Journal of Computer and System Sciences 80 (2014) 591–601

Contents lists available at SciVerse ScienceDirect

Journal of Computer and System Sciences

www.elsevier.com/locate/jcss

# Analysis of impersonation attacks on systems using RF fingerprinting and low-end receivers

Saeed Ur Rehman*, Kevin W. Sowerby, Colin Coghill

*Department of Electrical and Computer Engineering, The University of Auckland, 38 Princess St., Auckland Private Bag 92019, Auckland 1142, New Zealand*

ARTICLE INFO

*Article history:*
Received 30 November 2012
Received in revised form 30 April 2013
Accepted 14 June 2013
Available online 4 July 2013

*Keywords:*
Radio fingerprinting
Impersonation attack
Physical layer security
Hardware security

ABSTRACT

Recently, physical layer security commonly known as Radio Frequency (RF) fingerprinting has been proposed to provide an additional layer of security for wireless devices. A unique RF fingerprint can be used to establish the identity of a specific wireless device in order to prevent masquerading/impersonation attacks. In the literature, the performance of RF fingerprinting techniques is typically assessed using high-end (expensive) receiver hardware. However, in most practical situations receivers will not be high-end and will suffer from device specific impairments which affect the RF fingerprinting process. This paper evaluates the accuracy of RF fingerprinting employing low-end receivers. The vulnerability to an impersonation attack is assessed for a modulation-based RF fingerprinting system employing low-end commodity hardware (by legitimate and malicious users alike). Our results suggest that receiver impairment effectively decreases the success rate of impersonation attack on RF fingerprinting. In addition, the success rate of impersonation attack is receiver dependent.

## 1. Introduction

Wireless devices are vulnerable to identity spoofing due to the “broadcast” nature of the wireless medium and the programmability of wireless devices. For example, the software within a wireless device allows modification of the Medium Access Control (MAC) address of a network interface card [1]. The Erasable Programmable Read Only Memory (EPROM) of a cellular phone carries the information of Electronic Serial Number (ESN) and Mobile Identification Number (MIN), which can be changed by replacing the EPROM, hence allowing a modification in the identity of a cellular phone [2]. 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. Therefore, establishing the identities of wireless devices is crucial for the safe operation of wireless networks.

Cryptographic algorithms are mainly used for establishing the identity of a legitimate wireless device. A two-way communication is required to establish a session key in the cryptography. However, the security algorithm would be compromised upon access to the key, thus making it difficult to distinguish a legitimate key/device and cloned key/device [3]. This problem can be effectively tackled using physical layer security [4–6].

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 from the transmitters. These unique features are due to inherent randomness in the manufacturing process. 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 [7]. Physical layer

* Corresponding author.
*E-mail addresses:* sreh008@aucklanduni.ac.nz (S.U. Rehman), k.sowerby@auckland.ac.nz (K.W. Sowerby), c.coghill@auckland.ac.nz (C. Coghill).

0022-0000/$ – see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jcss.2013.06.013

security that is based on recognizing these unique features is known as Radio Frequency (RF) fingerprinting [8]. RF fingerprinting has been evaluated for a number of wireless devices operating on different standards, which include Cognitive Radio Networks (CRN) [9,10], Universal Mobile Telecommunications System (UMTS) [11], Wi-Fi [9,12], push-to-talk transmitters [13], Bluetooth [14,15] and Radio-Frequency Identification (RFID) [16,17]. It has been found that every transmitter has a unique RF fingerprint due to imperfection in the analog components present in the RF front end [18]. The main goal of RF fingerprinting is the detection of unique features from the received analog signals that allow the identification of a specific transmitter.

The majority of previously reported researches present promising results with up to 99% correct identification of transmitters using RF fingerprinting alone [4,5,9,11,13–16]. Generally, it is believed that RF fingerprinting is a secure and robust technique. RF fingerprints are considered hard to reproduce or replay because the replicating or replaying device suffers from its own impairments which disturb the features in the RF fingerprint. However there has been very little reported investigation of the actual performance and robustness of RF fingerprinting techniques in the presence of a malicious user. The two known examples in the literature have shown that modulation-based RF fingerprinting can be easily impersonated with an accuracy of up to 100% while transient-based RF fingerprinting is resilient to impersonation attack [8,19]. However, the analysis was performed with only one high-end receiver and results were not validated with multiple receivers.

Recent research in the RF fingerprinting suggests that receivers also have impairments, which affects the classification accuracy [20]. Additionally, different receivers form different RF fingerprint for the same transmitters due to impairments of the receiver front end. In this paper, the overall effect of receiver impairments on the classification accuracy of RF fingerprinting and its contribution in preventing the impersonation attack is analyzed. A typical modulation based RF fingerprinting technique is investigated for multiple low-end (low cost) receivers. Universal Software Radio Peripheral (USRP) platform is used for the validation of the results. Our results suggest that impairments in the receiver front end help significantly in mitigating the impersonation attack and thus, increases the robustness and reliability of RF fingerprinting technique. However, this robustness of RF fingerprinting is at the expense of lower classification accuracy in low-end receivers.

The main contributions in this paper are summarized as follows:

- Modulation-based RF fingerprinting is evaluated for multiple low-cost receivers, which further validates the results reported in [20]. The largest data set consisting of 490 000 signals captured with seven identical receivers are used for this analysis.
- Impersonation attack on modulation-based RF fingerprinting is evaluated for a number of identical low-cost receivers. To cross validates our results; evaluation is carried out for two identical impersonating wireless devices instead of relying only on one attacker and drawing the conclusion.
- The worst case scenario is considered, where all the transceivers (including impersonators) have the same manufacturer and their transceivers front end are equipped with similar components. Hence, RF fingerprinting evaluation is performed on a realistic and practical test bed.

The rest of the paper is organized as follows: Section 2 presents the literature review for RF fingerprinting. In Section 3, explanation of threat model and the RF fingerprinting scheme is provided. Section 4 provides the explanation for data collection along with details of equipment used in the experimental setup. Performance evaluation for baseline analysis and impersonation attack is provided in Section 5. Section 6 concludes the paper.

## 2. RF fingerprinting background

As with almost every technology, RF fingerprinting also stems from the military. The first RF fingerprinting system was utilized in the Vietnam War to differentiate between a friendly and foe radar [10]. In the past few years, researchers explored many RF fingerprinting techniques for identification of transmitters in commercial spheres [13,21–24]. One such example is in cellular industry, where RF fingerprinting is used to prevent cell phone cloning [25,26].

RF fingerprinting can be further divided into transient and steady state-based RF fingerprinting. In transient-based RF fingerprinting, the transition of a transmitter from the Off state to the On state triggers unique features, which appear before the transmission of the actual packet. These features are transmitter specific and vary across different transmitters, which can be utilized for identification of the transmitter [6,9,13,15,18,27–32]. The errors introduced by the modulator of the transmitter are utilized in steady state-based (modulation based) RF fingerprinting. Many researchers have explored ways to form unique RF fingerprint from these errors [9,12,23,24,33–38]. Mainly, the offset in Inphase/Quadrature (I/Q) components, frequency error, phase and magnitude errors of the frames, Power Spectral Density coefficients of preambles or variant of these features are used in the modulation-based fingerprinting.

Initially, the research community has given more attention to transient-based RF fingerprinting due to the unavailability of a steady state signal common to all transmitters. However, higher sampling rate is required for the transient detection and extraction due to its relatively short period compared to a steady state signal [35]. Therefore, real time implementation of transient-based fingerprinting presents serious technical challenges. On the other hand, the requirement of a common steady state signal for steady state-based RF fingerprinting is no longer an issue in the modern digital communication era. Nowadays, almost all digital communication systems (CRN, Wireless Sensor Network (WSN), RFID, Wireless Local Area

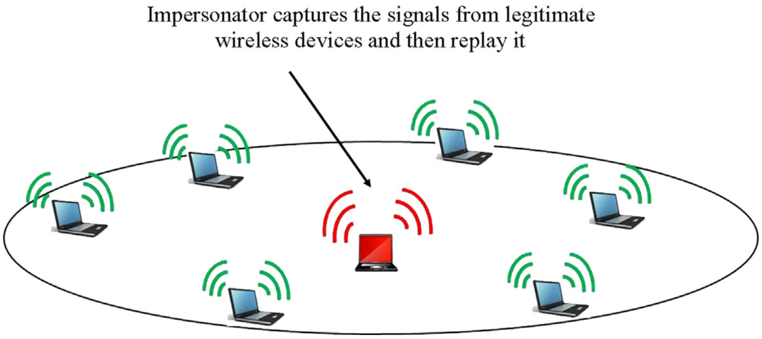
Impersonator captures the signals from legitimate
wireless devices and then replay it

**Fig. 1.** Threat model for Adhoc wireless network. The malicious device can capture and retransmits the legitimate signals.

Network (WLAN), UMTS etc.) introduce a preamble at the start of packet transmission in order to simplify the receiver design [11]. The preamble provides the common signal necessary for successful fingerprinting. Therefore, the impersonation attack on modulation-based (steady state) RF fingerprinting is analyzed in this work.

Most of the previous researches have concentrated more on developing unique RF fingerprint for the transmitters. High-end laboratory equipments (e.g. giga sampling rate oscilloscope, spectrum and vector signal analyzer) are used to validate the proposed techniques and promising results with up to 99% accuracy have been reported in the literature. High quality expensive analog components are used to build the front end of these laboratory equipments, which do not distort the minor (but distinctive) features imprinted in the received analog signal. This allows creating unique RF fingerprint for different transmitters and making the classification process easier. However, low-end receivers are built with inexpensive analog components, which would make it difficult to achieve the same results with low-end receivers. On the other hand, less attention is given to investigate the robustness of RF fingerprinting techniques against impersonation attack.

Two such examples are available in the literature, which have shown that modulation-based RF fingerprinting can be easily compromised with today's low-end wireless devices [8,19]. Danev et al. have used highly sophisticated equipment for impersonation attack, making it impractical due to unlimited capability of attacker which is not feasible in real-time [8]. Edman et al. have implemented an impersonation attack with more realistic equipment [19]. Only one receiver was used to achieve a success rate of up to 70%. However, recent research in RF fingerprinting has shown that classification accuracy varies across the low-end receivers for the same set of transmitters [20]. The variance in classification accuracy is due to the inexpensive analog components present in the receiver front-end. The analog components have their own imperfections, which make it difficult for a wireless device to extract the unique features from the received analog signal in order to form a valid unique RF fingerprint of the transmitter. Therefore, the robustness of RF fingerprinting against impersonation attack requires further analysis with multiple low-end receivers. This paper has considered the limitation of a practical RF hardware. The analysis has also taken into account the impairments of the inexpensive analog components present in the impersonator receiver front end. Additionally, a more realistic attacker with limited capabilities is considered.

## 3. Threat model

Fig. 1 shows the threat model for the analysis of impersonation attack on the wireless network. The wireless network consists of a number of legitimate wireless devices and an impersonator. All the legitimate devices are equipped with RF fingerprinting mechanism, which consists of two phases. In the initialization phase, the profile RF fingerprint of each legitimate wireless device is generated by extracting features from the received signal and is stored in the database. In the network operation phase, all legitimate wireless devices extract the features from the received signal and match it with the profile RF fingerprint stored in the database. The goal of the impersonator is to replay the legitimate wireless devices signals in such a way that the physical layer RF fingerprinting scheme is compromised and wireless devices are unable to discriminate between a legitimate and a malicious device.

### 3.1. Impersonator capabilities

In this research work a realistic impersonator is considered, which has the same capabilities as of a legitimate transceiver. The impersonator not only receives and records the signals from the legitimate transmitters within its transmission range but it can also retransmit (replay) the same received signal. Additionally, the impersonator has the capability to learn parameters from the received legitimate signals and then reproduce a new signal with the same parameters. Thus in this way, a malicious user will try to impersonate a legitimate transmitter by replaying the legitimate signals captured earlier. Furthermore, an impersonator can jam the wireless network by continuously transmitting in the same frequency, but jamming attacks are not in the scope of this paper.

### 3.2. RF fingerprinting scheme

A typical modulation-based RF fingerprinting scheme is evaluated for the impersonation attack. A modulation based RF fingerprinting scheme is easy to implement on low-end RF hardware as compared to transient based RF fingerprinting, which requires higher sampling rate due to its relatively short period. In previous works, the RF fingerprint of transmitters is generated by extracting the frequency domain features from the steady-state signal [11,12,34,35]. In this paper, the frequency domain RF fingerprinting technique proposed by the Suski et al. is used for impersonation attack evaluation. Suski et al. have identified WLAN transmitters by extracting features from the IEEE 802.11a preamble signals [12]. They have extracted Power Spectral Density (PSD) coefficients from the preamble signals to form the RF fingerprints of transmitters. An IEEE 802.11a standard preamble signal is generated in MATLAB and transmitted from different transmitters. The preamble signal is then captured using the measurement setup described in the next subsection. The identification is implemented by extracting the preamble from the signals and generating the PSD coefficients. The PSD coefficients are then used to develop the RF fingerprint for each transmitter and classification is performed using a classifier.

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

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

### 3.3. Preamble extraction

Preamble extraction plays an important role in the overall RF fingerprinting process because each acquired signals consists of channel noise, preamble and data. If a preamble were not extracted finely then the RF fingerprint created for a transmitter would change over the time, as it would have features from channel noise and the data part of the signal. Amplitude-based variance detection technique is employed for extracting the preamble from the acquired signals. The signal is first normalized and then preamble is extracted by the given equation [12,15,39].

$$V_i = K \frac{1}{w-1} \sum_{n=1}^{w} (X_{m-n} - \bar{X}_w)^2 \tag{3}$$

where $V_i$ is a new variance signal created from the input signal $X_m$, $w$ is the sliding window size, $\bar{X}_w$ is the mean of samples. $K$ is the scaling factor to make the signal comparable to the measured received signal. In case of a RF burst signal, the variance of the signal for a given window size $w$ would increase rapidly as compared to the variance of the last measured $w$ samples. The start of the preamble is the point where the $V_i$ signal power rises while the end point of preamble is 16 microseconds later, as per IEEE 802.11a standard [40].

## 4. Experimental setup

Our experimental test bed consists of USRP N210 equipped with seven SBX transceiver daughterboards and vert2450 antennas. The Universal Software Radio Peripheral (USRP) is an open source low-cost software defined radio platform produced by Ettus Research [41]. The USRP N210 consists of a motherboard and daughterboards. All the signal processing is performed on the motherboard and is equipped with a dual 14-bit Analog to Digital Converter (ADC) and dual 16 bit Digital to Analog Converter (DAC). The ADC and DAC operate at 100 MHz and 400 MHz, respectively. Gigabit Ethernet link is used to transfer the complex base band samples (In-phase and Quadrature components) from USRP to computer at 25 MSample/s.

USRP N210 motherboard has two slots for daughterboards. One slot is connected to transmission path utilizing DAC while the other slot uses the reception path on the motherboard. RF front-end is implemented on the daughterboards, and is available in the frequency range from DC to 5.9 GHz. Unique RF fingerprint is due to the analog components present in the RF front-end. Therefore, the effect of different transmit and receive chain on RF fingerprinting can be analyzed by installing different daughterboards on USRP's.

The SBX daughterboards act as a front end and have a frequency range from 0.4 GHz to 4.4 GHz, which allows transmitting and receiving in the 2.4 GHz ISM band. SBX daughterboards have different transmit and receive chain along with different local oscillators for transmission and reception [42]. All the SBX daughterboards used in this research work are listed in Table 1. The SBX daughterboards have identical transmit and receive chain build with the similar components originating from the same manufacturer at different times as can be seen in Table 1. The identifier column shows the naming convention used throughout this research paper. For example T1_R1 is used for transmit and receive chain on SBX daughterboard 1. Additionally, the short notation T1 and Tx1 refers to the same transmitter and is used for figures clarity. The

**Table 1**
Details of Ettus SBX daughterboards used in the experiment.

| Identifier | Serial | Version | Shipment date |
|---|---|---|---|
| T1_R1 | EOR10ZEXS | Rev 2.0 | Dec, 2011 |
| T2_R2 | EOR10ZFXS | Rev 2.0 | Dec, 2011 |
| T3_R3 | E4R12X9XS | Rev 3.0 | Feb, 2012 |
| T4_R4 | E4R12X7XS | Rev 3.0 | Feb, 2012 |
| T5_R5 | E9R16WAXS | Rev 4.0 | Aug, 2012 |
| T6_R6 | E9R16W3XS | Rev 4.0 | Aug, 2012 |
| T7_R7 | E9R16W6XS | Rev 4.0 | Aug, 2012 |

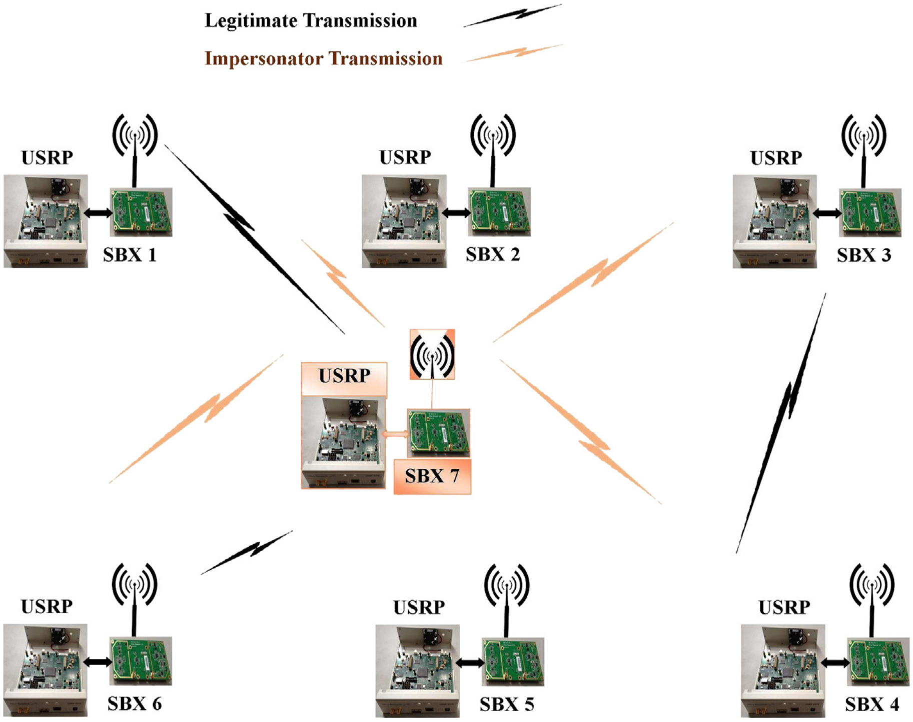

**Fig. 2.** Seven identical USRP transceivers are used to analyze the performance of RF fingerprinting in the presence of a malicious user. The malicious user impersonates legitimate USRP transmitters by replaying its signals.

SBX daughterboard T3_R3 and T7_R7 acts as an impersonator transceivers. More detail on impersonation attack is provided in later sections.

All the measurements were carried out in an office environment, representing a realistic reception scenario, where the interference from different wireless devices in the same frequency band was present during the measurements. An impersonation attack can be easily launched with the RF hardware used in the experiment, which is easily available and is less expensive representing real world RF hardware.

### *4.1. Data collection*

Each 802.11a packet transmission starts with 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 [37]. The IEEE 802.11a preamble signal is 16 microseconds long and consists of 10 short and 2 long training sequences [40]. The IEEE 802.11a preamble signal is generated in MATLAB as per standard. The preamble signal is transmitted and captured through SBX transceivers. Due to broadcast nature of the wireless medium, the impersonator shown in the measurement setup of Fig. 2 also captures the same transmitted preamble signal from the legitimate transmitters.

USRP daughterboards have different transmit and receive chain for transmission and reception [42]. In order to avoid any commonalities among the transmit and receive chain, we have either used a transmit or a receive chain of a daughterboard but both are not used simultaneously for transmission and reception (e.g., when Rx1 is used for capturing the transmitters signals then Tx1 is not used for evaluation as it is implemented on the same daughterboard).

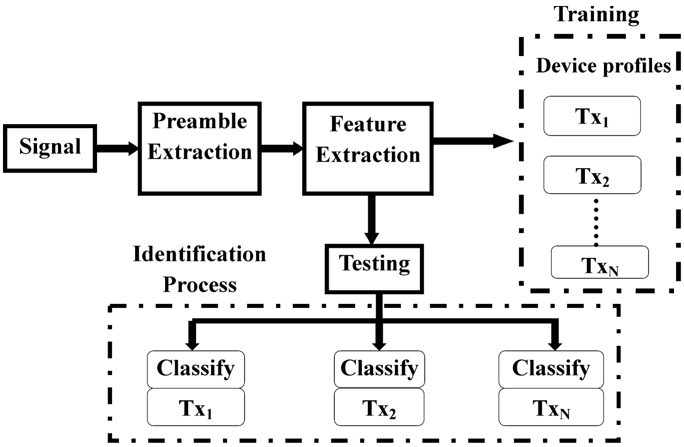

**Fig. 3.** RF Fingerprinting classification process.

A total of 10 000 signals from each transmitter (including impersonator) was captured and stored at each receivers; thus every receiver has 60 000 signals from six transmitters (e.g. Rx1 has captured signals from T2 to T7). This gives a total dataset of 490 000 signals for seven receivers. These signals are used to find out the baseline classification accuracy of low-end receivers.

For the impersonation attack analysis, the impersonator replays the legitimate transmitter's signals. In our analysis, impersonator has a total of 60 000 signals from six legitimate transmitters. These signals are used by the impersonator for replay attack across different receivers. Preamble extraction is performed with amplitude-based variance detection technique as explained previously. After preamble extraction, RF fingerprint of a transmitter is generated using the PSD coefficients. MATLAB is used for preamble extraction, RF fingerprint formation and classification.

## 5. Performance evaluation

The performance evaluation process consists of two phases: namely training and testing as shown in Fig. 3. In the training phase, signals of a specific transmitter are used to create the profile RF fingerprint of the transmitter. Whereas in the testing phase, a RF fingerprint is created from an input test signal. Then a classifier is used to classify this test RF fingerprint against the existing profiles of the transmitter. Training and testing is equivalent to initialization and network operation phase in RF fingerprinting. K-Nearest Neighbor (KNN) with three nearest neighbors is used as a classifier. The KNN classifier is used to classify an input feature vector into one of the class based on the closest training examples available in the feature space [8]. Classification is performed on a per signal basis; i.e. PSD coefficients are used to create the RF fingerprint of a signal. This RF fingerprint is then classified using the KNN classifier.

We used $k$-fold cross-validation to evaluate our results. The $k$-fold cross-validation method is used for performance evaluation in order to maximize the certainty of the results. In $k$-fold cross-validation, the data-set is divided into $k$ complementary subsets, and then performance evaluation is performed $k$ times, where each time a different subset is used for training while the remaining $k-1$ subsets are used for testing. In our evaluation, 10-fold cross validation is used, which results in the testing set being nine times greater than the training set.

### *5.1. Baseline analysis*

The first step in our evaluation was to develop the baseline accuracy of RF fingerprinting that might be affected by using low-end (low-cost) receivers without any impersonator interference. This will further validate the results reported for low-end receivers [20], which is based on three receivers and a dataset of 3600 signals only. The dataset of 490 000 signals captured in the data collection section are used for the baseline analysis. This is the largest dataset ever used for RF fingerprinting evaluation from the same identical transmitters across different receivers.

In the baseline evaluation, the profile RF fingerprints of the seven transmitters are generated for individual receiver. In a realistic scenario, the Signal-to-Noise Ratio (SNR) always varies due to mobility of transmitter/ receiver or environmental affects (shadowing, multipath, fading etc.). Therefore, simulated Additive White Gaussian Noise (AWGN) is added to the collected signals in order to evaluate the effect of SNR.

Fig. 4 shows the average classification accuracy of individual low-end receivers for varying Signal to Noise Ratio (SNR). The average accuracy does not distinguish between false positive and false negative but it merely gives the fraction of total samples that belong to appropriate transmitters. Later, false accept rate is used for the impersonator attack evaluation, which clearly measures the success of an attack.

The average classification accuracy varies across the low-end receivers. For example, Tx1 is 94% classified accurately by Rx4 at 15 dB SNR while for other low-end receivers, it varies from 30% to 80 % at 15 dB SNR, as shown in Fig. 4(b)–(e).

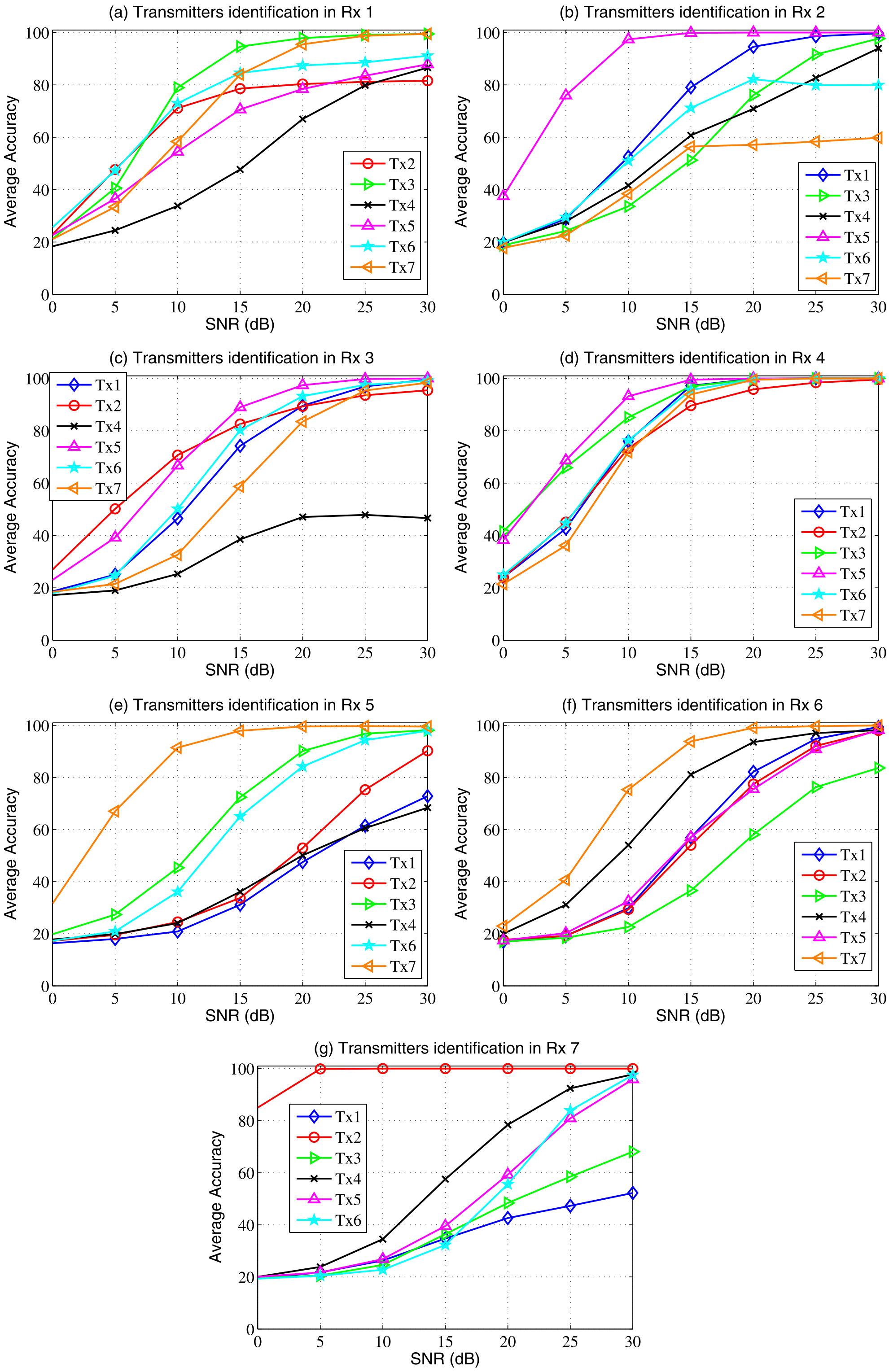

**Fig. 4.** RF fingerprinting classification accuracy for seven individual identical low-end receivers. Overall, the classification accuracy is high for Rx1 and Rx4, while all other receivers have acceptable accuracy above 20 dB SNR.

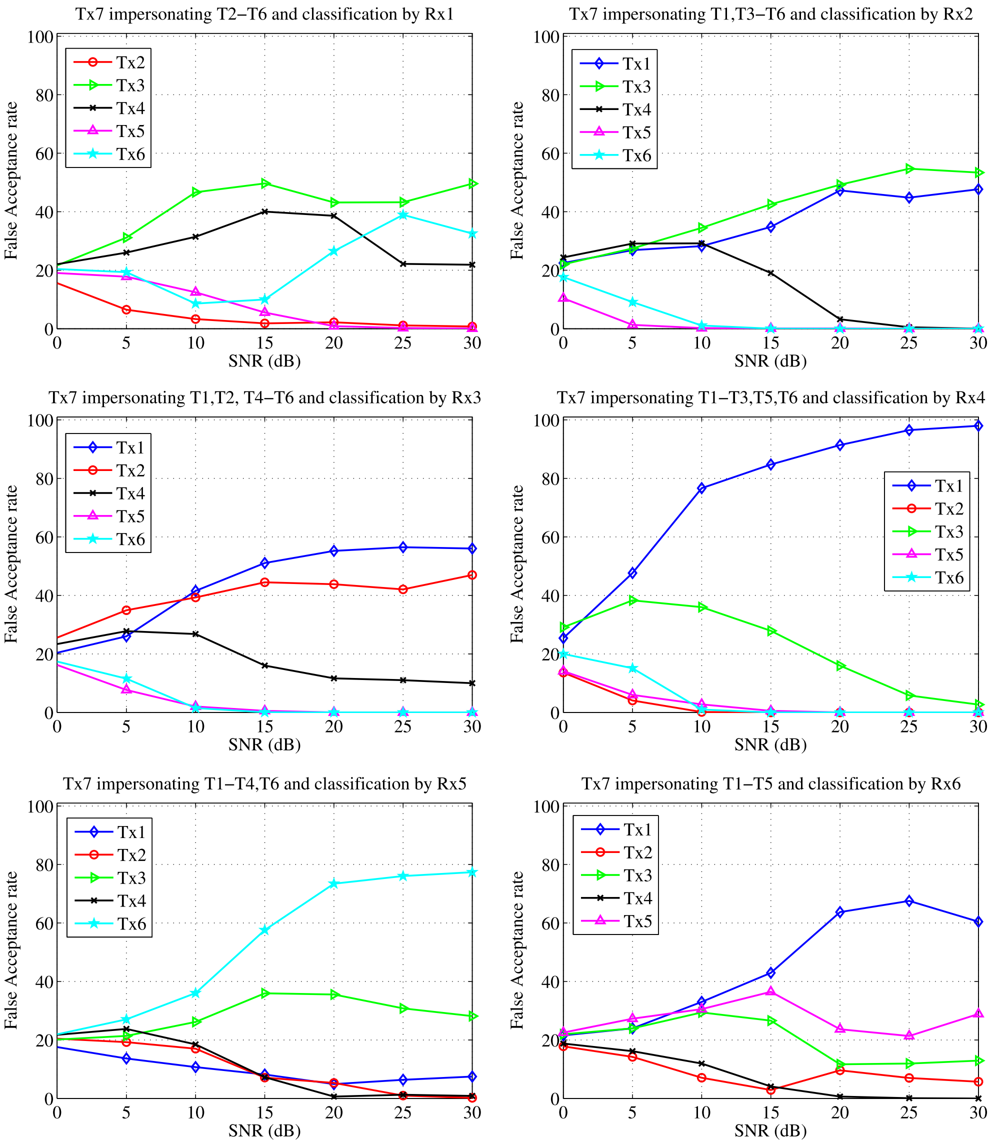

**Fig. 5.** Transmitter 7 has replayed the captured signals to impersonate different legitimate transmitters, while receivers have classified the replayed signal by matching it with the already stored profile RF fingerprint of the legitimate transmitters. The lowest acceptance rate of transmitters means that impersonation attack has failed.

Interestingly, all seven low-end receivers perform differently for the same set of transmitters as shown in Fig. 4. The best classification results are provided by Rx4 while all others were able to provide useful classification results at receiver SNRs of 15 dB or higher. Lower classification accuracy was expected for the low-end RF hardware as compared to 99% accuracy reported in the literature. A decreased in the accuracy is due to the lower sampling resolution and increased noise induced by the low-cost RF hardware. Furthermore, results show that accuracy varies across the receivers due to the impairments of the analog front-end of the receivers, which are acting like a distorting filter on the received signal.

### 5.2. *Impersonation attack analysis*

After developing the baseline accuracy for the low-end receivers, the next step is to evaluate the impact of impersonation attack on RF fingerprinting for low-end receivers. Due to broadcast nature of the wireless medium, the impersonator T7_R7 shown in the measurement setup of Fig. 2 also captures the preamble signals from the legitimate transmitters. A total of 60 000 signals from six legitimate transmitters was captured as discussed in the previous section. In the impersonation attack, these signals were then retransmitted by Tx7 and captured with the legitimate transceivers (Rx1 to Rx6). Every legitimate wireless device captured 50 000 impersonation signals for five transmitters (e.g. Rx1 captures the impersonation

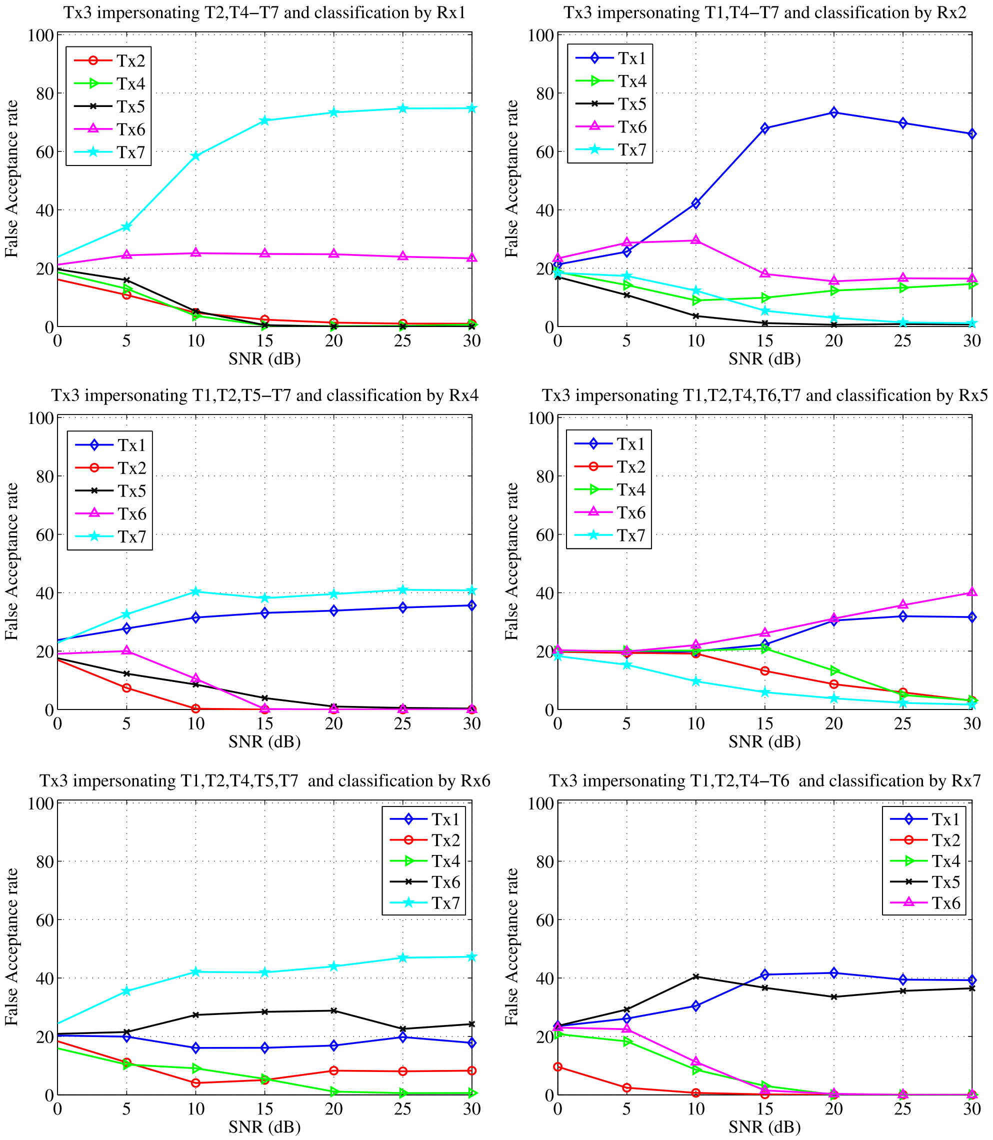

**Fig. 6.** False acceptance rate for the impersonator Tx3. The captured signals are replayed to launch impersonation attack on different legitimate transmitters.

signals of T2 to T6 from the impersonator Tx7). The legitimate transceivers would classify the replayed signals into one of the available classes by matching it with the already stored RF fingerprint of the legitimate transmitters.

In the performance evaluation phase, the KNN classifier is trained with the RF fingerprints of each legitimate transmitter. For example, receiver 1 has fingerprint of the legitimate transmitters T2 to T6. The same process is repeated for all other receivers. In the testing phase, the replayed signals captured by each receiver are then classified into one of the available classes.

Fig. 5 shows the false acceptance rate of impersonation attack for different low-end receivers. The false acceptance rate is for impersonation attack on transmitter T1 to T6 while transmitter Tx7 is the impersonator. In our analysis an impersonation attack is considered successful if the false acceptance rate is above 50%. As can be seen in Fig. 4, the false acceptance rate is different in each receiver. For example, Tx7 has successfully impersonated T1 in receiver 4 while T7 failed to impersonate T1 in receiver 5. This means that successful impersonation attack is largely dependent on receiver.

In order to further validate the results of Fig. 6, another setup is used in which transceiver T3_R3 was used as impersonator while the rest of the transceivers was used as legitimate devices. The same process is repeated for the performance evaluation, i.e. signals from the legitimate transmitters are used for training purpose while replayed signals of transmitter 3 are utilized for testing. The false acceptance rate of Tx3 is shown in Fig. 6. The same trend is observed for a different impersonator transceiver. The impersonation attack was successful on T1 and T7 in legitimate receiver Rx1 and Rx2 while other receivers successfully thwarted the impersonation attack on legitimate transmitters.

## 6. Conclusion

This paper has experimentally analyzed the effectiveness of impersonation attack using low-end transmitters and receivers. In the experiments, seven identical USRP transceivers were used. First, a baseline RF fingerprinting accuracy was developed and it was found that classification accuracy is receiver specific and is less accurate than that achieved with high-end receivers. Nevertheless, the low-end receivers were able to provide useful classification results at receiver SNRs of 15 dB or higher. The experimental results also imply that the RF fingerprint created for a specific transmitter varies across low-end receivers because the receiver front end also suffers from imperfection in its analog components. Hence, every receiver forms a unique (receiver specific) RF fingerprint of a specific transmitter.

Second, results have shown that impersonation attack on two transmitters was successful in a few receivers but receivers have effectively thwarted the impersonation attack on the same two transmitters. This is because a user's receiver front end also contributes to its RF fingerprinting of a specific transmitter. Hence an attacker (malicious user) would be unaware of the impairments of a legitimate receiver. More importantly, the attacker would probably also be unaware of its own receiver impairments (which influence the fingerprint it creates for a target transmitter) and its transmitter impairments. Hence the uncertainty associated with low end hardware increases the challenge for the attacker to create a signal that would deceive a legitimate user.

On the other hand, if a target device fingerprint differs significantly from the other devices in the network then a legitimate receiver may be unable to distinguish between a legitimate and an impersonating device. The success in this case would be dependent on the decision boundaries in the classifier.

This work is an initial step in our ongoing investigation of the practical use of low-end receivers for RF fingerprinting. Our results suggest that practical deployment of RF fingerprinting using today's typical low-end receivers is significantly more challenging than might be suggested by the experiments performed with high-end receivers in controlled environments. In addition, the accuracy of classification results is largely dependent on the receiver. High receiver SNRs yield good classification results for low-end receivers but high SNRs are not typical in real situations. Interestingly, because the receiver impairments contribute toward the final RF fingerprint in a receiver, this helps in mitigating an impersonation attack on a system employing RF fingerprinting.

## References

[1] D. Faria, 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.

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

[3] S. Mathur, A. Reznik, C. Ye, R. Mukherjee, A. Rahman, Y. Shah, W. Trappe, N. Mandayam, Exploiting the physical layer for enhanced security [security and privacy in emerging wireless networks], IEEE Wireless Communications 17 (5) (2010) 63–70.

[4] D.R. Reising, M.A. Temple, M.J. Mendenhall, Improving intra-cellular security using air monitoring with rf fingerprints, in: WCNC'10, 2010, pp. 1–6.

[5] A. Polak, S. Dolatshahi, D. Goeckel, Identifying wireless users via transmitter imperfections, IEEE Journal on Selected Areas in Communications 29 (7) (2011) 1469–1479.

[6] Y. Shiu, S. Chang, H. Wu, S. Huang, H. Chen, Physical layer security in wireless networks: a tutorial, IEEE Wireless Communications 18 (2) (2011) 66–74.

[7] K. Gard, L. Larson, M. Steer, The impact of rf front-end characteristics on the spectral regrowth of communications signals, IEEE Transactions on Microwave Theory and Techniques 53 (6) (2005) 2179–2186.

[8] B. Danev, H. Luecken, S. Capkun, K. El, Defrawy, attacks on physical-layer identification, in: Proc. ACM Conf. on Wireless Network Security, 2010, pp. 89–98.

[9] K. Kim, C. Spooner, I. Akbar, J. Reed, Specific emitter identification for cognitive radio with application to IEEE 802.11, in: Global Telecommunications Conference, IEEE GLOBECOM 2008, IEEE, 2008, pp. 1–5.

[10] Y.-D.Y. Nansai Hu, Identification of legacy radios in a cognitive radio network using a radio frequency fingerprinting based method, in: IEEE International Conference on Communications, ICC '12, 2012.

[11] P. Scanlon, I. Kennedy, Y. Liu, Feature extraction approaches to rf fingerprinting for device identification in femtocells, Bell Labs Technical Journal 15 (3) (2010) 141–151.

[12] W. Suski II, M. Temple, M. Mendenhall, R. Mills, Radio frequency fingerprinting commercial communication devices to enhance electronic security, International Journal of Electronic Security and Digital Forensics 1 (3) (2008) 301–322.

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

[14] M. Woelfle, M. Temple, M. Mullins, M. Mendenhall, Detecting, identifying and locating bluetooth devices using rf fingerprints, in: Military Communications Conference (MILCOM 2009), 2009.

[15] S. Rehman, K. Sowerby, C. Coghill, Rf fingerprint extraction from the energy envelope of an instantaneous transient signal, in: Communications Theory Workshop (AusCTW), Australian, 2012, pp. 90–95.

[16] D. Zanetti, B. Danev, S. Čapkun, Physical-layer identification of uhf rfid tags, in: Proceedings of the 16th ACM Conference on Mobile Computing and Networking, MobiCom '10, ACM, 2010.

[17] C. Bertoncini, K. Rudd, B. Nousain, M. Hinders, Wavelet fingerprinting of radio-frequency identification (rfid) tags, IEEE Transactions on Industrial Electronics 59 (12) (2012) 4843–4850, http://dx.doi.org/10.1109/TIE.2011.2179276.

[18] B. Danev, S. Čapkun, Transient-based identification of wireless sensor nodes, in: Proceedings of the 8th IEEE/ACM Information Processing in Sensor Networks, IPSN '09, IEEE/ACM, 2009, pp. 25–36.

[19] M. Edman, B. Yener, Active attacks against modulation-based radiometric identification, RPI Department of Computer Science Technical Report, 2009, pp. 09–02.

[20] S. Rehman, K. Sowerby, C. Coghill, Analysis of receiver front end on the performance of rf fingerprinting, in: IEEE 23rd PIMRC, 2012.

[21] M. Marcus, Progress in vhf/nhf mobile transmitter identification, University of Manitoba, Department of Electrical and Computer Engineering, Tech. Rep.
[22] R. Hippenstiel, Y. Payal, Wavelet based transmitter identification, in: Fourth International Symposium on Signal Processing and Its Applications, ISSPA 96, vol. 2, IEEE, 1996, pp. 740–742.
[23] S. Xu, L. Xu, Z. Xu, B. Huang, Individual radio transmitter identification based on spurious modulation characteristics of signal envelop, in: Military Communications Conference, MILCOM 2008, IEEE, 2008, pp. 1–5.
[24] G. Zamora, S. Bergin, I. Kennedy, Using support vector machines for passive steady state RF fingerprinting, Novel Algorithms and Techniques in Telecommunications and Networking (2010) 183–188.
[25] D. Kaplan, D. Stanhope, Waveform collection for use in wireless telephone identification, uS Patent 5999806, Dec. 7 1999.
[26] D. Hoogerwerf, E. Green, D. Stanhope, R. McKernan, Active waveform collection for use in transmitter identification, uS Patent 6035188, Mar. 7 2000.
[27] B. Danev, T.S. Heydt-Benjamin, S. Čapkun, Physical-layer identification of rfid devices, in: Proceedings of the 18th USENIX Security Symposium, USENIX Security '09, USENIX, 2009, pp. 125–136.
[28] K. Ellis, N. Serinken, Characteristics of radio transmitter fingerprints, Radio Science 36 (4) (2001) 585–597.
[29] J. Hall, M. Barbeau, E. Kranakis, Detection of transient in radio frequency fingerprinting using signal phase, Wireless and Optical Communications (2003) 13–18.
[30] J. Hall, M. Barbeau, E. Kranakis, Enhancing intrusion detection in wireless networks using radio frequency fingerprinting, in: Proceedings of the 3rd IASTED International Conference on Communications, Internet and Information Technology (CIIT), 2004, pp. 201–206.
[31] J. Hall, M. Barbeau, E. Kranakis, Radio frequency fingerprinting for intrusion detection in wireless networks, in: IEEE Transactions on Defendable and Secure Computing.
[32] J. Hall, M. Barbeau, E. Kranakis, Detecting rogue devices in bluetooth networks using radio frequency fingerprinting, in: IASTED International Conference on Communications and Computer Networks, 2006.
[33] I. Kennedy, A. Kuzminskiy, Rf fingerprint detection in a wireless multipath channel, in: 7th International Symposium on Wireless Communication Systems (ISWCS), IEEE, 2010, pp. 820–823.
[34] I. Kennedy, P. Scanlon, M. Buddhikot, Passive steady state rf fingerprinting: a cognitive technique for scalable deployment of co-channel femto cell underlays, in: 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN 2008, IEEE, 2008, pp. 1–12.
[35] I. Kennedy, P. Scanlon, F. Mullany, M. Buddhikot, K. Nolan, T. Rondeau, Radio transmitter fingerprinting: A steady state frequency domain approach, in: IEEE 68th Vehicular Technology Conference, VTC 2008-Fall, IEEE, 2008, pp. 1–5.
[36] S. Rehman, K. Sowerby, C. Coghill, W. Holmes, The analysis of rf fingerprinting for low-end wireless receivers with application to ieee 802.11 a, in: International Conference on Selected Topics in Mobile and Wireless Networking (iCOST), IEEE, 2012, pp. 24–29.
[37] W. Suski, M. Temple, M. Mendenhall, R. Mills, Using spectral fingerprints to improve wireless network security, in: Global Telecommunications Conference, IEEE GLOBECOM 2008, IEEE, 2008, pp. 1–5.
[38] V. Brik, S. Banerjee, M. Gruteser, S. Oh, Wireless device identification with radiometric signatures, in: Proceedings of the 14th ACM International Conference on Mobile Computing and Networking, ACM, 2008, pp. 116–127.
[39] K. Bonne Rasmussen, S. Capkun, Implications of radio fingerprinting on the security of sensor networks, in: Third International Conference on Security and Privacy in Communications Networks and the Workshops, SecureComm 2007, IEEE, 2007, pp. 331–340.
[40] 802.11a, wireless lan medium access control (mac) and physical layer (phy) specifications: High speed physical layer extension in the 5 ghz band, institute of electrical and electronics engineers, piscataway, nj 08855-1331, usa.
[41] M. Ettus, Universal software radio peripheral, Ettus Research, Mountain View, CA, www.ettus.com.
[42] M. Ettus, Sbx schematic, Ettus Research, Mountain View, CA, http://code.ettus.com/redmine/ettus/documents/21.