f), respectively. The accuracy varies in both scenarios 2 and 3, in which the profile fingerprint was generated in medium-fading and high-fading environments.

Our analysis showed that generating the profile fingerprint in the same channel increased the accuracy significantly (as shown in Figure 2). Nevertheless, training and testing in different channel conditions yield acceptable accuracy. Results were obtained for receiver Rx2 to Rx7, which show the same trend. However, due to the space limitation, it is not given here.

VI. CORNET Testbed

The Cognitive Radio Network Testbed (CORNET) is an open source Software Defined Radio (SDR) platform that is deployed in a four-story building, Kelly Hall, at Virginia Polytechnic Institute and State University, Blacksburg, USA [14, 15]. The CORNET testbed consists of 48 USRP2 nodes, which are scattered throughout the building. Twelve nodes are installed on each each floor [25]. The USRP2 can operate at 50 MHz of instantaneous bandwidth. The USRP2 are equipped with WBX daughterboards [26] as well a Radio Frequency Integrated Circuit (RFIC) daughterboard custom developed at Virginia Tech [15]. The WBX and RFIC daughterboards cover the frequency ranges 50 MHz - 2200 MHz and 100 MHz - 4 GHz, respectively. The USRP2s are connected to a centrally-located cluster of rack servers through Gigabit Ethernet. The servers provide a high-performance General Purpose Processor (GPP) environment for real-time software-based signal processing. All the nodes are centrally accessed using a web-based application.

During our research visit to the CORNET lab, In our extensive experiments we found only three nodes (on Floor 2) that were able to receive signals from each other. The rest of the nodes were either malfunctioning (software and network issues) or had weak signal reception owing to the concrete structure of Kelly Hall., and were therefore inappropriate to our purposes.

An IEEE802.11a/g preamble signal was generated and received on different USRPs at 5 pm, 6 pm and the next day at 11 am. A total of 5000 signals from each transmitter

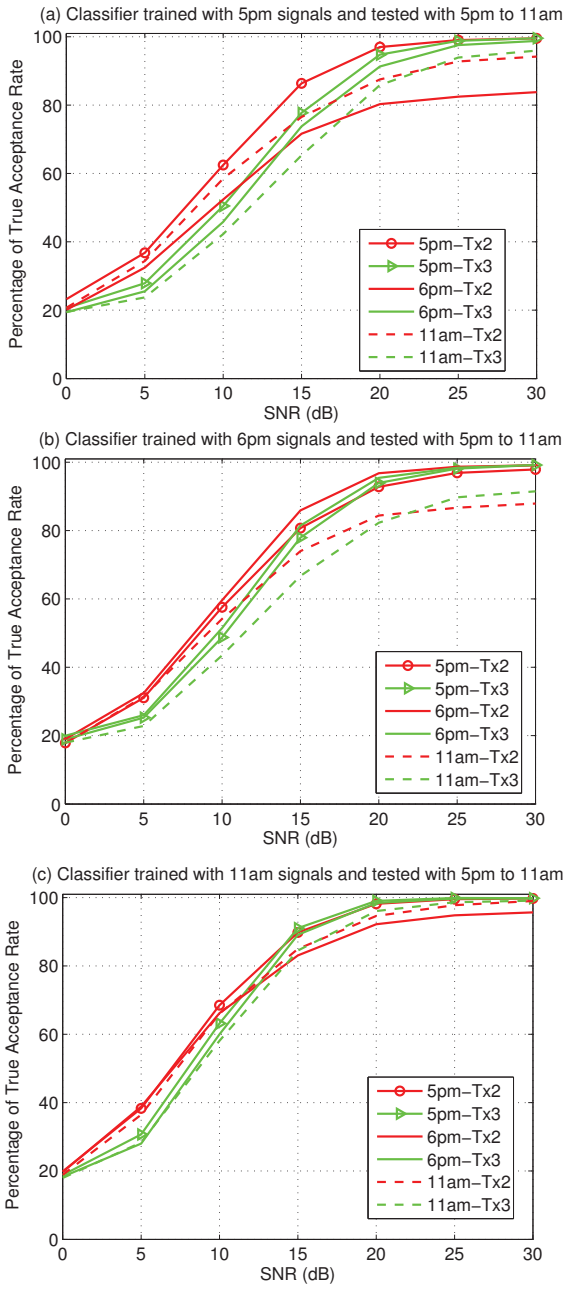

Figure 4. Classification for the data captured with Rx1. The profile fingerprint is generated with data captured at different time than the data used for testing.

were collected at the different receivers at one particular time. To avoid any commonalities between the transmit and receive chains, either a transmit or receive chain of a daughterboard was used for the measurements. Then preamble signals were extracted and the classification results were obtained using a MLP neural network.

Figure 4 shows the True Acceptance rate for receiver Rx1, in which the profile RF fingerprint was generated for the signals captured at a time different from the signals used for testing. In Figure 4, the legend with a "marker" depicts the classification results obtained when training and testing were implemented for the signals captured at the same time. The legends without a "marker" are for the classification results obtained when

training and testing were performed for the signals that were captured at a different time. Figure 4 (a) shows the results obtained when the profile fingerprint was generated for the signals captured at 5pm and testing was performed for the signals captured from 5pm to 11am. The results show that the accuracy is the same for all cases, which implies that the RF fingerprint of a transmitter is little affected by the channel. The results for receiver Rx2 and Rx3 were also obtained that showed the same trend as observed for receiver Rx1.

There are some limitations to the results obtained using the CORNET testbed: 1) measurements spanned only two days; time was limited and much of it was spent testing and rectifying the testbed. 2) the research trip was made during Virginia Tech's summer holidays, so, there was limited movement in the building hallways where USRPs were installed and thus minimum variation in the channel characteristics.

However, in spite of its limitations, the CORNET testbed provided some useful results that support our simulation results. In future, more experiments will be performed on a larger testbed spanning many days to validate the simulation results.

VII. Summary

This paper has analysed the effect of channel impairments on an RF fingerprint in an indoor environment. Our results show that channel impairments have limited effect on the performance of RF fingerprinting. Our results are supported by the experiments performed on the CORNET testbed. Furthermore, the profile fingerprint was generated in a channel condition different from the testing condition in order to analyse the effect of variations in the channel characteristics that might arise from movement of transmitter and receiver or the surrounding environment. Our results show that a profile fingerprint generated in a low-fading channel is likely to give accurate results as compared to those generated in the medium and high-fading channels.

References

[1] B. Danev, H. Luecken, S. Capkun, and K. El Defrawy, "Attacks on physical-layer identification," in *Proc. ACM Conf on Wireless network security*, 2010, pp. 89–98.

[2] K. Gard, L. Larson, and M. Steer, "The impact of rf front-end characteristics on the spectral regrowth of communications signals," *Microwave Theory and Techniques, IEEE Transactions on*, vol. 53, no. 6, pp. 2179–2186, 2005.

[3] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the ether: Using the physical layer for wireless authentication," in *Communications, 2007. ICC'07. IEEE International Conference on*. IEEE, 2007, pp. 4646–4651.

[4] ——, "Using the physical layer for wireless authentication in time-variant channels," *Wireless Communications, IEEE Transactions on*, vol. 7, no. 7, pp. 2571–2579, 2008.

[5] ——, "Fingerprints in the Ether: Channel-Based Authentication," *Securing Wireless Communications at the Physical Layer*, pp. 311–333, 2010.

[6] S. Mathur, A. Reznik, C. Ye, R. Mukherjee, A. Rahman, Y. Shah, W. Trappe, and N. Mandayam, "Exploiting the physical layer for enhanced security [security and privacy in emerging wireless networks]," *Wireless Communications, IEEE*, vol. 17, no. 5, pp. 63–70, 2010.

[7] Q. Li and W. Trappe, "Detecting spoofing and anomalous traffic in wireless networks via forge-resistant relationships," *Information Forensics and Security, IEEE Transactions on*, vol. 2, no. 4, pp. 793–808, 2007.

[8] R. Chen, J. Park, and J. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *Selected Areas in Communications, IEEE Journal on*, vol. 26, no. 1, pp. 25–37, 2008.

[9] I. Kennedy, P. Scanlon, and M. Buddhikot, "Passive steady state rf fingerprinting: a cognitive technique for scalable deployment of co-channel femto cell underlays," in *New Frontiers in Dynamic Spectrum Access Networks, 2008. DySPAN 2008. 3rd IEEE Symposium on*. IEEE, 2008, pp. 1–12.

[10] A. Polak, S. Dolatshahi, and D. Goeckel, "Identifying wireless users via transmitter imperfections," *Selected Areas in Communications, IEEE Journal on*, vol. 29, no. 7, pp. 1469–1479, 2011.

[11] J. Toonstra and W. Kinsner, "A radio transmitter fingerprinting system ODO-1," in *Electrical and Computer Engineering, 1996. Canadian Conference on*, vol. 1. IEEE, 2002, pp. 60–63.

[12] S. U. Rehman, K. Sowerby, and C. Coghill, "Rf fingerprint extraction from the energy envelope of an instantaneous transient signal," in *Communications Theory Workshop (AusCTW), 2012 Australian*, 30 2012-feb. 2 2012, pp. 90 –95.

[13] W. Suski II, M. Temple, M. Mendenhall, and R. Mills, "Radio frequency fingerprinting commercial communication devices to enhance electronic security," *International Journal of Electronic Security and Digital Forensics*, vol. 1, no. 3, pp. 301–322, 2008.

[14] (2013) Cornet. [Online]. Available: http://cornet.wireless.vt.edu/

[15] D. R. DePoy, "Cognitive radio network testbed (cornet): Design, deployment, administration and examples," Ph.D. dissertation, Virginia Polytechnic Institute and State University, 2012.

[16] 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.

[17] ——, "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.

[18] ——, "Experimental analysis of channel impairments on the performance of rf fingerprinting using low-end receivers," in *9th Annual wireless virginia summer school*. Virginia Tech, 2013.

[19] ——, "Rf fingerprinting for mitigating primary user emulation attack in low-end cognitive radio's," *Accepted with minor correction in IET Journal of Communication*, 2014.

[20] I. C. S. L. M. S. Committee *et al.*, "Ieee 802.11: Wireless lan medium access control and physical layer specifications," 1999.

[21] P. Scanlon, I. Kennedy, and Y. Liu, "Feature extraction approaches to rf fingerprinting for device identification in femtocells," *Bell Labs Technical Journal*, vol. 15, no. 3, pp. 141–151, 2010.

[22] I. Kennedy, P. Scanlon, F. Mullany, M. Buddhikot, K. Nolan, and T. Rondeau, "Radio transmitter fingerprinting: A steady state frequency domain approach," in *Vehicular Technology Conference, 2008. VTC 2008-Fall. IEEE 68th*. IEEE, 2008, pp. 1–5.

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

[24] 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.

[25] (2013) Cornet floor plan. [Online]. Available: http://trac.cornet.wireless.vt.edu/NetworkTopography/floor2.php

[26] M. Ettus, "Transceiver daughterboards for the usrp software radio system," *Ettus Research LLC,[Online*, 2008.