RF Fingerprinting of Users Who Actively Mask Their Identities with Artificial Distortion

Adam C. Polak and Dennis L. Goeckel

Electrical and Computer Engineering Department
University of Massachusetts Amherst
apolak@engin.umass.edu goeckel@ecs.umass.edu

Abstract—**Variations in the RF chain of radio transmitters caused by imperfections of manufacturing processes can be used as a signature to uniquely associate wireless devices with a given transmission. In our previous work [1], [2] we proposed a model based approach that allows for identification of wireless users with verifiable accuracy via time domain analysis of the signals received from the masquerading users. Here, more sophisticated criminals that, when masquerading, intentionally introduce nonlinear distortions to the data symbols in order to fake their signatures while allowing for proper data decoding are considered for the first time. The method proposed in this work is based on spectral analysis and on the observation that nonlinear components cause baseband distortion and spectral regrowth of the signal that is dependent on the parameters of the nonlinearity. Hence, by analysis of the in-band distortion and the spectral regrowth, the masquerading users can be successfully identified even when they are nonlinearly modifying their data symbols. Using parameters obtained from the measurements of commercially used RF transmitters, we demonstrate the utility of our approach.**

Index Terms—**radiometric identification, likelihood ratio test, privacy, process variations**

I. Introduction

Exploitation of the physical layer for purposes of user identification in wireless systems has recently been considered as an alternative to utilization of information available at higher layers of the protocol stack. Exploitation of imperfections of hardware caused by inaccuracies of production processes is especially attractive for identification purposes, because it makes identification independent from the location of wireless users, as opposed to the methods based on the channel properties [3], [4] that require a strong assumption on users' stationarity. Physical layer fingerprinting techniques that exploit hardware imperfections can generally be split into two groups: transient signal techniques [5], [6], [7] and steady state signal techniques [1], [2], [8], [9]. Transient based techniques require extremely high sample rates and accurate estimation of the start and end times of the transients, which very often makes them impractical. Recently techniques for user identification based on analysis of slight variations of steady state modulated signals have been proposed [1], [2], [8]. In [8] machine learning techniques were used on collected modulation data to train classifiers that are then able to distinguish wireless cards. In [1], [2] we introduced a model based approach that provides very good identification performance and allows for verifiable accuracy of the identification decisions.

All of the identification techniques based on steady state signal analysis exploit the fact that nonideal transmitters cause signal distortions that, while being slight enough for the transmitters to meet requirements of the communication standards, are significant enough to make the distortions observable and able to be tied with an individual transmitter. However a sophisticated user aware of the methods used for identification could inject slight distortions to the digital data signal that, while allowing for reliable data transmission, would change the character of the distortion observable at the receiver. Hence the sophisticated user could fake his signature and significantly degrade performance of the steady state signal based methods.

In [1], [2] we introduced a signal processing framework for the identification of users from nonidealities in their RF transmit chain. Here, we consider the much harder problem motivated above- identification when a sophisticated user intentionally distorts his/her data signals to avoid such RF fingerprinting. The method proposed here is based on the observation that the nonlinearity of the RF power amplifiers (PAs), which are the last elements of the transmitter chain and cannot be influenced by software modifications, cause slight spectral regrowth of the signal that is dependent on the parameters of the nonlinearity. Hence, with oversampling at the receiver and analysis of the in-band distortion of the spectrum as well as the spectral regrowth of the captured signals, the masquerading users can be identified even if they fake their signatures by injecting artificial distortions to the data signals.

The identification method proposed in this work exploits the fact that PAs, which seek to have linear characteristics, are often quite nonlinear even with significant compensation. What is important for the identification is that the nonlinearities can vary significantly across individual units. It is important to stress here that this work only exploits the differences in the nonlinear character of the amplifiers. Differences of values of the linear gain that could be caused by varying distance between transmitter and receiver or fading effects of the channel, are ignored. Thus, it is assumed that the linear gain is known at the receiver and all captured signals are normalized to the same gain value $G = 1$.

[1]This paper is based in part upon work supported by the National Science Foundation under grant CNS-0905349.

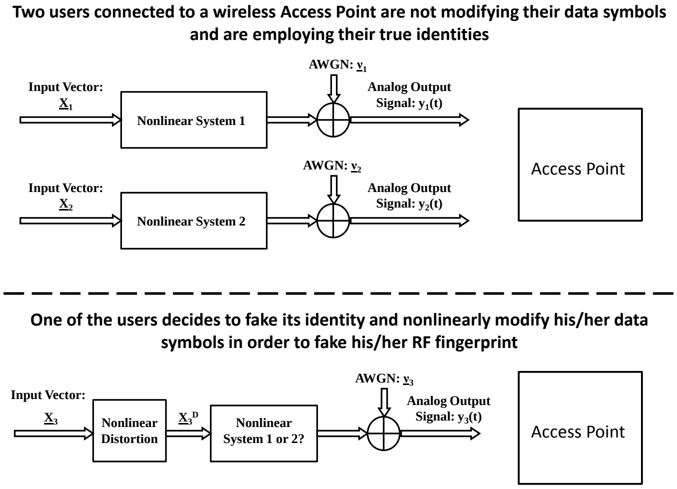
Two users connected to a wireless Access Point are not modifying their data symbols and are employing their true identities
Input Vector: X1
Nonlinear System 1
AWGN: v1
Analog Output Signal: y1(t)
Input Vector: X2
Nonlinear System 2
AWGN: v2
Analog Output Signal: y2(t)
Access Point
One of the users decides to fake its identity and nonlinearly modify his/her data symbols in order to fake his/her RF fingerprint
Input Vector: X3
Nonlinear Distortion
X3D
Nonlinear System 1 or 2?
AWGN: v3
Analog Output Signal: y3(t)
Access Point

Fig. 1. The two-system identification scenario: two authorized users employ their true identities (upper part); one of the users decides to fake his/her identity, modify the data symbols and commit a crime (lower part).

The remainder of the paper is organized as follows. Section II presents the formal problem statement. Section III introduces the proposed identification method. Numerical results that verify utility of the proposed method are presented in Section IV. Finally, Section V concludes the paper.

II. Problem Statement

Similarly as in [1] and [2], a two-user identification scenario is considered, in which two eligible users are connecting to an access point (generalization to the case of n users is straightforward using n-hypothesis testing techniques). At some point in time one of the users decides to fake his/her identity and commit a crime. The identification problem is to tie the transmission captured from the masquerading user to the transmissions captured and saved when the users were employing their true identities. In [1] and [2] we assumed that the symbols decoded at the receiver are identical with the data symbols generated at the transmitter. In this work we address a scenario when the decoded data symbols can differ from the data symbols generated at the transmitter, because of slight distortions that the transmitter could have injected in order to fake his signature that still allow for correct decoding. We want to make the identification decisions independent from the values of the data symbols, and be able to make them based only on the received signals oversampled at the receiver with a low oversampling rate. Figure 1 presents the considered scenario.

Our method is based on an assumption that when the users employ their true identities, they do not distort the data signals, and that they can be observed for a long enough time to obtain relatively accurate estimates of their true signatures. The identification decisions then need to be made based on possibly short transmissions captured from the masquerading transmitters that might or might have not injected distortions to their data symbols.

III. Proposed Method

According to Parseval's theorem, the power of a wide sense stationary random process $\mathcal{X}(t)$ can be expressed as:

$$P = \int_{-\infty}^{\infty} \lim_{T\to\infty} \frac{1}{T} E\left[|X(f)|^2\right] df \qquad (1)$$

where $X(f)$ is the Fourier Transform of a single realization $x(t)$ of the process. Therefore

$$S(f) = \lim_{T\to\infty} \frac{1}{T} E\left[|X(f)|^2\right] \qquad (2)$$

is equivalent to the power spectral density (psd) of the process $\mathcal{X}(t)$. For a digital communication signal modulated with a potentially distorted symbol stream (a_k) and shaped with an analog pulse $p(t)$, $x(t)$ and $X(f)$ are:

$$x(t) = \sum_{k=-\infty}^{\infty} a_k \cdot p(t-kT_s)$$

$$X(f) = \mathcal{F}\{x(t)\} = \sum_{k=-\infty}^{\infty} a_k \cdot \mathcal{F}\{p(t-kT_s)\} \qquad (3)$$

where T_s is the symbol period and $a_k's$ are data symbols modeled as i.i.d. complex random variables, whose distribution depends on the digital modulation scheme.

On the transmitter side $x(t)$ is amplified and sent through the channel. The psd of the random process $\mathcal{Y}(t)$ received by the receiver can then be expressed as:

$$S_{\mathcal{Y}}(f) = \lim_{N\to\infty} \frac{1}{2N+1} \cdot E\left[Y(f)\cdot Y(f)^*\right] + \sigma_\nu^2 \qquad (4)$$

where σ_ν^2 is the variance of the noise of the AWGN channel and $Y(f)$ is a spectrum of the signal $x(t)$ amplified with a nonlinear amplifier, the characteristic of which can be modeled with an an odd-order polynomial with coefficients h_i [10]:

$$Y(f) = \sum_{p=1}^{P} h_{2p-1} \cdot \mathcal{F}\left\{ \left(\lim_{N\to\infty} \sum_{k=-N}^{N} a_k \cdot p(t-kT_s) \right)^{(2p-1)} \right\} \qquad (5)$$

Because of the linearity of expectation and the Fourier Transform, $S_{\mathcal{Y}}(f)$ can be expressed as:

$$\begin{aligned} S_{\mathcal{Y}}(f) = \sigma_\nu^2 + \sum_{p_1=1}^{P} h_{2p_1-1} \sum_{p_2=1}^{P} h^*_{2p_2-1} \lim_{N\to\infty} \frac{1}{2N+1} \cdot \\ \cdot \sum_{k_1^1=-N}^{N} \cdots \sum_{k_{2p_1-1}^1=-N}^{N} \sum_{k_1^2=-N}^{N} \cdots \sum_{k_{2p_2-1}^2=-N}^{N} \\ E\left[a_{k_1^1} \cdot \ldots \cdot a_{k_{2p_1-1}^1} \cdot a^*_{k_1^2} \cdot \ldots \cdot a^*_{k_{2p_2-1}^2}\right] \cdot \\ \cdot \mathcal{F}\left\{p(t-k_1^1 T_s) \cdot \ldots \cdot p(t-k_{2p_1-1}^1 T_s)\right\} \cdot \\ \cdot \mathcal{F}\left\{p(t-k_1^2 T_s) \cdot \ldots \cdot p(t-k_{2p_2-1}^2 T_s)\right\}^* \end{aligned} \qquad (6)$$

For commonly used digital modulation schemes, $a_k's$ can be assumed to be uncorrelated, zero-mean random variables. This allows for a significant simplification of (6), because $E\left[a_{k_1^1} \cdot \ldots \cdot a_{k_{2p_1-1}^1} \cdot a^*_{k_1^2} \cdot \ldots \cdot a^*_{k_{2p_2-1}^2}\right]$ takes values unequal to zero only when among $(2p_1-1)+(2p_2-1)$ indices k, all groups of indices that take the same values have size that is an even number. Therefore, for a known pulse-shaping filter, the psd (6) can be simplified and expressed as a function of even order central moments of the (potentially distorted) random sequence (a_k), and coefficients of the nonlinearity of the amplifier. For a 5^{th} order odd polynomial representation of PAs I/O characteristic ($P = 3$ in (6)), which according to [10] allows for a good accuracy of modeling practical RF amplifiers that does not meaningfully increase with the increase of the polynomial order, (6) can be reduced to:

$$\begin{aligned}
&S_{\mathcal{Y}}(f, CM2, CM4, CM6, CM8, CM10, h_1, h_3, h_5) = \\
&= h_1^2 \cdot CM2 \cdot R_1(f) + h_1 h_3 (CM4 \cdot R_2(f) + \\
&+ CM2^2 \cdot R_3(f)) + h_1 h_5 (CM6 \cdot R_4(f) + CM2 \cdot CM4 \cdot \\
&\cdot R_5(f) + CM2^3 \cdot R_6(f)) + h_3^2 (CM6 \cdot R_7(f) + CM2 \cdot \\
&\cdot CM4 \cdot R_8(f) + CM2^3 \cdot R_9(f)) + h_3 h_5 (CM8 \cdot R_{10}(f) + \\
&+ CM6 \cdot CM2 \cdot R_{11}(f) + CM4^2 \cdot R_{12}(f) + CM4 \cdot \\
&\cdot CM2^2 \cdot R_{13}(f) + CM2^4 \cdot R_{14}(f)) + h_5^2 (CM10 \cdot \\
&\cdot R_{15}(f) + CM6 \cdot CM4 \cdot R_{16}(f) + CM6 \cdot CM2^2 \cdot R_{17}(f) + \\
&+ CM4 \cdot CM2^3 \cdot R_{18}(f) + CM2^5 \cdot R_{19}(f)) + \sigma_\nu^2
\end{aligned} \tag{7}$$

where $CMK's$ are K^{th} central moments of a_k and $R_l(f)'s$ only depend on the pulse $p(t)$ used for pulse-shaping and can be easily found as sums of products of Fourier Transforms of products of time shifted pulses $p(t)$. Although $N \to \infty$ in (6), in practice these sums are finite, because practical pulses have finite lengths and their shifted versions overlap only up to a given finite relative time shift. Eq. (7) shows how the psd changes with the change of the moments of the data symbols that can be caused by distortions intentionally injected by the sophisticated user.

Eq. (4) is a well known formula for a periodogram spectral estimator [11]. Because such an estimator relies on random data of limited length, at each frequency the estimate of the psd is a random variable itself. Although the mean value of the estimate goes to the true value as $N \to \infty$, the variance is unaffected by the length of the captured time sequence [11]. The variance of the estimate can only be reduced by averaging the periodograms calculated over multiple data sequences. Values of the periodogram at each frequency asymptotically behave like independently distributed Chi-square (for non averaged periodogram) or Gamma (for averaged periodogram) random variables with mean value equal to the true value of the psd [12]. Hence a likelihood ratio test can be performed to reveal the identity of the masquerading user. Two hypotheses of the test are: $\mathcal{H}_1$-masquerading user is user 1, $\mathcal{H}_2$-masquerading user is user 2, and the likelihood ratio test is:

$$\Lambda = \frac{p_{S_{\mathcal{Y}}|\mathcal{H}_1}(S_{\mathcal{Y}}|\mathcal{H}_1)}{p_{S_{\mathcal{Y}}|\mathcal{H}_2}(S_{\mathcal{Y}}|\mathcal{H}_2)} \underset{\mathcal{H}_2}{\overset{\mathcal{H}_1}{\gtrless}} \tau \tag{8}$$

Because the hypotheses are equally probable, for uniform costs a threshold that minimizes the risk of the test is $\tau = 1$. For a more general case of the averaged periodogram the likelihood functions are:

$$p_{S_{\mathcal{Y}}|\mathcal{H}_i}(S_{\mathcal{Y}}|\mathcal{H}_i) = \prod_{k=1}^{N_{FFT}} S_{\mathcal{Y}}(f_k)^{\kappa-1} \frac{\exp\{-S_{\mathcal{Y}}(f_k)/\Theta_i(f_k)\}}{\Gamma(\kappa)\Theta_i(f_k)^\kappa} \tag{9}$$

where N_{FFT} is length of FFT used to calculate the discrete version of $Y(f)$ in (4), κ is a shape parameter of the Gamma distribution that is equal to number of averaged periodograms, and $\Theta_i(f_k)$ is a scale parameter of the Gamma distribution at frequency f_k that under hypothesis i is equal to:

$$\Theta_i(f_k) = \mu_i(f_k)/\kappa \tag{10}$$

where $\mu_i(f_k)$ is the true value of the psd at frequency f_k. With (9) the likelihood ratio test from (8) can be rewritten as:

$$\sum_{k=1}^{N_{FFT}} S_{\mathcal{Y}}(f_k) \frac{\Theta_1(f_k) - \Theta_2(f_k)}{\Theta_1(f_k) \cdot \Theta_2(f_k)} - \kappa \cdot \ln\left(\frac{\Theta_1(f_k)}{\Theta_2(f_k)}\right) \underset{\mathcal{H}_2}{\overset{\mathcal{H}_1}{\gtrless}} 0 \tag{11}$$

In practice true psd values $\mu_i(f_k)$ from (10) are not available and accurate estimates of the psd's $\hat{\mu}_i(f_k)$ obtained when users are employing their true identities are used to calculate estimates of the scale parameters $\hat{\Theta}_i(f_k)$.

This basic test provides good performance only if the true value of the psd of the masquerading user is the same as when the user employs his/her true identity. If the masquerading user modifies moments of his/her data symbols, the performance of the likelihood test from (11) degrades significantly. However with the model from (7) it is possible to take into account changes of the psd caused by moments' modifications and accordingly correct the true psd vectors used in the likelihood ratio test. For that a knowledge of the moments of the data symbols of the masquerading user and the authorized users is needed. Since for authorized users unmodified decoded input data symbols are easily accessible, these moments can be accurately estimated. However for the masquerading user the decoded symbols are not necessarily identical to the data symbols generated at the transmitter and one cannot estimate the moments of the data symbols based on the decoded data. Therefore for the purpose of identification of the masquerading user, instead of decoding the received data, the receiver should apply functions that are the inverse of the nonlinear I/O characteristic of the amplifiers that under each hypothesis can be accurately estimated from the I/O data collected when the users are not faking their identities. Moments of the data obtained after applying these inverse functions can then be used for correction of $\hat{\mu}_i(f_k)$ and used to calculate the corrected parameters $\hat{\Theta}_i^C(f_k)$ needed for the likelihood ratio test:

$$\begin{aligned}
\hat{\Theta}_i^C(f_k) &= \frac{\hat{\mu}_i(f_k)}{\kappa} + \\
&- \frac{S_{\mathcal{Y}}(f, \widehat{CM}_i 2, \widehat{CM}_i 4, \widehat{CM}_i 6, \widehat{CM}_i 8, \widehat{CM}_i 10, \hat{h}_{i,1}, \hat{h}_{i,3}, \hat{h}_{i,5})}{\kappa} + \\
&+ \frac{S_{\mathcal{Y}}(f, \widehat{CM}_i' 2, \widehat{CM}_i' 4, \widehat{CM}_i' 6, \widehat{CM}_i' 8, \widehat{CM}_i' 10, \hat{h}_{i,1}, \hat{h}_{i,3}, \hat{h}_{i,5})}{\kappa}
\end{aligned} \tag{12}$$

where $\hat{\mu}_i(f_k)$ is psd estimated accurately for user i when he/she was employing his/her true identity, $S_{\mathcal{Y}}$ is the model from (7), $\widehat{CM}_iK$ and $\widehat{CM}_i'K$ are, respectively, K^{th} central moments of the data symbols accurately estimated for the authorized user i and K^{th} central moments of data symbols of the masquerading user obtained after applying functions inverse to the estimated nonlinearity of the amplifier under hypothesis $\mathcal{H}_i$. The $\hat{h}_{i,j}$ are estimated j^{th} coefficients of the odd 5^{th} order polynomial approximation of the I/O characteristic of amplifier of user i.

IV. Numerical Results

To be able to verify the utility of the proposed method, insight on the variations of the I/O characteristics of amplifiers used in practical applications is needed. I/O characteristics of two MAXIM MAX2242 WLAN amplifiers [13] loaded on MAX2242EVKIT evaluation boards were measured on a $12.5GHz$, $50GSa/s$ real time oscilloscope at the frequency $f = 2.45GHz$. Very accurate odd 13^{th} order polynomial models were used to approximate these characteristics. These polynomials were then used for generation of the amplified data in MATLAB. The input data symbols were assumed to be real numbers (one-dimensional digital modulation), which, motivated by the transmitted signal in orthogonal frequency division multiplexing (OFDM) systems, were modeled as realizations of zero-mean normal random variables with standard deviation σ_X. The value of σ_X was chosen such that 90% of the symbols where within the range specified as linear for the considered amplifiers [13]. All symbols that exceeded the linear range were clipped to the value of the border of that range. 500 input vectors containing 100000 data symbols were generated and filtered with a raise cosine pulse-shaping filter with roll-off factor $\beta = 0.5$, length $L = 7 \cdot T_s$ and sampling frequency $f_F = \frac{8}{T_s}$. Two sets of 500 amplified data vectors were generated for the two MAXIM amplifiers using the accurate odd 13^{th} order polynomial approximations of the measured I/O characteristics. Gaussian noise was added to the pulse-shaped, amplified data vectors. Based on the 500 data vectors and respective noisy amplified data vectors normalized to the gain $G = 1$, coefficients of odd polynomials of 5^{th} order were obtained to model nonlinearity characteristics of both amplifiers. The averaged periodograms (averaged over 500 sequences) were obtained for pulse-shaped, amplified, noisy and normalized outputs oversampled with ratio $M = 8$ and used as estimates of true psd values $\hat{\mu}_i(f_k)$ needed to calculate parameters $\hat{\Theta}_i(f_k)$ for (11). An FFT length of $N_{FFT} = 32768$ was chosen to obtain $Y(f_k)$ used to calculate the periodograms (4). Estimates of the moments of the data symbols $\widehat{CM}_iK$, $K = 2, 4, 6, 8, 10$ from (12) were obtained based on the 500 input data vectors.

Next, 5 input vectors of size 100000 were generated, pulse-shaped and amplified with the amplifier of the masquerading user. Noise was added to the amplified signals. The periodogram averaged over the 5 pulse-shaped, amplified, noisy signals oversampled with ratio $M = 8$ and normalized to gain $G = 1$ was calculated, and used as an input vector $S_{\mathcal{Y}}(f_k)$ for the likelihood ratio test (11). Because spectral regrowth of the psd caused by the nonlinearities of the amplifiers is very small, for the considered raise cosine pulse-shaping filter with a roll-off factor $\beta = 0.5$ only frequencies lower than $1.6 \cdot \frac{1}{T_s}$ were used to calculate the likelihood functions (9). Regrowth caused by the nonlinearities was negligibly small at higher frequencies. Figure 2 shows good performance of the likelihood ratio test from (11) when user 1 was masquerading, but not modifying his data symbols. However if the masquerading user modifies the moments of his/her input symbols, the performance of the likelihood ratio test can decrease significantly. Figure 2 shows degradation of the performance of the test when the masquerading user 1 modifies moments of his/her input data symbols by applying the nonlinear function of user 2 (normalized to a gain equal to 1) in order to fake his/her signature.

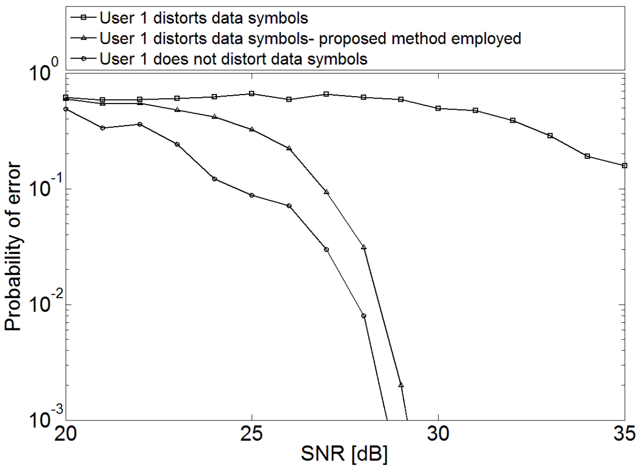

Fig. 2. Probability of error as a function of SNR (calculated over 3000 trials) of identification decision based on the likelihood ratio test from (11) for a pair of MAXIM MAX2242 amplifiers; 5 vectors of size 100000 captured from the masquerading user.

As a countermeasure for this undesired activity of the sophisticated user, the approach from Section III was followed at the receiver. $R_l(f)$ functions ($l = 1, \ldots, 19$) from (7) were calculated for the raise cosine pulse-shaping filter with the roll-off factor $\beta = 0.5$. Estimates of moments of the modified data symbols ($\widehat{CM}_i'K$, $K = 2, 4, 6, 8, 10$ from (12)) were estimated under both hypotheses by applying inverses to the estimated odd 5^{th} order polynomials modeling normalized I/O characteristics of the amplifiers. Corrected parameters $\hat{\Theta}_i^C(f_k)$ were calculated with (12) and used for the likelihood ratio test. Figure 2 shows the effectiveness of the approach. As can be seen, corrections of the estimated true value vectors $\hat{\mu}_i(f_k)$ allowed for efficient identification of the sophisticated user 1 that was trying to fake his/her signature by nonlinearly modifying the data symbols.

V. Conclusions

In this work, for the first time, we consider the problem of identification of sophisticated users that actively fake their RF signatures with artificial injection of slight distortion to the data symbols. While this is unlikely for a standard criminal employing a wireless card, its possibility motivates the consideration of techniques to address such. Our identification method does not require strict assumptions on the distribution of the data symbols. It is only assumed that elements of the data symbol stream are uncorrelated and have zero mean values. As shown with simulations based on parameters of commercially used PAs, application of the proposed method allows for the prevention of the performance degradation caused by modification of the data by the sophisticated users, as results are similar to those when criminals are not sophisticated enough to modify the data symbols. Because of the high data rates of modern communications networks, the relatively long data records that need to be captured to perform identification do not require long observation times of the masquerading users.

References

[1] S. Dolatshahi, A. Polak and D. Goeckel, “Identification of Wireless Users via Power Amplifier Imperfections,” *Asilomar Conference on Signals, Systems, and Computers*, November 2010.

[2] A. Polak, S. Dolatshahi and D. Goeckel, “Identifying Wireless Users via Transmitter Imperfections,” to appear in the *IEEE Journal on Selected Areas in Communications- Special Issue on Advances in Digital Forensics for Communications and Networking*, August 2011.

[3] N. Patwari and S. Kasera, “Robust location distinction using temporal link signatures,” *ACM MOBICOM*, 2007.

[4] Y. Sheng, K. Tan, G. Chen, D. Kotz and A. Campbell, “Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength,” *27th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, April 2008.

[5] J. Hall, M. Barbeau and E. Kranakis,“Enhancing intrusion detection in wireless networks using radio frequency fingerprinting,” *3rd IASTED International Conference on Communications,Internet and Information Technology (CIIT)*, November 2004.

[6] J. Hall,“Detection of Rogue Devices in Wireless Networks,” ,PhD Dissertation, School of Computer Science, Carleton University, Ottawa, Ontario, 2006.

[7] O. Ureten and N. Serinken,“Wireless Security Through RF Fingerprinting,” *Canadian Journal of Electrical and computer Engineering*, Winter 2007.

[8] V. Brik, S. Banerjee, M. Gruteser and S.Oh,“Wireless Device Identification with Radiometric Signatures,” *Proceedings of the 14th ACM international conference on Mobile computing and networking*, March 2008.

[9] I. Kennedy, P. Scanlon and B. Buddhikot,“Passive RF Fingerprinting: A Cognitive Technique for Scalable Deployment of Co-channel Femto Cell Underlays,” *IEEE Dynamic Spectrum Access Networks Conference*, 2008.

[10] M. Isaksson, D. Wisell and D. Ronnow,“A Comparative Analysis of Behavioral Models for RF Power Amplifiers,” *IEEE Transactions on Microwave Theory and Techniques*, January 2006.

[11] Steven M. Kay,“Modern Spectral Estimation: Theory and Application,” Prentice Hall, 1988.

[12] H. Ombao, J. Raz and R. Von Sachs,“A Simple Generalized Crossvalidation Method of Span Selection for Periodogram Smoothing,” *Biometrika*, vol. 88, 2001.

[13] Data Sheet, MAXIM MAX2242, 2.4GHz to 2.5GHz Linear Power Amplifier: http://datasheets.maxim-ic.com/en/ds/MAX2242.pdf