Robust Stable Radiometric Fingerprinting for Wireless Devices

Andrea Candore†, Ovunc Kocabas‡ and Farinaz Koushanfar‡
Dept. of Information Engineering, University of Pisa†, Pisa, Italy, 56122
Electrical and Engineering Dept., Rice University‡, Houston, TX, 77005

***Abstract*— We introduce a new method for radiometric fingerprinting that detects the unique variations in the antenna, oscillator properties, as well as the digital and analog interfaces of the radio by passively monitoring the radio packets. Several individual identifiers are used for extracting the unique physical characteristics of the radio, including the frequency offset, modulated phase offset, in-phase/quadrature-phase offset from the origin, and magnitude. Our method provides stable and robust identification by developing individual identifiers (classifiers) that may each be *weak* (i.e., incurring a high prediction error) but their committee can provide a *strong* classification technique. We use two methods for combining the classifiers: (1) weighted voting, and (2) maximum likelihood. Our hardware implementation and experimental evaluations over multiple radios demonstrate that our weighted voting approach can identify the radios with an average of 88% detection probability and an average of 12.8% probability of false alarm after testing only 5 frames. The probability of detection and probability of false alarms both rapidly improve by increasing the number of test frames.**

Index Terms **— Wireless Security, RF Fingerprinting**

I. Introduction

In the pervasive computing era, where the embedded computational devices are often seamlessly connected, identification of the origin of data and messages is important for many security and protection reasons. To enable device identification, tagging, and tracing, a number of existing methods including digital keys, and digital identifiers such as IP addresses provide a degree of protection by either actively locking the access, or by passively keeping the access record. However, the scope of identification and security methods based on digital keys and IP addresses are limited due to a number of reasons. First, the digital IDs can be cloned and replayed; all what an attacker needs is to compromise one node to gain access to the shared resources and communicated messages in the network. Second, most classic cryptographic methods that are used for locking incur a high overhead thus are inherently ill-suited for embedded computing devices. Lastly, the IP and MAC addresses can be easily changed either by riding on proxy servers in untrusted, unregistered and untraceable parts of the world, or by compromising the legitimate servers.

To overcome the limitations of identifications by digital tagging and digital keys, alternative methods based on the natural and unclonable variations in the underlying physical devices have been proposed, including physically unclonable functions and radiometric fingerprinting [1], [2], [3]. These methods leverage the physical properties of the silicon and circuit components that cannot be easily forged to provide unique means of device identification (IDs). The challenge is to utilize the analog device or circuit variations for extracting stable and robust IDs that can be recorded and later used for identifying and tracing the devices or for other forensic reasons. We use the terms classification and identification interchangeably: identification can be done by snooping, learning, and recording the properties of each radio's unique signature, and then classifying the properties of a new message by comparing against the stored radio signatures in the database.

In this paper, we propose new methods for stable and robust radiometric fingerprinting of a scalable and extensible radio platform. The method works by profiling the unique properties present in the radio's oscillation unit, power amplifier, and D-to-A converter. Radiometric fingerprinting is an active subject of study and research during the last three decades [4], [5], [2], [6], [3]. A large body of work in this area has addressed electromagnetic [7] and antenna-level correlation and properties. More recently, a number of authors have studied fingerprinting the devices that implement a radio or network protocol and have shown promising results for identifying the stored radio fingerprints. Much more work is still needed for ensuring data integrity and stability of the identification results.

The individual classifiers often provide a weak means of prediction. Generally speaking, a *weak classifier* is the one that can guess the output correctly slightly better than random, so it's output is not completely irrelevant [8]. Blindly combining the multi-dimensional data using simple clustering techniques does not work well because of the known problems of curse of dimensionality, where exponentially many more data points are needed for stable and robust clustering in multiple dimensions. Our contributions are as follows:

- We propose a new robust and stable radiometric signing and identification method based on combining (committee) of individual weak classifiers.
- The explicit method that we use is weighted voting that has been shown to be very effective yet simple for combining the results of multiple weak classifiers [9].
- We show the superior performance of the weighted voting method compared with maximum likelihood combining methods, especially for small number of test frames.
- Our evaluation results based on experimentations on the WARP radio testbed show that our new methods achieve stable and robust means of identifying the radios by snooping a few messages and fast signature matching methods.

978-1-4244-4804-3/09/$25.00

The remainder of the paper is organized as follows. Section II surveys the related literature. The background is presented in Section III. The overall flow of the signature extraction and matching is shown in Section IV where the classifying variables are also introduced. Experiment organization, single characteristic (weak) classification, and methods for combining the single weak classifiers to form a strong committee are discussed in Section V. The evaluation results on the WARP radios are shown in Section VI. Finally, Section VII concludes the paper.

II. Related work

Identifying the source of an emitted signal has long been a research subject especially in military applications where finding the source of radar signal is of utmost importance [10], [5]. Identification is done by mapping unique features of a signal to the known feature set of transmitters. The same technique is also used for detecting the frauds in cellular phone networks [11]. More recently, the ever increasing usage of wireless communication and the need for security and protection have amplified the importance of identification of unknown transmitters. Several new methods have been proposed for identification of wireless devices, e.g., EM radiation [7], or antenna orientation [12]. A number of recent work in this area has focused on identification of devices by RF fingerprinting which utilizes the unique hardware characteristics of each device.

Device identification by the unique variations in the physical properties has been subject of research in integrated circuits. The work in [13] uses the delay variation of CMOS logic components to extract a digital secret. The properties of reconfigurable platforms are used in [14] to build a secure and robust authentication system based on the present delay variations. A post-fabrication nondestructive gate-level characterization for IC identification is also presented in [15]. In similar, RF fingerprinting methods rely on the hardware imperfections inherited due to manufacturing variability to uniquely identify wireless devices [4], [2], [16], [6], [3]. These flaws cause deviations in the transmitted signal and detecting these deviations can be used for identification. For example, in [16] a matched filter is used to create signal profiles of devices for finding the origin of transmitted signal. It is also shown that the turn-on transient behavior is unique to each device and can be used for fingerprinting [2], [6], [3]. When a transmitter is activated, the transmitted signal will observe a transient behavior that would be distinct for each wireless device due to hardware differences. Unique features of the device, instantaneous phase and amplitude, can be extracted from the received signal and used for identification. However, transient signal identification requires regenerating the signal from the received *In-phase/Quadrature-phase (I/Q)* values and processing in the waveform domain, increasing the complexity. An alternative approach is proposed in [4] that uses the modulation domain characteristics of a signal for RF fingerprinting. This method exploits the deviations from the ideal I/Q plane (instead of the transient behavior) to identify different transmitters. Since each transmitter has different hardware characteristics, deviations from the ideal signal can be used as a fingerprint for each transmitter. Five unique features from the modulation domain are used for identification and these features are listed according to their level of significance as follows; frequency error, SYNC correlation, I/Q offset, magnitude error and phase error.

Our new identification method is also performed in the modulation domain. We achieve a much more robust and stable radio identification compared with the best previously reported results. Rather than using simple clustering methods such as K-nearest neighbor that does not perform well in higher dimensions [4], we form a committee of classifiers by weighted voting that combines the weak classifiers and provides stable and robust solutions.

We note here that several methods are proposed for preventing identity-based attacks in wireless networks [17], [18], [12]. Most of the methods in this area use the physical properties of the channel instead of the transmitter hardware characteristics. The channel between transmitter and receiver varies in space, time and frequency therefore, identification can be done by observing physical properties of the channel. Shortcomings of channel identification-based methods are that they assume the devices are not mobile and also the probability of correct identification relies on the distance between different transmitters.

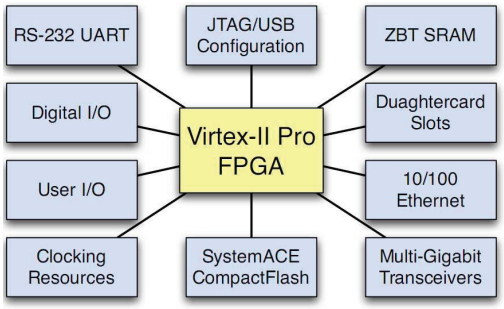


Fig. 1. The components on the WARP board [19].

III. Background

In this paper, we employ the Wireless Open-Access Research Platform (WARP) that is a custom platform designed for prototyping and implementing physical layer and network protocols [19]. WARP is a scalable and extensible platform based on custom hardware implementations of communication blocks. This open source platform has been adopted in more than forty universities and companies and is presently the most widely used. Hardware part of WARP consists of 3 elements [20] that are shown in Figure 1.

1) Xilinx Virtex-II Pro FPGA: FPGA is composed of configurable logic blocks and two PowerPC cores. While real-time DSP applications that require high-speed communication are implemented by configurable logic blocks, PowerPC processor cores execute network

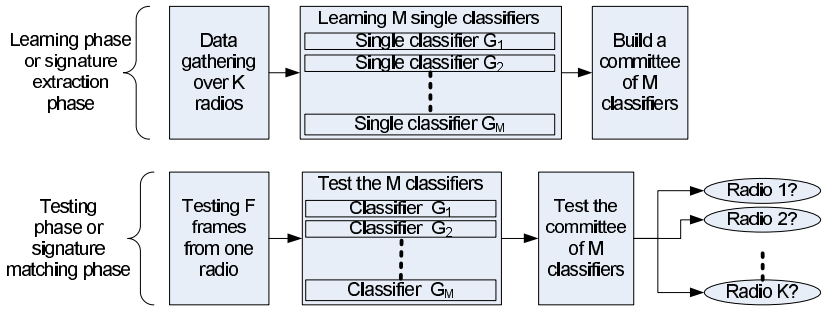


Fig. 2. The flow of signature extraction and signature matching approach.

layer protocols developed in C and provide flexible interface between PHY layer and MAC layer.

2) Radio Card: The radio card supports both 2.4 GHz and 5 GHz ISM /UNII bands and allows wideband applications such as OFDM.
3) 10/100 Ethernet Interface: Ethernet Interface is used for wired network connections which also capable of real-time communication between WARP boards.

IV. Signature extraction and matching

To authenticate a wireless device in a network, a signature that uniquely identifies each device is needed. Various signature extraction methods are proposed and used for network security but we are interested in a signature scheme based on the unique RF signal characteristics of a device. A signature can be generated for each device by extracting its specific information from the transmitted signal. For extraction, received signal should be processed. Processing of the signal can be done either in waveform domain or in modulation domain. We process the signal in the modulation domain where the Differential Quadrature phase-shift keying (DQPSK) is used for modulation. In DQPSK, the data is encoded by changing, or modulating, the phase difference of a reference signal (the carrier wave). Four phases are used that are each separated by $\pi/2$. In addition to the phase characteristics, the drift (offset) in the oscillation frequency and a number of other characteristics are used for classification. We denote each single-characteristic classifier by G_m, where $m = 1, \ldots, M$.

Figure 2 shows the overall flow of our signature extraction (learning phase) and signature matching (testing phase) method. Signature extraction process (demonstrated on the upper row on the figure) for each radio can be defined as follows. First, a predefined number of training message frames is specified and then transmitted by each radio card. Next, we define the single characteristics (G_m) that can be used to identify the source of messages. In this paper, we use data-driven density formation and maximum likelihood (ML) classification for representing and computing each G_m. As we mentioned earlier, each of the characteristics would be a weak classifier in the sense that we may get a high prediction error. The last step in signature extraction is to combine the results of the M classifiers. We select weighted voting as the committee formation method. Our reason for this choice is the simplicity and good performance of this method compared to other alternatives [9]. We also compare the performance of weighted voting to combining the weak classification results by the maximum likelihood procedure.

The signature checking phase (shown on the lower row on Figure 2) is much simpler. Upon arrival of a batch of F frames, the characteristics of the frames are evaluated against the M single classifier's extracted signatures using the maximum likelihood method. Next we combine the results of the M classifiers. The result would be identification of the radio source of the incoming batch of signals.

A. Classifying variables

In this subsection, we discuss extraction of the M classifying variables from the incoming data. The main characteristics that we use are:

- **Frequency difference:** The distance between the actual transmission frequency and the ideal carrier frequency (1 classifier);
- **Magnitude difference:** The distance between the magnitude of the transmitted symbol and the ideal symbol (4 classifiers);
- **Phase difference:** The angular distance between the transmitted symbol and the ideal symbol in the I/Q domain (4 classifiers);
- **Distance vector:** Vector distance between the transmitted symbol and the ideal symbol (4 classifiers);
- **I/Q origin offset:** Distance between the origin of the ideal I/Q plane and the origin of the transmitted symbol in the I/Q domain (1 classifier).

Figure 3 demonstrates more details about the characteristics. The magnitude difference is the difference between received symbol magnitudes (A_0, A_{90}, A_{180}, A_{270}) and ideal symbol magnitude (1). As we see on the figure, one can have four classifiers based on this entity, one for each quadratic symbol. The phase difference for symbol 0° is the angular difference between the vectors $\overrightarrow{oA_0}$ and $\overrightarrow{o0}$ which can be computed for the four quadratures (four classifiers) as well. The distance vector can also be determined for the four symbols, e.g., it would be $(\overrightarrow{oA_0} - \overrightarrow{o0})$ for the symbol 0°. Lastly, The I/O origin offset is the difference between the cross lines between the orthogonal

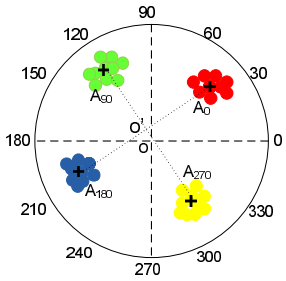


Fig. 3. Example for the quadrature modulated signals.

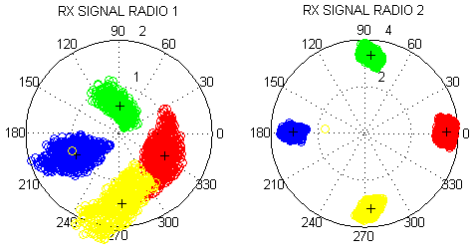


Fig. 5. Received frames from two different transmitters shown on the left and right charts.

frequencies (denoted by O') and the real origin (O). Therefore, counting the variables described above, each of the radios is detected by 14 (weak) classifiers.

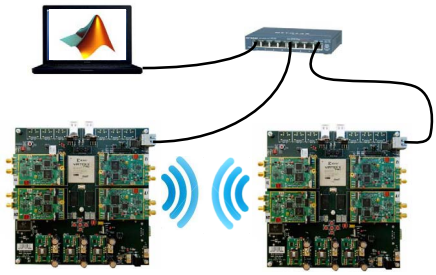


Fig. 4. Experiment setup.

In our implementation, classifier extraction is done by the WARPLab reference design (the WARP PHY layer) [19]. This design unifies MATLAB and WARP for non-real time wireless communication. WARP boards are utilized for real-time wireless communication and data processing is done offline by MATLAB functions. Figure 4 shows the setup for signature generation of a radio card. The transmitter and receiver boards are connected to a PC via an Ethernet switch. Frame generation and data processing parts are done in the MATLAB and real-time communication is performed by the WARP boards. The signature frame is modulated to I/Q domain by MATLAB and transferred to Tx buffer of the WARP board through the Ethernet. Once the data is loaded into the Tx buffer of WARP board, it is transmitted via the radio card. On the receiver side, signal is captured and I/Q values stored inside the Rx buffer. Stored values are transferred to the connected PC through the Ethernet cable for further processing and signature generation in MATLAB.

The main reasons for the deviation of the signal from the ideal signal are manufacturing variability of hardware, the channel between communicating parties and the environmental noise. Effects of channel and noise should be eliminated before signature generation because signature information is based on the hardware variability. Elimination can be done by sending *signature frame* several times and by averaging the received frames. Since channel and noise have random properties, averaging cancels their effect while signifying the effect of hardware variability. Figure 5 shows the averaged signature frame from two different transmitters. It can be seen that the symbols for each transmitter form a distinctively different cluster in the I/Q domain.

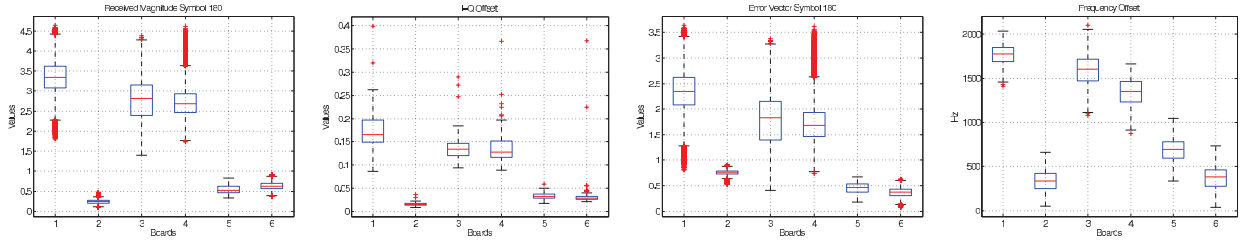
V. Building the Weak and Strong Classifiers

In this Section, we exploit the classifying variables described in Section IV-A to use the gathered data and build a statistical model for each of the 14 classifiers. Before we go into further discussions, we illustrate a few samples of our visual data analysis. The significance of this phase is that no pattern recognition software has been so far able to match the human pattern recognition ability [8]. The visual trends typically provide a sound guideline on how to organize the experiments and the classifier sensitivity.

To demonstrate the obvious differences in the stable radio characteristics, we show the side-by-side comparison of the radio characteristics for the six radios using boxplots. A boxplot is a convenient way of graphically depicting groups of numerical data through their five-number summaries (the smallest observation, lower quartile, median, upper quartile, and the largest observation). A boxplot also indicates which observations, if any, might be considered outliers. It provides a fast method for visual comparison of the density functions and outlier detection. Figure 6(a) shows the boxplots of magnitudes for symbol 180° for the six radios, Figure 6(b) demonstrates the boxplots for the I/Q offset, Figure 6(c) contains the boxplots for the error vector for 180° symbol, and Figure 6(d) shows the frequency offset boxplots. We see visible differences between the statistics of the signals coming from the six radio boards.

A. Data organization and weak classification

For learning the characteristics of different boards (signature extraction), we first transmit 200 frames of 1844 random QPSK symbols from each board. At this point, for every board we have recorded a matrix of 200x1844 values. The recorded matrix is used as the learning data set for extracting the 14 classifiers described in Subsection IV-A. For the frequency offset, we consider the difference between the carrier frequency in the 2.4 GHz band that each board is supposed to use and the carrier frequency that each board has transmitted. For each of the transmitted frames, we separate the symbols versus the quadrature used for modulation of the pertinent symbol. Thus, we get about 461 samples at each quadrature shown in Figure 3. The data is ready to be processed at this point.



(a) Magnitude (180°) (b) I/Q Offset (c) Error vector (180°) (d) frequency offset

Fig. 6. Boxplots over the six radio boards for the (a) Magnitude, (b) I/Q offset, (c) Error vector, and (d) Frequency offset.

For weak classification using a single variable we opt to use the maximum likelihood (ML) method. ML is the procedure of finding the value for a given statistic which maximizes the known likelihood distribution. We use the learning data to form a histogram for each of the 14 classifiers. The histogram approximates the probability density function, assuming that we normalize the number of values in each bin to the total number of elements (assuming equidistance bins). To avoid the adverse impact of the outliers, we use the boxplot function to identify the outliers and then remove the outliers before the histogram formation. Figure 7 shows the normalized histograms of the error distance vector for the symbol 90° for four radios. For each histogram, we used 10 bins. The output of the learning phase is a histogram with 10 probability values corresponding to the 10 bins for each classifying variable at each board, i.e., a 10x2 matrix.

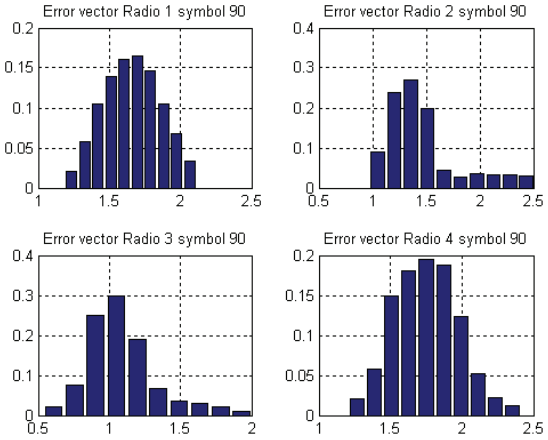


Fig. 7. Normalized histogram of the error vector for the symbol 90° for 4 different radios.

During the signature evaluation phase, we transmit from each board F sample frames. These samples are in effect the test set for our classification model. Using the likelihood functions above, it is easy to find the probability of each signal belonging to a board. For example, for the histograms shown in Figure 7, if the error vector is 2 for the symbol 90°, the probability of this error is 0.065 for R_1, 0.025 for R_2, 0.01 for R_3 and 0.12 for R_4. Naturally, the maximum likelihood principal (probability) leads to guessing R_4 as the potential source of this signal among those four radios. Now, for F frames coming from the same radio, the maximum probability can be found by multiplying the likelihood for each of the F frames coming from a certain radio, i.e.,

$$\max_k \text{ Prob}(F \text{ frames}, R_k) = \max_k \prod_{f=1}^{F} \text{Prob}(frame_f, R_k) \quad (1)$$

We do the evaluation step above and find the histogram that maximizes the probability over all the frames. This histogram belongs to the radio that is the most likely transmitter of the signal for the underlying weak classifier. Since the probabilities are often small numbers, in practice often log-likelihood is used [8]. The benefit of using the logarithm is that it changes the products above to sums. Since logarithm is a monotonic transformation it does not displace the maximum of the function and thus can be used for maximum likelihood without modifications.

B. Combining the classifiers

The last step of our procedure is to combine the several weak classifiers computed in Section V-A to form one stronger committee of the classifiers. To make the committee, our first method is to perform a weighted voting. In weighted voting, we find the probability of detection for each of the classifiers G_m, $m = 1, \ldots, M$. Next, we assign normalized weights α_m to each weak classifier G_m based on its probability of detection that can be learned by using standard statistical validation methods. In such validation methods, the probability of detection can be found during the signature learning phase by setting aside a part of the learn data and then testing the prediction ability of the built signature from the first part of the data on the second part of the data (the set aside part) [8]. The normalization is such that the sub of the weights is 1, i.e., $\Sigma_{m=1}^{M} \alpha_m = 1$.

In our evaluations, we find the non-normalized value of α_m, denoted by α'_m using the following formula for each of our weak classifiers G_m, $m = 1, \ldots, M$:

$$\alpha'_m = \overline{P_D(G_m(.))} - \overline{P_{FA}(G_m(.))} \quad (2)$$

where $\overline{P_D(G_m(.))}$ is the average probability of detection (derived using the statistical validation methods) for the weak classifier G_m over all the radios and $\overline{P_{FA}(G_m(.))}$ is the

average probability of false alarm computed like $\overline{P_D(G_m(.))}$. α_m can be easily found by normalizing the α'_ms.

To form the committee, we also map the classification results from each weak classifier to a value in the set {-1,1}. If the weak classifier G_m identifies the radio R_1 as the transmitter, then $G_m(R_1) = 1$, otherwise, $G_m(R_1) = -1$. Let G_{vote} denote the final voting function for a radio. The following voting function is used for weighting the votes of the different classifiers for one radio R_k:

$$G_{vote}(R_k) = \Sigma_{m=1}^{M} \quad \alpha_m G_m(R_k). \tag{3}$$

The radio with the highest G_{vote} would be selected to be the target radio.

In our experimental results, we compare the performance of this classifier against combining the results of the M classifiers by directly using the maximum likelihood methods. Using similar ML principle as Equation 4, one can write:

$$\max_k \quad \text{Prob}(G_{ML}(.)) = \max_k \quad \prod_{m=1}^{M} \quad \text{Prob}(G_m(R_k)). \tag{4}$$

Again, the radio R_k with the highest G_{ML} probability would be the target radio.

VI. Experimental evaluations

Our first set of results show the probability of detection and probability of false alarm for using a single classifier. In this set of experiments, we only use five frames to identify the radios based on the extracted signatures previously stored during the learning phase.

	R_1	R_2	R_3	R_4	R_5	R_6
I/Q offset	.4	1	0	0	1	1
$\|.\|_0$	0	1	1	.2	0	1
$\|.\|_{90}$	0	0	.4	0	.2	.6
$\|.\|_{180}$	0	0	.4	0	.8	.4
$\|.\|_{270}$	0	1	0	0	0	.2
PD_0	0	0	.4	0	0	0
PD_{90}	1	0	0	0	.8	0
PD_{180}	.6	.6	0	0	0	0
PD_{270}	.2	.8	0	0	0	0
Err_0	0	1	1	.2	1	1
Err_{90}	0	0	.4	0	.4	1
Err_{180}	0	0	0	0	0	1
Err_{270}	0	.2	0	.2	0	.4
frequency	1	.8	.6	.5	1	1

TABLE I

Probability of detection P_D for the weak classifiers.

Table I demonstrates our probability of detection (P_D) results for weak classification. Each column shows the probability of detection for one of our 6 radios. The weak classifiers in rows 2 to 15 are: I/Q offset, magnitude over 0° symbols, magnitude over the 90° symbols, magnitude over 180° symbols, magnitude over 270° symbols, phase difference (PD) over 0°, phase difference over 90°, phase difference over 180°, phase difference over 270°, and finally the frequency offset from the carrier.

	R_1	R_2	R_3	R_4	R_5	R_6
I/Q offset	.2	.2	0	0	0	0
$\|.\|_0$	0	.3	.1	0	0	0
$\|.\|_{90}$	0	.5	.2	0	.2	0
$\|.\|_{180}$	.1	.4	0	0	0	.2
$\|.\|_{270}$	0	.2	.2	0	0	0
PD_0	.3	.5	.3	.4	.3	.2
PD_{90}	.2	.4	.4	.6	.4	.3
PD_{180}	.3	.5	.4	.4	.5	.2
PD_{270}	.4	.4	.6	.4	.2	.1
Err_0	0	.1	.1	.2	.1	.1
Err_{90}	.1	.2	.2	0	0	.2
Err_{180}	.1	.2	0	.2	.2	.1
Err_{270}	0	.3	.2	.1	.1	.3
frequency	0	.2	.3	.1	0	0

TABLE II

Probability of false alarms P_{FA} for the weak classifiers.

We note that the P_D of the weak classifiers in Table I are not very high because: (i) we only use 5 test frames for classification, and (ii) the WARP boards are rather large and stable, and they contain many digital components which makes their variability less than the radios with more analog components. We also experiment with increasing the number of frames, and for more than 25 frames, almost all the weak classifiers can identify the radios with more than 50% probability, making a much better prediction. We opt to draw only 5 frames because our goal is to show that our method can do a reasonable classification, even with the low number of measurements. The results for larger number of measurements are much more stable, but we do not report them here because of space constraints.

Table II demonstrates our probability of false alarm (P_{FA}) results for weak classification. The rows and columns are similar to Table I. The probability of false alarm for the radio R_k is the probability that a signal that does not belong to R_k is falsely identified by the weak classifier to be from R_k. It is interesting to see that the probability of false alarm is mostly low, except for the radio R_2. Since R_2 has the noisiest characteristics, a number of other radios are misclassified as R_2. Also, another trend that is visible on the table is the probability of false alarm for the phase difference over the four symbols that is unreasonably high, indicating the instability of the phase-based classifiers especially with small number of frames. When we increase the number of frames to 25, the probability of false alarm for the phase goes to an average 0.2 and was still much higher than all the other identifiers that are well below 0.1. Both Tables I and II demonstrate that frequency offset is the best single classifier even for the small number of frame measurements. Increasing the measurements to 25 significantly improves the P_D's and also decreases the false alarm probability to below 0.1.

Our last evaluation is for combining the weak classifiers above. Table III demonstrates our results for the 6 radios.

The results are really promising and clearly show the superior performance of the voting-based classifier over the maximum likelihood. The results of the voting-based method

	R_1	R_2	R_3	R_4	R_5	R_6
$G_{vote}(P_D)$	0.92	0.81	0.84	0.90	0.85	0.92
$G_{ML}(P_D)$	0.36	0.44	0.24	0.22	0.37	0.40
$G_{vote}(P_{FA})$	0.12	0.26	0.20	0.07	0.07	0.05
$G_{ML}(P_{FA})$	0.58	0.78	0.73	0.70	0.53	0.54

TABLE III

P_D AND P_{FA} FOR THE COMBINING THE WEAK CLASSIFIERS: VOTING-BASED CLASSIFIERS AND THE MAXIMUM LIKELIHOOD.

certainly benefit from the frequency offset classifier in Tables I and II since the results of this classifier are much better than the other weak classifiers. As a result, this classifier gets a high value for its weight α_m and the prediction results are really good. For combining the probability using ML, we first eliminate the zeros since the large number of zeros in Tables I and II are because of the small number of frames used for classification. Even then, the ML combining method that works by multiplying the probabilities does not perform that well for a few measurements. The ML method is asymptotically optimal, which means that for a large number of test samples it would be able to do a good estimation of the densities and have a high P_D and low P_{FA}. However, for small number of samples the asymptotic optimality of the ML does not mean much and the results are not very good.

VII. CONCLUSION

Identification techniques based on unclonable variations of the radios are emerging. We presented a new radiometric signature extraction and evaluation that is more robust and stable than the existing techniques. Previously available methods in this area have used simple classification such as K-nearest neighbor techniques that are known to be unstable and nonrobust in multiple dimensions because of the curse of dimensionality problems. Our method overcomes this limitation by extracting the signatures over multiple weak classifiers and then by using the committee of classifiers techniques that are well known for their ability to produce robust and stable identifiers. Our weak classification techniques were built by forming the data-driven histograms, estimating the probability density function and the maximum likelihood (ML) method. We employed two methods for making a committee of classifiers: (1) weighted voting, and (2) maximum likelihood. We performed extensive experimentation and evaluation of our approach on the WARP open source radio platform. Our experimental results demonstrated that the voting-based approach performs better than the ML-based approach and it significantly improved the detection probability compared with the weak classification techniques.

VIII. ACKNOWLEDGEMENT

This work is in part supported by the National Science Foundation (NSF) CAREER Award (grant number 0644289) and by the Office of Naval Research (ONR) Young Investigator Program (grant number N000140910831).

REFERENCES

[1] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical One-Way Functions", *Science*, vol. 297, pp. 2026–2030, 2002.
[2] K.J. Ellis and N. Serinken, "Characteristics of radio transmitter fingerprints", *Radio Science*, vol. 36, no. 4, pp. 585–597, 2001.
[3] O. Ureten and N. Serinken, "Wireless security through RF fingerprinting", *Electrical and Computer Engineering, Canadian Journal of*, vol. 32, no. 1, pp. 27–33, 2007.
[4] V. Brik, S.Banerjee, M. Gruteser, and S.Oh, "Wireless device identification with radiometric signatures", in *MobiCom*, 2008, pp. 116–127.
[5] K.I. Talbot, P.R. Duley, and M.H. Hyatt, "Specific emitter identification and verification", in *Technology Review*, 2003.
[6] K.B. Rasmussen and S. Capkun, "Implications of radio fingerprinting on the security of sensor networks", *Security and Privacy in Communications Networks and the Workshops*, pp. 331–340, 2007.
[7] K.A. Remley, C.A. Grosvenor, R.T. Johnk, D.R. Novotny, P.D. Hale, M.D. McKinley, A. Karygiannis, and E. Antonakakis, "Electromagnetic signatures of WLAN cards and network security", *Signal Processing and Information Technology*, pp. 484–488, 2005.
[8] T. Hastie, R. Tibshirani, and J. Friedman, *The Elements of Statistical Learning*, Springer-Verlag, 2001.
[9] L. Breiman, "Arcing classifiers", *Annals of statistics*, , no. 26, pp. 801–849, 1998.
[10] L.E. Langley, "Specific emitter identification (SEI) and classical parameter fusion technology", WESCON, pp. 377–381, 1993.
[11] "http://www.decodesystems.com/mt/97dec/".
[12] N. Patwari and S. K. Kasera, "Robust location distinction using temporal link signatures", in *MobiCom*, 2007, pp. 111–122.
[13] G. Edward Suh and Srinivas Devadas, "Physical unclonable functions for device authentication and secret key generation", in *DAC '07: Proceedings of the 44th annual Design Automation Conference*, 2007, pp. 9–14.
[14] Mehrdad Majzoobi, Farinaz Koushanfar, and Miodrag Potkonjak, "Techniques for design and implementation of secure reconfigurable pufs", *ACM Trans. Reconfigurable Technol. Syst.*, vol. 2, no. 1, pp. 1–33, 2009.
[15] Yousra Alkabani, Farinaz Koushanfar, Negar Kiyavash, and Miodrag Potkonjak, "Trusted integrated circuits: A nondestructive hidden characteristics extraction approach.", 2008, vol. 5284, pp. 102–117.
[16] R. Gerdes, T. Daniels, M. Mina, and S. Russell, "Device identification via analog signal fingerprinting:a matched filter approach", in *NDSS*, 2006.
[17] D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints", in WISE*: Proceedings of ACM workshop on Wireless security*, 2006, pp. 43–52.
[18] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements", in WISE*: Proceedings of* ACM *workshop on Wireless security*, 2006, pp. 33–42.
[19] "Rice University WARP - Wireless Open-Access Research Platform, http://warp.rice.edu/".
[20] P. Murphy, A. Sabharwal, and B. Aazhang, "Design of WARP: A flexible Wireless Open-Access Research Platform", in *Proceedings of EUSIPCO*, 2006.