Portability of an RF Fingerprint of a Wireless Transmitter

Saeed Ur Rehman[*], Shafiq Burki [ϒ], Iman T Ardekani[*]
[*]Department of Computing, Unitec Institute of Technology, Auckland, New Zealand
[ϒ]Department of Computer Science, The University of Auckland, New Zealand
Email: {srehman, iardekani}@unitec.ac.nz, sala038@aucklanduni.ac.nz

***Abstract*—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 RF fingerprinting has shown that every transmitter has a unique RF fingerprint owing to imperfections in the analog components present in the RF front end. Generally, it is believed that the RF fingerprint of a specific transmitter is same across all receivers. That is, a fingerprint created in one receiver can be transported to another receiver to establish the identity of a transmitter. However, to the best of the author's knowledge, no such example is available in the literature in which an RF fingerprint generated in one receiver is used for identification in other receivers. This paper presents the results of experiments, and analyzing the feasibility of using an universal RF fingerprint of a transmitter for identification across different receivers.**

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

I. Introduction

The continued proliferation of inexpensive wireless Radio Frequency (RF) devices provides worldwide communication connectivity to virtually every individual. These wireless devices broadcast information to intended recipients in the form of an electromagnetic emission. Due to broadcast nature of wireless communication, the unintended recipient may simply listen to the communication activity and remain passive – an activity that is difficult to detect – or may become active and compromise the identity of the wireless device by launching "spoofing" or "man in the middle" type attacks [1]. Much of the current research is focused on traditional bit-level algorithmic approaches to improving network security and mitigating spoofing attacks. However, the security algorithm would be compromised upon access to the key, thus making it difficult to distinguish between a legitimate and a cloned key/device [2]. For example, the Medium Access Control (MAC) address of a network interface card can be changed in software [3]. The Electronic Serial Number (ESN) and Mobile Identification Number (MIN) of a cellular phone can be changed by replacing the Erasable Programmable Read Only Memory (EPROM), hence allowing a modification of its identity [4]. Additionally, higher-layer security key distribution and management may be difficult to implement and may be vulnerable to attacks in some environments, such as ad hoc or relay networks, in which transceivers may join or leave randomly [5, 6]. Furthermore, some recent wireless technologies do not allow an interactive communication for establishing a cryptography key owing to their unique architecture. One such example is a Cognitive Radio Network (CRN), which was invented in order to increase the efficiency of spectrum usage. If a Primary User Emulation (PUE) attack is launched then the whole operation of CRN is jeopardized by effectively limiting the access of legitimate users to idle spectrum [7]. Thus the compromised identity of wireless devices creates vulnerability to a variety of attacks, which can take the form of impersonation, intrusion, theft of bandwidth and denial of service.

More recently, consideration has been given to detecting and mitigating spoofing near or at the bottom of the Open Systems Interconnection (OSI) network stack. One such work includes the addition of a "lightweight security layer" hosted within the MAC layer to detect spoofing and anomalous traffic [8]. Other recent efforts have focused on Physical (PHY) layer implementations with the goal of exploiting RF characteristics (radio and environmental) that are difficult to mimic, thus minimizing opportunities for spoofing. Hence, identity theft can be effectively tackled using physical layer security.

Physical layer security is a new concept for securing the identity of wireless devices by extracting the unique features embedded in the electromagnetic waves emitted by the transmitters [9, 10]. These unique features arises due to the modulation errors from the modulator, phase noise from oscillators, spurious tones from mixers and Power Amplifiers (PA), non-linearity distortion from 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 chain [11]. Physical layer security that is based on recognizing these unique features is known as Radio Frequency (RF) fingerprinting [12]. The results published in our previous research work have shown that similar transmitters (same manufacturer and model) can have different RF fingerprint, which helps in identification [13–15]. This paper further investigates into the portability of an RF fingerprint across different receivers. The portability of an RF fingerprint can have different applications such as enabling regulatory authorities to identify a wireless intruder/interferer in a network and enable policing of the wireless spectrum

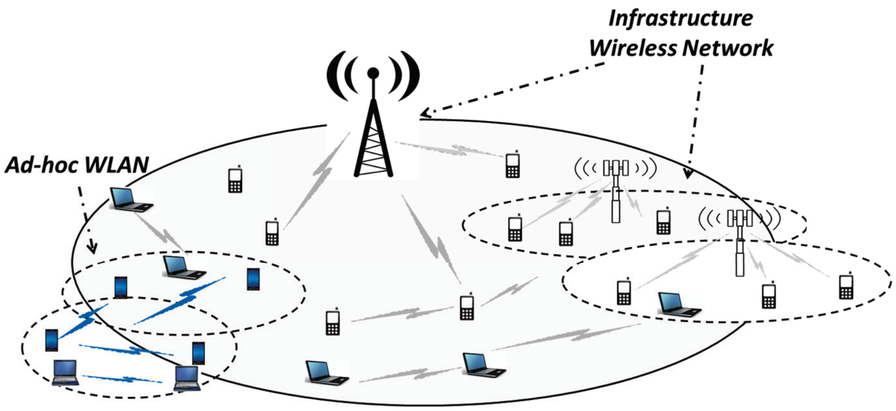


Figure 1: RF fingerprinting evaluation in ad hoc and infrastructure wireless networks

through identification of illegal wireless transmitters.

The main contribution of this paper is an investigation into the portability of an RF fingerprint across different receivers in two scenarios, namely (1) infrastructure and (2) ad hoc wireless network, as shown in Figure 1. In the infrastructure scenario, a high-end receiver was used for generating profile RF fingerprints of transmitters whereas in the ad hoc scenario, profile RF fingerprints were generated using low-end receivers. These profile RF fingerprints were used for identification in the low-end receivers. In this paper, "high-end receiver" means a receiver front-end built with high quality analog components, which can cost up to thousands of dollars. A "low-end receiver" means a receiver front-end built with inexpensive analog components, which might cost no more than a few hundred dollars.

The rest of the paper is organized as follows. Section II describes the experimental setup, including preamble/ feature extraction and data collection. Section III explains the classification process used in this paper. Section IV discusses performance evaluations for infrastructure and Ad hoc scenarios. Section V concludes the paper with a summary and identifies avenues for future research.

II. Experimental Setup

Figure 2 shows the overall experimental setup that was used for collecting the data from different transmitters and receivers. The red and blue dashed boundaries show the processes that were implemented in hardware and in software, respectively. 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 classifier. The details of the hardwares, experimental setup, preamble extraction and RF fingerprints formation can be found in our previous published works [14–17]. Data collection and classification process is explained in next subsection.

A. Data collection

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 [18]. Seven SBX daughter boards are used as low-end transmitter and receiver as explained in [15]. 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.

III. Classification Process

The RF fingerprinting process consists of two phases: namely training and testing. In the training phase, a specific transmitter's signals were used to create the profile RF fingerprint for that transmitter. Whereas in the testing phase, an RF fingerprint was created from an input test signal. Then a trained classifier was used to classify this test RF fingerprint against the existing profiles of the transmitter. The RF fingerprinting computational complexity is largely dependent on the RF feature extraction technique. Our technique involves two steps in creating the RF fingerprint from a received signal: a) extracting the signal of interest (i.e., preamble); b) creating the RF fingerprint from PSD coefficients. The PSD coefficients are calculated using the Fast Fourier Transform (FFT), which is computationally inexpensive and can be implemented using today's low power DSP chips [19, 20]. Once an RF fingerprint is created then the rest of computational complexity is dependent on the classifier. A commonly used Multi-Layer Perceptron (MLP) neural network was used for identification in this research work [21, 22], although other simpler classifiers like K-Nearest Neigbor (KNN) can be used,

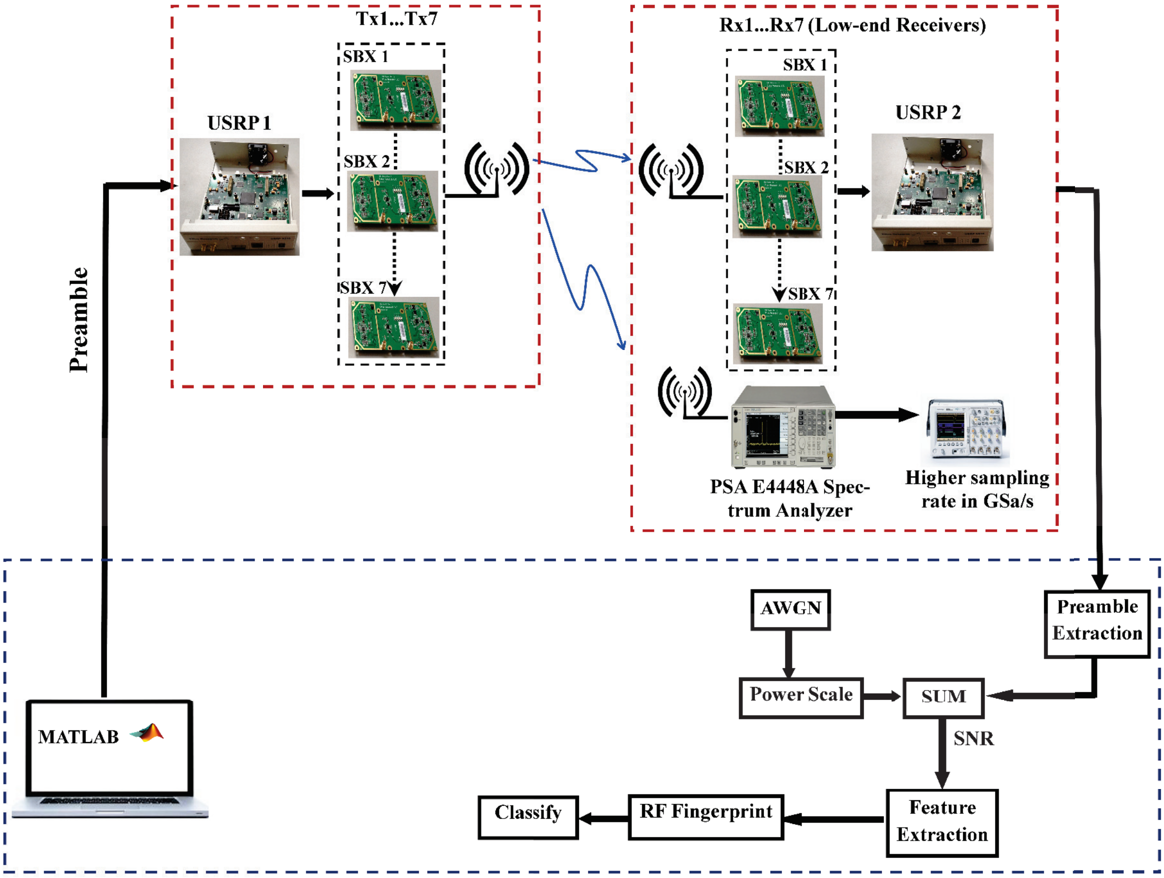


Figure 2: Overall RF fingerprinting analysis process for preamble signal generation, transmission/reception, SNR analysis, RF fingerprint creation and classification.

Table II: **Confusion matrix for a system trained with high-end receivers signals. The confusion matrix is obtained for signals collected at 15 dB SNR. The confusion matrix shows predictions in percentage.**

(a) Testing using signals received with low-end Rx 7

		Predicted Class of transmitters					
		Tx1	Tx2	Tx3	Tx4	Tx5	Tx6
Actual Class	Tx1	**0.1**	0	0.1	0	99.7	0
	Tx2	0	**0**	2.5	0.3	96.8	0.1
	Tx3	0	0.2	**0.1**	0	99.6	0
	Tx4	0.1	0.2	0.3	**0**	99.2	0
	Tx5	0.1	0.7	0.4	0.1	**98**	0.4
	Tx6	0	0.1	0.3	0	99.3	**0.1**

which we have demonstrated in our previous work [14, 15]. In both the scenarios, the K-fold cross validation technique was used for assessing the overall performance.

IV. Performance evaluation

Figure 1 shows an infrastructure wireless network, in which all of the wireless devices report to the central node in order to establish a communication link. A cellular phone network is a typical example, in which a central base station disseminates information to the cellular phones. The central node is assumed to be a highly specialized node with a high-end receiver front end. The central node performs training in order to create a profile fingerprint of each the transmitter. Then these profiles are distributed to the low-end wireless devices through a secure channel. The following is the rationale for creating a profile RF fingerprint in a high-end receiver

- First, the front-end of low-end devices are built with imperfect analog components, which are unable to create unique profile RF fingerprints of transmitters. Therefore, the burden of creating the profile RF fingerprint is left to the central node, which is equipped with a specialized receiver.
- Second, the central node keeps a record of the profile RF fingerprints of all the transmitters with whom it has communicated. If a wireless node behaves suspiciously or an interfering node appears in the network then the central node can disseminate the profile RF fingerprints of the problematic node to the other low-end devices, which can then take action to thwart the effects of the problem node.

Figure 1 shows an ad hoc wireless network in which all of the wireless nodes have the same specifications. An ad hoc wireless network is formed without the presence of a

Table I: **Confusion matrix for a system trained with high-end receivers signals. The confusion matrix is obtained for signals collected at 15 dB SNR. The confusion matrix shows predictions in percentage.**

(a) Testing using signals received with low-end Rx 1

		Predicted Class of transmitters					
		Tx2	Tx3	Tx4	Tx5	Tx6	Tx7
Actual Class	Tx2	**0.2**	0	5.8	0.1	0.2	93.3
	Tx3	1	**0**	2.8	0.1	0.2	95.6
	Tx4	0.3	0	**0.4**	0.2	0.2	98.6
	Tx5	0.3	0	0.2	**0.2**	0.1	98.9
	Tx6	0	0	0	0	**0.1**	99.8
	Tx7	0	0	0	0	0	**99.8**

(b) Testing using signals received with low-end Rx 2

		Predicted Class of transmitters					
		Tx1	Tx3	Tx4	Tx5	Tx6	Tx7
Actual Class	Tx1	**0**	0	0	1.5	0	98.4
	Tx3	0	**0**	0.1	2.3	0	97.3
	Tx4	0	0	**0.19**	1.7	0	97.9
	Tx5	0	0	0	**1.7**	0	98.2
	Tx6	0	0	0.1	1.4	**0.1**	98.2
	Tx7	0	0	0	0.8	0.1	**98.9**

(c) Testing using signals received with low-end Rx 3

		Predicted Class of transmitters					
		Tx1	Tx2	Tx4	Tx5	Tx6	Tx7
Actual Class	Tx1	**0**	0	0	0.7	0	99.2
	Tx2	0	**0**	0.1	0.7	0	99
	Tx4	0	0.1	**0.1**	1	0	98.6
	Tx5	0	0	0	**0.6**	0	99.2
	Tx6	0	0.3	0.2	1.8	**0.1**	97.3
	Tx7	0	0.1	0	0.9	0	**98.8**

(d) Testing using signals received with low-end Rx 4

		Predicted Class of transmitters					
		Tx1	Tx2	Tx3	Tx5	Tx6	Tx7
Actual Class	Tx1	**0**	0	0	0	0	100
	Tx2	0	**0**	0	0	0	100
	Tx3	0	0	**0**	0	0	99.9
	Tx5	0	0	0	**0**	0	99.9
	Tx6	0	0	0	0.1	**0**	99.8
	Tx7	0	0	0	0.9	0	**98.9**

(e) Testing using signals received with low-end Rx 5

		Predicted Class of transmitters					
		Tx1	Tx2	Tx3	Tx4	Tx6	Tx7
Actual Class	Tx1	**0**	0	0	0	0	99.9
	Tx2	0	**0**	0	0	0	100
	Tx3	0	0	**0**	0	0.2	99.6
	Tx4	0	0	0	**0**	0.1	99.7
	Tx6	0	0	0	0	**0**	100
	Tx7	0	0	0	0	0.1	**99.8**

(f) Testing using signals received with low-end Rx 6

		Predicted Class of transmitters					
		Tx1	Tx2	Tx3	Tx4	Tx5	Tx7
Actual Class	Tx1	**0**	0	0	0	0	99.9
	Tx2	0	**0**	0	0.1	0	99.8
	Tx3	0.1	0.1	**0**	0.4	0.7	98.3
	Tx4	0.2	0.3	0	**0.5**	0.3	98.3
	Tx5	0	0.4	0	0.7	**0.7**	98
	Tx7	0	0	0	0	0	**99.8**

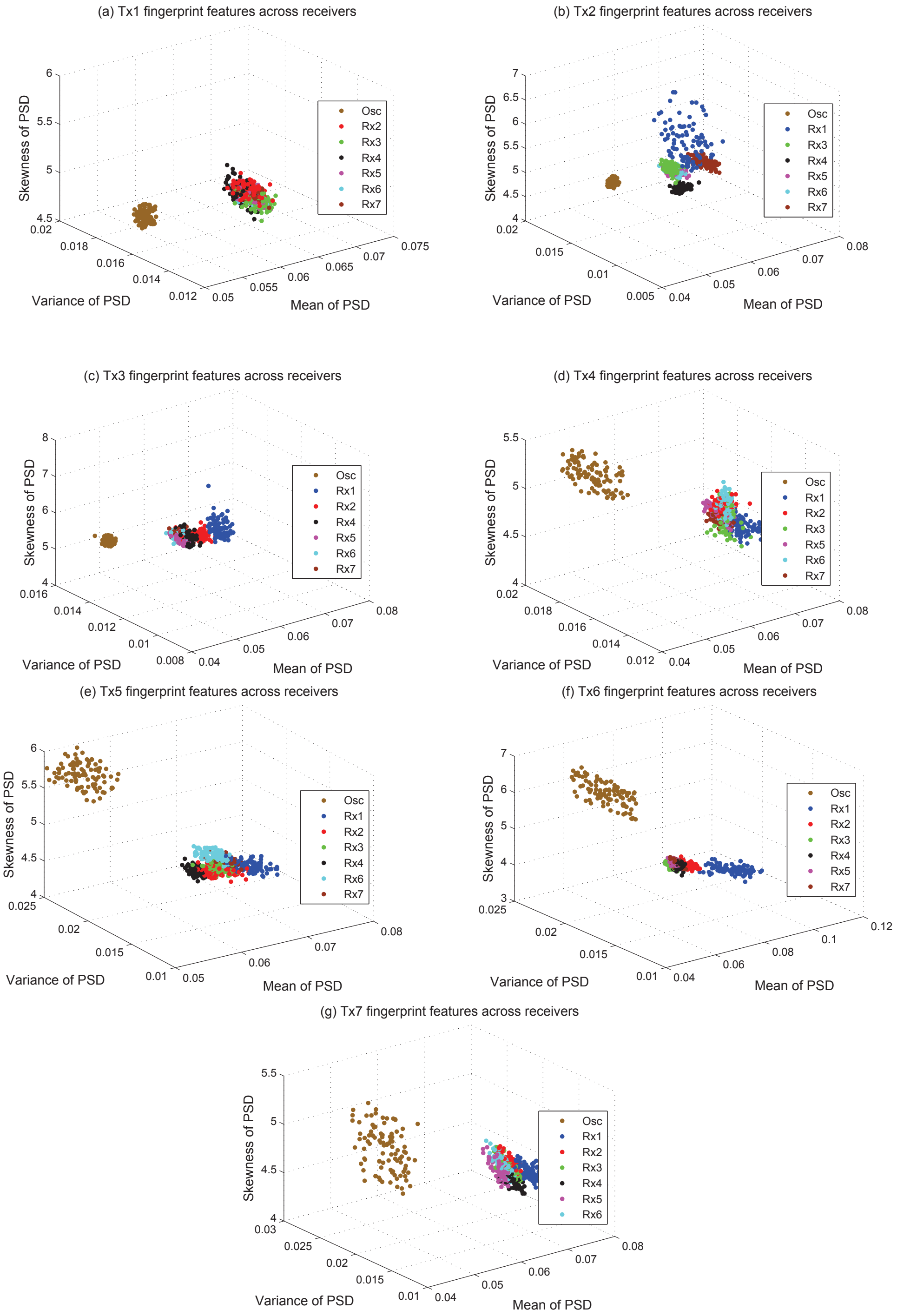
central node. In an ad hoc network, it is assumed that all the wireless devices are equipped with a front end built with inexpensive analog components. Every low-end receiver implements training and creates a profile RF fingerprint of the wireless devices in the ad hoc wireless network because there is no specialized centralized node. Once a profile is created, it is tested by matching the RF fingerprint of a received signal against the already stored profiles. If a match is found then a wireless device is considered to be a legal transmitter; otherwise it is considered to be an attacker.

In both scenarios, the profile RF fingerprint of wireless devices can be created during the initialization phase of a wireless network such as LTE, IEEE 802.16 [23], IEEE 802.11 [18] and IEEE 802.22 [24]. The initialization phase involves registration, key exchange and synchronization of wireless devices [24–26]. This sequence of requests and responses provides an opportunity to create the profile RF fingerprint of legitimate wireless devices. Later on, if an impersonation attack is launched, then the attacker's RF fingerprints are checked against the existing RF fingerprint profiles of users stored in the low-end devices. If a match is not found then it would be identified as being an impersonation attack.

A. Scenario 1: - Infrastructure Wireless Radio Network

In this scenario, the high-end receiver acts as a specialized central radio node and the profile RF fingerprints of the seven transmitters are created with the preamble signals collected by the high-end receiver. Signals captured from all seven transmitters by the low-end receivers are used for testing the effectiveness of the fingerprinting scheme.

Tables 1 and 2 show the confusion matrix at 15 dB SNR for seven low-end receivers. Table 1 shows that each low-end receiver (from 1 to 6) incorrectly identifies all transmitters as Tx7. Low-end receiver Rx7 incorrectly identifies all transmitters as Tx5. In other words, the low-end receivers cannot rely on the profile fingerprints recorded by the high-end receiver



(a) Tx1 fingerprint features across receivers

(b) Tx2 fingerprint features across receivers

(c) Tx3 fingerprint features across receivers

(d) Tx4 fingerprint features across receivers

(e) Tx5 fingerprint features across receivers

(f) Tx6 fingerprint features across receivers

(g) Tx7 fingerprint features across receivers

Figure 3: Receivers create different RF fingerprints for the same set of transmitters at 15dB SNR. In the feature space, the RF fingerprint created by the high-end receiver is far away from the fingerprint created by the low-end receivers. Note that the USRP daughterboards have different chains for transmission and reception [27]. In order to avoid any commonalities between the transmit and receive chains, either the transmit chain or the receive chain of a daughterboard was used; both were not used at the same time (e.g. when Rx1 was used for capturing the transmitter signals, Tx1 was not captured as it was implemented on the same daughterboard).

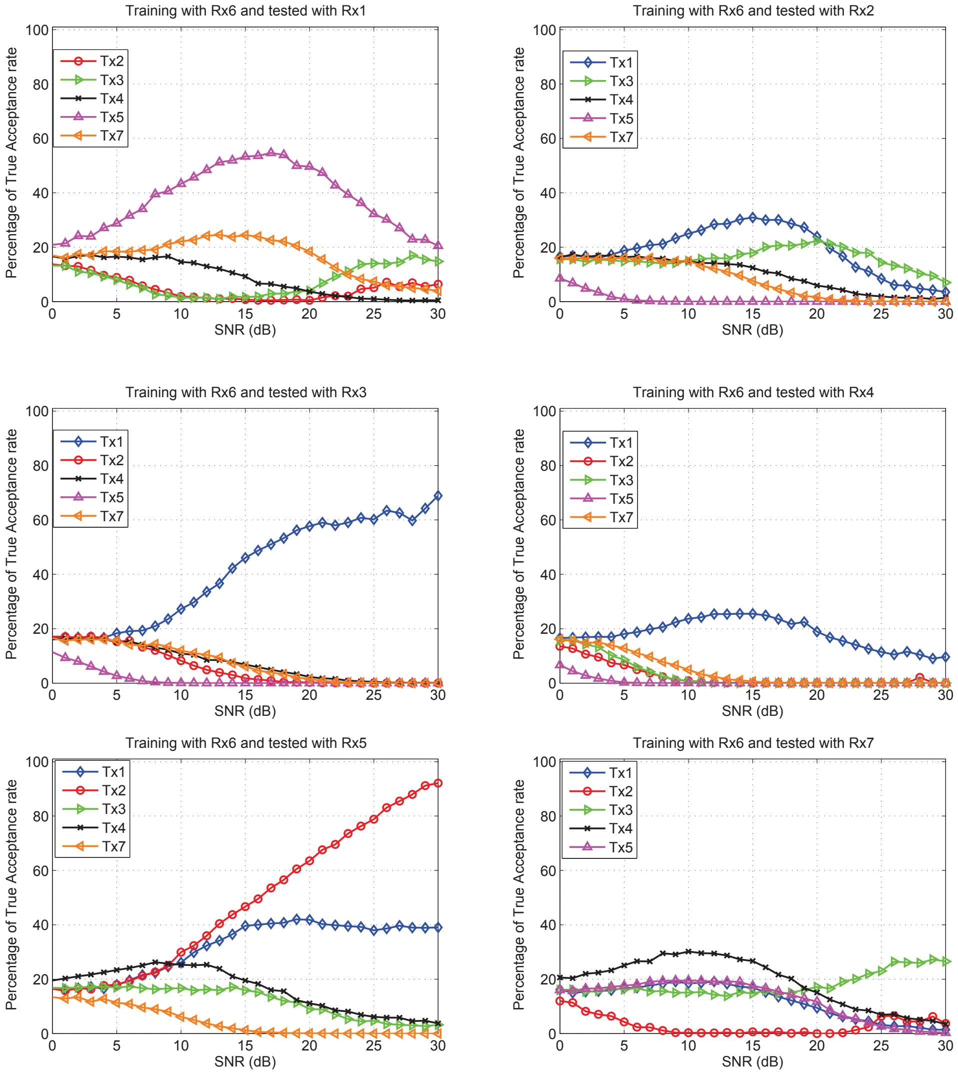


Figure 4: Profile RF fingerprint of transmitters are generated with the signals captured by Rx 6 and testing is performed with signals captured by other receivers.

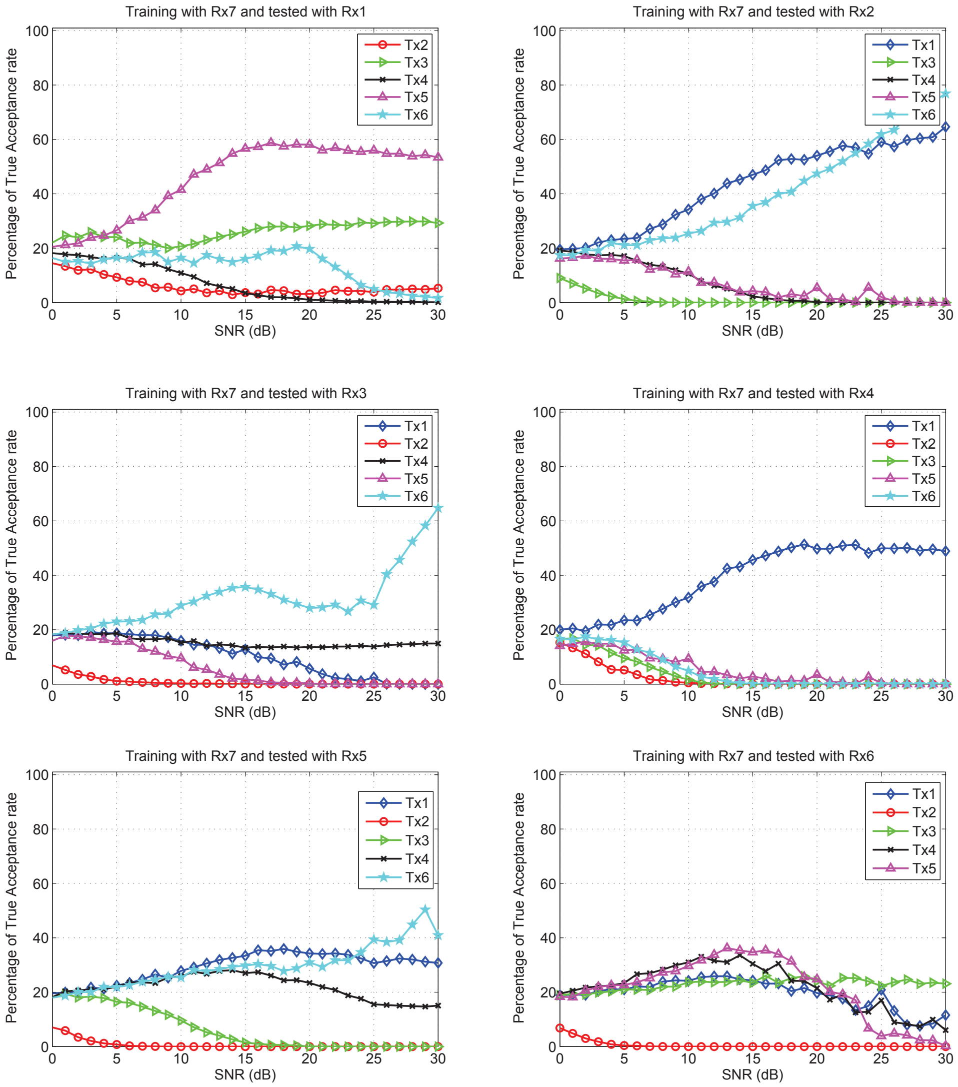
because the low-end receivers (and their impairments) create fingerprints different from those of the high-end receiver. Figure 3 illustrates how different the high-end fingerprint of a transmitters is from the low-end fingerprints of the same transmitters. Such differences make accurate classification unlikely.

The RF fingerprint created with a high-end receiver cannot be reliably transferred to a low-end receiver without compensating for the imperfections of the receivers. The results suggest that, because of their imperfections, every receiver forms a different RF fingerprint for the same transmitter, so the RF fingerprints generated in a single receiver cannot be used as a universal RF fingerprint of the transmitter. If a legitimate transmitter fingerprint created with a high-end receiver is used for identification in a low-end receiver then the low-end receiver would be likely to identify the legitimate transmitter as malicious. This implies that RF fingerprinting is not a viable option for mitigating impersonation attacks in an infrastructure wireless network, in which a profile RF fingerprint is created with a high-end receiver different from the one being used for testing.

B. Scenario 2: - Ad hoc Wireless Network

In the ad hoc wireless network analysis, the profile RF fingerprints of seven transmitters were created with signals captured by low-end receivers and tested also with low-end receiver signals. In the analysis, simulated Additive White Gaussian Noise (AWGN) was added to the collected signals in order to assess the effect of SNR.

Figure 3 shows that every low-end receiver forms its own RF fingerprint from the received signal of the same transmitter. To investigate further that the RF fingerprint of a specific transmitter varies across all receivers or it is limited to a specific receiver, we trained our MLP neural network with the signals captured by one low-end receiver and tested with the signals captured by the other receivers. For example, the profile RF fingerprints of Tx2 to Tx7 were created with the



Training with Rx7 and tested with Rx1

Training with Rx7 and tested with Rx2

Training with Rx7 and tested with Rx3

Training with Rx7 and tested with Rx4

Training with Rx7 and tested with Rx5

Training with Rx7 and tested with Rx6

Figure 5: Profile RF fingerprint of transmitters are generated with the signals captured by Rx7 and testing is performed with signals captured by other receivers.

signals captured by Rx1, then tested using the signals from the same transmitters but captured by the other receivers.

The classification accuracy is plotted in Figure 4, which is for the profile RF fingerprint generated from the receiver Rx6 signals and tested using the signals captured by all of the other receivers. The True Acceptance rate for different transmitters showed that correct identification decreased when the profile fingerprint generated with a different receiver was used for identification. This shows that every receiver forms a different RF fingerprint for the same transmitter irrespective of the receiver type (high or low-end). This implies that the RF fingerprint of a transmitter is not portable across receivers. Figure 5 shows the same trend, where profile RF fingerprints were generated with receiver Rx7 and tested with signals captured by other receivers. Similar results were obtained for all other receivers but only two are presented here due to the space limitation.

V. Summary

The RF fingerprint of a specific transmitter varies across the receivers due to its front-end, which makes the portability of an RF fingerprint difficult. The experimental results show that the RF fingerprint created with a specific receiver (either a high-end or a low-end) cannot be used as a universal profile RF fingerprint of a specific transmitter across different receivers. If a low-end receiver uses profile fingerprints created using any other receiver (high or low-end alike), it is likely that the low-end receiver will misclassify transmitters. Our analysis has shown that the profile fingerprints are specific to the transmitter-receiver pair and can be used only by the receiver that created the original profile.

References

[1] U. Meyer and S. Wetzel, “A man-in-the-middle attack on umts,” in *Proceedings of the 3rd ACM workshop on Wireless security*. ACM, 2004, pp. 90–97.

[2] 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.

[3] D. Faria and D. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in *Proceedings of the 5th ACM workshop on Wireless security*. ACM, 2006, pp. 43–52.

[4] N. Nguyen, G. Zheng, Z. Han, and R. Zheng, "Device fingerprinting to enhance wireless security using nonparametric bayesian method," in *INFOCOM, 2011 Proceedings IEEE*. IEEE, 2011, pp. 1404–1412.

[5] M. Debbah, "Mobile flexible networks: The challenges ahead," in *Advanced Technologies for Communications, 2008. ATC 2008. International Conference on*. IEEE, 2008, pp. 3–7.

[6] B. Kauffmann, F. Baccelli, A. Chaintreau, V. Mhatre, K. Papagiannaki, and C. Diot, "Measurement-based self organization of interfering 802.11 wireless access networks," in *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*. IEEE, 2007, pp. 1451–1459.

[7] 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.

[8] 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.

[9] O. Ureten and N. Serinken, "Wireless security through rf fingerprinting," *Electrical and Computer Engineering, Canadian Journal of*, vol. 32, no. 1, pp. 27 –33, winter 2007.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] ——, "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.

[16] ——, "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.

[17] S. Rehman, K. Sowerby, C. Coghill, and W. Holmes, "The analysis of rf fingerprinting for low-end wireless receivers with application to ieee 802.11 a," in *Mobile and Wireless Networking (iCOST), 2012 International Conference on Selected Topics in*. IEEE, 2012, pp. 24–29.

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

[19] 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.

[20] 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.

[21] B. Widrow and M. Lehr, "30 years of adaptive neural networks: perceptron, madaline, and backpropagation," *Proceedings of the IEEE*, vol. 78, no. 9, pp. 1415–1442, 1990.

[22] A. Jain, J. Mao, and K. M. Mohiuddin, "Artificial neural networks: a tutorial," *Computer*, vol. 29, no. 3, pp. 31–44, 1996.

[23] C. Eklund, R. B. Marks, K. L. Stanwood, and S. Wang, "Ieee standard 802.16: a technical overview of the wirelessman/sup tm/air interface for broadband wireless access," *Communications Magazine, IEEE*, vol. 40, no. 6, pp. 98–107, 2002.

[24] C. Stevenson, G. Chouinard, Z. Lei, W. Hu, S. Shellhammer, and W. Caldwell, "Ieee 802.22: The first cognitive radio wireless regional area network standard," *Communications Magazine, IEEE*, vol. 47, no. 1, pp. 130–138, 2009.

[25] R. Shaukat, S. Khan, and A. Ahmed, "Augmented Security in IEEE 802.22 MAC Layer Protocol," in *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08. 4th International Conference on*. IEEE, 2008, pp. 1–4.

[26] K. Bian and J. Park, "Security vulnerabilities in IEEE 802.22," in *Proceedings of the 4th Annual International Conference on Wireless Internet*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2008, pp. 1–9.

[27] M. Ettus, "Sbx schematic," *Ettus Research, Mountain View, CA, http://code.ettus.com/redmine/ettus/documents/21*, Aug, 2012.