Wireless Device Identification Based on RF Oscillator Imperfections

Adam C. Polak and Dennis L. Goeckel
Department of Electrical and Computer Engineering, University of Massachusetts Amherst

***Abstract*—The exploitation of slight imperfections of transmitters' hardware for identification of wireless devices has recently emerged as an effective method for security enhancement in wireless access networks. Previously, we introduced a model-based approach for device identification based on the imperfections of two main wireless transmitter components: the digital-to-analog converter and the power amplifier. Here, motivated by applications with transmit power control mechanisms, we analyze the degree to which a device can be identified from the unique, power mode independent characteristics of a third main component: the RF oscillator. The model-based device identification method introduced here allows for effective device identification even from short time records at relatively low signal-to-noise ratios when exploiting imperfections of commercially used RF oscillators.**

***Index Terms*—radiometric identification, wireless security, process variations, RF oscillators**

I. Introduction

A significant increase in the number of crimes, such as distribution of contraband music and video, identity theft, intellectual property theft, fraud etc., committed via the Internet, as well as the increase of financial losses caused by these crimes, have been reported in recent years [1]. Techniques exploiting information available at the physical layer have recently been considered for security level enhancement in wireless systems. 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 channel properties [2], [3], [4], [5] that require a strong assumption on users' stationarity. Physical layer identification techniques that exploit hardware imperfections can generally be divided into two groups: transient signal techniques [6], [7], [8], [9] and steady state signal techniques [10], [11], [12], [13]. In [10], [11] we considered steady state signal techniques for security enhancement in wireless Internet access systems and introduced a model-based approach for wireless device identification. This approach falls in the field of RF fingerprinting based on hardware imperfections; however, in contrast to the prior empirical work (e.g.[12]), it is based on statistical models amenable for analysis.

In [11] we considered two components of the transmitter chain: the digital-to-analog-converter (DAC) and the power amplifier (PA). Here we analyze the degree to which a wireless device can be correctly identified from measurable non-idealities of RF oscillators, employed by wireless transmitters. Work presented here is motivated by the fact that, in contrast to the PAs, which in transmit power controlled applications might be switching modes over time, characteristics of the RF oscillators are power level independent, and thus can be used as unique device tags in systems with implemented transmit power control mechanisms.

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

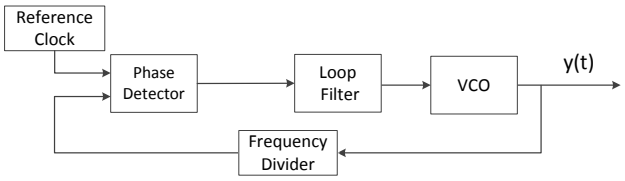

Fig. 1. A basic PLL block diagram.

The main practical application of the identification method proposed in this work is testing devices from a pool of suspects in order to decide which one was most likely used while the crime was committed, when high-layer identification mechanisms fail or are not implemented. The only print from the crime scene is a signature captured from the wireless transmitter by an access point or cell tower. Having the signature and a group of devices that have been potentially used to commit the crime, the proposed method can be used to successfully select the offender's device.

In mobile devices RF oscillators are typically implemented as phased-locked-loops (PLLs). Fig. 1 shows a basic block diagram of a PLL. An ideal PLL would generate a sinusoidal oscillation at a carrier frequency f_0. Instead, in practice, the PLL generates a signal of the form:

$$y(t) = \cos\left(2\pi(f_0 + \Delta(t))t + \Theta(t)\right) \tag{1}$$

where $\Delta(t)$ is the frequency offset and $\Theta(t)$ is the complex phase noise process. The frequency offset $\Delta(t)$ is specific to a given PLL chip, however, it is sensitive to chip temperature changes. Moreover it can be easily compromised by sophisticated cyber-criminals [14] via multiplication of the digital symbols with a time-varying factor, in a manner similar to receivers' digital frequency compensation (Ch. 6 [15]). Therefore this work concentrates on the extraction of devices' RF fingerprints based on differences in the characteristics of the PLL's phase noise, which is caused by variations in the components that comprise the PLL circuit and cannot be modified by the user without causing performance impairments.

978-1-4799-2893-4/14/$31.00 ©2014 IEEE

II. PLL Phase Noise Model and RF Fingerprint Extraction

For the case of a free running (open loop) RF oscillator $\Theta(t)$ becomes a Wiener process as $t \to \infty$ [16]. The phase noise is then characterized with a single quality parameter that determines the width of the oscillator's spectrum, which exhibits a Lorenzian shape [17]. For PLLs, the analytic description of the phase noise is more complex. In [18], the PLL is modeled with a set of stochastic differential equations and the autocorrelation of the phase noise corrupted PLL's output $y(t)$ is found as

$$R_y(\tau) = \sum_{i=-\infty}^{\infty} X_i X_i^* \exp(-ji\omega_0\tau) \cdot \cdot \exp\left[-0.5\omega_0^2 i^2 \left[c_{xtl}|\tau| + 2\sum_{l=1}^{n}(\nu_l + \mu_l)\left[1 - \exp(-\lambda_l|\tau|)\right]\right]\right], \tag{2}$$

where X_i are coefficients of the Fourier series expansion of the PLL crystal's reference signal oscillating with nominal angular frequency ω_0, c_{xtl} is a quality parameter of the crystal oscillator, and λ_l, ν_l and μ_l, $l = 1, 2, \ldots, n$, are parameters that depend on entries of matrices defining the set of differential stochastic equations modeling the PLL (Appendix of [18]). For the 1^{st} order charge pump loop filter with cut-off frequency ω_{cp} and transfer function $\frac{s+\omega_{cp}}{s}$, $n = 2$ and we find μ_l and ν_l, $l = 1, 2$:

$$\mu_1 = c_{xtl}\frac{-\lambda_2(\lambda_1 - \omega_{cp})}{\omega_{cp}(\lambda_1 - \lambda_2)\lambda_1} \qquad \mu_2 = c_{xtl}\frac{-\lambda_1(\omega_{cp} - \lambda_2)}{\omega_{cp}(\lambda_1 - \lambda_2)\lambda_2} \tag{3}$$

$$\nu_1 = \frac{c_{VCO} + c_{xtl}}{(\lambda_1 - \lambda_2)^2}\left(\frac{\lambda_2^2(\omega_{cp} - \lambda_1)^2}{2\omega_{cp}^2\lambda_1} - \frac{\frac{\lambda_1\lambda_2}{\omega_{cp}^2}\left(-\omega_{cp}^2 + \omega_{cp}(\lambda_1 + \lambda_2) - \lambda_1\lambda_2\right)}{2(\lambda_1 + \lambda_2)}\right)$$

$$\nu_2 = \frac{c_{VCO} + c_{xtl}}{(\lambda_1 - \lambda_2)^2}\left(\frac{\lambda_1^2(\omega_{cp} - \lambda_2)^2}{2\omega_{cp}^2\lambda_2} - \frac{\frac{\lambda_1\lambda_2}{\omega_{cp}^2}\left(-\omega_{cp}^2 + \omega_{cp}(\lambda_1 + \lambda_2) - \lambda_1\lambda_2\right)}{2(\lambda_1 + \lambda_2)}\right) \tag{4}$$

Typically $\lambda_1 = \lambda_2^*$, which further implies that $\mu_1 = \mu_2^*$ and $\nu_1 = \nu_2^*$. If the reference signal is generated with a high quality crystal oscillator, its Fourier series expansion can be accurately approximated with a single non-zero element. This allows for simplification of (2). Let $p = \mu_1 + \nu_1$ and $\lambda = \lambda_1$, then

$$\begin{aligned} R_y(\tau) &= \exp(-j\omega_0\tau) \cdot \exp\left[-0.5\omega_0^2 c_{xtl}|\tau|\right] \cdot \\ &\cdot \exp\left[-\omega_0^2\left[p \cdot (1 - \exp[-\lambda|\tau|]) + p^* \cdot \left(1 - \exp[-\lambda^*|\tau|]\right)\right]\right] = \\ &= \exp(-j\omega_0\tau) \cdot \exp\left[-0.5\omega_0^2 c_{xtl}|\tau|\right] \cdot \exp\left[-2\omega_0^2\left[\Re\{p\} - \right.\right. \\ &\left.\left.\exp\left[-\Re\{\lambda\}|\tau|\right] \cdot (\Re\{p\}\cos(\Im\{\lambda\}|\tau|) + \Im\{p\}\sin(\Im\{\lambda\}|\tau|))\right]\right], \end{aligned} \tag{5}$$

Eq. (5) shows multiple factors that determine the dependence of the envelope of the autocorrelation function on the PLL parameters. The exponential decay factor $\exp\left[-0.5\omega_0^2 c_{xtl}|\tau|\right]$ depends on the quality of the crystal oscillator. The dependence of the envelope of $R_y(\tau)$ on other PLL components, which we want to use for user identification, is most pronounced at small values of $|\tau|$, for which the $\exp\left[-0.5\omega_0^2 c_{xtl}|\tau|\right]$ factor is close to 1, and hence can be neglected in the signature extraction process. The envelope $\mathcal{E}_{R_y}(\tau)$ of the autocorrelation function for small values of $|\tau|$ can thus be expressed as

$$\begin{aligned} \mathcal{E}_{R_y}(\tau) &= \exp\left[-2\omega_0^2\left[\Re\{p\} - \exp\left[-\Re\{\lambda\}|\tau|\right] \cdot \right.\right. \\ &\left.\left. \cdot (\Re\{p\}\cos(\Im\{\lambda\}|\tau|) + \Im\{p\}\sin(\Im\{\lambda\}|\tau|))\right]\right] = \\ &= \exp\left[-2\omega_0^2\left[\Re\{p\} - \exp\left[-\Re\{\lambda\}|\tau|\right] \cdot \sqrt{\Re\{p\}^2 + \Im\{p\}^2} \cdot \right.\right. \\ &\left.\left. \cdot \cos\left(\Im\{\lambda\}|\tau| + sgn\left(\Im\{\lambda\}\right) \cdot \arccos\left(\frac{\Re\{p\}}{\sqrt{\Re\{p\}^2 + \Im\{p\}^2}}\right)\right)\right]\right], \end{aligned} \tag{6}$$

which, with $\mathcal{E}_{R_y}(0) = 1$, becomes

$$\mathcal{E}_{R_y}(\tau) = \exp\left[-2\omega_0^2\Re\{p\}\left(1 - \exp\{-\Re\{\lambda\}|\tau|\} \cdot \cos\left(\Im\{\lambda\}|\tau|\right)\right)\right] \tag{7}$$

The characteristics of the envelope of the autocorrelation function at small $|\tau|$ can be used as a unique feature identifying a given oscillator, and the parameter vector

$$F = [\Re\{p\} \quad \Re\{\lambda\} \quad \Im\{\lambda\}] \tag{8}$$

can be used as a unique fingerprint that directly depends on the values of the components comprising the PLL circuit.

III. Identification Method

A. Distribution of the Envelope of the Sample Estimate of the Autocorrelation Function of the PLL Output

Consider an output $y(t)$ of the PLL, sampled with the frequency f_s. A sample estimate of the autocorrelation of the random process $y(t)$ calculated based on a record $y[n]$, $n = 1, \ldots, N$ can be obtained as

$$\underline{\hat{R}}_y[m] = \frac{1}{(N-m)}\sum_{n=1}^{N-k} y[n]y[n+m] \tag{9}$$

If N goes to infinity, then the joint distribution of any finite set of elements of $\left(\underline{\hat{R}}_y[m]/\underline{\hat{R}}_y[0] - \rho_m\right)$ becomes jointly normally distributed with the covariance matrix W, the elements of which are defined with (1.4) [19]

Assume access to the noise-corrupted PLL output records $y[n] = p[n] + \eta[n]$ undersampled with sampling rate f_s. $\underline{\hat{R}}_y[m]$, calculated from these undersampled records, oscillates with frequency $f = \min_N(f_0 - Nf_s)$, which because of the variations of f_0 and $\Delta(t)$ from (1) varies among the devices and over time. Wireless devices could potentially be identified by comparing vectors of envelopes of sample estimates of the autocorrelation functions $\underline{\mathcal{E}}_{\underline{\hat{R}}_y}[m]$ at small values of $|m|$. Vectors $\underline{\mathcal{E}}_{\underline{\hat{R}}_y}$ are normally distributed with covariance matrix elements given in (1.4) [19]. Because (7) was derived for small values of the time shift, $\underline{\mathcal{E}}_{\underline{R}_y}(\infty) = \exp\left[-2\omega_0^2\Re\{p\}\right]$, where p is device dependent. As a simplification, to calculate the covariance matrices with the infinite sums from (1.4) [19], we subtract the offset $\underline{\mathcal{E}}_{\underline{R}_y}(\infty)$, and, for the white noise corrupted PLL output records, obtain $\rho_m = cov(y(t), y(t+m))/var(y(t))$ [19]

$$\rho_m = \frac{\underline{\mathcal{E}}_{\underline{R}_y}(|m \cdot T_s|) - \underline{\mathcal{E}}_{\underline{R}_y}(\infty) + \sigma_\eta^2 \cdot \delta[|m \cdot T_s|]}{1 - \underline{\mathcal{E}}_{\underline{R}_y}(\infty) + \sigma_\eta^2}, \tag{10}$$

with a unit impulse $\delta[n]$, $\underline{\mathcal{E}}_{\underline{R}_y}$ from (7), and $\sigma_\eta^2 = 10^{NPNR/10}$, where $NPNR$ is the ratio of the power of the white noise to that of the phase noise

$$NPNR = 10\log_{10}(P_\eta/P_p). \tag{11}$$

B. Optimal Hypothesis Test

Consider first a two-device identification scenario. After the PLL output record has been captured from the device on the crime scene, the two hypotheses of the identification test are $\mathcal{H}_1$: device 1 is the transmitting device; $\mathcal{H}_2$: device 2 is the transmitting device. The likelihood ratio test is

$$\Lambda = \frac{p_{\underline{\mathcal{E}}_{\underline{\hat{R}}_y}|\mathcal{H}_1}(\underline{\mathcal{E}}_{\underline{\hat{R}}_y}|\mathcal{H}_1)}{p_{\underline{\mathcal{E}}_{\underline{\hat{R}}_y}|\mathcal{H}_2}(\underline{\mathcal{E}}_{\underline{\hat{R}}_y}|\mathcal{H}_2)} \underset{\mathcal{H}_2}{\overset{\mathcal{H}_1}{\gtrless}} \varsigma \tag{12}$$

For equally probable hypotheses the threshold $\varsigma = 1$ minimizes the risk of the test (12) (p.26 Section 2.2 [20]). With jointly Gaussian distributed vectors $\underline{\mathcal{E}}_{\underline{\hat{R}}_y}$,

$$p(\underline{\mathcal{E}}_{\underline{\hat{R}}_y}\,|\,\mathcal{H}_k) = \frac{1}{(2\pi)^{M/2}\det\{W_{\mathcal{H}_k}\}^{1/2}}\times$$
$$\times\exp\left\{-\frac{1}{2}\left(\underline{\mathcal{E}}_{\underline{\hat{R}}_y} - \underline{\mathcal{E}}_{\underline{\hat{R}}_{y,\mathcal{H}_k}}\right)^H W_{\mathcal{H}_k}^{-1}\left(\underline{\mathcal{E}}_{\underline{\hat{R}}_y} - \underline{\mathcal{E}}_{\underline{\hat{R}}_{y,\mathcal{H}_k}}\right)\right\}, \tag{13}$$

where $\underline{\mathcal{E}}_{\underline{\hat{R}}_{y,\mathcal{H}_k}}$ are envelopes of accurate estimates of the autocorrelation functions obtained from the devices from the pool of suspects. The binary decision rule becomes

$$\ln\left(\det\{W_{\mathcal{H}_1}\}\right) + \left(\underline{\mathcal{E}}_{\underline{\hat{R}}_y} - \underline{\mathcal{E}}_{\underline{\hat{R}}_{y,\mathcal{H}_1}}\right)^H W_{\mathcal{H}_1}^{-1}\left(\underline{\mathcal{E}}_{\underline{\hat{R}}_y} - \underline{\mathcal{E}}_{\underline{\hat{R}}_{y,\mathcal{H}_1}}\right) \underset{\mathcal{H}_1}{\overset{\mathcal{H}_2}{\gtrless}}$$
$$\ln\left(\det\{W_{\mathcal{H}_2}\}\right) + \left(\underline{\mathcal{E}}_{\underline{\hat{R}}_y} - \underline{\mathcal{E}}_{\underline{\hat{R}}_{y,\mathcal{H}_2}}\right)^H W_{\mathcal{H}_2}^{-1}\left(\underline{\mathcal{E}}_{\underline{\hat{R}}_y} - \underline{\mathcal{E}}_{\underline{\hat{R}}_{y,\mathcal{H}_2}}\right) \tag{14}$$

The two-device scenario can easily be generalized to a K-device scenario, for which the identified device k is the device for which the likelihood function takes its maximal value:

$$k_{opt} = \max_{k=1,\ldots,K} p(\underline{R}_y\,|\,\mathcal{H}_k) = \min_{k=1,\ldots,K}\ln\left(\det\{W_{\mathcal{H}_k}\}\right) +$$
$$+\left(\underline{\mathcal{E}}_{\underline{\hat{R}}_y} - \underline{\mathcal{E}}_{\underline{\hat{R}}_{y,\mathcal{H}_k}}\right)^H W_{\mathcal{H}_k}^{-1}\left(\underline{\mathcal{E}}_{\underline{\hat{R}}_y} - \underline{\mathcal{E}}_{\underline{\hat{R}}_{y,\mathcal{H}_k}}\right). \tag{15}$$

The power levels of the phase noise are much below the carrier power even for inexpensive commercially used PLLs (e.g. -81dBc/Hz at 1kHz offset from the carrier for ADF4360-1 [21]). Thus the measurement noise dominates the phase noise at common SNR values. For the discrete additive white Gaussian noise (AWGN) random process, ρ_m from (10) is dominated by the unit impulse and the covariance matrix W becomes an identity matrix. As will be shown in Section IV, for practical SNR levels the approximation of W from (14) and (15) with the identity matrix does not cause a noticeable degradation in identification performance. This allows for significant simplification of the decision rules (14) and (15). Respectively, for the binary scenario,

$$||\underline{\mathcal{E}}_{\underline{\hat{R}}_y} - \underline{\mathcal{E}}_{\underline{\hat{R}}_{y,\mathcal{H}_1}}||_2 \underset{\mathcal{H}_1}{\overset{\mathcal{H}_2}{\gtrless}} ||\underline{\mathcal{E}}_{\underline{\hat{R}}_y} - \underline{\mathcal{E}}_{\underline{\hat{R}}_{y,\mathcal{H}_2}}||_2, \tag{16}$$

and, for the K-ary scenario,

$$k_{opt} = \min_{k=1,\ldots,K}||\underline{\mathcal{E}}_{\underline{\hat{R}}_y} - \underline{\mathcal{E}}_{\underline{\hat{R}}_{y,\mathcal{H}_k}}||_2. \tag{17}$$

C. Practical Identification Algorithm

One possible way to obtain access to the undersampled PLL output in practice is to utilize (at least one) carrier phase recovery pilot tone, which for accurate extraction of the phase noise needs to be sufficiently separated from the data tones [22]. Although not present in current standards, security is becoming a critical issue in mobile radio applications, and it is reasonable to understand the potential benefit if future communication standards provide additional tones for security level enhancements. In fact the relative expense required decreases with the increase of bandwidth utilized by individual users, and such an increase has been observed in recent years.

The autocorrelation function estimates (9) are calculated based on individual signal records captured from the devices over time. From all samples of the autocorrelation function estimate, only for a subset of samples do we have $\underline{\mathcal{E}}_{\underline{\hat{R}}_y} \approx \underline{\hat{R}}_y$ (samples close to the local extrema of the autocorrelation function). With a fixed sampling rate, because of variations of f_0 among devices, as well as because of the time-varying frequency offset $\Delta(t)$ from (1), the subsets of samples for which $\underline{\mathcal{E}}_{\underline{\hat{R}}_y} \approx \underline{\hat{R}}_y$ can be different among the devices and vary over time. Thus to obtain accurate estimates of the fingerprint F (8) for each device from the pool of suspects, the envelopes of the estimates at small values of $|\tau|$ are matched to the model (7) through exhaustive search of the values of (8) for each record available from a given device and averaged over these records. To identify the device from the crime scene, the estimate of the envelope of the autocorrelation function is calculated based on the full captured record, and $p(\underline{\mathcal{E}}_{\underline{\hat{R}}_y}\,|\,\mathcal{H}_k)$ are calculated for each hypothesis with $\underline{\mathcal{E}}_{\underline{\hat{R}}_{y,\mathcal{H}_k}}$ reconstructed from the fingerprint of device k from the pool of suspects and the model (7).

IV. Measurements and Numerical Results

The performance of the proposed identification method is considered here with simulations and hardware measurements. Most important is Section IV-B, where PLL output signals were captured from commercially used PLLs and the performance of the identification method was analyzed at 15dB and 35dB SNR with records of length 200ms.

A. Synthetic Oscillators

Pairs of phase noise paths $p_k[n], k = 1, 2$ were generated by numerically solving a discrete-time version of the set of equations modeling a 1^{st} order, charge pump PLL ((8), (11) in [23]) for $\Delta t = 0.04\mu s$ (sampling rate $f_s = 25Msps$). The parameters used to generate each of the paths were generated randomly by multiplying nominal values of the parameters defined in [23]: quality parameters, of respectively, the voltage controlled and crystal oscillators $c_{VCO} = 15\cdot 10^{-19}$ and $c_{xtl} = 10^{-25}$; cut-off frequency of the PLL structure $\omega_{G_{PLL}} = 2\pi\cdot 10^4$ and cut-off frequency of the charge pump $\omega_{cp} = 2\pi\cdot 16\cdot 10^3$, with a factor $(1+|\kappa|)$, where $\kappa \sim \mathcal{N}(0,\sigma_\kappa)$. The third path (potential capture from the crime scene) was then generated using the first set of parameters. White Gaussian noise with elements $\eta[n] \sim \mathcal{N}(0,\sigma_\eta)$ was then added

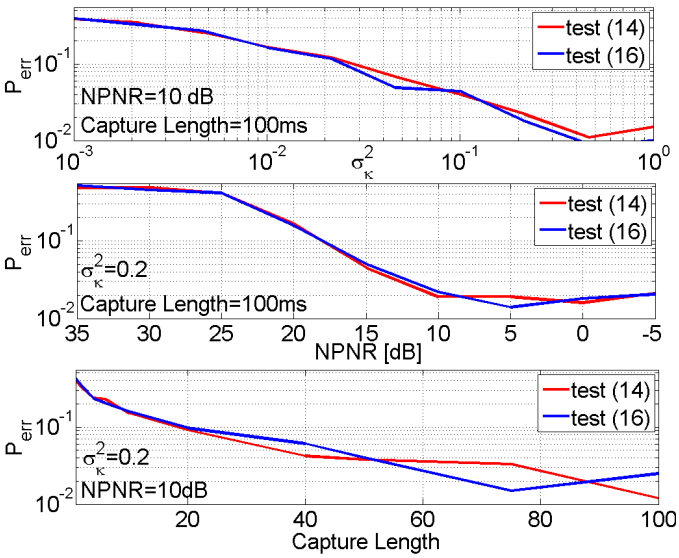

Fig. 2. Probability of error of the binary hypothesis test (14) and (16) averaged over 1000 trials for $NPNR = 10dB$ and for capture length $l_c = 100ms$ as a function of the standard deviation σ_κ used to artificially generate the oscillator pairs (top); for the standard deviation $\sigma_\kappa = 0.2$ used to artificially generate the oscillator pairs and for capture length $l_c = 100ms$ as a function of the $NPNR$ (middle); and for the standard deviation $\sigma_\kappa = 0.2$ used to artificially generate the oscillator pairs and for $NPNR = 10dB$ as a function the capture length (bottom).

to the three phase noise paths and autocorrelation functions were estimated from the white noise corrupted phase noise paths $y_k[n] = p_k[n] + \eta[n]$. Fig. 2 shows the probability of error P_{err} of the binary hypothesis test (14) and (16) averaged over 1000 trials as a function of the standard deviation σ_κ used to artificially generate the oscillator pairs (top); as a function of the additive white noise power to the phase noise power ratio $NPNR$ (11) (middle); and as a function the capture length (bottom). The region of the autocorrelation function employed was $\tau \in (0.01,\ 0.15)ms$. Covariance matrices $W_{\mathcal{H}_k}$ from (14) were calculated with (7), (1.4) [19], (10) with the assumption of known oscillators' parameters. Plots from Fig. 2 show a potential for effective device identification based of oscillator non-idealities, even if only a single capture from the devices building the pool of suspects and from the crime scene is available; however, the variation of component values was generated quite artificially; hence, hardware measurements are critical. These are provided in the next section.

B. Measured Oscillators

After the qualitative performance analysis from Section IV-A, the effectiveness of the proposed technique is analyzed for the case of commercially employed PLLs. The most challenging identification scenario, when the PLL's that need to be told apart are of the same model and from the same manufacturer, is considered. Eight Analog Devices ADF4360-1 [21] oscillators, oscillating at $f_0 = 2.4$GHz, were measured on a Tektronix $DPO71254B$ oscilloscope. 50 output records of length 200ms sampled with $f_s = 62.5$Msps were captured for each of the PLLs. Table I shows P_{err} averaged over 250 trials for all possible pairs from the group of 8 measured oscillators for the test (16) at $SNR = 15$dB (lower left, below the diagonal) and at $SNR = 35$ dB (upper right, above the diagonal), when all 50 captured records were used to extract the fingerprints (8), and a single record, randomly chosen from the group of all 50 captured records, was used as a capture from the crime scene. The region of the autocorrelation function employed was $\tau \in (0,\ 0.075)ms$. P_{err} values from Table I at $SNR = 15$dB are similar to values from Table I from [11]. In contrast to [11] however, an increase of the SNR did not bring significant performance improvement, as error floors emerged for some pairs of oscillators. Based on conversations with law enforcement authorities, error probabilities from Table I justify application of the proposed identification method for establishing probable cause and make it attractive for cyber-crime investigations. All 8 PLLs were re-measured 3 months after the original measurements were taken. Almost no change of the identification performance was observed when the measurement sets used for fingerprint extraction and for criminal identification were 3 months apart.

PLL #	1	2	3	4	5	6	7	8
1	-	0.000	0.000	0.000	0.000	0.000	0.016	0.000
2	0.000	-	0.000	0.164	0.000	0.000	0.000	0.000
3	0.000	0.000	-	0.000	0.216	0.000	0.000	0.000
4	0.000	0.228	0.000	-	0.00	0.00	0.00	0.00
5	0.000	0.000	0.228	0.000	-	0.000	0.000	0.020
6	0.000	0.000	0.000	0.000	0.000	-	0.000	0.008
7	0.008	0.000	0.000	0.000	0.000	0.000	-	0.000
8	0.000	0.000	0.000	0.000	0.028	0.036	0.000	-

TABLE I

P_{err} AVERAGED OVER 250 TRIALS FOR ALL POSSIBLE PAIRS FROM THE GROUP OF 8 MEASURED OSCILLATORS FOR THE TEST (16) AT $SNR = 15$DB (LOWER LEFT, BELOW THE DIAGONAL) AND AT $SNR = 35$DB (UPPER RIGHT, ABOVE THE DIAGONAL), WHEN ALL 50 CAPTURED RECORDS WERE USED TO EXTRACT THE FINGERPRINTS OF THE DEVICES FROM THE POOL OF SUSPECTS, AND A SINGLE RECORD FROM THE CRIME SCENE, RANDOMLY CHOSEN FROM THE GROUP OF ALL 50 CAPTURED RECORDS, WAS USED FOR IDENTIFICATION.

V. Conclusions and Future Work

In this paper we analyzed the degree to which a wireless device can be identified from unique characteristics of the phase noise of the transmitter's RF oscillator. Measurements of commercially used chips indicate that oscillators can be identified even at low SNRs and with very short observed sequences to the accuracy required to establish probable cause. The extension to higher-order PLL models that more accurately match characteristic of commercial PLLs could lead to improvement of the identification performance. Among the topics for future research are the consideration of the dependence of the characteristics of the phase noise on the carrier frequency, as well as environmental conditions. While the first is not critical, as the access point can assign devices that need to be identified to arbitrary frequency channels, the latter should be an important consideration for further refinement of the identification methods. To further establish the feasibility of the proposed method, the extension of the measurements to a larger number of units, also from different vendors, is foreseen.

REFERENCES

[1] Internet Crime Complaint Center annual reports: http://www.ic3.gov/media/annualreports.aspx.

[2] N. Patwari and S. Kasera, "Robust location distinction using temporal link signatures," in *Proc. of the* 13^{th} *annual ACM international conference on Mobile computing and networking (ACM MOBICOM)*, September 2007, pp. 111–122.

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

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

[5] ——, "Channel-based detection of sybil attacks in wireless networks," *IEEE Transactions on Information Forensics and Security*, vol. 4, pp. 492–503, September 2009.

[6] J. Hall, M. Barbeau, and E. Kranakis, "Enhancing intrusion detection in wireless networks using radio frequency fingerprinting," in *Proc. of* 3^{rd} *IASTED International Conference on Communications,Internet and Information Technology (CIIT)*, November 2004, pp. 201–206.

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

[8] O. Ureten and N. Serinken, "Bayesian detection of WiFi transmitter RF fingerprints," *IEEE Electronics Letters*, vol. 41, pp. 373–374, March 2005.

[9] ——, "Wireless security through RF fingerprinting," *Canadian Journal of Electrical and computer Engineering*, vol. 32, pp. 27–33, Winter 2007.

[10] S. Dolatshahi, A. Polak, and D. Goeckel, "Identification of wireless users via power amplifier imperfections," in *Proc. of the* 44^{th} *Asilomar Conference on Signals, Systems, and Computers*, November 2010, pp. 1553–1557.

[11] A. Polak, C. Dolatshahi, and D. Goeckel, "Identifying wireless users via transmitter imperfections," *IEEE Journal on Selected Areas in Communications*, vol. 29, pp. 1469–1479, August 2011.

[12] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proc. of the* 14^{th} *annual ACM international conference on Mobile computing and networking (ACM MOBICOM)*, March 2008, pp. 116–127.

[13] I. Kennedy, P. Scanlon, and M. Buddhikot, "Passive steady state RF fingerprinting: A cognitive technique for scalable deployment of co-channel femto cell underlays," in *Proc. of IEEE Dynamic Spectrum Access Networks Conference (DySPAN)*, 2008.

[14] A. Polak and D. Goeckel, "Identification of wireless users who actively fake their rf fingerprints with artificial distortion," *Submitted to: IEEE Transactions on Signal Processing*, 2013.

[15] G. R., H. J., and W. S., *Data Communication Principles*. Springer., 1992.

[16] A. Demir, A. Mehrotra, and J. Roychowdhury, "Phase noise in oscillators: a unifying theory and numerical methods for characterization," *IEEE Transactions on Circuits and Systems*, vol. 47, pp. 655–674, May 2000.

[17] T. C. W. Schenk, *RF imperfections in high-rate wireless systems: impact and digital compensation*. Springer Publisher, 2008.

[18] A. Mehrotra, "Noise analysis of phase-locked loops," *IEEE Transactions on Circuits and Systems*, vol. 49, pp. 1309–1316, September 2002.

[19] T. W. Anderson and A. M. Walker, "On the asymptotic distribution of the autocorrelations of a sample from a linear stochastic process," *The Annals of Mathematical Statistics*, vol. 35, pp. 1296–1303, 1964.

[20] H. V. Trees, *Detection, Estimation and Modulation Theory*. John Wiley & Sons, Inc., 1968.

[21] Data Sheet, ADF4360-1, Integrated Synthesizer and VCO: http://www.analog.com/static/imported-files/data_sheets/ADF4360-1.pdf.

[22] M. El-Tanany, Y. Wu, and L. Hazy, "Analytical modeling and simulation of phase noise interference in ofdm-based digital television terrestrial broadcasting systems," *IEEE Transactions on Broadcasting*, vol. 47, March 2001.

[23] S. K. S. Bittner and G. Fettweis, "Tutorial on discrete time phase noise modeling for phase locked loops." [Online]. Available: https://mns.ifn.et.tu-dresden.de/personalSites/stefan.krone/Documents/Bittner_S_PN_Tutorial.pdf