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

Jinsong Han, *Member, IEEE,* Chen Qian, *Member, IEEE,* Panlong Yang, *Member, IEEE* Dan Ma, *Student Member, IEEE,* Zhiping Jiang, *Student Member, IEEE,* Wei Xi, *Member, IEEE,* Jizhong Zhao, *Member, IEEE*

***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 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.**

***Index Terms*—RFID, physical-layer identification, similarity**

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, 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, such as [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.

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 robust 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]–[5].

It is crucial to select a qualified feature for physical-layer identification. A feature or feature set used in physical-layer identification must present three properties : (i) Robustness. The feature should be resilient to the environmental changes, e.g. the tag orientation or interference. (ii) Uniqueness. If using the feature, devices should be sufficiently distinguishable with each other. (iii) Availability. Signals for identification should be collected in a cost-effective way and without the need of specific devices, e.g. dedicated oscilloscope or spectrum analyzer. However, existing approaches do not provide features with all above properties. For example, some approaches (e.g., [6] and [7]) use the time interval error (∂_{TIE}) as the feature for identifying passive tags. The TIE-based feature has properties (i) and (iii), but can hardly support property (ii) since it presents a relatively low entropy. On the other hand, the spectral feature proposed in [6] has the property (ii), but is not robust to the tag orientation and requires dedicated equipment. Hence, we are motivated to pursue a feature presenting all three properties.

To this end, 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,

Jinsong Han, Dan Ma, Wei Xi, Zhiping jiang, and Jizhong Zhao are with the School of Electronic and Information Engineering, Xi'an Jiaotong University, China. (e-mail: {xjtumd, zhiping}@stu.xjtu.edu.cn, {hanjinsong, weixi}@mail.xjtu.edu.cn.)

Chen Qian is with the Department of Computer Science, University of Kentucky, Lexington, Ky. (e-mail: qian@cs.uky.edu)

Panlong Yang is with the College of Communications Engineering, PLA University of Science and Technology, China. (e-mail: panlongyang@gmail.com)

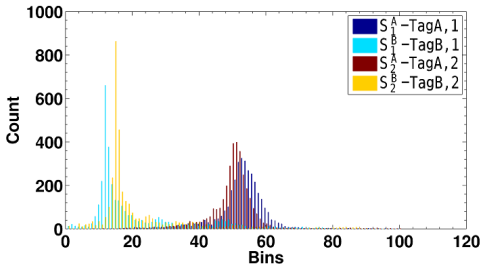


Fig. 1. Distributions of the pulse-inter-covariance-sequence of 4 different RN16 preambles from two Alien 9640 tags. The number of bins is 500 and the first 120 bins are presented in the figure.

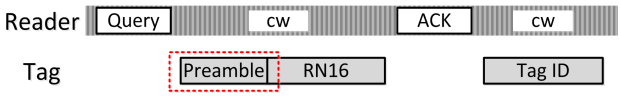


Fig. 2. The communication process between reader and one tag. The signal we use is the preamble of the RN16 which is prior to the ID signal.

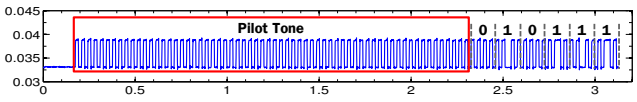


Fig. 3. The T⇒R link preamble form under Miller-modulated subcarrier 4.

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 rate. 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 an RN16 packet, which does not contain any application data such as the tag ID. In addition, our approach is more resilient to attacks such as 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 robust 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. Meeting the need of having three important properties of physical-layer identification, the extracted feature can serve as the fingerprint of a tag with high identification accuracy.
- Without reporting their IDs, the identification process of GenePrint can improve the privacy protection for RFID UHF tags. Besides, the feature extracted by GenePrint is resilient to the feature replay attack, which can enhance the authenticity of RFID identification.

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 a same RN16 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 explicitly reflects the exact physical-layer information correlated to the tag. We choose the preamble of the RN16 packet.

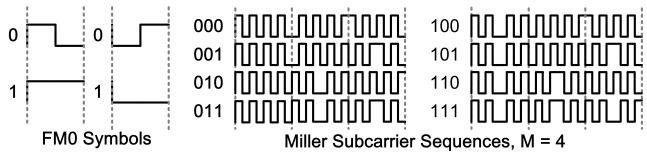


Fig. 4. Examples of the FM0 sequences and Miller-4 sequences [2]

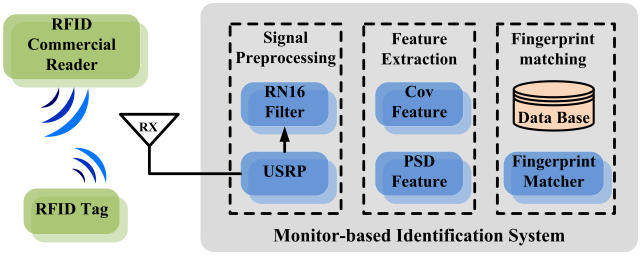


Fig. 5. The monitor-based system collects the response signals from tags under the reader's interrogation. The system consists of 3 components: signal preprocessing, feature extraction and fingerprint matching.

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.

C. Representation of 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. We plot two examples of FM0 sequences and Miller subcarrier sequences symbols in Figure 4. 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 a unique and robust 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.

TABLE I
PROPERTIES OF FEATURES USED IN EXISTING WORKS

Feature	Uniqueness	Robustness	Collectability
Minimum Power [11]	√		
∂_{TIE} [6] [7]		√	√
Spectral feature [6]	√		

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 5.

The protocol is performed as follows. The commercial RFID reader queries a fixed 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 5, 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.

Among all the components, Feature Extraction is the most primary and kernel work for GenePrint, like all the other physical-layer identification systems. In this module, it is essential to determine the criteria of feature selection and a qualified feature. We adapt the criteria used by Danev et al. [10] as aforementioned in Section I. Before presenting the details of our system, we summarize existing features used for identifying RFID UHF tags in Table I.

In Table I, minimum power [11] represents target tag's response energy, which is usually sensitive to the propagate distance of signals. In addition, to obtain this feature, the experiments in [11] are conducted in an anechoic chamber, and a specialized device, Voyantic Tag-formance Lite System, is used to reduce the feature's collectability. ∂_{TIE} and spectral feature are proposed by Zanetti *et al.* [6] [7]. They both provide high identification accuracy on UHF tags. However, ∂_{TIE} owns a relatively low entropy which limits the uniqueness property, while the spectral feature depends on specific signal acquisition equipment and is not robust to tag

locations (accuracy of 37.6% in robustness test). In contrast, the feature extraction component in GenePrint aims at finding a new physical-layer feature (set) for RFID UHF tags, which is qualified for all the three properties.

In our system, the hardware of the monitor is a Universal Software Radio Peripheral (USRP) N210 [12] with SBX daughterboard. The software is partially derived from a Gen2 RFID project developed by Buettner and Wetherall [13]–[15].

Comparing with other dedicated devices, such as the spectrum analyzer, USRP is limited in the precision and analysis, due to its lower sampling rate and weaker processing capability. For example, our USRP + SBX has a detecting spectrum ranging from 400 MHz to 4 GHz, while a typical spectrum analyzer has wider frequency ranging from 9 KHz to 22GHz. Nevertheless, the dedicated device is usually with high cost. A typical dedicated spectrum analyzer is more expensive than USRP by ten times.

In addition, 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 [14], the current GNURadio [16] 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. Experiment results in Section V show that our internal similarity based solution successfully extracts the signal feature using the generic and low-cost hardware with higher accuracy. We also believe if using dedicated devices in the signal acquisition, the system may derive benefit from the sampling precision which leads to a higher identification accuracy. However, the improvement may be limited.

B. Signal PreProcessing

The raw signal received by USRP includes the carrier wave, reader command and tag responses. To achieve data-independent feature extraction, in the first step, we should adopt a fast scheme to separate RN16 packets from the raw signal as illustrated in Figure 6. Since the frequency of the tag response is higher than that of reader commands, an intuitive solution is to implement a bandpass filter followed by an inverse Fourier transform. The data rate of tags is determinated from the monitor's perspective by decoding the *Query* command of the reader [2]. Hence the output of the bandpass filter is the frequency domain of the tag's response. Thus using an inverse Fourier transform module can recover the original signal from the specific signal's Fourier transform. However, as the parameters in the bandpass filter cannot be completely precise when applying to real implementations, this process will incur signal distortion.

In order to solve this problem, we propose a fine-grained RN16 Filter component, which can work with a variety of signal magnitudes and frequency channels. This solution is based on our observation that in the frequency domain, the signal of tags shows a significant difference from that of

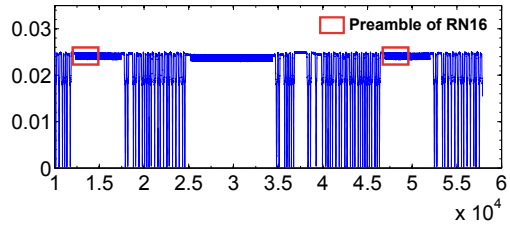


Fig. 6. Raw signal captured by USRP, which is composed of carrier wave, reader commands and tag responses.

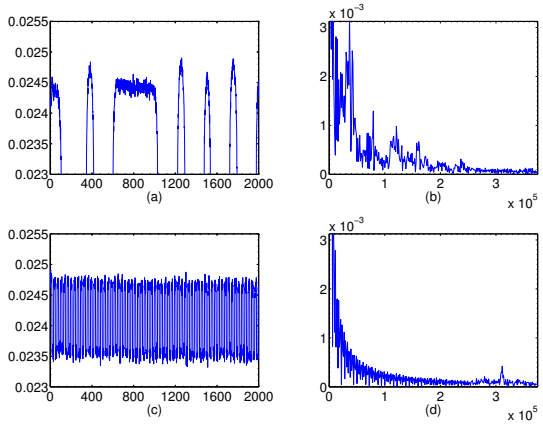


Fig. 7. Different performance of reader command signal and tag response signal. (a) Tag response signal in time domain. (b) Tag response signal in frequency domain. (c) Reader signal in time domain. (d) Reader signal in frequency domain.

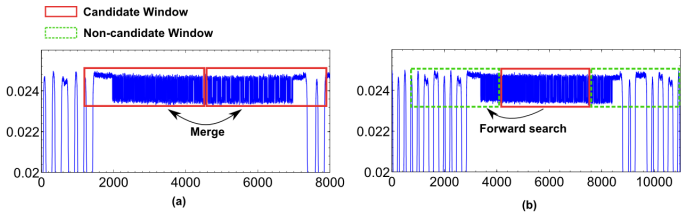


Fig. 8. Different manipulation of sliding window in RN16 Filter component. (a) Two adjacent candidate windows will be merged together. (b) Isolated candidate window will search forward for the preamble.

readers. We show this difference in Figure 7. In Figure 7 (a) and (c), we show the signal of a randomly chosen reader command Query, and the signal of corresponding tag's RN16 response. Transformed to the frequency domain, they show a big difference, as plotted in Figure 7 (b) and (d). Such differences can be used to filter the tag response from the reader's signal.

More specifically, we use a sliding window to traverse through the whole signal. Fast Fourier transform is applied to detect whether the signal's energy in this window follows the signal pattern of tags. 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. If two adjacent windows are

Fig. 9. 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.

both valid, we merge them to form a long candidate signal. For the isolated window, we will perform a forward search by merging the preceding signal part. The search scope will be one-third of the length of RN16, as shown in Figure 8 (b). In this way, we can ensure that the preamble of tag's response is not missed.

Another challenge is to distinguish RN16 signal from tag ID signal. Since both of them have the same pattern in frequency domain, the only feature to distinguish them is their signal length. When we use Miller-4 as the data encoding method and a BLF equal to $DR/TRcal = \frac{64/3}{74} = 288kHz$ (these parameters are calculated by decoding the reader command *Query*) [2], the length of an RN16 signal is about 5000 points with a USRP sampling rate of 10MS/s while the length of tag ID signal is about 9500 points.

For obtaining the preamble signal of RN16, GenePrint needs to perform a fine-grained pattern recognition scheme on all candidate RN16 signals. A much smaller window (width = 20 points) is used to find the pulse pattern, facilitating to precisely locate the transient point between the carrier wave and the tag preamble. Consequently, a real RN16 signal can be separated.

For the RN16 Filter component, we assume there is no collision happens. That means GenePrint identifies one tag at a time to simplify the signal acquisition process. 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 fails to identify the tag (no *ACK* replied by the reader). However, in our protocol, the monitor records all RN16 signals in a sequential order, which indicates that even if the observed RN16 signals cannot be decoded by a commercial reader, they can still be considered 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 effectively reflects the hardware feature of tags.

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 9. 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

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

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

$$Cov(P_i^h, P_j^h) = Cov(f_i^h, f_j^h) \tag{4}$$

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

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:

$$S^h = [Cov(f_1^h, f_2^h), .., Cov(f_i^h, f_j^h), .., Cov(f_{63}^h, f_{64}^h)] \quad \text{for integers } i, j \in [1, 64], i < j \tag{5}$$

$$S^l = [Cov(f_1^l, f_2^l), .., Cov(f_i^l, f_j^l), .., Cov(f_{63}^l, f_{64}^l)] \quad \text{for integers } i, j \in [1, 64], i < j \tag{6}$$

Note that each of S^h and S^l has $C(64, 2) = 2016$ elements. Combining Equation 5 and Equation 6, the signal feature can be extracted as a covariance sequence in a length of $2 \times C(64, 2)$:

$$S = [S^h, S^l] \tag{7}$$

For the signal of each tag, we can construct a vector in the form of Equation 7.

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 V 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 [17]:

$$R_{XX}(t, t+\tau) = E(X(t)X(t+\tau)) \tag{8}$$

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 [17]:

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

$$S_{XX}(f) = \int_{-\infty}^{+\infty} R_{XX}(\tau) e^{-j2\pi f\tau} d\tau \tag{9}$$

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 [18] utilized the power spectrum feature to classify images.

In out system, the power spectral density of a signal is estimated by the Yule-Walker algorithm [19] [20] which is an autoregressive model-based PSD estimation method. The length of the result vector is determined by the length of input signal and the FFT. In our experiments, we only choose the first 20 dimensions of the result vector because the remaining parts are too sparse.

In GenePrint, 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 construct 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, generates its fingerprint via proposed feature extraction methods, and computes 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 V.

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 V-C. If there is no valid entry, a "reject" will be reported.

IV. Classifier Selection and Analysis

In this section, we implement different classifiers to evaluate their performance in the fingerprint classification on our UHF passive tags. Generally, the best selection of classifier should depend on the inner structure of fingerprints used. However, due to the affect from complicated environments and unpredictable hardware performance in sampling, it is impossible to formulate an accurate and universal model for all fingerprints. In addition, different applications may tend to utilize different classifiers based on the trade-off of accuracy, computational complexity and memory requirement. Therefore, the purpose of this section is to give a guide in the classifier selection for the real implementation of GenePrint by comparing the performance of different classifiers when using the GenePrint's fingerprints.

A. Candidate Classifiers

A classifier is one of the most commonly used modules in a physical-layer identification system. A classifier tool works

as follows. It takes a collection of fingerprint entries as the input, each belonging to one class. These entries are described by their fixed size of attributes. The output is a predicted class to which a entry belongs.

We choose 7 different candidate classifiers: C4.5, RIPPER, k-NN, KStar, Naïve Bayes, ANN and SVM based on three main considerations: The classifier should be 1) typical and commonly used, 2) easy to implement and 3) covering most categories of classification approaches. Details about the classifiers are listed in [21]:

In the context of marching learning, all the classifiers we choose are based on supervised learning. Simply using one of the above classifier may be not good enough. Other techniques, such as feature selection and ensemble methods may be also required. These issues are beyond the scope of this paper. In our experiment, we simply utilize each classifier to classify fingerprint entries and present the classification accuracy for each classifier.

B. Classifier Selection Experiments

In this set of experiments, we use two small groups of data: *Accuracy Group* and *Robustness Group*. The *Accuracy Group* contains fingerprints from 15 tags captured in the same location. For each tag, we record 80 preamble signals and generate their fingerprints. Tag populations are randomly selected from 3 different tag models which are described in Section V-A. On the other hand, the *Robustness Group* is composed of fingerprints captured from 35 different locations with the distance d varying from 0.3m to 1m and angle θ changing from $-60°$ to $60°$ (Definitions of d and θ are detailed in Section V-C2). 10 tags are used in this data set and for each tag, we also calculate 80 fingerprints in each location.

We firstly test the performance of different classifiers for the combined fingerprint (Cov, PSD). As shown in Figure 10, the classification accuracy of *Accuracy Group* is better than that of the *Robustness Group*. This is because longer distance and greater angle between the reader antenna and the tag will lead to a lower Signal Noise Ratio (SNR), introducing much more outliers and errors to the fingerprints. Among all the classifiers, the KStar has the best performance, i.e. a classification accuracy of 97.58% and 97.5% for *Accuracy Group* and *Robustness Group*. Another observation from Figure 10 is that the Naïve Bayes classifier has the greatest variations in classification performance. This inspires us to further explore the performances of two individual fingerprints when applying different classifiers.

In Figure 11, we compare the performance of 7 classifiers when processing different single fingerprints. For the first 4 classifiers, PSD-based fingerprint can achieve a higher accuracy comparing with the Cov-based fingerprint, but this strength is not significant in the *Robustness Group* data set. The Naïve Bayes learner has the greatest variations in classification performance, indicating that the PSD-based fingerprint is more likely to be unsuitable for this classifier. Especially, Naïve Bayes only achieves an accuracy of 34.08% for the *Robustness Group*-PSD data set.

C. Classifier Selection Analysis

We find that we can categorize the features into two categories, one-dimensional (e.g. ∂_{TIE} [6] [7]) and multi-dimensional (e.g. Cov and PSD of GenePrint) features. In particular, we analyze the experimental results using different classifiers on the (Cov and PSD) feature, as shown in Figure 10 and Figure 11.

First, we find the Naïve Bayes classifier has the biggest limitation when classifying both Cov-based and PSD-based fingerprints. This is mainly because the performance of Naïve Bayes classifier will be degraded in terms of the correlated attribute. Serving as a kind of distribution (Cov) and spectrum (PSD) information, both fingerprints cannot hold the conditional independence assumption for their attributes.

Since fingerprints in GenePrint are multi-dimensional, they are more likely to bring noises for classifiers. We find that ANN and SVM classifiers are not qualified for GenePrint. This is because both ANN and SVM classifiers suffer from high computational complexity in building up their models, which tends to overfit the training set during the learning phase. In contrast, some simple classifiers, such as the C4.5, RIPPER and two instance-based methods are more appropriate for GenePrint's fingerprints. A more elegant strategy to classify GenePrint's fingerprints is to implement a dimensionality deduction approach. For the high dimensional fingerprints used in GenePrint, this can not only reduce the computational complexity, but also improve the classified accuracy by removing redundant attributes.

On the other hand, in the domain of physical-layer identification for wireless devices, many one-dimensional features are utilized to distinguish different devices, e.g. ∂_{TIE}, $\bar{P}_B$ [6], frame frequency offset [3]. With fewer dimensions, these features require less computational resource and fewer restrictions on classifiers. They are more adaptable to different classifiers, such as k-NN [6] and SVM [3].

V. 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 V-A and the accuracy metrics used to evaluate classification and identification in Section V-B. The experiment results will be presented and analyzed in Section V-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 12 shows the testbed.

To show the GenePrint system is universally applicable, we test tags in different design models. The 150 tags for evaluation

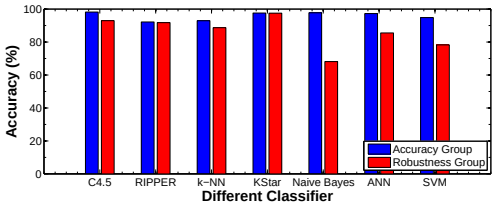


Fig. 10. Classification accuracy of combined fingerprint (Cov, PSD) when implementing different classifiers to both of the *Accuracy Group* and *Robustness Group* data sets.

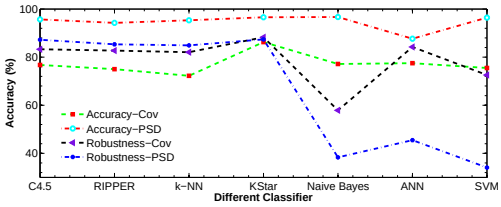


Fig. 11. Classification accuracy of different classifiers for Cov-based fingerprint and PSD-based fingerprint in *Accuracy Group* and *Robustness Group* data sets.

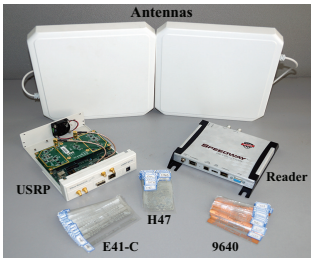


Fig. 12. Experiment equipments

TABLE II
TAG MODELS INVOLVED IN THE EXPERIMENT

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

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 robustness, we purposely use those tags with different designs as shown in Table II.

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 communication channel between reader and tag is fixed which has a center frequency of 912.75 MHz. 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 30 cm to 1 m. 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 robustness 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 a 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, FRR is the percentage of scores correspond to the same tag but lower than the threshold, and FAR is the percentage of scores higher than the threshold but locate tags to wrong reference entries. We select a fixed value as the threshold with which FRR is equal to FAR. The error rate at this threshold is the *Equal Error Rate* (EER) [22].

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 rates. 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.

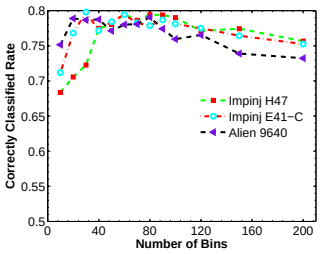


Fig. 13. Classification accuracy of Cov distribution feature for different settings of the number of bins in the distribution estimation approach. This classification is performed on 150 RFID UHF tags (80 samples for each tag) and the classifier is a 5-fold KStar.

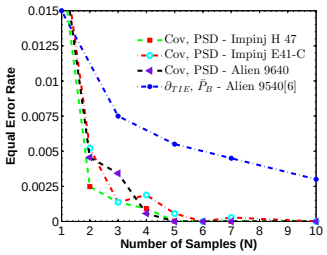


Fig. 14. Identification accuracy of the feature set (Cov, PSD) for different number of samples. (The accuracy of feature $(\partial_{TIE}, \bar{P}_B)$) is from [6].

TABLE III
CLASSIFICATION ACCURACY

Feature	Cov			∂_{TIE}	$\bar{P}_B$	Spectral
Tag Model	E41-C	H47	9640	9540		
# of signals	1	1	1	5	5	5
accuracy	77.88	79.42	79.06	71.4	43.2	99.6

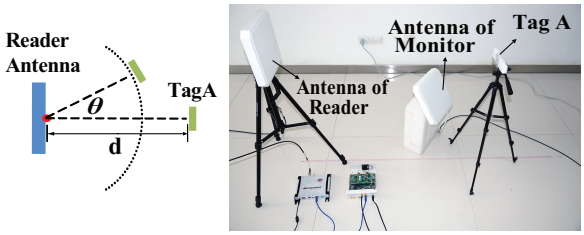


Fig. 15. Experimental deployment

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 use a subset of our tag population to evaluate the feature classification accuracy with different numbers of bins. Figure 13 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 13, in general the identification accuracy is robust 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, 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 a 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 III shows the Cov-based Pulse Inter Feature classification accuracy on a population of 150 tags, when M equals to 80. 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 III shows the results for every of the three models. We also compare our experiment results with the work in [6]. Limited by the lack of hardware, we are not able to get the purpose-built reader. 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. Therefore, we use the classification accuracy claimed in [6] directly as the benchmark. 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 III, the three models of tags have an average accuracy of 78.79%, which is higher than that of feature ∂_{TIE} and $\bar{P}_B$. However, Cov-based feature is multi-dimensional, indicating that it needs more storage space and computational overhead. On the other hand, the Spectral feature [6] is more accurate than Cov-based feature, but it suffers from lower robustness and require specific signal acquisition device.

We implement the threshold-based identification mechanism described in Section V-B. In this experiment, we establish the fingerprints for 150 tags by using the fingerprint set (Cov PSD). Both of them are multi-dimensional features and we simply group them into one big vector which has 100 attributes (Cov: 80, PSD: 20). 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 improve the identification accuracy, the sample-combination method is adopted. Let N be the number of samples acquired to produce one fingerprint. Figure 14 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 14, 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 $(\partial_{TIE}, \bar{P}_B)$-based approach. 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 robustness: In this section, we analyze the robustness of the extracted feature set (Cov, PSD).

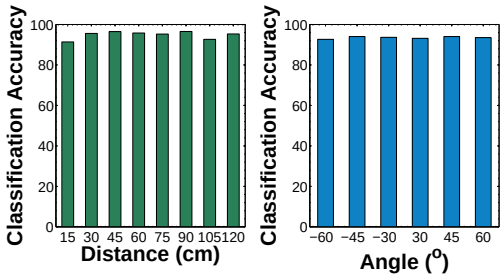


Fig. 16. Feature extraction robustness by varying the distance and angle.

We vary the distance and the angle between the reader's antenna and the tags, as illustrated in Figure 15. The d is defined as the distance between the centroid of reader antenna and the tag. We conduct 8 different experiments with $d = 15cm$ to $d = 120cm$. In the experiment with changed orientations, we vary the value of θ: $\pm 30°$, $\pm 45°$ and $\pm 60°$. We use 30 different tags (10 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 $19200 + 14400 = 33600$ (distance: $19200 = 30 \times 80 \times 8$; orientation: $14400 = 30 \times 80 \times 6$) signals altogether.

We first show the classification accuracy in Figure 16. We used the KStar classifier with 5-fold cross-validation to evaluate the classified accuracy and the number of signals to generate a fingerprint (N) is 1. The average classification accuracy of distance and orientation tests are 94.87% and 92.45% respectively. The beamwidth of a regular UHF RFID antenna is $70°$. Considering real-world aspects, we set the maximum orientation angle as $\pm 60°$ to ensure normal reading of RFID reader. 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]. If the tag's response transmits a longer distance, the signal we collected will be suffered from lower signal noise ratio. Using a low sampling rate on the signal with strong noise, it is difficult to obtain enough information to extract a good fingerprint. This problem is part of our future work and we will try to enlarge the distance of identification.

To investigate the GenePrint's robustness, we group the same tags' fingerprints from different locations. In the distance experiment, we define different range zones between the reader antenna and the target tag, which are from 30 cm to 120 cm. For example, in the $30cm$ range zone test, we combine the fingerprint sets of 15 cm and 30 cm used in the previous experiment (Figure 16). This means for each tag, it has 160 fingerprints generated from 2 locations. The orientation experiment is essentially the same. We then vary the angle ranges from $60°$ to $120°$. The purpose of this experiment is to find out GenePrint's feasible service range. The threshold-based identification mechanism which uses $N = 3$ is implemented in this experiment. Figure 17 and 18 show the experiment results under different settings of distance and angle range. In both experiments, the EER of the worse situation is about 0.05, which is higher than the fixed location experiment results in Figure 14. This may be caused by the indoor multi-path effect, which introduces uncontrollable environment noises. However, this negative influence is not serious and we can reduce this effect by increasing the number of signals N to build a more unbiased fingerprint.

Considering all the locations in our experiment, we further calculate 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 19 reflect that GenePrint can achieve very high TAR even if the FAR is very small.

We also investigate the benefit from the combination of Cov and PSD. We re-generate the fingerprints under the same experiment settings, *e.g.* range zones, as shown in Figure 17. Each newly generated fingerprint is only composed of 100 PSD attributes. We then compare it with the combined fingerprint (Cov, PSD), which has the same size of attributes but in the form of (Cov:80, PSD:20). Figure 20 shows the average EERs of the two types of fingerprints for three types of tags. As shown in the figure, the combined fingerprint (Cov, PSD) significantly reduces the EER from the PSD only fingerprint. This is because PSD is sensitive to the location of tags, like other spectral fingerprints. It is known that the received signal and its PSD are determined by the channel distortion, including the attenuation and delay. According to the spatial selectivity theory [23], the channel distortion will change significantly even if the communicating party moves a distance as short as the wavelength of wireless signals, *e.g.* 32.5cm for the 924.38MHz UHF RF used by the commercial RFID reader in our system. In other words, the PSD of a tag is highly correlated to its location. The result reveals that the proposed Cov feature well complement the PSD feature. The combination of them can effectively amend the influence from location changes, and hence improve the identification accuracy for Geneprint.

VI. Security Analysis

Existing attacks targeted to RFID systems can be categorized into active and passive attacks.

Active attack: The ultimate goal of active attacks to an identification mechanism is to successfully impersonate a victim. For example, in an access control system, an adversary can use specific equipment or the same device as GenePrint's monitor, e.g. spectrum analyzer and USRP, to generate forged fingerprints for cheating the system or impersonating some valid users. As discussed in [24], there are two major active 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 tags for impersonation. We assume the attacker knows the types of features used by the tag, 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 (F1),

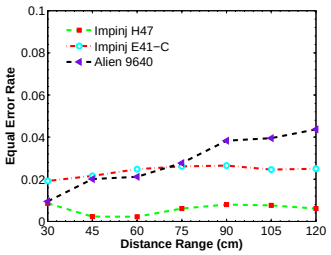


Fig. 17. GenePrint's EER of different distance ranges

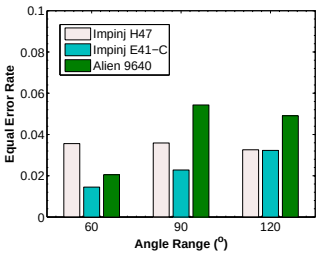


Fig. 18. GenePrint's EER of different angle ranges

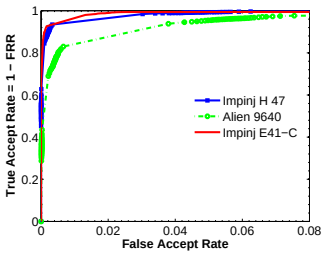


Fig. 19. True accept rate under small settings of FAR

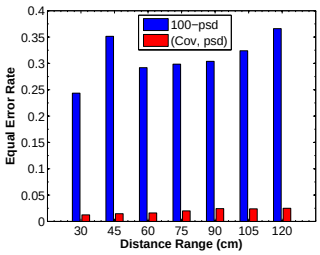


Fig. 20. GenePrint's EER for three types of tags

Frame SYNC correlation (F2), Frame I/Q origin offset (F3), Frame magnitude error (F4), Frame phase error (F5) [3], Time Interval Error (TIE), and Average Baseband Power (PB) [6]. Some earlier works use signal transients to extract hardware feature [5]. 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 [24]. Such an attack is more easily to be conducted if using programming radio devices, e.g. USRP N210.

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 has to perform brute-force search by the following steps for impersonating a victim tag, which increases the overhead or difficulty of attacks. **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. The attacker may shrink the scope of pulse generation to improve the attacking efficiency. But the scope size depends on the number of fingerprints accumulated by the attacker.

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. Note that impersonation is still possible in practice, e.g. the work in [24] successfully implemented a device impersonation attack by signal replay with an arbitrary waveform generator. The use of GenePrint can effectively mitigate the impact of impersonation attacks.

Passive attack: Passive attacks are mainly conducted by "overhearing" the communication between the reader and tag. For example, in the access control example aforementioned, passive adversary can use the off-the-shelf reader or monitoring devices, e.g. USRP to perform the overhearing. We discuss the passive attack whose objective is to obtain the application data, i.e. IDs of tags, from the RFID system. Passive attacks targeted on the application data do not work for GenePrint due to the data-independence of GenePrint. In our protocol, the entire communication between the reader and tag does not involve the tag ID or any other application information. Therefore those attackers can obtain nothing from the system. Even if the attacker owns the same capability as our system that can analyze RN16 signals, it gets no information of the tags as it has no authorization to access the reference database.

In fact, our protocol includes two kind of trustworthy identification approaches. The basic protocol could skip all operations related to the tag IDs, such as the selecting and acknowledging in the standard inventory round defined in EPCglobal C1G2 specification [2]. In order to achieve a stronger privacy-preserving protocol, GenePrint could use an incomplete inventory round, which implies the inventory will be ended by receiving the tag's RN16 response. We propose two approaches: 1) calling the corresponding interfaces provided by the manufactures of commercial readers, and 2) implementing an RFID reader using USRP-like devices and making changes in the communication mode of readers by software radio. Buettner et al. [13] has shown the implementation of an RFID reader by USRP. The advanced protocol could cooperate the ID information and physical-layer fingerprints. In this protocol, one tag is verified only if its ID and the fingerprint extracted are matching. This can achieve a high-level trustworthy identification.

Privacy: For physical-layer identification protocols, privacy

is also an important concern. GenePrint provides strong privacy protection for application information. This means the protocol is ID-free, which leaves less opportunities to attackers to compromise user privacy. However, it is still possible for a very powerful attacker to track a tag using physical-layer information. An attacker with the capability of signal replaying can record the signals of targeted tags. Using the similar feature extraction mechanism to our protocol, or other feature extraction, the attacker can track the movement and appearance of a tag without knowing the tag ID. In fact signal recording is able to effectively break the privacy of RFID tags as well as other wireless devices. Preventing unauthorized physical-layer identifications remains an open issue. We will address it in our future work.

VII. RELATED WORK

Physical-layer identification mechanism has been proposed in variant platforms [3]. 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 [25], and some others focus on UHF tags, such as [6] and [11]. The authors in [11] proposed a Minimum Power Response feature extraction method to distinguish different tags. To the best of our knowledge, [11] is the first work on feature extraction of RFID UHF tags. The authors in [6] propose 3 different features. Comparing with those features, fingerprints of GenePrint are based on the extraction of signal internal similarity which can reflect the hardware feature and is more resilient to environment noise. However, the multi-dimensional feature set (Cov, PSD) also requires more storage space and increases system's computational complexity.

For other purposes, Zheng and Li [26] proposed to identify missing tags by using the aggregated physical signals from concurrent tag responses. C. Hekimian-Williams et al. [27] proposed a 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, some works took the collision responses from tags as useful information. In the work proposed by Wang et al. [28], collisions were regarded as transmitted code and the decoding was proceeded with the compressive sensing algorithm. Blink [29] 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 [30], 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 [31], 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 suffering from low efficiency on key search. Later, researchers attempted to develop the security-related applications. Halevi er al. [32] 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].

VIII. 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 robust.

Our future work will be conducted on the extension of GenePrint to support identification in the existence of signal collisions. We are also trying to design a general physical-layer identification solution for a variety of wireless devices.

IX. ACKNOWLEDGEMENTS

This work was supported in part by NSFC under Grant No. 61190112, 61325013, 61373175, and 61172090; the Natural Science Basic Research Plan in Shaanxi Province of China under Grant No. 2014JQ832; the Specialized Research Fund for the Doctoral Program of Higher Education under Grant No. 20130201120016; the Fundamental Research Funds for the Central Universities under Grant No. XJJ2014049 and XKJC2014008. Chen Qian is the corresponding author.

REFERENCES

[1] L. Yang, J. Han, Y. Qi, and Y. Liu, "Identification-free Batch Authentication for RFID tags," in *Proceedings of IEEE 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 MobiCom*, 2008.

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

[5] B. Danev and S. Čapkun, "Transient-based Identification of Wireless Sensor Nodes," in *Proceedings of the ACM IPSN*, 2009.

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

[7] D. Zanetti, P. Sachs, and S. Capkun, "On the practicality of uhf rfid fingerprinting: How real is the rfid tracking problem?" in *Proceedings of ACM PETS*, 2011, pp. 97–116.

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

[9] V. K. Pang-Ning Tan, Michael Steinbach, *Introduction to Data Mining*. Pearson Education, 2006.

[10] B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices," *ACM Comput. Surv.*, vol. 45, no. 1, pp. 6:1–6:29, 2012.

[11] 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.

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

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

[14] M. Buettner and D. Wetherall, "A "Gen 2" RFID monitor based on the USRP," in *Proceedings of ACM SIGCOMM*, 2010.

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

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

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

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

[19] U. G. Yule, "On a Method of Investigating Periodicities in Disturbed Series, with Special Reference to Wolfer's Sunspot Numbers," *Philosophical Transactions of the Royal Society*, vol. 226, pp. 267–298, 1927.

[20] G. Walker, "On Periodicity in Series of Related Terms," in *Proceedings of the Royal Society*, vol. 131, 1931, pp. 518–532.

[21] D. Ma, C. Qian, W. Li, J. Han, and J. Zhao, "GenePrint: Generic and Accurate Physical-Layer Identfication for UHF RFID Tags," in *Proceedings of IEEE ICNP*, 2013.

[22] S. Mahadeva Prasanna, S. Sahoo, and T. Choubisa, "Multimodal Biometric Person Authentication : A Review," *IETE Technical Review*, vol. 29, no. 1, pp. 54–75, 2012.

[23] G. Franceschetti and S. Stornelli, *Wireless Networks: From the Physical Layer to Communication, Computing, Sensing and Control*. Academic Press, 2006.

[24] B. Danev, H. Luecken, S. Capkun, and K. El Defrawy, "Attacks on Physical-layer Identification," in *Proceedings of ACM WiSec*, 2010.

[25] 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.

[26] Y. Zheng and M. Li, "P-MTI: Physical-layer Missing Tag Identification via Compressive Sensing," in *Proceedings of IEEE INFOCOM*, 2013.

[27] 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.

[28] J. Wang, H. Hassanieh, D. Katabi, and P. Indyk, "Efficient and Reliable Low-power Backscatter Networks," in *Proceedings of ACM SIGCOMM*, 2012.

[29] P. Zhang, J. Gummeson, and D. Ganesan, "BLINK: A High Throughput Link Layer for Backscatter Communication," in *Proceedings of ACM MobiSys*, 2012.

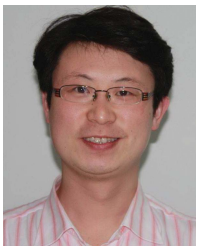
[30] M. Shahzad and A. X. Liu, "Every Bit Counts: Fast and Scalable RFID Estimation," in *Proceedings of ACM Mobicom*, 2012.

[31] 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.

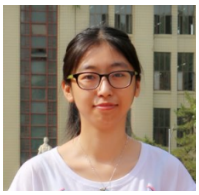
[32] T. Halevi, S. Lin, D. Ma, A. Prasad, N. Saxena, J. Voris, and T. Xiang, "Sensing-enabled Defenses to RFID Unauthorized Reading and Relay Attacks Without Changing the Usage Model," in *Proceedings of IEEE PerCom*, 2012.

Jinsong Han is currently an associate professor at Xi'an Jiaotong University. He received his Ph.D. degree on Computer Science from Hong Kong University of Science and Technology. His research interests include pervasive computing, distributed system, and wireless network. He is a member of CCF, ACM, and IEEE.

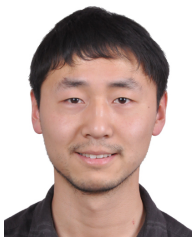
Chen Qian (M'08) is an Assistant Professor at the Department of Computer Science, University of Kentucky. He received the B.Sc. degree from Nanjing University in 2006, the M.Phil. degree from the Hong Kong University of Science and Technology in 2008, and the Ph.D. degree from the University of Texas at Austin in 2013, all in Computer Science. His research interests include computer networking, data-center networks, software-defined networking, and mobile computing. He is the recipient of the James C. Browne Outstanding Graduate Fellowship in 2011. He is a member of IEEE and ACM.



Panlong Yang (M02) received his B.S. degree, M.S. degree, and Ph.D. degree in communication and information system from Nanjing Institute of Communication Engineering, China, in 1999, 2002, and 2005 respectively. During September 2010 to September 2011, he was a visiting scholar in HKUST. Dr. Yang is now an associate professor in the Nanjing Institute of Communication Engineering, PLA University of Science and Technology. He is a member of the IEEE Computer Society and ACM SIGMOBILE Society.



Dan Ma received her MPhil degree from Dept. of Computer Science and Engineering, Xi'an Jiaotong University. Her research interests include RFID, Information Security, and Wireless Network.



Zhiping Jiang is a Ph.D candidate at Xi'an Jiaotong University, Xi'an. His research interests include localization, smart sensing, wireless communication, and image processing.

Wei Xi is a postdoctoral research fellow at Xi'an Jiaotong University. He received his Ph.D degree on Computer Science from Xi'an Jiaotong University in 2014. His main research interests include wireless networks, smart sensing, and mobile computing. He is a member of CCF, ACM, and IEEE.

Jizhong Zhao He is a Professor at the Department of Computer Science and Technology, Xi'an Jiaotong University. His research interests include computer software, pervasive computing, distributed systems, network security. He is a member of CCF, ACM, and IEEE.