CHARACTERIZATION OF RF DEVICES USING TWO-TONE PROBE SIGNALS

Anthony F. Martone and Edward J. Delp

School of Electrical and Computer Engineering
Purdue University
West Lafayette, Indiana

ABSTRACT

This paper describes a method for forensic characterization of RF devices using two-tone probe signals. When transmitted to an RF device, the two-tone signal is affected by nonlinear circuit components such as amplifiers or diodes. The nonlinear components cause intermodulation distortion to the input signal, which is reradiated by the device. Features of the intermodulation distortion products are used to construct a device fingerprint. The fingerprint is then used to characterize the device so that it can be identified from other RF devices.

Index Terms— RF Devices, Forensic Characterization, Intermodulation Distortion, Probe Signals, Circuit Models

1. INTRODUCTION

Given the wide use of wireless devices for applications ranging from data networks to wireless sensors, it is of interest to identify the types of devices that are located in an environment. In order to locate and characterize wireless devices, the environment must be probed. This becomes the problem of determining the properties of an RF circuit by sending it a carefully designed signal (a probe) and examining the returned signal. The returned signal, which will be referred to as the *reradiated* signal, contains unique distortions that are generated by nonlinearities in the circuitry of the wireless device. The distortion is inherent to the circuit components and is used to form a device *signature* or *fingerprint* [1].

A block diagram of our wireless device detection system is shown in Figure 1. A probe signal is transmitted to the wireless device. The probe signal is received by the RF front-end of the device, where it encounters filters, amplifiers, and random noise. The amplifier (i.e., the nonlinearity) reflects and distorts the probe signal, which causes the device to reradiate the distorted signal. Features are then extracted from the reradiated signal. The features (feature vector) form the wireless device signature or fingerprint. The feature vector is used to classify or identify the device.

The proposed detection scheme can be used for a variety of applications including the detection of Part 15 devices. Part 15 is a Federal Communication Commission (FCC) mandate that specifies the procedures for the transmission of unlicensed radiators. Examples of Part 15 devices are walkie-talkies, cordless phones, wireless surveillance systems, wireless fences, wireless microphones, and garage door openers. The general conditions of operation for Part 15 devices state that “an intentional, unintentional, or incidental radiator is subject to the conditions that no harmful interference is caused and that interference must be accepted that may be caused by the operation of an authorized radio station, by another intentional or unintentional radiator, by industrial, scientific and medical (ISM) equipment, or by an incidental radiator” [2]. The term *harmful interference* is any transmission that “seriously degrades, obstructs, or repeatedly interrupts a radio communications service” [3]. If an unlicensed radiator is causing harmful interference in the environment, our proposed wireless device detection scheme would alert the operator of the Part 15 device so that the generation of harmful interference can be prevented.

In this paper we describe a detection system based on using a two-tone probe and examine what types of features can be used to construct a device signature. We will also examine the performance of various classification schemes.

2. TWO-TONE PROBE SIGNALS

A two-tone signal is the sum of two sinusoidal signals, where each sinusoid has a different frequency. The frequency of the second sinusoid equals the frequency of the first sinusoid plus some offset value. A two-tone signal is described by Equa-

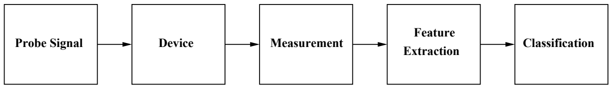

Fig. 1. Wireless Device Detection System.

This research was supported by a grant from the U.S. Army Research Office as a Multi-disciplinary University Research Initiative on Standoff Inverse Analysis and Manipulation of Electronic Systems under grant number W911NF-05-1-0337. Address all correspondence to E. J. Delp, ace@ecn.purdue.edu

Parameter	Definition
A_1	Amplitude of first sinusoid
A_2	Amplitude of second sinusoid
t	Time (seconds)
f_1	Frequency of first sinusoid (Hz)
f_2	$f_2 = f_1 + \Delta$
Δ	Frequency Offset (Hz)

Table 1. Two-Tone Probe Signal Parameters.

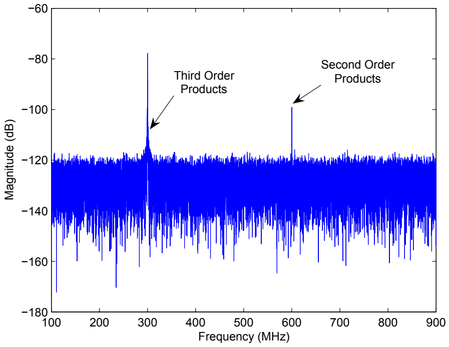

Fig. 2. Power Spectrum of $y(t)$ with the IMD Products Shown.

tion 1 with the parameters of the signal defined in Table 1. Let $X(f)$ be the Fourier Transform of $x(t)$. The power spectrum of $x(t)$ is defined as $P_x(f) = X(f)X^*(f)$, where $X^*(f)$ is the complex conjugate of $X(f)$. The energy of a two-tone signal is concentrated near the locations of the discrete probe frequencies.

$$x(t) = A_1 \cos(2\pi f_1 t) + A_2 \cos(2\pi f_2 t) \qquad (1)$$

When $x(t)$ is used to examine an RF circuit, it will encounter a nonlinearity and will be reradiated. The reradiated signal, $y(t)$, contains Intermodulation Distortion (IMD) products [4] that are generated by the two-tone probe. In this paper, the nonlinearity is modelled as a power series [4]. The energy of the IMD products are located at discrete positions in the power spectrum $P_y(t)$, of $y(t)$. The IMD product locations are defined by Equation 2 and the order of the IMD product is defined by Equation 3 [5], where n_1 and n_2 are integers. An example of a power spectrum with IMD products is shown in Figure 2. The two probe frequencies are located at 300 MHz and 300.1 MHz. The second and third order products are illustrated in the Figure.

$$f_{imd} = n_1 f_1 + n_2 f_2 \qquad (2)$$

$$o = |n_1| + |n_2| \qquad (3)$$

The IMD products are distributed throughout the power spectrum at various discrete frequency locations. Some odd-ordered IMD products are located very close to the probe frequencies. These products are referred to as the *in-band distortion products (IDP's)* [6]. When the reradiated signal containing the IDP's is filtered, the IDP's remain in the narrow band of the filter. Therefore, if the probe is modulated to the receive band of the wireless device, the IDP's remain present in the power spectrum. The energies of the IDP's are used to form a feature vector [7]. The IDP engeries are effective for two reasons. The first is that the locations of the IDP's are known prior to probing based on Equation 2. This simplifies the feature extraction process. The second, as mentioned above, is that the IDP's are within the narrow band of the wireless device filter.

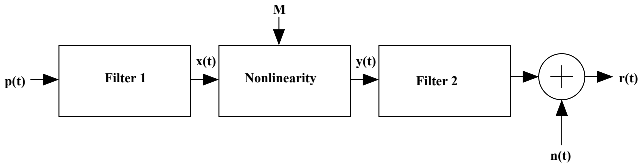

Fig. 3. Synthetic Circuit Model.

3. CIRCUIT MODEL

A circuit model must be capable of simulating the IDP's that are generated by the wireless device in response to a two-tone probe signal. For a given wireless device, the IDP's are generated in the RF front-end. The probe signal is received by the antenna of the RF front-end and transferred to a filter. The filtered signal is amplified, where the amplifier is a nonlinear component. A percent of the filtered signal is reflected from the amplifier and transferred back through the filter. The reflected signal is reradiated by the antenna. The reradiated signal contains the IDP's, which are used to construct a feature vector. A block diagram of the synthetic circuit model (SCM) used to simulate the RF front-end is shown in Figure 3 [1]. $p(t)$ is the two-tone signal. Filter 1 equals filter 2. The nonlinearity is modelled as a power series as defined by Equation 4 [4]. The coefficients in the power series characterize the amplitudes of the IDP's and M is the order of the power series. The noise $n(t)$ is modeled by i.i.d. Gaussian random variables $N(\mu, \sigma^2)$. $r(t)$ is the output.

$$y(t) = \sum_{j=1}^{M} a_j [x(t)]^j \qquad (4)$$

4. FEATURE EXTRACTION

The features introduced in this section are obtained by the IDP's from the reradiated signal $r(t)$. The energy of the IDP's

[1] This circuit model was suggested by Professor Larry Carin of Duke University

are extracted from the power spectrum, $P_r(f)$, of $r(t)$ and used as features. For a given $P_r(f)$, four amplitudes are extracted and used as features. The amplitudes are extracted at the locations of the probe frequencies and the 3^{rd} order IDP's. Only the positive frequency locations are considered. The location of the probe frequencies are f_1 and f_2. The location of the 3^{rd} order IDP's are $(2f_1 - f_2)$ and $(2f_2 - f_1)$. The feature frequency locations are defined as $\rho = \{\rho_1 = f_1, \rho_2 = f_2, \rho_3 = (2f_1 - f_2), \rho_4 = (2f_2 - f_1)\}$. A feature value is determined by Equation 5, where $1 \leq g \leq 4$.

$$e_g = P_r(\rho_g) \tag{5}$$

5. CLASSIFICATION SYSTEMS

The classifiers we used are trained from a set of observations referred to as the *training set*. A total of J observations are considered. Each observation consists of a training feature vector, or *training vector*, θ_j and a label τ_j. The training vector θ_j denotes the j^{th} vector in a set of J total training vectors. Each training vector contains G features as defined in Equation 6. The feature $e_{(tr,j,g)}$ in Equation 6 is adapted from the notation in Equation 5 to signify the jth training vector. The label τ_j identifies the category of θ_j. A set of D wireless device categories are defined by Equation 7. Let $\tau_j \in \Upsilon$. Define Q as the number of training vectors in each class, where $J = QD$. The training set is denoted as $\Theta = \{[\theta_1, \tau_1], ...[\theta_J, \tau_J]\}$. The classifier estimates the mapping $\varphi : \theta_j \Rightarrow \tau_j$ for each observation [8]. Once trained, the classifier is used to decide the class χ_i for a given *test vector* ω_i, where $\chi_i \in \Upsilon$. The test vector is defined by Equation 8. The feature $e_{(te,i,g)}$ in Equation 8 is adapted from the notation in Equation 5 to signify the ith test vector. Each test vector has a ground truth label λ_i, where $\lambda_i \in \Upsilon$. The accuracy of the classifier is determined by comparing λ_i to χ_i. For an average classification accuracy estimate, several test vectors must be tested by the classifier.

$$\theta_j = [e_{(tr,j,1)} \; e_{(tr,j,2)} \; ... \; e_{(tr,j,G)}] \tag{6}$$

$$\Upsilon = \{\Upsilon_1, ...\Upsilon_D\} \tag{7}$$

$$\omega_i = [e_{(te,i,1)} \; e_{(te,i,2)} \; ... \; e_{(te,i,G)}] \tag{8}$$

Six classification systems are used to categorize the test vectors. The first system is a *support vector machine* (SVM). This classifier constructs a hyperplane in the feature space to separate the feature vectors. The SVM algorithm we used generates its training model using the LIBSVM library [9]. The second classifier is a *binary tree classifier* (BTC). The BTC splits a single classification decision into a set refined decisions. The binary tree is constructed using the classification and regression tree (CART) method in [10].

The third and fourth classifiers are a *distance classifier* [11] and a *Gaussian maximum likelihood classifier* (GMLC) [12]. Both classifiers use Bayesian methods with a Gaussian assumptions, to estimate a posterior density function for each class for a given test vector. These posterior density functions are then used to estimate the category for the given test vector. The mean of the Gaussian density is estimated by the maximum likelihood (ML) estimate. This estimate is used by both classifiers. In addition, a covariance matrix is estimated for the GMLC.

The fifth and sixth classifiers are a *Parzen window* classifier [13] and a *K nearest neighbor* (K-NN) classifier [14]. The Parzen window classifier estimates a posterior density function for each class based on a window function, the set of training vectors, and the test vector. These posterior density functions are then used to estimate the category for the given test vector. The K-NN estimates a distance between the test vector and all training vectors. The distance values are sorted from smallest to largest. The first K smallest distance values are used to estimate the category of the test vector based on a majority vote.

6. EXPERIMENTAL RESULTS

The experiments in this section use the circuit model to generate training and testing signals. These experiments are designed to test the classification accuracy for the proposed wireless device detection system. In addition, these experiments are designed only to study the effects of the nonlinearities and not the front-end filters. The filters in all our circuit models are assumed to have the same filter response. The filter response is designed such that the probe frequencies are within the passband of the filter. We assume we have 5 different circuit models and 1 "noise model" and referenced as $\{\Upsilon_1, ...\Upsilon_6\}$. The noise model Υ_6 addresses the case when the output signal from the circuit model is generated only by circuit noise. This occurs by removing the filters and nonlinearity in the circuit model and letting $p(t) = 0$. This results in $r(t) = n(t)$. Note that the noise class Υ_6 is generated by the same Gaussian random variable as used by the noise in each circuit model. The filters are modelled by Chebychev Type 1 filter of order 8. The frequency response of the filter is shown in Figure 4. As illustrated in the figure, the passband ranges from 100MHz to 1000MHz. The probe frequencies are within this range. The nonlinearities of each circuit model are defined in Table 2. The noise $n(t)$ differs between the training and testing sets.

A set of two-tone signals are designed to generate training and testing signals. The two-tone signal set contains 899 probe signals and is denoted as $\{p_1(t), ...p_{899}(t)\}$. The probe frequencies f_1 and f_2 are unique for each probe signal. The frequency f_1 for any j probe signal $p_j(t)$ is defined as κ_j. The second frequency f_2 is defined as $\iota_j = \kappa_j + \Delta$, where $\Delta = 0.1$MHz. The set of all probe frequencies is $\{\kappa_1 =$

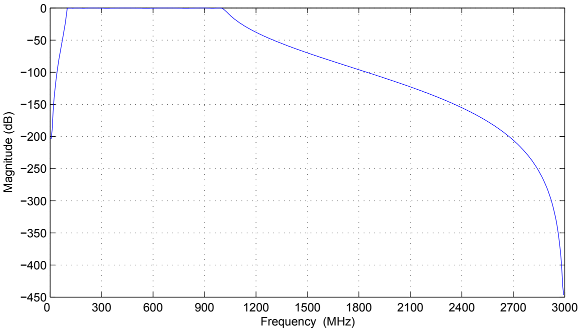

Fig. 4. Frequency Response of the Filter Used in the Circuit Model.

	Υ_1	Υ_2	Υ_3	Υ_4	Υ_5
a_1	5.0μ	0.39μ	0.2μ	0.08μ	0.003μ
a_2	0.5μ	0.01μ	0.01μ	0.05μ	0.01μ
a_3	0.05μ	0.039μ	0.02μ	0.008μ	0.0001μ

Table 2. Power Series Coefficients Used in Each Circuit Model, where $\mu = 10^{-6}$.

$101\text{MHz}, ...\kappa_{899} = 1000\text{MHz}\}$, where $\kappa_j - \kappa_{j-1} = 1\text{MHz}$.

The set of probe signals are input into each of the 6 models. A total of $J = 5394$ training signals $\{r_1(t), ...r_{5394}(t)\}$ are generated. The noise $n(t)$ used for the training set is generated by $N(0, 5x10^{-13})$. The noise is randomly generated each time a probe is input into the models. The only distinction between the training signals for a given model is the noise. Each training signal has a label τ_j denoting the model used to generate the signal. The number of training signals in each class is $Q = 899$. The power spectrum $P_{r_j}(f)$ is then obtained for each returned signal. As described in Section 4, 4 IDP's are extracted using $e_{(tr,j,g)} = P_{r_j}(\rho_g)$, where $1 \leq g \leq 4$. A training vector is formed as $\theta_j = [e_{(tr,j,1)}...e_{(tr,j,4)}]$. The training set consists of the training vectors and class labels denoted as $\Theta = \{(\theta_1, \tau_1), ...(\theta_{5394}, \tau_{5394})\}$.

	E_{μ_1}	E_{μ_2}	E_{μ_3}	E_{μ_4}	S_μ	ϱ_μ
Υ_1	-30.9	-30.9	-49.7	-44.2	35.5	3.71
Υ_2	-33.1	-33.1	-51.8	-46.3	33.4	3.71
Υ_3	-57.4	-57.4	-75.5	-70.8	8.9	3.70
Υ_4	-65.3	-65.4	-83.0	-78.6	0.98	3.85
Υ_5	-91.1	-90.9	-92.0	-91.9	-24.9	89.1
Υ_6	-89.4	-90.5	-89.4	-91.1	N/A	N/A

Table 3. Average Feature Values, Average SNR, and Average Percent IMD Statistics for Each Class in the Training Set. All entries are in units of dBm.

	E_{μ_1}	E_{μ_2}	E_{μ_3}	E_{μ_4}	S_μ	ϱ_μ
Υ_1	-30.9	-30.9	-49.7	-44.2	27.70	3.71
Υ_2	-33.1	-33.1	-51.9	-46.3	25.57	3.71
Υ_3	-57.4	-57.4	-75.1	-70.7	1.12	3.83
Υ_4	-65.3	-65.4	-80.8	-78.0	-6.80	4.75
Υ_5	-84.1	-84.2	-84.2	-84.2	-32.69	112
Υ_6	-90.1	-89.9	-90.1	-90.1	N/A	N/A

Table 4. Average Feature Value, Average SNR, and Average Percent IMD Statistics for the Testing Set. All entries are in units of dBm.

For a given power spectrum, the signal to noise ratio (SNR) [6] is estimated. For the set of power spectrums $P_{\Upsilon_d} = \{P_{r_1}(f), ...P_{r_Q}(f)\}$ that are generated by class Υ_d, an average SNR value is estimated as $S_\mu = [\sum_{q=1}^{Q} SNR_q]/Q$, where SNR_q is the SNR of $P_{r_q}(f)$. An average SNR value is estimated for each class. The percentage of IMD present in the power spectrum $P_{r_q}(f)$ is estimated by Equation 9. Given the set of power spectrums in P_{Υ_d}, an average percent IMD value is defined as $\varrho_\mu = [\sum_{q=1}^{Q} \varrho_q]/Q$, where ϱ_q is the percent IMD in $P_{r_q}(f)$. An average percent IMD value is estimated for each class. Finally, given the set of power spectrums in P_{Υ_d}, an average feature value is estimated as $E_{\mu_g} = [\sum_{q=1}^{Q} e_{(tr,q,g)}]/Q$, for each g feature. An average feature value is estimated for each class. Statistics for the training set are shown in Table 3. It is of interest to note that the average feature values between Υ_1 and Υ_2 are similar. This is also true for Υ_5 and Υ_6.

$$\varrho = \frac{\sqrt{[P_{r_q}(\rho_3)]^2 + [P_{r_q}(\rho_4)]^2}}{\sqrt{[P_{r_q}(f_1)]^2 + [P_{r_q}(f_2)]^2}} \quad (9)$$

A test set is generated by the same procedure as the training set. The difference between the training set and the testing set is $n(t)$, the random noise. For the testing set, $n(t)$ is generated by $N(0, 3x10^{-12})$. The set of two-tone signals are once again input into each circuit model and the set of test vectors $\Omega = \{\omega_1, ...\omega_{5394}\}$ are generated. The labels for the testing set are used as ground truth information and denoted as $\{\lambda_1, ...\lambda_{5394}\}$. Statistics for the testing set are shown in Table 4.

The accuracy of each classifier is measured based on the classification results of the test vectors in Ω. For a given test vector ω_i, the classifier outputs the classification decision χ_i, where $1 \leq i \leq 5394$. χ_i is then compared with the ground truth label λ_i. An indicator function, as defined by Equation 10, is used to indicate if $\chi_i = \lambda_i$. A probability is estimated for each class. Define P_d to be the probability estimate for class Υ_d, where $1 \leq d \leq 6$. P_d is estimated only by the test vectors that belong to class Υ_d as shown in Equation 11. Note the condition $\lambda_i = \Upsilon_d$ in the sum, which requires that only the test vectors that have the label $\lambda_i = \Upsilon_d$ are used to estimate P_d. The classification results for these experiment are shown in Table 5. The majority of the errors caused during classification are due to the similarity between the features between classes. This is noticeable between classes Υ_1 and

	P_1	P_2	P_3	P_4	P_5	P_6
SVM	100	100	100	96.1	0	99.3
BTC	100	100	100	99.2	2.8	96.9
Distance	85.1	90.2	100	100	99.1	71.9
GMLC	100	100	100	100	100	0
Parzen	90	93.4	100	100	83	93.2
K-NN	100	100	100	100	100	94

Table 5. Classification Results (in percent) for the Two-Tone Experiments.

Υ_2. It is also noticeable between classes Υ_5 and Υ_6.

$$I(i) = \begin{cases} 1 & , \quad \lambda_i = \chi_i \\ 0 & , \quad \text{else} \end{cases} \tag{10}$$

$$P_d = \frac{\sum\limits_{\substack{i=1 \\ \lambda_i=\Upsilon_d}} I(i)}{899} \qquad 1 \leq d \leq 6 \tag{11}$$

7. CONCLUSION

A wireless device characterization system was described in this paper. The proposed approach used a two-tone probe to generate IMD products. The amplituds of the IMD products were used to construct a feature vector unique to each wireless device model. Classification results indicated accurate characterization of feature vectors, thereby verifying the effectiveness of the proposed approach. The majority of the errors caused during classification are due to the similarity between the features between classes. The K-NN classier produced the best overall results. All classifiers had difficulties classifying the testing vectors from class Υ_6 (noise only). These classification errors are caused by the similarity of the features between Υ_5 and Υ_6.

8. REFERENCES

[1] A. F. Martone, A. K. Mikkilineni, and E. J. Delp, "Forensics of things," in *Proceedings of the 2006 IEEE Southwest Symposium on Image Analysis and Interpretation*, Denver, Colorado, March 2006, pp. 149–152.

[2] F. C. Commission, *Part 15 - Radio Frequency Devices*, 2006, section 15.5, Part B.

[3] ——, *Part 15 - Radio Frequency Devices*, 2006, section 15.3, Definitions.

[4] M. Steer and P. Khan, "Generalized power series analysis of intermodulation distortion in a mesfet amplifier: Simulation and experiment," *IEEE Transactions on Microwave Theory and Techniques*, vol. 35, pp. 1248–1255, December 1987.

[5] V. Golikov, S. Hienonen, and P. Vainikainen, "Passive intermodulation distortion measurements in mobile communication antennas," in *Vehicular Technology Conference, 2001*, vol. 4, October 2001, pp. 2623–2625.

[6] J. Pedro and N. Carvalho, *Intermodulation Distortion in Microwave and Wireless Circuits*. Norwood, MA: Artech House, INC., 2003.

[7] N. Khanna, A. K. Mikkilineni, A. F. Martone, G. N. Ali, G. T.-C. Chiu, J. P. Allebach, and E. J. Delp, "A survey of forensic characterization methods for physical devices." *Digital Investigation*, vol. 3, no. Supplement-1, pp. 17–28, 2006.

[8] C. J. C. Burges, "A tutorial on support vector machines for pattern recognition," *Data Mining and Knowledge Discovery*, vol. 2, no. 2, pp. 121–167, 1998. [Online]. Available: citeseer.ist.psu.edu/burges98tutorial.html

[9] C.-C. Chang and C.-J. Lin, "Libsvm: A library for support vector machines." [Online]. Available: http://www.csie.ntu.edu.tw/ cjlin/libsvm/

[10] L. Breiman, J. Friedman, R. Olshen, and C. Stone, "Classification and regression trees," Belmont, CA, 1984.

[11] K. Fukunaga, *Introduction to Statistical Pattern Recognition*. San Diego, Ca: Academic Press, 1990.

[12] J. Hoffbeck and D. Landgrebe, "Covariance estimation for classifying high dimensional data," in *International Geoscience and Remote Sensing Symposium (IGARSS95)*, vol. 2, July 1995, pp. 1023 – 1025.

[13] G. Babich and O. Camps, "Weighted parzen windows for pattern classification," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 18, pp. 567 – 570, May 1996.

[14] T. Cover and P. Hart, "Nearest neighbor pattern classification," *IEEE Transactions on Information Theory*, vol. 13, pp. 21 – 27, January 1967.