Identifying Wireless Users via Transmitter Imperfections

Adam C. Polak, Sepideh Dolatshahi, and Dennis L. Goeckel, *Fellow, IEEE*

***Abstract*—Variations in the RF chain of radio transmitters can be used as a signature to uniquely associate wireless devices with a given transmission. Previous approaches, which have varied from transient analysis to machine learning, do not provide verifiable accuracy, which is essential for admissibility of the methods in the court. Here we detail a first step toward a model-based approach, which uses statistical models of RF transmitter components that are amenable for analysis. Algorithms based on statistical signal processing methods are developed to exploit non-linearities of wireless transmitters for the purpose of user identification in wireless systems. The decision rules are derived and their performance is analyzed. In order to establish the viability of the proposed approach, the practical variations of transmitter chain components are analyzed based on simulations, measurements and manufacturers' specifications. Results show that the proposed identification methods can be effective, even for short data records and relatively low signal-to-noise ratios, when exploiting imperfections of commercially used RF transmitters.**

***Index Terms*—Radiometric identification, Volterra series, Brownian Bridge, Likelihood Ratio Test, breaking anonymity, process variations.**

I. Introduction

THE UBIQUITY of mobile computing has revolutionized certain types of crime. Sexual exploitation of children [1], software piracy [2], intellectual property and identity theft [3], financial fraud [4] and many others are examples of violations that have become easier and cheaper due to the expansion of the Internet. Furthermore, the exploitation of widespread, open wireless access points (APs) hosted by private homes, businesses, and municipalities provides offenders with significant anonymity, making it difficult to identify them. Most of the current digital forensic techniques focus on desktop systems on the wired Internet and exploit artifacts like IP addresses and MAC addresses as consistent tags uniquely characterizing the users for identification. However MAC addresses can be easily reconfigured by the users. Also, the consistency of the IP addresses is questionable in wireless access networks, as wireless offenders can simply drive around, use different access points and commit the crimes with different, temporarily assigned, IP addresses each time [5], [6].

This work concentrates on breaking criminals' anonymity in wireless systems. The proposed digital forensics approach exploits the standard assumption that a criminal at some point of time employs his/her true identity. An exemplary scenario, where the proposed work might find its application, is as follows: investigators searching a popular file sharing network come across a user sharing contents associated with child sexual exploitation. Determination of the street address based on the IP address leads them to an apartment building in a busy municipal area. After a voluntary interview the investigators prove the innocence of the apartment's occupant. They monitor the area and discover that third-parties with a series of MAC addresses regularly connect to the occupant's network; however, none of the MAC addresses matches the recorded MAC address of the offender. Furthermore given the density of the private apartments and businesses in the area, these radios cannot be located with sufficient geographical accuracy. At this point, the investigation would normally end unsolved.

Using the techniques we propose, the investigators could monitor the area and record characteristics (Radio Frequency fingerprints) of wireless users. They then note that several MAC addresses that connect to the occupant's wireless router all have consistent radio properties, suggesting they are aliases of a single transmitter. During further observations investigators discover that a machine with matching transmitter characteristics is using an open Internet AP at a cafe nearby most mornings. Investigators sit in the cafe and measure the characteristics of machines that are in use. A user with matching transmitter characteristics appears to be a young man living in an apartment across the street. The investigators state a match of his transmitter's characteristics with characteristics of the transmitter that regularly connects to occupant's network, and present records from the file sharing network to a magistrate. The magistrate issues a warrant. The contents associated with child sexual exploitation are found on man's hard drive, and he is arrested.

There has been a number of Radio Frequency fingerprinting efforts over the years. These can roughly be divided into two main approaches. The first of the approaches exploits channel information. In a rich multi-path environment, because of rapid path decorrelation, users can be almost uniquely characterized by their channel conditions. This property allows for grouping transmissions from stationary users [7], [8], [9], [10]. Another channel based fingerprinting technique uses the received signal strength information (RSSI) to distinguish transmitters [11], [12]. Both of these techniques make a strong assumption on user's stationarity, which makes them unapplicable in many practical scenarios, like the one described as the exemplary scenario in the previous paragraph.

The second main fingerprinting approach, which this work

Manuscript received 1 August 2010; revised 31 December 2010 and 31 January 2011. A preliminary version of this work appeared at the Asilomar Conference on Signals, Systems, and Computers. This paper is based in part upon work supported by the National Science Foundation under grant CNS-0905349.

The authors are with

Digital Object Identifier 10.1109/JSAC.2011.1107xx.

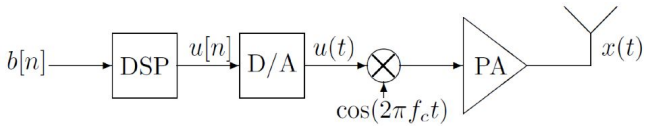

Fig. 1. Basic components of wireless transmitter, imperfections of which can be exploited for user identification.

is following, exploits hardware imperfections of the RF devices. At the physical layer, despite decades of significant efforts by the microwave circuits community, there still exist longstanding imperfections in the RF portion of the wireless transmitter. Furthermore, since these cannot be altered by the user without significant effort, they can be exploited to group together signals from one radio. There has been a number of efforts over the years to utilize the hardware imperfections for the purpose of distinguishing the users. Much of the work has focused on the detection and analysis of transients (e.g. [13], [14], [15]). A transient is a brief radio emission produced while the power of the output of an RF transmitter goes from zero to the level required for data communication. Transient durations range from a few microseconds to tens of milliseconds. Their nature is such that they are difficult to detect and to describe in a succinct way. In [16] slight deviations of clock skews are proposed as unique parameters characterizing physical devices of the Internet users. In [17] authors build histograms of features like received power, or frequency error for each packet from each network user. Then they extract user fingerprints as parameters used to fit the histograms to a Gaussian model and use these parameters for user identification. Recently Brik et al [18] followed the hardware fingerprinting approach and used machine learning techniques on collected modulation data to train data-agnostic classifiers that are then able to distinguish wireless cards, even when produced by the same vendor.

Our broad approach to device modeling, algorithm design and anonymity analysis is significantly different from prior efforts. In particular, in contrast to the recent empirical classification results of [18] on commercial 802.11 cards, the approach here is focused on a comprehensive understanding and exploitation of the phenomena being exploited for node identification. It is based on statistical models amenable for analysis, allowing us to answer questions about key device characteristics that cause anonymity loss, about possible countermeasures that can be applied by the nodes to regain the anonymity, and about ways of thwarting such countermeasures. Furthermore, and most importantly, the proposed model based approach allows for verifiable accuracy, which is essential for admissibility of the methods in court.

A simplified block diagram of a wireless transmitter is shown in Figure 1. Each of the components of the transmitter chain demonstrates imperfections caused by nonidealities of production processes. MOS transistors, which the components' circuits are made of, exhibit broad variations in major device parameters (eg. channel length, channel doping concentration, oxide thickness) among production lots. These variations may occur for many reasons, such as minor changes in the humidity or temperature in the clean-room, or due to the position of the die relative to the center of the wafer. Changes of the parameters influence transistors switching speed and thereby components' characteristics. Similarly, parameters of passive electronic devices, rather than taking a constant specified value, follow distributions caused by production inaccuracies. Despite technological advancements, constant market push for low-price, high-volume products results in variations among individual devices caused by the production imperfections. These variations, while being small enough for the devices to meet specifications of communication standards, are significant enough to allow for unique characterization of these devices via RF fingerprints.

In this work we concentrate our attention on two components of the transmitter's chain from Figure 1: the digital-to-analog converter (DAC) and the power amplifier (PA). Nonidealities of the oscillators are ignored because the carrier frequency offsets do not necessarily have to result from the hardware imperfections, but can be introduced by masquerading nodes via software manipulations.

II. Problem Statement

Consider the block diagram shown in Figure 1. A digital (discrete-time, discrete-amplitude) baseband signal $u[n]$ that carries the information bits is generated by a digital signal processor (DSP) and converted to an analog signal $u(t)$ by a digital-to-analog converter. Then it is translated to the desired carrier frequency by the mixer and amplified by the power amplifier. In an ideal system, the transmitted signal would be given by:

$$x(t) = Au(t)\cos(2\pi f_c t + \Theta) \tag{1}$$

where A is the gain of the power amplifier, $u(t)$ is the ideal analog form of $u[n]$ (i.e. the $sinc(\cdot)$-interpolated version of $u[n]$), f_c is the desired carrier frequency, and Θ is the (constant) phase of the oscillator. However the digital-to-analog converters suffer from the finite precision of the digital input and more importantly, particularly for forensics work, demonstrate nonlinearities, which can vary significantly across individual units. Similarly, PAs, which seek to have linear characteristics such that the response to input $u(t)$ is $Au(t)$, are often quite nonlinear even with significant compensation. As in case of the DACs, the nonlinearity variations of PAs can be significant across the devices. Because of these variations, each user in a multiple user network can be characterized with a group of parameters that uniquely describe input/output (I/O) characteristics of its transmitter components. These parameters can then be used by access points for the purpose of user identification.

The goal of this work is to tie criminal transmissions of a user to other transmissions of that same user. Under the assumption that a user employs his/her true identity at some point, this allows us to identify the offending party. The exemplary scenario of Section I gives a clear example of the utility of such an approach. To simplify the exposition, this work considers a setup shown in Figure 2 for the two-user case, but the generalization to the case of n users is straightforward (using n-hypothesis testing techniques). Each of the users in Figure 2 is characterized with a parameter vector $\underline{\boldsymbol{h}}_i$, $i = 1, 2$. Because access points in wireless networks perform inverse operations to all operations performed by the

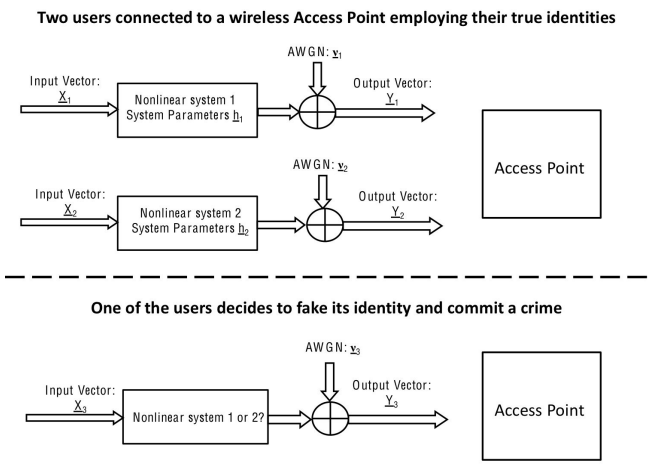

Fig. 2. The two-system identification scenario: two authorized users employ their true identities (upper part); one of the users decides to fake its identity and commit a crime (lower part). An additive white Gaussian noise (AWGN) channel model is assumed.

transmitters of wireless users (demodulation, A/D conversion, decoding etc.), in this work it is reasonable to assume that input samples (which can be reconstructed from the decoded data) and corresponding noise-corrupted output samples are accessible for all elements of the transmitter chain, in particular for both considered components: DACs and PAs, if the rest of the chain is assumed linear. The input vectors of a considered component of user one and user two are denoted as $\underline{\boldsymbol{X}}_1$ and $\underline{\boldsymbol{X}}_2$, respectively, and their respective output vectors are $\underline{\boldsymbol{Y}}_1$ and $\underline{\boldsymbol{Y}}_2$. These correspond to the case when the users are employing their true identities, which they assume at some time when they are not committing a crime. Now, at some point in time, one of the users decides to fake its identity and to commit a crime. The binary hypothesis problem is to identify this user given access to $\underline{\boldsymbol{X}}_i$ and $\underline{\boldsymbol{Y}}_i$, $i = 1, 2, 3$. In other words, it needs to be found out which of the two transmitters vector $\underline{\boldsymbol{X}}_3$ passed through, so that it resulted in $\underline{\boldsymbol{Y}}_3$.

III. Modeling Transmitter Components

Both considered transmitter components display nonlinearities of their I/O characteristics. In general the I/O characteristic of a given transmitter component, for user i, can be described with a matrix equation of the form:

$$\underline{\boldsymbol{Y}}_i = P_i \underline{\boldsymbol{h}}_i + \underline{\boldsymbol{\nu}}_i \quad ; \quad i = 1, 2 \tag{2}$$

where P_i is a matrix, elements of which are nonlinear functions of elements of the input vector $\underline{\boldsymbol{X}}_i$. These functions are determined by the model adopted for a given *type* of transmitter component (i.e. DAC or PA) and are the same for all devices of that type (i.e. they do not vary across DACs or across PAs), which will be described in the successive subsections. The $\underline{\boldsymbol{h}}_i$ vector is a column vector that contains the unique component parameters of user i and $\underline{\boldsymbol{\nu}}_i$ is an additive white Gausssian noise (AWGN) vector $\sim \mathcal{N}(0, \sigma_\nu^2)$. In the next two subsections, mathematical models that allow for the construction of matrices P_i for both DACs and PAs are introduced.

A. DAC

An N-bit DAC converts an N-bit input word to one of $n = 2^N - 1$ analog output values. One of the most important parameters of the DAC is the integral nonlinearity (INL). The INL specifies the deviation of the actual DAC's output level for a given input word from the ideal output level and is defined as:

$$INL_x = \frac{I_{out,x} - x \cdot I_{LSB}}{I_{LSB}} \tag{3}$$

where $I_{out,x}$ is the output level generated by an input word x, and I_{LSB} is the maximal output level divided by the number of all input words:

$$I_{LSB} = \frac{I_{out,(2^N-1)}}{2^N - 1} \tag{4}$$

The I/O relation of the DAC can thus be expressed as:

$$I_{out,x} = (INL_x + x) \cdot I_{LSB} \tag{5}$$

The INL is caused by production inaccuracies that cause output levels of individual analog sources of the DAC to vary around their nominal values. If individual DAC analog sources are modeled as independent normally distributed random variables with standard deviation σ_S, then the INL of a thermometer-coded DAC, for which all analog sources have identical nominal values and for which each increase of the input word by one causes activation of an additional source, can be modeled with a discrete Brownian Bridge random process BB [19]:

$$INL_x = \sigma_s \sqrt{n} \cdot BB\left(\frac{x}{n}\right) \tag{6}$$

where recall x is an input word and n is the number of all input words. For a high number of bits N, $n = 2^{N-1}$ becomes very large and the discrete Brownian Bridge random process from (6) can be approximated with its continuous counterpart. A continuous Brownian Bridge random process is defined as:

$$BB(t) = W(t) - t \cdot W(1); \quad t \in (0, 1) \tag{7}$$

where $W(t)$ is a Wiener random process [20]. A Wiener random process takes value equal to zero for $t = 0$ and its increments are normally distributed random variables with variance equal to the argument difference. In other words:

$$W(0) = 0$$
$$W(t_2) - W(t_1) \sim \mathcal{N}(0, t_2 - t_1) \tag{8}$$

Using the Karhunen-Loeve theorem, a continuous Brownian Bridge random process can be represented with its eigenfunctions and eigenvalues found as solutions of the integral equation [20]:

$$\{\varphi_j(t) : j = 1, 2, ...\} \qquad \{\lambda_i : j = 1, 2, ...\}$$
$$\int_0^1 R_{BB}(t, \tau) \cdot \varphi_j(\tau) d\tau = \lambda_j \varphi_j(t); \quad t \in (0, 1) \tag{9}$$

where R_{BB} is the autocorrelation function of the Brownian Bridge random process. Solutions of this equation are:

$$\varphi_j(t) = \frac{\sqrt{2}}{\pi j} \sin(\pi j t) \quad ; \quad \lambda_j = 1$$

$$j = 1, \ldots, \infty \tag{10}$$

and the Karhunen-Loeve expansion of the the continuous Brownian Bridge is:

$$BB(t) = \lim_{J\to\infty} \sum_{j=1}^{J} \frac{\Lambda_j}{\pi j} \cdot \sqrt{2} sin(\pi \cdot j \cdot t) \tag{11}$$

where Λ_j are i.i.d. normal random variables $\sim \mathcal{N}(0, \lambda_j)$. After replacing the continuous argument t with x/n, the I/O characteristic of the DAC can be described with the matrix equation:

$$\frac{\underline{\boldsymbol{I}}_{i,out} - \underline{\boldsymbol{X}}_i \cdot I_{LSB,i}}{I_{LSB,i}} = BB(\underline{\boldsymbol{X}}_i/n) + \frac{\underline{\boldsymbol{\nu}}_i}{I_{LSB,i}} \tag{12}$$

which, when using the J first eigenfunctions to approximate the process has form (13) (see the top of the next page), where M is the length of the input sequence. This with:

$$\underline{\boldsymbol{Y}}_i = \frac{\underline{\boldsymbol{I}}_{i,out} - \underline{\boldsymbol{X}}_i \cdot I_{LSB,i}}{I_{LSB,i}} \tag{15}$$

and (14) (see the top of the next page) is the I/O equation introduced with (2). Elements of the vector $\underline{\boldsymbol{h}}_i$ are realizations of J random variables $\frac{\Lambda_j}{\pi j}$ (eigenvalues of the Brownian Bridge random process) that uniquely describe the single INL path of user i. Because of the assumption that the component's input and output signals $\underline{\boldsymbol{X}}_i$ and $\underline{\boldsymbol{Y}}_i$ are known and because of the existence of a fixed model for the I/O relation, the only parameters that the receiver needs to estimate to build the digital signature of a user i are elements of the vector $\underline{\boldsymbol{h}}_i$. Algorithms and numerical results for the adopted models of the transmitter components are reserved for Sections IV and V respectively.

B. Power Amplifier

Power amplifiers are attractive for digital forensics purposes in that they are the last elements of the transmitter chain and thus are the most difficult for a user to modify via software or even baseband control. In this work the nonlinear characteristics of power amplifiers are modeled with Volterra series representations, as well-established in the microwave literature (see Chapter 4 of [21]). For the sake of exposition, we use a Volterra series representation with a memory of one and an order of two (a linear quadratic system), but the extension to higher memory and orders is straightforward. Hence the I/O relation is:

$$\begin{aligned}\underline{\boldsymbol{Y}}_i(n) &= \Sigma_{k_1=0}^{1} h_{i,1}(k_1)\underline{\boldsymbol{X}}_i(n-k_1) + \\ &+\Sigma_{k_1=0}^{1}\Sigma_{k_2=0}^{1} h_{i,2}(k_1,k_2)\underline{\boldsymbol{X}}_i(n-k_1)\underline{\boldsymbol{X}}_i(n-k_2) + \underline{\boldsymbol{\nu}}_i(n) = \\ &= h_{i,1}(0)\underline{\boldsymbol{X}}_i(n) + h_{i,1}(1)\underline{\boldsymbol{X}}_i(n-1) + h_{i,2}(0,0)\underline{\boldsymbol{X}}_i^2(n) + \\ &+h_{i,2}(1,1)\underline{\boldsymbol{X}}_i^2(n-1) + h_{i,2}(0,1)\underline{\boldsymbol{X}}_i(n)\underline{\boldsymbol{X}}_i(n-1) + \underline{\boldsymbol{\nu}}_i(n)\end{aligned} \tag{16}$$

The parameter vector $\underline{\boldsymbol{h}}_i$ contains the Volterra coefficients capturing the I/O characteristic of amplifier i. For the considered Volterra representation:

$$\underline{\boldsymbol{h}}_i = \begin{bmatrix} h_{i,1}(0) & h_{i,1}(1) & h_{i,2}(0,0) & h_{i,2}(1,1) & h_{i,2}(0,1) \end{bmatrix}^T \tag{17}$$

Similarly as in case of the DAC, the I/O relation of the PA can be characterized with the matrix equation of the form (2), with the matrix P_i being built out of the nonlinear functions of the inputs required in (16) for an input vector of length M (i.e. the "kernels" of the Volterra representation) and with the vector $\underline{\boldsymbol{h}}_i$ built out of the Volterra coefficients. Hence the I/O relation has form (18) (see the top of the next page).

Recall that the *model* is common to all PAs, and hence is known to the receiver. Therefore, with assumed knowledge of the inputs $\underline{\boldsymbol{X}}_i(n), \underline{\boldsymbol{X}}_i(n-1), ...\underline{\boldsymbol{X}}_i(n-M)$ at the access point (recall that the access point is decoding the data packets of the user), the matrix P_i containing known nonlinear combinations of known inputs is known by the receiver. All that is to be estimated to build the digital signature of user i are the elements of the vector $\underline{\boldsymbol{h}}_i$.

IV. Algorithms

Having modeled the nonlinear transmitter components, algorithms for solving the hypothesis testing problem stated in Section II are developed next. First we consider the case when the parameter vectors $\underline{\boldsymbol{h}}_1$ and $\underline{\boldsymbol{h}}_2$ of users 1 and 2, respectively, are exactly known in order to find an upper bound on the identifiability in the noisy channel. This assumption is also practically reasonable when the users can be observed over a long period of time that allows for a very accurate parameter estimation or when the parameters are obtained and saved before the transmitters are available on the market. Under this assumption, well-defined, optimal methods are known for solving the hypothesis testing problem. Next, we consider a scenario when the parameters are unknown and only short observations: $\underline{\boldsymbol{X}}_i, \underline{\boldsymbol{Y}}_i$, $i = 1, 2, 3$ are available. In this case the optimal method is not straightforward and multiple approaches are considered.

A. Likelihood Ratio Test with Known Parameter Vectors

1) Decision Rule: If the parameter vectors describing the nonlinear aspects of the user's transmitters are exactly known, then, in the case of uniform costs, the probability of error of the receiver is minimized by a likelihood ratio test (LRT). Formally, define the following hypotheses: $\mathcal{H}_1$- the masquerading user is user one; $\mathcal{H}_2$- the masquerading user is user 2. For equally probable hypotheses, the decision rule for solving the problem presented in Section II is then:

$$\Lambda(\underline{\boldsymbol{Y}}_3) \triangleq \frac{P_{\underline{\boldsymbol{Y}}_3|\underline{\boldsymbol{h}}_1,\underline{\boldsymbol{X}}_3}(\underline{\boldsymbol{Y}}_3|\underline{\boldsymbol{h}}_1,\underline{\boldsymbol{X}}_3)}{P_{\underline{\boldsymbol{Y}}_3|\underline{\boldsymbol{h}}_2,\underline{\boldsymbol{X}}_3}(\underline{\boldsymbol{Y}}_3|\underline{\boldsymbol{h}}_2,\underline{\boldsymbol{X}}_3)} \underset{\mathcal{H}_2}{\overset{\mathcal{H}_1}{\gtrless}} 1 \tag{19}$$

where $P_{\underline{\boldsymbol{Y}}_3|\underline{\boldsymbol{h}}_i,\underline{\boldsymbol{X}}_3}(\underline{\boldsymbol{Y}}_3|\underline{\boldsymbol{h}}_i,\underline{\boldsymbol{X}}_3)$, $i = 1, 2$ are the conditional probability density functions. In the AWGN channel:

$$\begin{aligned}P(\underline{\boldsymbol{Y}}_3 \,|\, \underline{\boldsymbol{h}}_i, \underline{\boldsymbol{X}}_3) &= \frac{1}{(\sqrt{2\pi}\sigma_\nu^2)^M} \times \\ &\times \exp\left\{ -\frac{(\underline{\boldsymbol{Y}}_3 - P_3 \cdot \underline{\boldsymbol{h}}_i)^H (\underline{\boldsymbol{Y}}_3 - P_3 \cdot \underline{\boldsymbol{h}}_i)}{2\sigma_\nu^2} \right\} \\ &i = 1, 2\end{aligned} \tag{20}$$

$$\frac{\underline{\boldsymbol{I}}_{i,out} - \underline{\boldsymbol{X}}_i \cdot I_{LSB,i}}{I_{LSB,i}} =$$

$$= \sqrt{2} \begin{bmatrix} sin(\pi \cdot 1 \cdot \underline{\boldsymbol{X}}_i(1)/n) & sin(\pi \cdot 2 \cdot \underline{\boldsymbol{X}}_i(1)/n) & \cdots & sin(\pi \cdot J \cdot \underline{\boldsymbol{X}}_i(1)/n) \\ sin(\pi \cdot 1 \cdot \underline{\boldsymbol{X}}_i(2)/n) & sin(\pi \cdot 2 \cdot \underline{\boldsymbol{X}}_i(2)/n) & \cdots & sin(\pi \cdot J \cdot \underline{\boldsymbol{X}}_i(2)/n) \\ \vdots & \vdots & \ddots & \vdots \\ sin(\pi \cdot 1 \cdot \underline{\boldsymbol{X}}_i(M)/n) & sin(\pi \cdot 2 \cdot \underline{\boldsymbol{X}}_i(M))/n & \cdots & sin(\pi \cdot J \cdot \underline{\boldsymbol{X}}_i(M)/n) \end{bmatrix} \cdot \begin{bmatrix} h_i(1) \\ h_i(2) \\ \vdots \\ h_i(J) \end{bmatrix} + \frac{\boldsymbol{\nu}_i}{I_{LSB,i}} \tag{13}$$

$$P_i = \sqrt{2} \begin{bmatrix} sin(\pi \cdot 1 \cdot \underline{\boldsymbol{X}}_i(1)/n) & sin(\pi \cdot 2 \cdot \underline{\boldsymbol{X}}_i(1)/n) & \cdots & sin(\pi \cdot J \cdot \underline{\boldsymbol{X}}_i(1)/n) \\ sin(\pi \cdot 1 \cdot \underline{\boldsymbol{X}}_i(2)/n) & sin(\pi \cdot 2 \cdot \underline{\boldsymbol{X}}_i(2)/n) & \cdots & sin(\pi \cdot J \cdot \underline{\boldsymbol{X}}_i(2)/n) \\ \vdots & \vdots & \ddots & \vdots \\ sin(\pi \cdot 1 \cdot \underline{\boldsymbol{X}}_i(M)/n) & sin(\pi \cdot 2 \cdot \underline{\boldsymbol{X}}_i(M))/n & \cdots & sin(\pi \cdot J \cdot \underline{\boldsymbol{X}}_i(M)/n) \end{bmatrix} \tag{14}$$

$$\underline{\boldsymbol{Y}}_i = \begin{bmatrix} \underline{\boldsymbol{X}}_i(n) & \underline{\boldsymbol{X}}_i(n-1) & \cdots & \underline{\boldsymbol{X}}_i(n-M+1) \\ \underline{\boldsymbol{X}}_i(n-1) & \underline{\boldsymbol{X}}_i(n-2) & \cdots & \underline{\boldsymbol{X}}_i(n-M) \\ \underline{\boldsymbol{X}}_i^2(n) & \underline{\boldsymbol{X}}_i^2(n-1) & \ddots & \vdots \\ \underline{\boldsymbol{X}}_i^2(n-1) & \underline{\boldsymbol{X}}_i^2(n-2) & \ddots & \vdots \\ \underline{\boldsymbol{X}}_i(n)\underline{\boldsymbol{X}}_i(n-1) & \underline{\boldsymbol{X}}_i(n-1)\underline{\boldsymbol{X}}_i(n-2) & \cdots & \underline{\boldsymbol{X}}_i(n-M+1)\underline{\boldsymbol{X}}_i(n-M) \end{bmatrix}^T \cdot \underline{\boldsymbol{h}}_i + \underline{\boldsymbol{\nu}}_i \tag{18}$$

which allows to simplify the decision rule (19) to:

$$||(\underline{\boldsymbol{Y}}_3 - P_3\underline{\boldsymbol{h}}_1)|| \underset{\mathcal{H}_1}{\overset{\mathcal{H}_2}{\gtrless}} ||(\underline{\boldsymbol{Y}}_3 - P_3\underline{\boldsymbol{h}}_2)|| \tag{21}$$

2) Algorithm Performance: The probability of error is the probability that the algorithm decides for a different user than the one that decided to fake its identity and commit the crime. In the case of the two-user scenario from Figure 2, the probability of error can be expressed as:

$$P_e = Pr\{\mathcal{H}_1\} \cdot Pr\{test\ results\ in\ \mathcal{H}_2|\mathcal{H}_1\} +$$

$$+Pr\{\mathcal{H}_2\} \cdot Pr\{test\ results\ in\ \mathcal{H}_1|\mathcal{H}_2\} \tag{22}$$

which, with the assumption of equally probable hypotheses and the symmetry of the problem reduces to:

$$P_e = Pr\{test\ results\ in\ \mathcal{H}_2|\mathcal{H}_1\} \tag{23}$$

With (21), P_e can be expressed as:

$$P_e = Pr\{(\underline{\boldsymbol{Y}}_3 - P_3\underline{\boldsymbol{h}}_1)^H(\underline{\boldsymbol{Y}}_3 - P_3\underline{\boldsymbol{h}}_1) > (\underline{\boldsymbol{Y}}_3 - P_3\underline{\boldsymbol{h}}_2)^H(\underline{\boldsymbol{Y}}_3 - P_3\underline{\boldsymbol{h}}_2)\} \tag{24}$$

which, with

$$\underline{\boldsymbol{Y}}_3 = P_3\underline{\boldsymbol{h}}_1 + \underline{\boldsymbol{\nu}}_3 \tag{25}$$

under $\mathcal{H}_1$ simplifies to:

$$P_e = Pr\left\{\underline{\boldsymbol{d}}^H P_3^H P_3 \underline{\boldsymbol{d}} - \underline{\boldsymbol{d}}^H (P_3^H \underline{\boldsymbol{\nu}}_3) - (P_3^H \underline{\boldsymbol{\nu}}_3)^H \underline{\boldsymbol{d}} < 0\right\} \tag{26}$$

where $\underline{\boldsymbol{d}} = \underline{\boldsymbol{h}}_2 - \underline{\boldsymbol{h}}_1$.

B. Likelihood Ratio Test with Estimated Parameters

1) Decision Rule: In practical applications, when parameters of the components are unknown and only short input and output vectors $\underline{\boldsymbol{X}}_i$ and $\underline{\boldsymbol{Y}}_i$, $i = 1, 2, 3$ are available, the decision rule from (21) with the true parameter values replaced with their estimates is no longer optimal. However it is still reasonable to use such a rule with the estimated parameters replacing the true values, since the result converges to the optimal rule when the parameter estimates become more and more accurate. The decision rule is then:

$$||(\underline{\boldsymbol{Y}}_3 - P_3\hat{\underline{\boldsymbol{h}}}_1)|| \underset{\mathcal{H}_1}{\overset{\mathcal{H}_2}{\gtrless}} ||(\underline{\boldsymbol{Y}}_3 - P_3\hat{\underline{\boldsymbol{h}}}_2)|| \tag{27}$$

and the probability of error P_e is:

$$P_e = Pr\left\{\hat{\underline{\boldsymbol{d}}}^H P_3^H P_3 \hat{\underline{\boldsymbol{d}}} - \hat{\underline{\boldsymbol{d}}}^H (P_3^H \underline{\boldsymbol{\nu}}_3) - (P_3^H \underline{\boldsymbol{\nu}}_3)^H \hat{\underline{\boldsymbol{d}}} < 0\right\} \tag{28}$$

where $\hat{\underline{\boldsymbol{d}}} = \hat{\underline{\boldsymbol{h}}}_2 - \hat{\underline{\boldsymbol{h}}}_1$ and $\hat{\underline{\boldsymbol{h}}}_1$ and $\hat{\underline{\boldsymbol{h}}}_2$ are estimates of the parameter vectors $\underline{\boldsymbol{h}}_1$ and $\underline{\boldsymbol{h}}_2$.

Interestingly, the decision rule from (27) can also be derived in a different way, which further motivates its usage. In particular the receiver can first estimate the parameters of the transmitters ($\hat{\underline{\boldsymbol{h}}}_1$ and $\hat{\underline{\boldsymbol{h}}}_2$) and the parameters of the masquerading unit ($\hat{\underline{\boldsymbol{h}}}_3$). Next the receiver can compare the probability density functions of the estimate $\hat{\underline{\boldsymbol{h}}}_3$ under hypothesis $\mathcal{H}_1$ (parameter vector of masquerading user is $\hat{\underline{\boldsymbol{h}}}_1$) and $\mathcal{H}_2$ (parameter vector of masquerading user is $\hat{\underline{\boldsymbol{h}}}_2$) and make a decision based on this comparison. For equally probable hypotheses, the decision rule can be expressed as:

$$\Lambda(\hat{\underline{\boldsymbol{h}}}_3) = \frac{P_{\hat{\underline{\boldsymbol{h}}}_3|\hat{\underline{\boldsymbol{h}}}_1}(\hat{\underline{\boldsymbol{h}}}_3|\hat{\underline{\boldsymbol{h}}}_1)}{P_{\hat{\underline{\boldsymbol{h}}}_3|\hat{\underline{\boldsymbol{h}}}_2}(\hat{\underline{\boldsymbol{h}}}_3|\hat{\underline{\boldsymbol{h}}}_2)} \underset{\mathcal{H}_2}{\overset{\mathcal{H}_1}{\gtrless}} 1 \tag{29}$$

The estimates $\hat{\underline{\boldsymbol{h}}}_i$ that minimize the squared error:

$$e_i = ||\underline{\boldsymbol{Y}}_i - P_i \cdot \underline{\boldsymbol{h}}_i||^2 \tag{30}$$

can be found using standard Least Squares (LS):

$$\hat{\underline{\boldsymbol{h}}}_i = (P_i^H P_i)^{-1} P_i^H \underline{\boldsymbol{Y}}_i^H, \quad i = 1,2,3 \tag{31}$$

Further $\hat{\underline{\boldsymbol{h}}}_3$ given $\hat{\underline{\boldsymbol{h}}}_i$ is:

$$\hat{\underline{\boldsymbol{h}}}_3|\hat{\underline{\boldsymbol{h}}}_i = (P_3^H P_3)^{-1} P_3^H (P_3 \hat{\underline{\boldsymbol{h}}}_i + \underline{\boldsymbol{\nu}}_3) = \hat{\underline{\boldsymbol{h}}}_i + (P_3^H P_3)^{-1} P_3^H \underline{\boldsymbol{\nu}}_3 \quad i = 1,2 \tag{32}$$

Because $\underline{\boldsymbol{\nu}}_3$ is a Gaussian random vector, so is $\hat{\underline{\boldsymbol{h}}}_3|\hat{\underline{\boldsymbol{h}}}_i$. Also:

$$\underline{\boldsymbol{X}} \sim \mathcal{N}(\underline{\boldsymbol{m}}, C) \quad \Rightarrow \quad A\underline{\boldsymbol{X}} + \underline{\boldsymbol{b}} \sim \mathcal{N}(A\underline{\boldsymbol{m}} + \underline{\boldsymbol{b}}, ACA^H)$$

Thus:

$$P_{\hat{\underline{\boldsymbol{h}}}_3|\hat{\underline{\boldsymbol{h}}}_i}(\hat{\underline{\boldsymbol{h}}}_3|\hat{\underline{\boldsymbol{h}}}_i) = \frac{1}{\sqrt{det(C)}(2\pi)^{\frac{n}{2}}} e^{-\frac{1}{2}(\hat{\underline{\boldsymbol{h}}}_3 - \hat{\underline{\boldsymbol{h}}}_i)^H C^{-1} (\hat{\underline{\boldsymbol{h}}}_3 - \hat{\underline{\boldsymbol{h}}}_i)} \tag{33}$$

where the covariance matrix C is:

$$C = ((P_3^H P_3)^{-1} P_3^H) \cdot \sigma_\nu^2 I_{MXM} \cdot ((P_3^H P_3)^{-1} P_3^H)^H = = \sigma_\nu^2 (P_3^H P_3)^{-1} \tag{34}$$

This yields:

$$P_{\hat{\underline{\boldsymbol{h}}}_3|\hat{\underline{\boldsymbol{h}}}_i}(\hat{\underline{\boldsymbol{h}}}_3|\hat{\underline{\boldsymbol{h}}}_i) = = \frac{1}{\sqrt{det(C)}(2\pi)^{\frac{n}{2}}} e^{-\frac{1}{2\sigma_\nu^2}(\hat{\underline{\boldsymbol{h}}}_3 - \hat{\underline{\boldsymbol{h}}}_i)^H (P_3^H P_3)(\hat{\underline{\boldsymbol{h}}}_3 - \hat{\underline{\boldsymbol{h}}}_i)} \tag{35}$$

and (29) can then be rewritten as:

$$(\hat{\underline{\boldsymbol{h}}}_3 - \hat{\underline{\boldsymbol{h}}}_1)^H (P_3^H P_3)(\hat{\underline{\boldsymbol{h}}}_3 - \hat{\underline{\boldsymbol{h}}}_1) \underset{\mathcal{H}_1}{\overset{\mathcal{H}_2}{\gtrless}} (\hat{\underline{\boldsymbol{h}}}_3 - \hat{\underline{\boldsymbol{h}}}_2)^H (P_3^H P_3)(\hat{\underline{\boldsymbol{h}}}_3 - \hat{\underline{\boldsymbol{h}}}_2) \tag{36}$$

which, after substituting $\hat{\underline{\boldsymbol{h}}}_3$ with $(P_3^H P_3)^{-1} P_3^H \underline{\boldsymbol{Y}}_3^H$, is exactly (27).

2) Algorithm Performance: The expected value of the left side of the inequality from (28) is:

$$E\{\hat{\underline{\boldsymbol{d}}}^H P_3^H P_3 \hat{\underline{\boldsymbol{d}}} + \hat{\underline{\boldsymbol{d}}}^H (P_3^H \underline{\boldsymbol{\nu}}_3) + (P_3^H \underline{\boldsymbol{\nu}}_3)^H \hat{\underline{\boldsymbol{d}}}\} = = \hat{\underline{\boldsymbol{d}}}^H E\{P_3^H P_3\} \hat{\underline{\boldsymbol{d}}} = \hat{\underline{\boldsymbol{d}}}^H R_{P_3} \hat{\underline{\boldsymbol{d}}} = \hat{\underline{\boldsymbol{d}}}^H U \Theta U^H \hat{\underline{\boldsymbol{d}}} = = M \sum_{j=1}^{J} \theta_i ||u_i^H \hat{\underline{\boldsymbol{d}}}||^2 \tag{37}$$

where Θ is a diagonal matrix built out of the eigenvalues $\theta_i, i = 1,2,...,J$ of matrix R_{P_3} (the covariance matrix of P_3) and U is a matrix built out of the corresponding eigenvectors $u_i, i = 1,2,...,J$. Motivated by the transmitted signal in orthogonal frequency division multiplexing (OFDM) systems, elements of the input vectors are assumed to be realizations of zero-mean normal random variables with standard deviation σ_x. With this assumption, in the case of the considered Volterra representation (16) of nonlinear power amplifiers:

$$\sum_{j=1}^{J} \theta_i ||u_i^H \hat{\underline{\boldsymbol{d}}}||^2 = = \hat{\underline{\boldsymbol{d}}}(1)^2 \cdot \sigma_x^2 + \hat{\underline{\boldsymbol{d}}}(2)^2 \cdot \sigma_x^2 + \hat{\underline{\boldsymbol{d}}}(3)^2 \cdot 2\sigma_x^4 + \hat{\underline{\boldsymbol{d}}}(4)^2 \cdot 2\sigma_x^4 + + (\hat{\underline{\boldsymbol{d}}}(3) + \hat{\underline{\boldsymbol{d}}}(4))^2 \cdot \sigma_x^4 + \hat{\underline{\boldsymbol{d}}}(5)^2 \cdot \sigma_x^4 = WS(\hat{\underline{\boldsymbol{d}}}) \tag{38}$$

$WS(\hat{\underline{\boldsymbol{d}}})$ is a weighted sum of the components of the distance vector $\hat{\underline{\boldsymbol{d}}}$. Eq. (38) shows how the importance of different Volterra coefficients changes with the standard deviation of the elements of the input vectors. For large values of σ_x, the elements of the Volterra representation that model nonlinearities are more important. This is intuitively correct since the increase of the input power beyond the linear range of the PAs should allow for better exploitation of the differences in the nonlinearities of the considered units.

C. Generalized Likelihood Ratio Test

Another algorithm that can be used to solve the hypothesis testing problem from Section II, when the parameter vectors of the users are unknown, is based on the Generalized Likelihood Ratio Test (GLRT). In the case of the GLRT, the receiver does not estimate the parameters, but rather builds and compares the maxima of the likelihood functions over the unknown parameter vectors.

1) Decision Rule: For equally probable hypotheses $\mathcal{H}_1$ and $\mathcal{H}_2$ the decision rule of the GLRT can be expressed as:

$$\Lambda(\underline{\boldsymbol{Y}}_3) \triangleq \frac{\max_{\underline{\boldsymbol{h}}_1}\{P(\underline{\boldsymbol{Y}}_1, \underline{\boldsymbol{Y}}_3 \,|\, \underline{\boldsymbol{h}}_1, \underline{\boldsymbol{X}}_1, \underline{\boldsymbol{X}}_3)\}}{\max_{\underline{\boldsymbol{h}}_2}\{P(\underline{\boldsymbol{Y}}_2, \underline{\boldsymbol{Y}}_3 \,|\, \underline{\boldsymbol{h}}_2, \underline{\boldsymbol{X}}_2, \underline{\boldsymbol{X}}_3)\}} \underset{\mathcal{H}_2}{\overset{\mathcal{H}_1}{\gtrless}} 1 \tag{39}$$

In the AWGN channel:

$$P(\underline{\boldsymbol{Y}}_i, \underline{\boldsymbol{Y}}_3 \,|\, \underline{\boldsymbol{h}}_i, \underline{\boldsymbol{X}}_i, \underline{\boldsymbol{X}}_3) = = \frac{1}{(\sqrt{2\pi}\sigma_\nu)^{2M}} \cdot \exp\left\{ -\frac{(\underline{\boldsymbol{Y}}_{i3} - P_{i3} \cdot \underline{\boldsymbol{h}}_i)^H (\underline{\boldsymbol{Y}}_{i3} - P_{i3} \cdot \underline{\boldsymbol{h}}_i)}{2\sigma_\nu^2} \right\} \tag{40}$$

where P_{i3} and $\underline{\boldsymbol{Y}}_{i3}$ are obtained by stacking matrices P_i, P_3 and vectors $\underline{\boldsymbol{Y}}_i$, $\underline{\boldsymbol{Y}}_3$ respectively:

$$P_{i3} = \begin{bmatrix} P_i \\ P_3 \end{bmatrix} \qquad i = 1,2 \tag{41}$$

$$\underline{\boldsymbol{Y}}_{i3} = \begin{bmatrix} \underline{\boldsymbol{Y}}_i \\ \underline{\boldsymbol{Y}}_3 \end{bmatrix} \qquad i = 1,2 \tag{42}$$

and where M is the size of the input vector. After substitution of the corresponding probability density functions into (39) the decision rule can be rewritten as:

$$\min_{\underline{\boldsymbol{h}}_1}\{(\underline{\boldsymbol{Y}}_{13} - P_{13}\underline{\boldsymbol{h}}_1)^H (\underline{\boldsymbol{Y}}_{13} - P_{13}\underline{\boldsymbol{h}}_1)\} \underset{\mathcal{H}_1}{\overset{\mathcal{H}_2}{\gtrless}} \min_{\underline{\boldsymbol{h}}_2}\{(\underline{\boldsymbol{Y}}_{23} - P_{23}\underline{\boldsymbol{h}}_2)^H (\underline{\boldsymbol{Y}}_{23} - P_{23}\underline{\boldsymbol{h}}_2)\} \tag{43}$$

Since:

$$(\underline{\boldsymbol{Y}}_{i3} - P_{i3}\underline{\boldsymbol{h}}_i)^H (\underline{\boldsymbol{Y}}_{i3} - P_{i3}\underline{\boldsymbol{h}}_i) = ||(\underline{\boldsymbol{Y}}_{i3} - P_{i3}\underline{\boldsymbol{h}}_i)||^2 \tag{44}$$

the minimizations on each side of (43) are typical LS problems. Vectors minimizing the squared error are:

$$\hat{\underline{\boldsymbol{h}}}_i = (P_{i3}^H P_{i3})^{-1} P_{i3}^H \underline{\boldsymbol{Y}}_{i3}^H, \quad i = 1,2 \tag{45}$$

and

$$\min_{\underline{\boldsymbol{h}}_i} ||(\underline{\boldsymbol{Y}}_{i3} - P_{i3} \cdot \underline{\boldsymbol{h}}_i)||^2 = ||(\underline{\boldsymbol{Y}}_{i3} - P_{i3} \cdot \hat{\underline{\boldsymbol{h}}}_i)||^2 =$$

$$= \underline{\boldsymbol{Y}}_{i3}^H (I_{2M\times 2M} - P_{i3}(P_{i3}^H P_{i3})^{-1} P_{i3}^H)\underline{\boldsymbol{Y}}_{i3} \quad (46)$$

With (46), the decision rule (43) can be written as:

$$\underline{\boldsymbol{Y}}_{13}^H (I_{2M\times 2M} - P_{13}(P_{13}^H P_{13})^{-1} P_{13}^H)\underline{\boldsymbol{Y}}_{13} \underset{\mathcal{H}_1}{\overset{\mathcal{H}_2}{\gtrless}} \underline{\boldsymbol{Y}}_{23}^H (I_{2M\times 2M} - P_{23}(P_{23}^H P_{23})^{-1} P_{23}^H)\underline{\boldsymbol{Y}}_{23} \quad (47)$$

2) Algorithm Performance: Eq. (23) together with the decision rule (47) yields:

$$P_e = Pr\{(\underline{\boldsymbol{Y}}_{13}^H (I_{2M\times 2M} - P_{13}(P_{13}^H P_{13})^{-1} P_{13}^H)\underline{\boldsymbol{Y}}_{13} > \underline{\boldsymbol{Y}}_{23}^H (I_{2M\times 2M} - P_{23}(P_{23}^H P_{23})^{-1} P_{23}^H)\underline{\boldsymbol{Y}}_{23})|\mathcal{H}_1\} \quad (48)$$

Under $\mathcal{H}_1$ the third system is actually system 1 with parameters $\underline{\boldsymbol{h}}_1$. Thus vectors $\underline{\boldsymbol{Y}}_{13}$ and $\underline{\boldsymbol{Y}}_{23}$ in (48) can be replaced with:

$$\underline{\boldsymbol{Y}}_{13} = \begin{bmatrix} \underline{\boldsymbol{Y}}_1 \\ \underline{\boldsymbol{Y}}_3 \end{bmatrix} = \begin{bmatrix} P_1\underline{\boldsymbol{h}}_1 + \underline{\boldsymbol{\nu}}_1 \\ P_3\underline{\boldsymbol{h}}_1 + \underline{\boldsymbol{\nu}}_3 \end{bmatrix} = P_{13}\underline{\boldsymbol{h}}_1 + \begin{bmatrix} \underline{\boldsymbol{\nu}}_1 \\ \underline{\boldsymbol{\nu}}_3 \end{bmatrix} \quad (49)$$

$$\underline{\boldsymbol{Y}}_{23} = \begin{bmatrix} \underline{\boldsymbol{Y}}_2 \\ \underline{\boldsymbol{Y}}_3 \end{bmatrix} = \begin{bmatrix} P_2\underline{\boldsymbol{h}}_2 + \underline{\boldsymbol{\nu}}_2 \\ P_3\underline{\boldsymbol{h}}_1 + \underline{\boldsymbol{\nu}}_3 \end{bmatrix} = \begin{bmatrix} P_2\underline{\boldsymbol{h}}_2 \\ P_3\underline{\boldsymbol{h}}_1 \end{bmatrix} + \begin{bmatrix} \underline{\boldsymbol{\nu}}_1 \\ \underline{\boldsymbol{\nu}}_3 \end{bmatrix} \quad (50)$$

With this substitution and after simple algebraic manipulations the probability of error from (48) can be finally put in the form:

$$P_e = Pr\{(\underline{\boldsymbol{\nu}} + \underline{\boldsymbol{B}})^H \mathbf{P}\ (\underline{\boldsymbol{\nu}} + \underline{\boldsymbol{B}}) < 0\} \quad (51)$$

where:

$$\mathbf{P}_{(3M\times 3M)} = \begin{bmatrix} -(I - P_1 X^* P_1^H) & 0 & P_1 X^* P_3^H \\ 0 & (I - P_2 X P_2) & -P_2 X P_3^H \\ P_3 X^* P_1^H & -P_3 X P_2^H & -P_3(X - X^*)P_3^H \end{bmatrix}$$

$$\underline{\boldsymbol{B}}_{(3M\times 1)} = \begin{bmatrix} \underline{\mathbf{0}} \\ P_2.\underline{\boldsymbol{d}} \\ \underline{\mathbf{0}} \end{bmatrix} \ ; \ \underline{\boldsymbol{\nu}}_{(3M\times 1)} = \begin{bmatrix} \underline{\boldsymbol{\nu}}_1 \\ \underline{\boldsymbol{\nu}}_2 \\ \underline{\boldsymbol{\nu}}_3 \end{bmatrix}$$

$$X = \left(P_2^H P_2 + P_3^H P_3\right)^{-1} \quad ; \quad X^* = \left(P_1^H P_1 + P_3^H P_3\right)^{-1}$$

and

$$\underline{\boldsymbol{d}} = \underline{\boldsymbol{h}}_2 - \underline{\boldsymbol{h}}_1$$

After ignoring the matrix $\mathbf{P}$, which is just a rotation matrix, the expected value of the left side of the inequality from (51), with the assumption of zero-mean normal random input, for power amplifier model from (16) is:

$$E\{(\underline{\boldsymbol{\nu}} + \underline{\boldsymbol{B}})^H (\underline{\boldsymbol{\nu}} + \underline{\boldsymbol{B}})\} = M\left(\sigma_\nu^2 + WS(\underline{\boldsymbol{d}})\right) \quad (52)$$

with WS defined as in (38). Eq. (52) together with (37) shows that probability of error for user identification based on the PA's imperfections does not only depend on the Euclidean distance between the parameter vectors of the considered units, but also on the range of the input signal driving them.

D. Naive Method

In addition to the algorithms introduced in the previous subsections, another algorithm termed the "Naive Method" is considered. In this algorithm, the detection system outputs the user number for which the estimated parameter vector $\underline{\hat{\boldsymbol{h}}}_i, i = 1, 2$, estimated with standard Least Squares, is closest to the estimated parameter vector of the masquerading user $\underline{\hat{\boldsymbol{h}}}_3$ under an L_2-norm criterion.

$$||\underline{\hat{\boldsymbol{h}}}_3 - \underline{\hat{\boldsymbol{h}}}_2|| \underset{\mathcal{H}_2}{\overset{\mathcal{H}_1}{\gtrless}} ||\underline{\hat{\boldsymbol{h}}}_3 - \underline{\hat{\boldsymbol{h}}}_1||$$

V. Simulations and Measurements

In this section, the performance of the methods from Section IV is investigated. In particular, the influence of parameters such as the power of the input signal and the SNR on the probability of error is analyzed. This section also provides insight on the variations of components of transmitters used in practical applications, and, most importantly, demonstrates the utility of the approaches for such components even for very short input sequences and low SNRs.

Data sheets of digital-to-analog converters usually specify the maximal value of the integral nonlinearity: INL_{max}. In addition to this information, the data sheets often include exemplary INL paths [22]. Because of this, we found no need to perform measurements to examine the variations of the I/O characteristics among the DACs. In the case of the PAs, nonlinearity variations across individual devices are usually not described in the data sheets. Thus measurements were performed on commercial RF PAs to analyze variations of the I/O characteristics among the PAs.

A. Exploitation of Digital-to-Analog Converter Nonlinearities for User Identification

The required DAC size for commercial OFDM-based communication applications varies from 6 to 18 bits and depends on the largest signal constellation and number of OFDM subcarriers [23]. For our simulations, we considered 10-bit DACs. We set the standard deviation σ_s of individual DAC sources to be 2% of their nominal value. The upper plot of Figure 3 shows 1000 exemplary INL paths of 10-bit, thermometer-coded DACs with $\sigma_s = 2\%$. The lower plot shows the INL_{max} histogram. For 10-bit DACs used in commercial communication transceivers, the value of INL_{max} is typically in the range: ± 1 LSB [24], which justifies the choice of 2% as a value for the σ_S.

The algorithms introduced in Section IV were applied to recognize users based on their DAC INL paths. Figure 4 shows the probability of error as a function of SNR, averaged over 100 DAC pairs and over 500 input vectors of size 100, the elements of which were chosen as realizations of normal random variables (rounded to an integer) with mean value equal to half of the the DAC input range and standard deviation chosen as one third of the half of the input range (which resulted in 99% of the input values within the input range, values outside the input range were ignored). The first eight eigenfunctions of the Brownian Bridge random process were

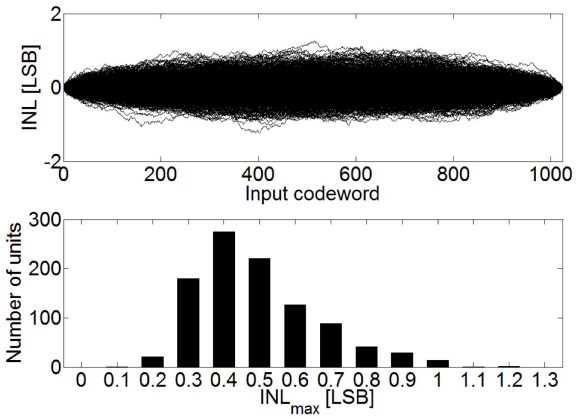

Fig. 3. INL Brownian Bridge paths of one thousand 10-bit, thermometer-coded DACs with standard deviation of individual sources $\sigma_s = 2\%$ (upper plot) and INL_{max} histogram (lower plot)

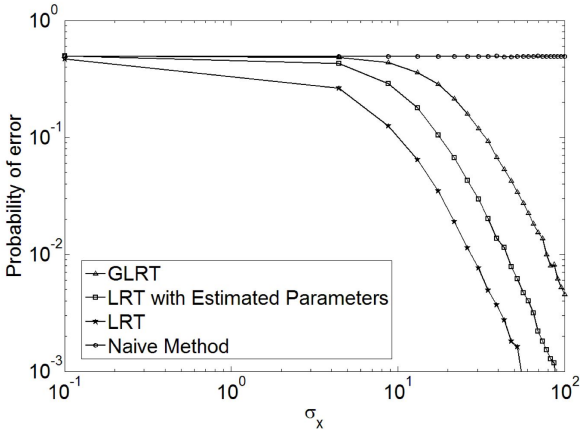

Fig. 5. Probability of error vs. the standard deviation of the elements of the input vectors averaged over 200 different input vectors of size $M = 100$ and over 200 randomly generated Volterra vector pairs, with standard deviation of elements $\sigma_h = 10^{-3}$; $SNR = 30dB$.

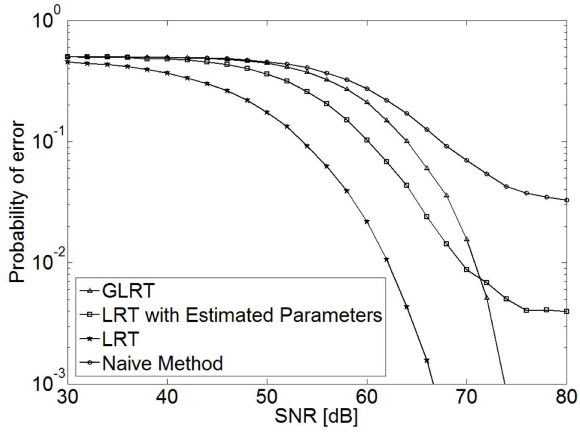

Fig. 4. Probability of error vs. SNR averaged over 100 DAC pairs with $\sigma_S = 2\%$ and over 500 input vectors of size M=100, with normally distributed elements with mean value equal to half of the input range and standard deviation equal to $\frac{1}{6}$ of the input range (which resulted in 99% of the input values within the input range, values outside the input range were ignored). The first eight eigenfunctions of the Brownian Bridge random process were used for INL representation.

used for INL representation. Note that a relatively high SNR was required for user identification at these short input lengths in this case.

B. Exploitation of Power Amplifier Nonlinearities for User Identification

Similarly the performance of the considered methods was simulated when the nonlinearities of PAs were exploited for user identification. The elements of the input vectors were assumed to be realizations of zero-mean normal random variable with standard deviation σ_x. First the Volterra series representation of the amplifiers and standard deviation of the elements of the input vectors were chosen artificially to investigate the behavior of P_e as a function of increasing input power and increasing difference of the Volterra representations of considered units. Next, and most importantly, the Volterra series representations were obtained by measurement for actual RF amplifiers and the performance of the methods was analyzed at input power levels specified as linear by the manufacturers.

Consider first the artificial generation of amplifier characteristics. Figure 5 shows the simulated probability of error of the considered methods, for $SNR = 30dB$, versus standard deviation σ_x of the elements of the input vectors, averaged over 200 different input vectors of size $M = 100$ and over 200 randomly generated Volterra vector pairs. For generation of Volterra vector pairs, random vectors with normally distributed elements $\sim \mathcal{N}(0, 10^{-6})$ were added to a mean value vector: [1 0.01 0.01 0.01 0.01].

Figure 6 also shows simulated P_e, but this time for the standard deviation of the elements of the input vectors kept constant ($\sigma_x = 100$) and for the standard deviation σ_h of elements of random vectors added to the mean value vector [1 0.01 0.01 0.01 0.01] for Volterra vector pairs generation varied in the range $\sigma_h \in (0, 0.001)$. Each point of the curve was obtained as an average over 1000 different input vectors of size $M = 100$ and over 1000 randomly generated Volterra vector pairs. Similarly, as in case of Figure 5, the SNR was set to $30dB$.

As expected, Figures 5 and 6 demonstrate that the performance of the methods increases when the power of input signals increases and when the differences among amplifiers get larger. But speaking more precisely, the methods perform better when the value of the weighted sum from (38) increases. In particular the differences in the Volterra series representation of PAs should always be analyzed together with the input power for complete insight into performance of the methods. Figure 7 shows P_e as a function of weighted sum $WS(\underline{\boldsymbol{d}})$ (upper plot) and the L_2 distance $||\underline{\boldsymbol{d}}||$ (lower plot) for 100 randomly generated amplifier pairs with $\sigma_h = 2.5 \cdot 10^{-4}$ averaged over 10000 input vectors of size $M = 100$ with the standard deviation of elements set to $\sigma_x = 100$. It can be seen that the weighted sum is a much more appropriate metric.

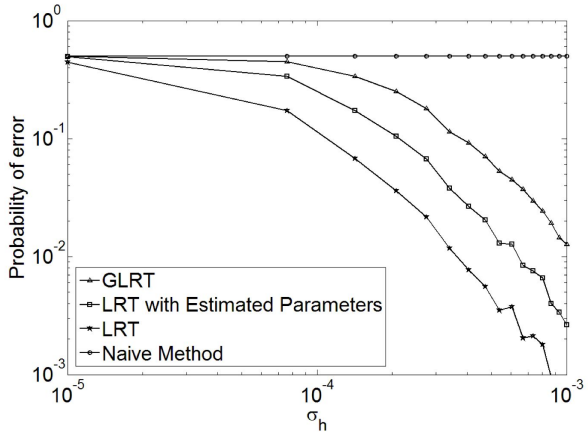

Fig. 6. Probability of error vs. the standard deviation of the Volterra coefficients averaged over 1000 randomly generated Volterra vector pairs and 1000 different input vectors of size $M = 100$, with standard deviation of the elements $\sigma_x = 100$; SNR=30dB.

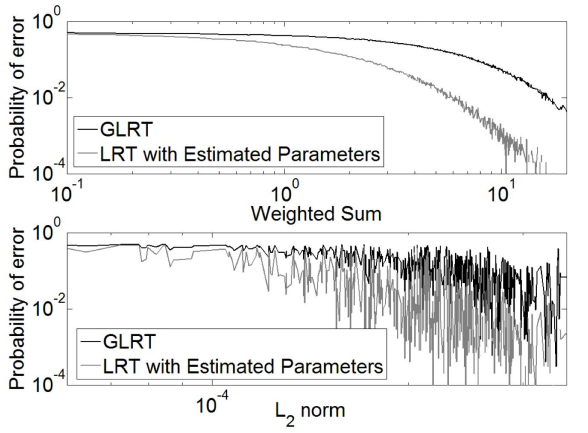

Fig. 7. Probability of error vs. weighted sum from (38)- metric that combines differences in Volterra coefficients and power of the input signal (upper plot) and vs. L_2 norm of the vector $\underline{\boldsymbol{d}}$- metric that takes into account only differences in Volterra coefficients (lower plot).

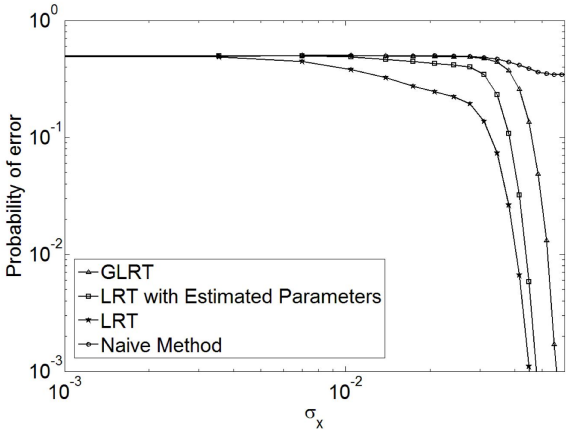

Fig. 8. Probability of error for measured MAXIM MAX2242 amplifiers vs. the standard deviation of the elements of input vectors σ_x, averaged over 50000 input vectors of size $M = 300$; $SNR = 15dB$.

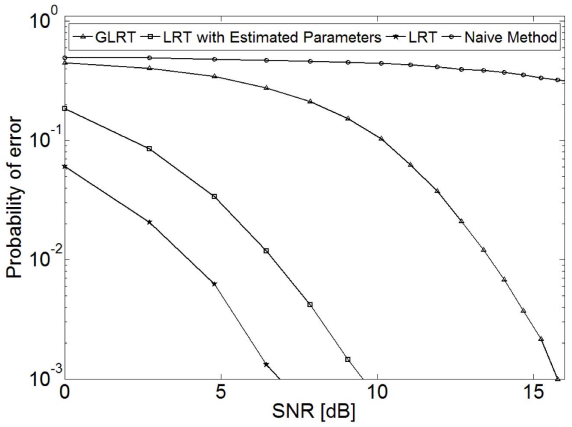

Fig. 9. Probability of error for measured MAXIM MAX2242 amplifiers vs. SNR, averaged over 50000 input vectors of size $M = 300$, with standard deviation of the elements of input vectors $\sigma_x = 0.055$.

To be able to validate effectiveness of the presented anonymity breaking techniques when exploiting imperfections of PAs, we next consider how the nonlinearities of power amplifiers, even these of the same model and from the same manufacturer, differ in practice due to the production process inaccuracies. As mentioned previously nonlinearity variations across devices are usually not described in the data sheets of commercial RF PAs.

Measurements were performed on two different sets of power amplifier chips commercially used in WLAN transmitters. First, two amplifier evaluation boards (MAX2242EVKIT) loaded with MAXIM MAX2242 [26] amplifiers were stimulated with a $2.45GHz$ sinusoidal signal and the I/O characteristics were measured on a $12.5GHz$, $50GSa/s$ real time oscilloscope. Both measured characteristics were normalized to the same linear gain and this gain was used as the linear coefficient of the Volterra representation for both of the amplifiers. Then the linear part was subtracted from the normalized characteristics and the nonlinear memoryless coefficients were obtained via curve fitting of the remaining nonlinear part of the normalized characteristics to a fourth order polynomial without a linear part. This resulted in the following parameter vectors (fourth order memoryless Volterra representation):

$$\underline{\boldsymbol{h}}_1 = [32.5462, 29.5342, -509.5277, 1311.5641]$$

$$\underline{\boldsymbol{h}}_2 = [32.5462, 29.4025, -479.4057, 928.3273]$$

which were used for performance simulations (Figure 8 and 9).

For the plots in Figures 8 and 9 the elements of the input vectors were chosen as the absolute value of realizations of a zero mean random variable $\sim \mathcal{N}(0, \sigma_x^2)$. Figure 8 shows how the P_e decreased as the standard deviation of the input went up (while the SNR was kept constant at a level of $15dB$ and length of the input vector was set to $M = 300$). For standard deviation equal to $\sigma_x = 0.055$ the probability that power of the input signal exceeded -7dBm (upper level of linear range

TABLE I
SIMULATED PROBABILITY OF ERROR OF GENERALIZED LIKELIHOOD RATIO TEST (UPPER RIGHT PART) AND LIKELIHOOD RATIO TEST WITH ESTIMATED PARAMETERS (LOWER LEFT PART) FOR ALL POSSIBLE PAIRS OF 8 SKYWORKS SKY65006-348LF WLAN AMPLIFIERS, AVERAGED OVER 50000 INPUT VECTORS OF SIZE M = 300. THE STANDARD DEVIATION OF THE COMPONENTS OF THE INPUT VECTORS WAS CHOSEN SUCH THAT THE OUTPUT POWER EXCEEDED 21DBM (FOR WHICH, ACCORDING TO [25], THE PARTS ARE STILL 802.11B MASK-COMPLIANT) WITH PROBABILITY EQUAL TO 1%. THE INPUT WAS CLIPPED TO THE UPPER LEVEL OF THE LINEAR INPUT RANGE. SNR WAS SET TO $15dB$. FOR SNR=$35dB$, NO ERRORS WERE OBSERVED FOR ANY PAIR IN 50000 TRIALS.

# amplifier	1	2	3	4	5	6	7	8
1	-	0.0731	0	0	0.1707	0	0.1437	0.0001
2	0	-	0.0041	0.1406	0.4679	0.0092	0.0195	0
3	0	0	-	0.3138	0.0006	0.4758	0	0
4	0	0.0005	0.0178	-	0.0514	0.3464	0.0001	0
5	0.0010	0.2769	0	0.0001	-	0.0021	0.0269	0
6	0	0	0.3422	0.0329	0	-	0	0
7	0.0005	0	0	0	0	0	-	0
8	0	0	0	0	0	0	0	-

of considered amplifiers [26]) was only 1%. Whenever the input signal exceeded the the linear range, it was clipped to its upper level. This means that the amplifiers worked in the range specified as linear all the time. Figure 9 shows how the P_e behaved for a fixed $\sigma_x = 0.055$ as a function of SNR (again the input signal was clipped to the upper level of the linear region).

Motivated by our success with the MAXIM evaluation boards, we next prepared a larger experiment using SKYWORKS SKY 65006-348LF [25] amplifiers. For cost reasons, this motivated the development of our own evaluation board. A similar procedure as in the case of the MAXIM amplifiers was executed to measure the I/O characteristics and to obtain parameter vectors for the SKYWORKS amplifiers. Once more, elements of input vectors were chosen to be the absolute value of realizations of a zero-mean normal random variable, with a standard deviation set to a value, for which 99% of the time the input power was within the linear input range specified by the manufacturer and 1% of the time the input power exceeded the linear range and was clipped to its upper level. Table 1 shows the simulated probability of error for the Generalized Likelihood Ratio Test (upper right part) and the Likelihood Ratio Test with Estimated Parameters (lower left part) for all possible amplifier pairs from a group of 8 measured SKYWORKS amplifiers, averaged over 50000 input vectors of size $M = 300$ for SNR set to $15dB$. Note that the identifiability of the parts was very good, even at the low SNR of $15dB$ and for the very short input sequence of only 300 physical-layer symbols. For SNR$= 35dB$, for both of the methods, we found no identification errors for any pair in 50000 trials. In reality of course, even short sessions will generally consist of thousands of symbols that can be used for user identification.

One of the main concerns about RF fingerprinting approaches exploiting transmitter hardware imperfections is that they can be negatively influenced by the variation of the performance of the transmitter components across the temperature. In particular, a meaningful variation of the performance of the power amplifiers can be observed as a function of temperature. This is particularly true in large base station amplifiers, where such temperature variation is the bane of designers attempting to linearize such. However power amplifier chips used on wireless cards of today's mobile devices are very small (usually in the range of $4 - 6mm^2$). These small chips achieve their normal operating temperature very quickly, and in fact, we have observed such stabilization of the chip temperature after tens of seconds. This is a very short time that is often needed for the mobile device to boot up. Therefore, we believe it is fair to ignore the temperature variations in this initial investigation (other environmental conditions have negligible influence on the performance of the chips). However, we do believe that it is an important consideration as we consider further refinement of our algorithms.

C. Evaluation of the Results

To our knowledge, model based approaches similar to ours have not yet been investigated. Thus, it is to hard conduct a comparison of our results with results of the previous work. In particular, it is not possible to conclusively compare our simulation and measurement results with the strictly empirical results from [13] and [18], for which numerous parameters are not specified, including such basic ones as the operating signal-to-noise ratio (SNR). Hence, we are reduced to restating the experimental outcomes of [13] and [18] and comparing them quite roughly to our work. [13] reports an average success rate of 94-100%, while trying to distinguish among 14 802.11 transceivers. [18] reports identification error rates equal to fractions of a percent (0.34% for their best scheme), while distinguishing among 138 802.11 transceivers. As mentioned previously, for SNR=$35dB$, even for very short input sequences, no errors were observed during 50000 simulation trials, while trying to distinguish among 8 802.11b mask-compliant PAs from the same manufacturer. This suggests that our methods can outperform methods from [13] and [18], when applied to the same setup, but, per above, we cannot make this statement conclusively. While methods from [13] and [18] are strictly experimental and their results hard to reproduce, one advantage of our model-based approach is that the results are easy to replicate for comparison to the performance of methods developed by others in the future.

VI. CONCLUSIONS AND FUTURE WORK

In this paper, a new approach based on minute imperfections of different components of the transmitter hardware has been

proposed for breaking user anonymity in wireless communication systems. The general models used to model the transmitter components allow for the determination of the probability of error of the decisions, which makes the proposed methods especially interesting for establishing probable cause and for use in court. Simulations have shown that the nonlinear variations of digital-to-analog converters can only be exploited when the signal-to-noise ratio is relatively high. However, in the case of power amplifiers, measurements from commercially employed chips indicate that amplifiers can be easily identified at typical power levels even at low SNRs and with very short observed sequences.

As future work, we are extending the methods to address more sophisticated criminals. In particular, a sophisticated user could intentionally introduce nonlinear distortions to the baseband signal to attempt to hide his/her signature, while allowing for proper data decoding. While this is unlikely for the standard criminal employing a wireless card, its possibility motivates the consideration of techniques to address such. Our approach is based on the observation that nonlinear components cause spectral regrowth of the signal that is dependent on the parameters of the nonlinearity. Hence, by observing the relation of the regrowth to the in-band portion of the signal, the signature can be found independently from distortions of the transmitted baseband signal. Therefore with an oversampling receiver, it is possible to make our methods independent from any modifications made by the sophisticated masquerading user to the transmitted baseband signal. In addition, because of the fast stabilization of the operating temperature of the components considered in this work, temperature variations were ignored in the initial investigation. Refinement of the algorithms by taking into consideration these variations is also an interesting topic for future research.

REFERENCES

[1] National Center for Missing Exploited and Children. Child Pornography Fact Sheet: http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=enUS&PageId=2451.

[2] Business Software Alliance 2009 Year in Review: http://www.bsa.org/~/media/Files/General/YIR2009.ashx.

[3] Federal Trade Commission 2006 Identity Theft Survey Report: http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.

[4] Francois Paget, McAfee Avert Labs, "Financial Fraud and Internet Banking: Threats and Countermeasures": http://www.mcafee.com/us/local_content/reports/6168rpt_fraud_0409.pdf.

[5] R. Shore, "Pedophiles exploiting wireless loopholes," http://www.canada.com/vancouversun/news/story.html?id=cff3073b-ceea-4ba4-877f-d020715358e9, February 13 2007.

[6] J. Stockwell, "Wifi turns internet into hideout for criminals," http://www.washingtonpost.com/wp-dyn/content/article/2007/02/10/AR2007021001457.html, February 11 2007.

[7] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in ether: Using the physical layer for wireless authentication," in *Proc. IEEE Int. Conf. Communications (ICC)*, June 2007, pp. 4646–4651.

[8] ——, "Channel-based detection of sybil attacks in wireless networks," in *IEEE Transactions on Information Forensics and Security*, September 2009, pp. VOL. 4, NO. 3.

[9] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," in *Proc. 5th ACM workshop on Wireless security*, 2006, pp. 33–42.

[10] N. Patwari and S. Kasera, "Robust location distinction using temporal link signatures," in *ACM MOBICOM*, 2007, pp. 111–122.

[11] D. Faria and D. Cheriton, "Radio-layer security: Detecting identity-based attacks in wireless networks using signalprints," in *IProc. 5th ACM Workshop on Wireless Security (WiSe'06)*, Sep 2006, pp. 43–52.

[12] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 mac layer spoofing using received signal strength," in *27th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, April 2008, pp. 1768–1776.

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

[14] J. Hall, "Detection of rogue devices in wireless networks." PhD Dissertation, School of Computer Science, Carleton University, Ottawa, Ontario, 2006.

[15] O. Ureten and N. Serinken, "Bayesian detection of radio transmitter turn-on transients," in *NSIP99*, 1999, pp. 830–834.

[16] T. Kohno, A. Broido, and k. Claffy, "Remote physical device fingerprinting," in *IEEE Transactions on Dependable Secure Comput.*, 2005, pp. 93–108.

[17] A. Tomko, A. Rieser, and L. Buell, "Physical-layer intrusion detection in wireless networks," in *Military Communications Conference*, 2006, pp. 1–6.

[18] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proc. 14th ACM international conference on Mobile computing and networking*, March 2008, pp. 116–127.

[19] G. I. Radulov, M. Heydenreich, R. W. van der Hofstad, J. A. Hegt, and A. H. van Roermund, "Brownian-bridge-based statistical analysis of the dac inl caused by current mismatch," in *IEEE Trans. Circuits Syst. II, Exp. Briefs, VOL. 54, NO. 2*, 2007.

[20] T. Anderson, M. Stevens, N. Mandayam, and W. Trappe, "Linear algebra and its applications." Volume 264, Number 1, October 1997 , pp. 145-171(27).

[21] P. Wambacq and W. Sansen, *The Distortion Analysis of Analog Integrated Circuits*. Kluwer, 1998.

[22] Data Sheet, Analog Devices AD9776A/AD9778A/AD9779A: http://www.analog.com/static/imported-files/data_sheets/AD9776_9778_9779.pdf.

[23] A. Mehrnia, "Optimum dac resolution for wman, wlan and wpan ofdm based standards," in *International Conference on Consumer Electronics*, 2005, pp. 355–356.

[24] Data Sheet, MAXIM MAX5858 dual, 10-bit, 300Msps digital to analog converter: http://datasheets.maxim-ic.com/en/ds/MAX5858.pdf.

[25] Data Sheet, SKYWORKS SKY65006-348LF: http://www.skyworksinc.com/uploads/documents/200122H.pdf.

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

Adam Polak received his Dipl.-Ing. degree in electrical engineering from Karlsruhe Institute of Technology and his MSEE degree from Gdansk University of Technology in year 2009. He is currently pursuing his Ph.D. degree in the Electrical and Computer Engineering department at the University of Massachusetts- Amherst. His research is concentrated on signal processing, communications and hardware verification.

Sepideh Dolatshahi received her B.S. degree in electrical engineering from University of Tehran, Iran, in July 2007, and her M.S. degree in electrical engineering, telecommunications from University of Massachusetts- Amherst in 2009. She is currently a Ph.D. student in electrical engineering at Georgia Institute of technology. Her research interests include information theory, communication systems, systems biology, and metabolic pathway modeling.

Dennis L. Goeckel split time between Purdue University and Sundstrand Corporation from 1987-1992, receiving his BSEE from Purdue in 1992. From 1992-1996, he was a National Science Foundation Graduate Fellow and then Rackham Pre-Doctoral Fellow at the University of Michigan, where he received his MSEE in 1993 and his Ph.D. in 1996, both in Electrical Engineering with a specialty in Communication Systems. In September 1996, he joined the Electrical and Computer Engineering department at the University of Massachusetts, where he is currently a Professor. His current research interests are in the areas of signal processing, communication systems, and wireless network theory.

Dr. Goeckel was the recipient of a 1999 CAREER Award from the National Science Foundation for "Coded Modulation for High-Speed Wireless Communications". He was a Lilly Teaching Fellow at UMass-Amherst for the 2000-2001 academic year and received the University of Massachusetts Distinguished Teaching Award in 2007. He is a Fellow of the IEEE.