GenePrint: Generic and Accurate Physical-Layer Identification for UHF RFID Tags

Dan Ma*, Chen Qian†, Wenpu Li*, Jinsong Han*, and Jizhong Zhao*
*School of Electronic and Information Engineering, Xi'an Jiaotong University, China
†Department of Computer Science, University of Kentucky, Lexington, Ky
Email: {xjtumd, atools_cook}@stu.xjtu.edu.cn, qian@cs.uky.edu,
{hanjinsong, zjz}@mail.xjtu.edu.cn

***Abstract*—Physical-layer identification utilizes unique features of wireless devices as their fingerprints, providing authenticity and security guarantee. Prior physical-layer identification techniques on RFID tags require non-generic equipments and are not fully compatible with existing standards. In this paper, we propose a novel physical-layer identification system, GenePrint, for UHF passive tags. The GenePrint prototype system is implemented by a commercial reader, a USRP-based monitor, and off-the-shelf UHF passive tags. Our solution is generic and completely compatible with the existing standard, EPCglobal C1G2 specification. GenePrint leverages the internal similarity among the pulses of tags' RN16 preamble signals to extract a hardware feature as the fingerprint. We conduct extensive experiments on over 10,000 RN16 preamble signals from 150 off-the-shelf RFID tags. The results show that GenePrint achieves a high identification accuracy of 99.68%+. The feature extraction of GenePrint is resilient to various malicious attacks, such as the feature replay attack.**

I. Introduction

Radio Frequency IDentification (RFID) systems have become important platforms to facilitate the automation for various ubiquitous applications. Passive RFID tags provide numerous attractive features, including remote and non-sight-of-line access, low cost, battery-freedom, and high identification efficiency. As the name suggests, the most fundamental and essential function of RFID systems is tag identification. However, the identities (IDs) stored in tags are considered a kind of "naked data". It is hard for readers to verify the authenticity of the tag ID transmitted from a wireless device. In fact, attackers can easily forge a tag with the identical ID of the genuine one for impersonation or counterfeiting. In addition, attackers can also "overhear" the communication between the reader and tags to obtain the application data such as tag IDs.

As the authenticity and privacy of tags are of importance, many efforts have been done in recent years to design secure identification and authentication protocols [1]. They are commonly with a need of changing the current standard or using more powerful tag circuitry, in order to support cryptographic mechanisms. Most of prior solutions suffer from at least one of the following drawbacks. First, it is difficult for those techniques to be adopted by manufacturers because they are not compatible with the current industrial standards, such as the EPCglobal C1G2 specification [2]. Second, cost concern will place a barrier to introducing more powerful circuitry to tags. Third, some data, though has been encrypted, are still exposed to attackers, which leaves a risk of privacy leakage. Designing an identification protocol that achieves compatibility, security, and cost-efficiency is challenging.

978-1-4799-1270-4/13/$31.00 ©2013 IEEE

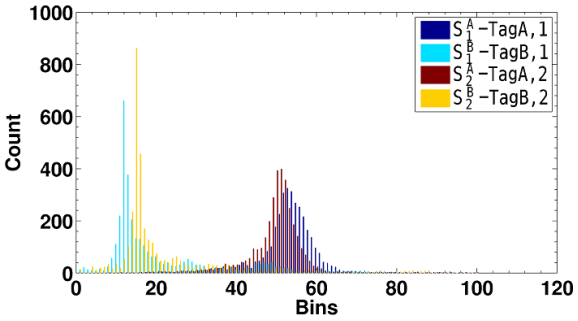

Fig. 1. Distributions of the pulse-inter-covariance-sequence of 4 different RN16 preambles from two Alien 9640 tags. The number of bins is 500 and the first 120 bins are presented in the figure.

Recently, researchers have proposed physical-layer identification for wireless devices. Physical-layer identification solutions leverage the minor variations in analog hardware and obtain the device-related fingerprints by analyzing the communication signals. The main task of physical-layer identification is to find a favorable feature or feature set, which can be used as a unique and stable fingerprint of the target device. It aims at distinguishing different devices by what they are (hardware feature) rather than what they hold (ID), which enables the authentic identification. This technique has been adopted by many wireless device platforms [3]–[6].

Existing physical-layer identification techniques for RFID tags, however, suffer from two main drawbacks. First, these solutions are not generic. They often use purpose-built and costly equipment for supporting a high sampling rate on tag signals in order to make the observed signals resilient to noises. For example, The time interval error (TIE) based approach [6] uses an oscilloscope with a sampling rate up to 1 GS/s as the signal acquisition device. It also employs a purpose-built reader that sends a few of commands out of the standard specification. Second, the feature used by prior solutions may be vulnerable to various attacks. For example, the ∂_{TIE} extracted from the preamble of RN16 can be used as the fingerprint of tags [6]. Attackers can adjust the signals

of their attacking device to simulate the value, and perform a *feature replay attack* [7].

With the motivation of addressing these problems, we propose a new internal similarity based physical-layer identification system, *GenePrint*, for passive tags. Our approach is based on analyzing the internal similarity of the tag communication signal. Our observation is that signals transmitted by the same tag may differ in average power or frequency band with different deployments, but the internal hardware feature is stable. From the RN16 preamble signals of tags, we extract two internal similarity features, namely covariance-based distribution feature (Cov) and power spectrum density (PSD), which can effectively differentiate UHF RFID tags. Moreover, we show that the calculation of Cov-based similarity will not be affected by the environmental noise. Hence the proposed feature extraction methods do not require devices with very high sampling rates. Figure 1 shows some experimental results of the Cov-based feature extraction. S_1^A and S_2^A are the feature vectors from two RN16 preamble signals of tag A. S_1^B and S_2^B are the feature vectors from two RN16 preamble signals of tag B. We can obviously see that the two distributions of A's feature vectors are very similar and can be clearly distinguished from the two distributions of B.

We implemented a GenePrint prototype system using a Universal Software Radio Peripheral (USRP) based programming radio device, a commercial RFID reader, and off-the-shelf tags. GenePrint performs physical-layer identification of RFID UHF passive tags while being fully compatible with current RFID standards and off-the-shelf RFID products. The feature extraction only needs the preamble of the RN16 packet, which does not contain any application data such as the tag ID. In addition, our approach is more resilient to malicious attacks, e.g. feature replaying, by fingerprinting all pulses into a distribution-based feature instead of a single value. We conduct extensive experiments on over 10,000 RN16 preamble signals from 150 off-the-shelf RFID tags. Tags are in three types, namely Impinj E41-C, Impinj H47 and Alien 9640, with chips from two mainstream RFID manufactures. The results show that, only using the Cov feature, 12,000 RN16 preamble signals can be classified to different tags with the accuracy of 78.79%. Jointly utilizing Cov and PSD, the identification accuracy of the same tag population can reach 99.68%+ in a standard environment. The results also demonstrate the stable performance of GenePrint by changing the distance and angle between the antennas of the reader and tags. The major contributions of this work are summarized as follows:

- The GenePrint system is compatible with the current UHF RFID standard specification. It is a generic solution and can be implemented by off-the-shelf RFID readers and tags.
- GenePrint uses a new internal similarity based feature extraction method to identify RFID UHF passive tags through the physical-layer information. The extracted feature can serve as the fingerprint of a tag with high identification accuracy.
- The identification process of GenePrint can effectively protect the user privacy. Besides, the feature extracted by GenePrint is resilient to the feature replay attack, which can enhance the authenticity of RFID identification.

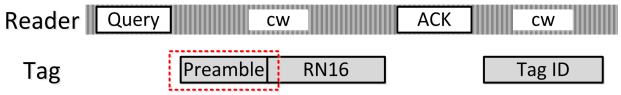

Fig. 2. The communication process between reader and one tag. The signal we use is the preamble of the RN16 which is prior to the ID signal.

II. BACKGROUND

In this section, we briefly overview the backscattering based communication between an RFID reader and tags. We also introduce two essential components of the RFID backscattering, RN16 and Miller-modulated subcarrier.

A. Basic Signaling Interface

Existing UHF RFID systems commonly follow the EPCglobal C1G2 air protocol specification [2], which is regarded as the state-of-art communication standard for connecting passive UHF tags and readers. As described in this specification, the signaling interface can be viewed as the physical-layer in the communication between a reader and tags, which defines all parameters required for RF communications.

Figure 2 shows a successful read process between the reader and tag. According to the specification in [2], an inventory round begins with a *Query* command from the reader that includes a slot-count value Q and other parameters for tag modulation, e.g. Backscatter Link Frequency (BLF). Each tag receiving *Query* will pick a random value in the range of $[0, 2^Q - 1]$ and preload the value as its slot counter. The inventory frame can be divided into 2^Q slots and two neighbouring slots are separated by the reader command *QueryRep* or *QueryAdjust*. Upon each *QueryRep* command, a tag will decrement its slot counter. When the slot counter reaches 0, the tag will reply an RN16 packet, containing a 16-bit random or pseudo-random number. Assuming that in a given slot there is only a single tag replying to the reader, the reader will send an *ACK* command containing the same RN16 numbers as an acknowledgement to the tag. The acknowledged tag will then reply its ID to the reader.

B. Data-independent physical-layer information

One of the objectives of our approach is to seek a feature that more explicitly reflects the exact physical-layer information correlated to the tag. We choose the preamble of the RN16 packet. Like most wireless communication mechanisms, EPCglobal C1G2 also specifies a preamble before RN16. The formats of preambles differ on their encoding methods. We show a preamble signal captured by our USRP device in Figure 3. This preamble is composed of 64 square wave pulses, which are usually called Pilot Tone, followed by a bit sequence "010111". In order to minimize the impact of the logic data as much as possible, we only use **the 64 pulses** as the source of each tag's physical-layer information.

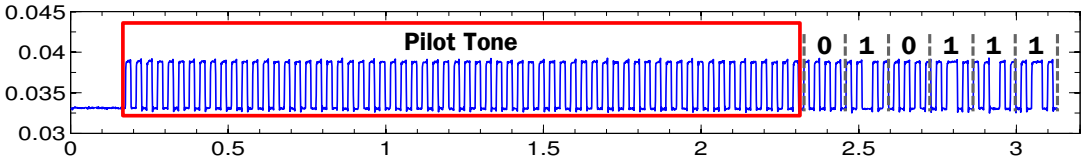

Fig. 3. The T⇒R link preamble form under Miller-modulated subcarrier 4.

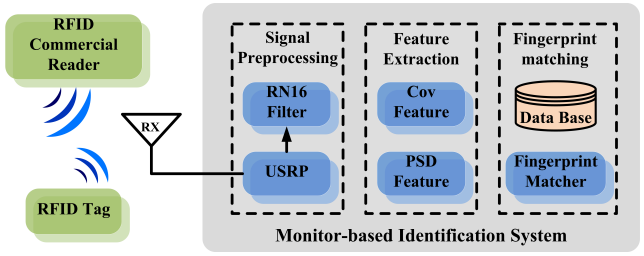

Fig. 4. The monitor-based system collects the response signals from tags under the reader's interrogation. The system consists of 3 components: signal preprocessing, feature extraction and fingerprint matching.

C. Representation of tags' physical-layer information

Following EPCglobal C1G2 [2], tags shall encode their preambles as one of the FM0 baseband, Miller-2, 4, or 8 modulated subcarriers. Indeed, all of them are variations of frequency-shift keying (FSK) [8] modulation. It is obviously that the FSK modulated signals can be decoded by counting the number of changes of signal state. For example, the FM0 symbol "0" contains a state change from HIGH output to LOW output in the middle of the signal, while "1" does not. In this paper, we use **pulse** to denote such changes. **The physical-layer features (fingerprint) of a tag can be extracted from the RN16 preamble signal**. We propose to leverage the similarity among the pulses of a tag's preamble signal to formulate this a unique and stable feature, presented in Section III.

In our system, we choose the preamble under the Miller-4 modulation. Our system can also use other modulation methods that have different numbers of pulses, such as FM0 and Miller-2. However there is a trade-off: modulation methods with less numbers of pulses provide higher data transmission rate but less accurate representation of physical-layer information.

III. System Design

A. System Overview

In this section, we present the design of our physical-layer identification protocol and monitor-based identification system. The GenePrint system architecture is shown in Figure 4.

The protocol is performed as follows. The commercial RFID reader queries a tag within its view field by sending a "Query" command, as specified in [2]. Upon receiving the command, the tag replies a response with an RN16 packet. A monitor based identification system then processes the collected signals for identification. Suppose the fingerprints of all valid tags are stored in a local database. If the hardware feature extracted from the signals has a matched record corresponding to a valid tag, the system successfully identifies this tag.

The monitor based identification system consists of 3 components: 1) Signal Preprocessing, which is for seperating the RN16 packets from raw signals, 2) Feature Extraction, which analyses the RN16 packet to yield a unique fingerprint, and 3) Fingerprint Matching module, which accomplishes matching the fingerprint with the one of a valid tag and notifies the upper-layer application to accept/reject the candidate tag. Initially, the features of all tags are extracted and stored in a database. The extraction can be performed by using data mining methods, e.g., the KStar [9] algorithm. As shown in Figure 4, this monitor-based system can be seamlessly adopted in any existing commercial UHF RFID system. It does not disturb normal communications between the off-the-shelf reader and tag. Instead, it only passively listens to the communication and records signals for extracting the hardware features of tags.

In our system, the hardware of the monitor is a Universal Software Radio Peripheral (USRP) N210 [10]. The software is partially derived from a Gen2 RFID project developed by Buettner and Wetherall [11]–[13]. We use a SBX daughterboard [10] whose frequency coverage is $400MHz - 4GHz$. Optimally, the USRP connects to a host machine which can sustain up to $50MS/s$ sampling rate over the GigE interface. Unfortunately, as explained by Buettner [12], the current GNURadio [14] may lose a large amount of data if processing in such a high sampling rate. By using this generic hardware, we are only allowed to use a sampling rate of 10MS/s, two-magnitude lower to that of the purpose-built readers of previous physical-layer solutions such as [6]. It is a great challenge for extracting the hardware feature from tags' weak signals with the impact of strong and complex environmental signals. Our internal similarity based solution successfully extracts the signal feature using the generic and low-cost hardware with higher accuracy.

B. Signal PreProcessing

The raw signal received by USRP includes the carrier wave, the reader commands and the tag responses. For achieving data-independent feature extraction, we should separate RN16 from the raw signal. Since the frequency of the tag response is higher than that of the reader commands, the conventional technique is to implement a high-pass filter followed by an inverse Fourier transform. However, the high-pass filter will

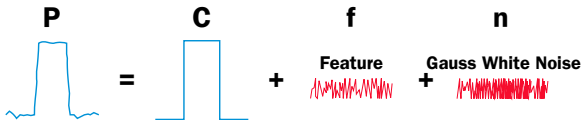

Fig. 5. The pulse can be viewed as the sum of a standard square wave pulse, signals representing the hardware feature, and a random gauss white noise.

attenuate the power of the frequency, leading to unavoidable signal distortion.

In order to solve this problem, we propose an RN16 Filter component, which can work with different signal powers and frequency channels. In this solution, we use a sliding window to traverse through the whole signal. Then the fast Fourier transform is applied to confirm whether the signal's energy in this window is focused on a certain range of frequency. The width of the sliding window is crucial to the filter's accuracy and efficiency. In our implementation, we set the window width approximately equal to the two-third of the length of RN16. This setting can guarantee that for each RN16, the monitor will get at least one valid candidate RN16 window signal. The adjacent windows are grouped to form a long continuous signal. For obtaining real RN16 signals, GenePrint needs to perform a fined-grained pattern recognition scheme on all candidate signals. A much smaller window is used to find the transient between the carrier wave (CW) and the tag response, thus a real RN16 signal can be separated.

In this component, we only process RN16 signals that are valid, which means each of them is transmitted by only one tag and no collision happens. In addition, a commercial reader may not be able to decode a valid RN16 successfully in a *Query* round due to the low Received Signal Strength (RSS) of the signal backscattered from a tag. The reader then fail to identify the tag. However, in our protocol, the monitor record all RN16 signals in a sequential order, which indicates that even if observed RN16 signals cannot be decoded by a commercial reader, they can still be regarded as valid samples and then the corresponding tag can be identified.

C. Feature Extraction

In this subsection, we detail the extraction procedure for two different features: the covariance-based pulse inter feature (Cov) and the power spectrum density based signal inner feature (PSD).

1) Cov-based Pulse Inter Feature: We develop a theoretical model to show that the similarity among the pulses of the preamble signal can effectively reflect the hardware feature of a tag.

For the given tag, let P_i and P_j be signal vectors of the ith and the jth pulses at the given observed RN16's preamble signal. P_i can be considered as the sum of 1) a constant vector of the standard square wave pulse C, 2) a value representing the tag's inherent hardware feature f_i, and 3) a series of random gauss white noise n_i, as shown in Figure 5. We have:

$$P_i = C + f_i + n_i \tag{1}$$
$$P_j = C + f_j + n_j \tag{2}$$

By exploiting the internal similarity of the given signal, we show that the covariance of P_i and P_j can be used to represent the tag's hardware feature.

STEP 1: Noise Cancellation

Theorem 1: Let $A_i = P_i - n_i$, $A_j = P_j - n_j$, and Cov be the covariance operator. Then

$$Cov(P_i, P_j) = Cov(A_i, A_j) \tag{3}$$

Proof: Let E be the expected value operator. The covariance of P_i and P_j is given by:

$$\begin{aligned} &Cov(P_i, P_j) \\ &= Cov(A_i + n_i, A_j + n_j) \\ &= E((A_i + n_i)(A_j + n_j)) - \\ &\quad E(A_i + n_i)E(A_j + n_j) \end{aligned} \tag{4}$$

According to the linearity property of mathematical expectation, Equation 4 has the form:

$$\begin{aligned} &Cov(P_i, P_j) \\ &= E(A_iA_j + A_jn_i + A_in_j + n_in_j) - \\ &\quad E(A_i)E(A_j) - E(A_i)E(n_j) - \\ &\quad E(A_j)E(n_i) - E(n_i)E(n_j) \\ &= E(A_iA_j) + E(A_jn_i) + E(A_in_j) + \\ &\quad E(n_in_j) - E(A_i)E(A_j) - E(A_i)E(n_j) - \\ &\quad E(A_j)E(n_i) - E(n_i)E(n_j) \end{aligned} \tag{5}$$

Note that two noise signal vectors n_i and n_j are independent. A_i and n_j, A_j and n_i are also independent. For independent X and Y, $E(XY) = E(X)E(Y)$. From Equation 5 we have:

$$\begin{aligned} &Cov(P_i, P_j) \\ &= E(A_iA_j) - E(A_i)E(A_j) \\ &= Cov(A_i, A_j) \end{aligned} \tag{6}$$

■

STEP 2: Feature Extraction

Theorem 2: Let P_i^h and P_j^h be the high state parts of P_i and P_j, and f_i^h and f_j^h be the corresponding signal vectors of hardware features, respectively. We have

$$Cov(P_i^h, P_j^h) = Cov(f_i^h, f_j^h) \tag{7}$$

Proof: $A_i = P_i - n_i = C + f_i$ and $A_j = P_j - n_j = C + f_j$. From Equation 6 we have:

$$\begin{aligned} &Cov(P_i, P_j) \\ &= Cov(C + f_i, C + f_j) \\ &= E((C + f_i)(C + f_j)) - \\ &\quad E(C + f_i)E(C + f_j) \end{aligned} \tag{8}$$

Since C is independent of f_i and f_j, we now have:

$$\begin{aligned} &Cov(P_i, P_j) \\ &=E(C^2) + E(Cf_i) + E(Cf_j) + \\ &\quad E(f_i f_j) - E(C)E(C) - E(C)E(f_j) - \\ &\quad E(C)E(f_i) - E(f_i)E(f_j) \\ &=E(C^2) + E(f_i f_j) - E^2(C) - E(f_i)E(f_j) \end{aligned} \tag{9}$$

Note that C is a constant vector, hence $E((C^h)^2) = E^2(C^h)$, where C^h is the high state part of C.

Apply P_i^h and P_j^h into Equation 9:

$$\begin{aligned} &Cov(P_i^h, P_j^h) \\ &=E(f_i^h f_j^h) - E(f_i^h)E(f_j^h) \\ &=Cov(f_i^h, f_j^h) \end{aligned} \tag{10}$$

■

Theorems 1 and 2 show that the calculation of Cov-based similarity will not be affected by the environmental noise.

STEP 3: Signal Feature Establishment

Equation 10 indicates that if we calculate the covariance of two arbitrary pulses' high state parts, we finally get the covariance of the corresponding hardware features. Extending this method to all the 64 pulses' high states and low states, then for one single signal we have two vectors:

$$\begin{aligned} &S^h = [Cov(f_1^h, f_2^h), .., Cov(f_i^h, f_j^h), .., Cov(f_{63}^h, f_{64}^h)] \\ &\text{for integers } i, j \in [1, 64], i < j \end{aligned} \tag{11}$$

$$\begin{aligned} &S^l = [Cov(f_1^l, f_2^l), .., Cov(f_i^l, f_j^l), .., Cov(f_{63}^l, f_{64}^l)] \\ &\text{for integers } i, j \in [1, 64], i < j \end{aligned} \tag{12}$$

Note that each of S^h and S^l has $C(64, 2) = 2016$ elements. Combining Equation 11 and Equation 12, the signal feature can be extracted as a covariance sequence in a length of $2 \times C(64, 2)$:

$$S = [S^h, S^l] \tag{13}$$

For the signal of each tag, we can construct a vector in the form of Equation 13.

Although the elements in a vector S are only correlated with the hardware inherent features, the hardware inherent feature reflected in a specific pulse is uncertain. This means the value of one particular element of the vector S is unpredictable. Nevertheless, as the vector S can present the characteristic of the tag's hardware, it should follow a certain probabilistic distribution.

In order to verify this idea, we use an equi-width histogram to estimate the distribution of S. We first choose two different Alien 9640 tags A and B, and randomly pick two RN16 preamble signals for each tag. Performing the above process of feature extraction, we obtain 4 covariance sequences: S_1^A and S_2^A for Tag A, and S_1^B and S_2^B for Tag B. Each of them is a vector containing $2 \times C(64, 2) = 4032$ elements. For each vector, all elements are sorted into 500 equally spaced bins between the minimum and maximum value of it. The bins are displayed as rectangles such that the height of each rectangle indicates the number of elements in the bin. Figure 1 shows the results of the first 120 bins. As shown in Figure 1, the two distributions from Tag A are very similar and they can be clearly distinguished from the two distributions from Tag B.

In our system, for each RN16 preamble, we use the distribution of the Cov-based feature as the main hardware fingerprint of tags. Experiment results shown in Section IV demonstrated that using this feature can achieve an identification accuracy of 77.88%, 79.42% and 79.06% for 3 different tag models Impinj E41-C, Impinj H47, and Alien 9640, repectively.

2) PSD-based Signal Inner Feature: In this section, we propose another similarity-based feature extraction mechanism by using power spectrum density (PSD). Different from the Cov-based pulse inter feature which takes pulses as basic elements, this approach focuses on the whole signal (64 consecutive pulses) and extracts the inner similarity of the signal in the frequency domain.

First, we consider the preamble signal as a random process. For mathematically describing this random process, a probability density function (PDF) is usually used. However, the PDF is not a complete description. For instance, at two arbitrary points in the time domain, we have samples $X_1 = X(t_1)$ and $X_2 = X(t_2)$. The PDF function $f_X(x = t)$ only describes X_1 and X_2, but cannot infer the relationship between them. In order to characterize such a relationship, the *autocorrelation function* can be utilized as follows.

Defining τ as a time difference variable, the autocorrelation function can be expressed as [15]:

$$R_{XX}(t, t + \tau) = E(X(t)X(t + \tau)) \tag{14}$$

This function can draw out the correlation between two samples depending on the distance they are spaced. Using this metric in the frequency domain, we obtain the power spectrum density function according to the Wiener-Khintchine-Einstein Theorem [15]:

Theorem 3 (Wiener-Khintchine-Einstein Theorem): For a wide sense stationary random process $X(t)$ whose *autocorrelation function* is given by $R_{XX}(\tau)$, the PSD of the process is

$$S_{XX}(f) = \int_{-\infty}^{+\infty} R_{XX}(\tau) e^{-j2\pi f \tau} d\tau \tag{15}$$

Like the autocorrelation function in the time domain, PSD is a deterministic representation of the spectral characteristics of a random process. This can also be proved in many other domains. For example, the authors in [16] utilized the power spectrum feature to classify images.

In out system, PSD is used as the secondary feature for identification. According to the experimental results, combining with the Cov-based feature the identification accuracy of GenePrint is over 99.68%.

D. Fingerprint Matching

Like all other physical-layer identification solutions, the system should obtain the reference fingerprint database for tags based on the extracted features. In our prototype system, we collect RN16 preamble signals from all 150 tags that

will be identified. For the captured signals, the proposed feature extraction methods are employed to generate the tag features. GenePrint then employs a KStar learning tool to produce a single reference fingerprint from each tag's features extracted. Each tag will have a reference fingerprint recorded together with its ID in the database. In order to improve the identification accuracy, multiple feature fingerprints are jointed applied to generate a reference fingerprint. In practical RFID systems, the database can be established using the above methods by manufacturers when producing tags, or by the system administer before deploying the tags.

For identifying a given tag, the monitor captures the RN16 preamble of the tag, generate its fingerprint via proposed feature extraction methods, and compute a matching score for every entry in the database. The higher the matching score is, the more similar two fingerprints are. The score is computed using the distance computation mechanism in the learning tool. In GenePrint, we use the entropy based distance computation. An entry that is scored higher than a threshold is considered as a valid entry. We will discuss how to set the threshold in Section IV.

If there is a single valid entry, the system just reports an "accept" and the tag ID in the entry. If there are multiple valid entries for a tag in the database, there are two possible strategies for GenePrint: 1) reporting an "accept" and the tag ID in the highest scored entry, or 2) continuing to capture multiple RN16 signals from the candidate tag and taking the average of scores from multiple fingerprints. If there are still multiple entries, the system reports an "accept" and the tag ID in the highest scored entry. In our performance evaluation, we choose the strategy 2 and take at most 3 RN16 signals for identifying a given tag, as described in Section IV-C. If there is no valid entry, a "reject" will be reported.

IV. Experiments and Evaluation

In this section, we present the implementation and the performance evaluation of the GenePrint system. We describe the experiment setup in Section IV-A and the accuracy metrics used to evaluate classification and identification in Section IV-B. The experiment results will be presented and analyzed in Section IV-B.

A. Experiment Setup

We implement and evaluate our system in an indoor environment with the existence of RF noises including Wifi, AM/FM, and Bluetooth signals. The testbed consists of a commercial RFID system with an Impinj R220 reader and 150 off-the-shelf RFID UHF passive tags from 3 different models. For the low-cost and generic monitor, we use a USRP N210 plus a SBX daughterboard which has been introduced in Section III. Antennas used by both the reader and the monitor are circularly polarized with a gain of $8dBi$ (Laird S9028PCL). Figure 6 shows the testbed.

To show the GenePrint system is universally applicable, we test tags in different design models. The 150 tags for evaluation are in 3 different models from 2 manufactures. They are Impinj E41-C, Impinj H47 and Alien 9640. To better evaluate the system's accuracy and stability, we purposely use those tags with different designs as shown in Table I.

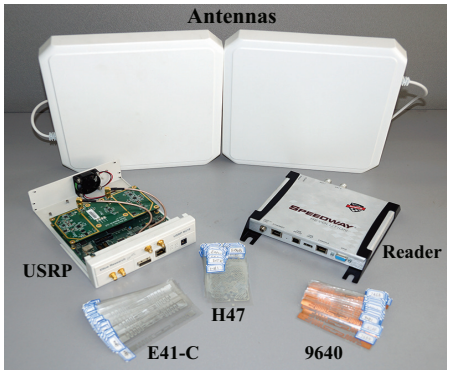

Fig. 6. Experiment equipments

TABLE I
TAG MODELS INVOLVED IN THE EXPERIMENT

Tag Model	E41-C	H47	9640
Chip Manufacture	Impinj	Impinj	Alien
Antenna Num.	1	2	1

We conducted three main sets of experiments to evaluate the performance of our system. For each set of experiments, different models of tags are used and 80 RN16 preambles are collected for each tag. The first set of experiments aims to evaluate the classification and identification accuracy of the GenePrint system. In the second set of experiments, we vary the distance between the reader and tags from 30cm to 1m. This leads to a variation of the averaged baseband power of the signals, which introduces a negative impact due to the environment noise increase. In the last set of experiments, we perform an antenna-orientation-aware experiment to further study the stability of identification.

B. Metrics and methodology

We evaluate the performance of both classification and identification. For classification, we test whether features extracted from different RN16 preamble signals of one tag can be classified to the same feature class. For identification, we use reference features in the database to identify each tag.

1) Classification: We employ a *Correctly Classified Rate* (CCR) to evaluate the classification capability of extracted features. Each individual tag is viewed as one class. For each tag, we use its 80 signals as the classifier instances. The CCR is measured by the result of the classifier, which is the average percentage of correctly classified instances using the cross-validation mechanism. The classifier we use is an instance-based classifier, KStar algorithm, based on the entropic distance measurement.

2) Identification: For evaluating the identification performance, we implement a threshold-based identification system and calculate the *Equal Error Rate* (EER) as our performance

metric. The system is built as follows. Assuming after the training process, we have already obtained the reference fingerprint of each tag. For each candidate fingerprint to be identified, we first measure its matching scores to all reference fingerprints stored in database. Here, the higher the matching score is, the more similar the two fingerprints are. We define two metrics, *False Accept Rate* (FAR) and *False Reject Rate* (FRR). For a given threshold, FAR is the percentage of scores higher than the threshold but locate tags to wrong reference entries, and FRR is the percentage of scores correspond to the same tag but lower than the threshold. We select a fixed value as the threshold with which FRR is equal to FAR. The error rate at this threshold value is the *Equal Error Rate* (EER).

To improve the identification accuracy and address the problem of multiple entries, we detail the strategy 2 mentioned in Section III-D by a method called sample-combination, in which multiple sampled RN16 signals from a candidate tag are used to generate a single reference fingerprint. For each reference fingerprint, N matching scores can be calculated. We take the average of them as the combined score of this tag. This solution needs capture multiple RN16 preamble signals from the given tag. In our protocol, this is feasible because in one second, a commercial reader can successfully recognize one single tag 100+ times such that our monitor can easily record multiple preamble signals. Finally, we locate an entry with the highest similarity, if there are still multiple entries in the database.

C. Experiment Results

1) Recognition Results: In this section, we discuss the accuracy of our system for classification and identification. We used $12,000$ RN16 preambles (80 signals$\times$ 150 tags) as our data set. A 5-fold cross validation is used to calculate the error rate. In each fold, 60 signals are used as the training set and the rest 20 signals are used to evaluate the testing accuracy for each tag.

Note that as explained in Section III-C1, in order to build the Cov-based feature, we use a histogram method to estimate the distribution of the covariances vector. To our knowledge, there is no feasible approach to estimate the optimal number of bins, denoted as (M), which is used for containing covariances values of pulses, if the shape of the distribution is unknown. However, different settings on the number of bins can reveal different features of the data. In order to best estimate the distribution of the pulse-inter covariances vector, we evaluate the feature classification accuracy with different numbers of bins. Figure 7 shows the experiment results of 150 tags. We collect 80 RN16 preambles from each tag in this experiment. We perform 13 groups of experiments with the number of bins varying from 10 to 200, and evaluate the accuracy with the metric *Correctly Classified Rate* (CCR). As shown in Figure 7, in general the identification accuracy is stable even if M varies significantly. If M is too small, i.e., less than 10, the classification accuracy becomes relatively low. This is because the feature is not fine-grained enough to represent sufficient difference between the tag and other tags. On the other hand,

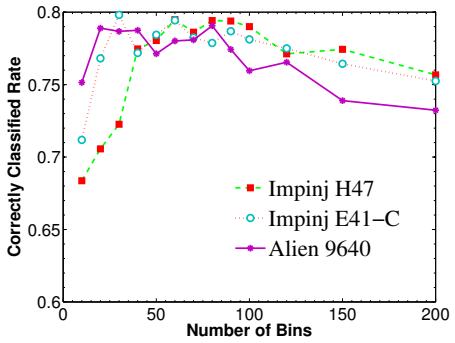

Fig. 7. Classification accuracy of Cov distribution feature for different setting of the number of bins. This classification is performed on 150 RFID UHF tags (80 samples for each tag) and the classifier is a 5-fold KStar.

TABLE II
CLASSIFICATION ACCURACY

Tag Model	E41-C	H47	9640	9540 [6]
# tags	50	50	50	50
# of signals	1	1	1	5
accuracy	77.88	79.42	79.06	71.4

under a large number of bins, for instance 150 or 200, the feature may be sparsely distributed to many bins. Therefore, there might be some bins containing no covariances, resulting in a decrease of classification accuracy. We recommend to set M ranging from 50 to 100, where the system can yield highly-correct classification rate in average. In the following experiments, we set M as 80.

Table II shows the system classification accuracy on a population of 150 tags. In our evaluation, we focused on classifying RFID tags with the same model, which is a very challenging task. It is obvious that classifying tags with different models will be much easier, because their hardware models are fundamentally different. Table II shows the results for every of the three models. We also compare our experiment results with the work in [6]. We use the classification accuracy claimed in [6] directly as the benchmark. This is because we are limited by the lack of hardware. The sampling rate of our USRP is only 10MS/s while that of their purpose-built oscilloscope can be as high as 100MS/s $\sim$ 1GS/s. Note that, in [6], 5 signals are required to compose a single fingerprint. However, for the evaluation of classification, we treat each signal received as a valid sample and the feature extracted as an individual fingerprint for the classifier. As a result, our solution is much more efficient. As shown in the Table II, the three models of tags have an average accuracy of 78.79%, which is higher than that of the work in [6].

We implement the threshold-based identification mechanism described in Section IV-B. In this experiment, we establish the fingerprints for 150 tags by using the combination of the Cov-feature and PSD-feature. The matching score in this system is measured as the distance defined in the KStar algorithm, which is the complexity of transforming one instance into another. To

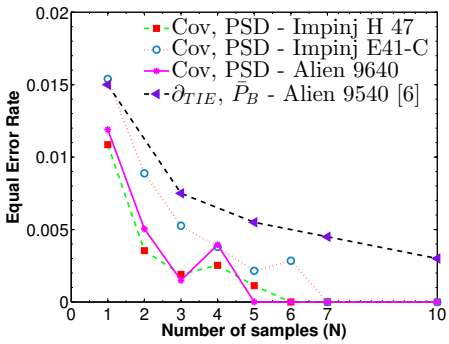

Fig. 8. Identification accuracy of the feature set (Cov, PSD) for different number of samples.(The accuracy of feature $(\partial_{TIE}, \bar{P}_B)$) is from [6].

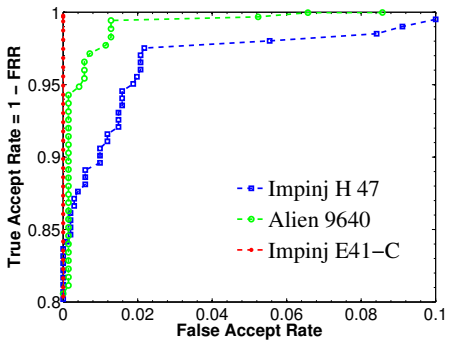

Fig. 10. True accept rate under small settings of FAR

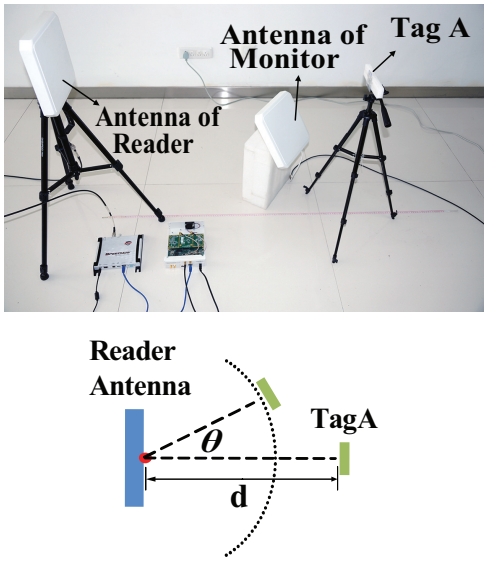

Fig. 9. Experimental deployment

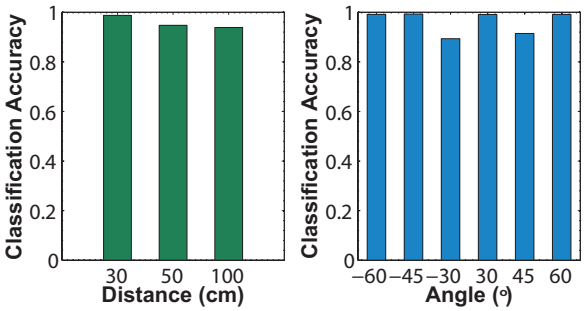

Fig. 11. Feature extraction stability by varying the distance and angle.

improve the identification accuracy, the sample-combination method is adopted. Let N be the number of samples acquired to produce one fingerprint. Figure 8 indicates the experiment results when $N = 1, 2, 3, 4, 5, 6, 7, 10$. We compare our results with the identification accuracy of the $(\partial_{TIE}, \bar{P}_B)$ feature based method presented in [6]. Note we mainly focus on the Alien 9640 tags for the comparison, as the work in [6] mainly test Alien 9549 tags. As shown in the Figure 8, our GenePrint system achieves a very high accuracy ($> 99\%$) as long as the number of samples is greater than 1, which is better than that of the $(\partial_{TIE}, \bar{P}_B)$ feature based approach. Specifically, in our case, when $N = 3$, the identification accuracy is 99.68% and when $N \geq 5$, our system can achieve an accuracy of 100%. In practice, the setting of N is determined based on the accuracy requirement of real applications. We set the default value of N as 3 in the rest experiments.

2) Feature extraction stability: In this section, we analyze the stability of the extracted feature set. We vary the distance and the angle between the reader's antenna and the tags, as illustrated in Figure 9. The d is defined as the distance between the centroid of reader antenna and the tag. We conduct 3 different experiments with $d = 30cm$, $d = 50cm$, $d = 1m$. The distances used in the experiment is relatively short compared to those in [6]. This is mainly because USRP has a much lower sampling rate than that of the purpose-built reader in [6]. In the experiment with changed orientations, we vary the value of θ: $\pm 30°$, $\pm 45°$ and $\pm 60°$. We use 12 different tags (4 tags for each model) for both of the distance and orientation experiments. For each different position, 80 RN16 preambles are collected for each tag. That means the distance and the orientation experiments have used $2880+5760 = 8640$ (distance: $2880 = 12 \times 80 \times 3$; orientation: $5760 = 12 \times 80 \times 6$) signals altogether. We used the KStar classifier with 5-fold cross-validation to evaluate the classified accuracy. We first show the True Accept Rate (TAR), defined as the percentage of the tags that are correctly identified/classified, with various values of FAR. The results shown in Figure 10 reflect that GenePrint can achieve very high TAR even if the FAR is very small. Figure 11 demonstrates that the classification accuracy is higher than 93% under different distance values. We note that the classification accuracy will slightly decrease if enlarging the distance. On the other hand, the impact of changing the angle is negligible, given an angle variation $\pm 60°$. These results indicates that the identification accuracy of GenePrint is resilient to the spatial deployment changes.

V. Security Analysis

The ultimate goal of attacks to an identification mechanism is to successfully impersonate a victim. Attackers may forge or replay a tag's signals to impersonate the tag. As discussed in [7], there are two major attacks potentially threat the physical-layer identification, feature replay based and signal replay based impersonations.

Impersonation by Feature Replay. This attack attempts to partially or fully simulate the features of genuine tag for impersonation. We assume the attacker knows the types of features used by the tags, as well as the identification mechanisms, including the feature extraction, classification, and matching methods. But he does not know the exact value of the features. To our knowledge, the major features used for physical-layer identification are extracted from distinctive signal properties, such as the Frame frequency offset, Frame SYNC correlation, Frame I/Q origin offset, Frame magnitude error, Frame phase error [3], Time Interval Error (TIE), and Average Baseband Power [6]. Some earlier works use signal transients in the waveform domain [6]. If the feature extracted is related to a value, for example TIE, the attacker can adjust the signals of attacking device to approach the value, and hence simulate the feature. The adjustment is usually achieved by linearly tuning the analog circuit of attacking devices, or digitally shrink or expand the ideal constellation symbols' position in the I/Q plane [7]. Such an attack is more easily to be conducted if using programming radio devices, e.g. USRP.

GenePrint is very robust against the feature replay attack. It utilizes the internal similarity of pulses as the physical-layer feature, which involves all preamble signals in the feature extraction. To impersonate a targeted tag, the attacker should generate the signals with the same feature using his own devices. This impersonation requires the attacker repeatedly generating different 64 preamble pulses until one try can be accepted to a valid entry, which is extremely time/resource-consuming. Even if we assume that the attacker knows the exact values of features, i.e., the distribution of covariances of pulses, GenePrint is still hard to be broken. Note that with such an assumption, most other physical-layer identification approaches are easily to be broken because the feature can be directly generated. To break GenePrint, the attacker have to perform brute-force search by the following steps for impersonating a victim tag. **a)** generating 64 preamble pulses, **b)** calculating the covariance for each pair of pulses, **c)** obtaining the distribution of these covariances, and **d)** verifying whether this result matches the known feature of targeted tag. Even though the attacker may shrink the scope of pulse generation to improve the attacking efficiency, each try of feature generation is non-trivial. In short, the overhead of feature replay based attack to GenePrint is impractical.

Impersonation by Signal Replay. The attacker can record signals from a targeted tag, and later retransmit an identical signal to the reader for impersonation. The reader cannot distinguish the retransmitted signals from the genuine ones, if the attacker can successfully make them identical. To our knowledge, no existing work can effectively defend against such an attack, including our work. Nevertheless, performing such an attack usually require very sophisticated and costly equipments, such as the oscilloscope and signal generator, etc. The oscilloscope in [6] has a 100MS/s - 1GS/s sampling rate for data collection. Recording/forging signals may require equipments whose sampling rates are higher than those values. Low-cost equipments used to record RF signals like USRP can only reach a maximum 100MS/s sampling rate. The bandwidth of the Ethernet cable between the USRP and PC is even lower, only 50MS/s. All these facts make the signal replay based impersonation extremely difficult, if not impossible, in practice.

VI. Related Work

Physical-layer identification mechanism has been proposed in variant platforms [3], [17]. The feasibility of these approaches is the fact that hardware imperfections in the transmitter circuitry are introduced during the manufacturing process. Such imperfections are transmitter-specific and affect the communication signal, which makes the device fingerprint measurable. Some systems were implemented to distinguish HF tags [18], and some others focus on UHF tags, such as [6] and [19]. The authors in [19] proposed a Minimum Power Response feature extraction method to distinguish different tags. To the best of our knowledge, [19] is the first work on feature extraction of RFID UHF tags.

For other purposes, Zheng and Li [20] proposed to identify missing tags by using the aggregated physical signals from concurrent tag responses. Wu et al. [21] designed an indoor localization system by exploiting radio signatures without site survey. C. Hekimian-Williams et al. [22] proposed an RFID tag based localization method by using phase difference. Although these works are not for physical-layer identification, they are based on the analysis of physical feature to some extent.

For RFID tags, throughput optimization and cardinality estimation are also important topics. Instead of using traditional anti-collision methods [23], some works took the collision responses from tags as useful information. In the work proposed by Wang et al. [24], collisions were regarded as transmitted code and the decoding was proceeded with the compressive sensing algorithm. Blink [25] exploited characteristics of backscatter link layer and achieved the mobility detection and rate adaptation designs. On the other hand, efforts on the cardinality estimation, such as [26]–[29], focus on designing fast and accurate estimators by counting the numbers of slots in different types.

In the literature of RFID-oriented privacy-preserving, researchers focus on the security of IDs as well as the search efficiency of an optional key. In [30], the authors proposed a Hash-Lock based authentication protocol with high security performance. However, its search complexity is $O(N)$ due to the key's linear structure, which made the system suffer from low efficiency on key search. Later, researchers attempted to develop the security-related applications. Halevi er al. [31] proposed a novel posture sensing approach based on wisp tags

to defend the unauthorized reading and replay attack. Other approaches studied the design of anti-counterfeiting protocols by using efficient batch authentication techniques [1], [32].

VII. Conclusion

In this paper, we propose a physical-layer identification system, GenePrint, for UHF passive tags. Being fully compatible with existing industrial standard EPCglobal C1G2, GenePrint can be implemented by a commercial reader, a USRP-based monitor, and off-the-shelf UHF passive tags. Therefore it is a generic solution. We propose a novel internal similarity based feature extraction method and theoretically prove its feasibility. The accuracy of GenePrint to identify passive tags can be higher than 99.68%. In addition, GenePrint can effectively defend against the severe feature replay attack. We conduct extensive experiments on over 10,000 RN16 preamble signals from 150 off-the-shelf RFID tags. The results demonstrate GenePrint identification is highly accurate and stable.

Acknowledgment

This work is partially supported by the NSFC Project under Grant No. 61033015 and 61373175, the 973 Program of China under Grant No. 2011CB302705, and the Fundamental Research Funds for the Central Universities of China under Project No. 2012jdgz02 (Xi'an Jiaotong University). We acknowledge the support from the codes of USRP2 reader from the Open RFID Lab (ORL) project [13].

References

[1] L. Yang, J. Han, Y. Qi, and Y. Liu, "Identification-free Batch Authentication for RFID tags," in *Proceedings of IEEE International Conference on Network Protocols (ICNP)*, 2010.

[2] EPCglobal, *Specification for RFID Air Interface EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz-960 MHz*, 2008.

[3] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless Device Identification with Radiometric Signatures," in *Proceedings of ACM Mobile Computing and Networking (MobiCom)*, 2008.

[4] R. Gerdes, M. Mina, S. Russell, and T. Daniels, "Physical-layer Identification of Wired Ethernet Devices," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1339–1353, 2012.

[5] M. Williams, M. A. Temple, and D. Reising, "Augmenting Bit-Level Network Security Using Physical Layer RF-DNA Fingerprinting," in *Proceedings of IEEE Global Communications Conference (GLOBECOM)*, 2010.

[6] D. Zanetti, B. Danev, and S. Capkun, "Physical-layer Identification of UHF RFID Tags," in *Proceedings of ACM Mobile Computing and Networking (MobiCom)*, 2010.

[7] B. Danev, H. Luecken, S. Capkun, and K. El Defrawy, "Attacks on Physical-layer Identification," in *Proceedings of ACM Conference on Wireless Network Security (WiSec)*, 2010.

[8] D. M. Dobkin, *RF in RFID - Passive UHF RFID in Practice*. Elsevier, 2008.

[9] J. G. Cleary and L. E. Trigg, "K*: An Instance-based Learner Using an Entropic Distance Measure," in *Proceedings of International Conference on Machine Learning*, 1995.

[10] ETTUS, "Universal Software Radio Peripheral(USRP)," 2009. [Online]. Available: http://www.ettus.com/

[11] M. Buettner, "Gen 2 rfid tools," 2010. [Online]. Available: https://www.cgran.org/wiki/Gen2

[12] M. Buettner and D. Wetherall, "A "Gen 2" RFID monitor based on the USRP," in *Proceedings of ACM Special Interest Group on Data Communication (SIGCOMM)*, 2010.

[13] Y. Zheng and M. Li, "Open RFID Lab," 2013. [Online]. Available: http://pdcc.ntu.edu.sg/wands/ORL/

[14] GNURadio, 2012. [Online]. Available: http://www.gnuradio.org

[15] D. C. Scott Miller, *Probability and Random Processes, Second Edition: With Application to Signal Processing and Communications*. Elsevier, 2012.

[16] P. Amin and K. P. Subbalakshmi, "Detecting Hidden Messages Using Image Power Spectrum," in *Proceedings of IEEE Image Processing*, 2007.

[17] B. Danev and S. Čapkun, "Transient-based Identification of Wireless Sensor Nodes," in *Proceedings of the ACM International Conference on Information Processing in Sensor Networks (IPSN)*, 2009.

[18] B. Danev, S. Capkun, R. Jayaram Masti, and T. S. Benjamin, "Towards Practical Identification of HF RFID Devices," *ACM Transactions on Information and System Security*, vol. 15, no. 2, pp. 7:1–7:24, 2012.

[19] S. Periaswamy, D. Thompson, and J. Di, "Fingerprinting RFID Tags," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 6, pp. 938–943, 2011.

[20] Y. Zheng and M. Li, "P-MTI: Physical-layer Missing Tag Identification via Compressive Sensing," in *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*, 2013.

[21] C. Wu, Z. Yang, Y. Liu, and W. Xi, "WILL: Wireless Indoor Localization without Site Survey," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 4, pp. 839–848, 2013.

[22] C. Hekimian-Williams, B. Grant, X. Liu, Z. Zhang, and P. Kumar, "Accurate Localization of RFID Tags Using Phase Difference," in *Proceedings of IEEE RFID*, 2010.

[23] L. Yang, J. Han, Y. Qi, C. Wang, T. Gu, and Y. Liu, "Season: Shelving Interference and Joint Identification in Large-scale RFID Systems," in *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*, 2011.

[24] J. Wang, H. Hassanieh, D. Katabi, and P. Indyk, "Efficient and Reliable Low-power Backscatter Networks," in *Proceedings of ACM Special Interest Group on Data Communication (SIGCOMM)*, 2012.

[25] P. Zhang, J. Gummeson, and D. Ganesan, "BLINK: A High Throughput Link Layer for Backscatter Communication," in *Proceedings of ACM Mobile Systems, Applications, and Services (MobiSys)*, 2012.

[26] C. Qian, H. Ngan, Y. Liu, and L. Ni, "Cardinality Estimation for Large-Scale RFID Systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 9, pp. 1441–1454, 2011.

[27] C. Qian, Y. Liu, H. Ngan, and L. Ni, "ASAP: Scalable Identification and Counting for Contactless RFID Systems," in *Proceedings of IEEE International Conference on Distributed Computing Systems (ICDCS)*, 2010.

[28] Y. Zheng, Z. Li, and C. Qian, "PET: Probabilistic Estimating Tree for Large-Scale RFID Estimation," in *Proceedings of IEEE International Conference on Distributed Computing Systems (ICDCS)*, 2011.

[29] Y. Zheng and M. Li, "Fast Tag Searching Protocol for Large-Scale RFID Systems," *IEEE/ACM Transactions on Networking*, vol. 21, no. 3, pp. 924–934, 2013.

[30] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," in *Security in Pervasive Computing*, 2003.

[31] T. Halevi, S. Lin, D. Ma, A. Prasad, N. Saxena, J. Voris, and T. Xiang, "Sensing-enabled Defenses to RFID Unauthorized Reading and Relay Attacks Without Changing the Usage Model," in *Proceedings of IEEE International Conference on Pervasive Computing and Communications (PerCom)*, 2012.

[32] W. Gong, K. Liu, X. Miao, Q. Ma, Z. Yang, and Y. Liu, "Informative Counting: Fine-grained Batch Authentication for Large-scale RFID Systems," in *Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2013.