Physical-layer Identification of UHF RFID Tags

Author(s):
Zanetti, Davide; Danev, Boris; Capkun, Srdjan

Publication date:
2010

Permanent link:
https://doi.org/10.3929/ethz-a-007584818

Physical-layer Identification of UHF RFID Tags

Davide Zanetti, Boris Danev and Srdjan Čapkun
Department of Computer Science
ETH Zurich, Switzerland
{zanettid, bdanev, capkuns}@inf.ethz.ch

ABSTRACT

In this work, we study physical-layer identification of passive UHF RFID tags. We collect signals from a population of 70 tags using a purpose-built reader and we analyze time domain and spectral features of the collected signals. We show that, based on timing features of the signals, UHF RFID tags can be classified, independently of the location and distance to the reader (evaluated up to 6 meters), with an accuracy of approx. 71% (within our population). Additionally, we show that is possible to uniquely identify a maximum of approx. 2^6 UHF RFID tags independently of the population size. We analyze the implications of these results on tag holder privacy. We further show that, in controlled environments, UHF RFID tags can be uniquely identified based on their signal spectral features with an Equal Error Rate of 0% (within our population); we discuss the application of those techniques to cloning detection in RFID-enabled supply chains.

Categories and Subject Descriptors

C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*Wireless communication*; C.3 [**Computer Systems Organization**]: Special-Purpose And Application-Based Systems—*Signal processing systems*; K.6.5 [**Management of computing and informations systems**]: Security and Protection—*Authentication, Physical security, Unauthorized access*

General Terms

Design, Experimentation, Measurement, Security

Keywords

Fingerprinting, Physical-layer Identification, Privacy, RFID, Tracking, Wireless Security

1. INTRODUCTION

Radio Frequency IDentification (RFID) devices are becoming increasingly important components of a number of systems such as electronic passports [1], transportation systems [51], and supply chain systems [19]. As a result, a number of security protocols have been proposed for RFID authentication [21, 27, 49], key management [30, 33], and privacy-preserving deployment [7, 14, 16, 28, 31, 35]. The literature contains a number of investigations of RFID security and privacy protocols [2, 29] on the logical level; however, little attention has been dedicated to the security and privacy implications of the RFID physical communication layer.

Physical-layer device identification techniques aim at identifying a device or a class of devices based on fingerprints obtained by analyzing a device's communication at the physical layer. Such techniques have been proposed for several applications and wireless platforms [11, 12, 24, 26, 39, 46, 48, 50] and few investigations addressed HF [12, 40] and UHF [38] RFID tags.

The implication of applying physical-layer device identification techniques on RFID-based applications is twofold: they can provide additional security guarantees by enabling physical-layer-based identification, but they can also invalidate privacy guarantees of protocols running at the upper layers of communication.

In this work, we study physical-layer identification of passive UHF RFID tags. We performed experiments on a population of 70 UHF RFID tags (EPC C1G2) from three different manufacturers. We built an RFID reader that challenged tags by simulating an inventorying protocol. From the (fixed) preambles of tags' replies, we extracted RF signal features that allowed us to classify and identify tag models and individual tags. The features that we extracted contain timing and spectral information of the collected signals.

We show that, using timing features, individual UHF RFID tags can be classified with an accuracy of 71.4% (within our population) from different locations and distances up to 6 meters, and that is possible to uniquely identify a maximum of approx. 2^6 UHF RFID tags independently of the population size. These results have implications for users' privacy: tracking of RFID tag users will be indeed possible (i) with high accuracy, especially given that users are expected to carry several RFID tags (e.g., on their glasses, medical devices, clothes, etc), and (ii) despite most privacy-preserving countermeasures on upper communication layers. Namely, if communication with an RFID tag is possible, physical-layer identification techniques will enable it to be tracked disregarding the location of the tag. This result is the first that shows that tracking of UHF RFID tags is possible with high accuracy from their nominal operating distance (i.e., within 6 meters).

We further show that, using spectral features, in controlled environments, UHF RFID tags can be classified with an accuracy of 99.6% and identified with an Equal Error Rate of 0.0% (within our population). Although this result shows that spectral features are not stable when measured from varying distances, the highly-accurate classification and identification provided by this technique might motivate its use to the detection of product cloning in RFID-enabled supply chain.

MobiCom'10, September 20–24, 2010, Chicago, Illinois, USA.

The rest of this paper is organized as follows. In Section 2, we define our problem statement and provide a system overview. In Section 3, we present our acquisition setup, the performed experiments, and summarize the collected data. We introduce our physical-layer identification techniques in Section 4 and present their performance results in Section 5. In Section 6, we discuss the implications of our techniques. We make an overview of background and related work in Section 7 and conclude the paper in Section 8.

2. PROBLEM STATEMENT AND SYSTEM OVERVIEW

The main goal of our work is to study the feasibility and the accuracy of physical-layer identification (identity verification) and classification of passive UHF RFID tags. The former refers to the verification of tag identities based on accept/reject decisions: the fingerprint of the tag under identification is verified against a reference fingerprint representing the claimed identity (1:1 comparison). The latter refers to the association of tags to previously defined sets of classes based on similarity rules: the tag under classification is assigned to one and only one class, which, in our study, represents either a tag or a tag model.

In our study, we use a single experimental setup for the examination of classification and identification. Our setup consists of two main components: a signal acquisition setup (i.e., a purpose-built tag reader, Section 3.1) and a feature extraction and matching module (Section 4). Our acquisition setup challenges the tags with in- and out-of-specification commands (Section 3.2) and captures their responses. Our feature extraction module then extracts timing and spectral features from the collected responses; more specifically, our module extracts the time interval error, the average baseband power, and the frequency components of the responses.

To evaluate both classification and identification accuracies of our physical-layer identification techniques, we deploy a tag population composed of 70 EPC class-1 generation-2 (C1G2) RFID tags [18] of three models and manufactures. EPC C1G2 tags are the *de facto* standard passive UHF tags and the most pervasive in the current market.

In summary, in this work we address the following questions:

1. Is it possible to identify passive UHF RFID tags using physical-layer identification techniques?
2. What is the classification and identification accuracy of our setup, within our tag population?
3. What is the impact of environmental and signal acquisition factors like tag position, tag orientation, communication power, and sampling rate on the classification and identification accuracy?
4. What are the implications of the proposed techniques for users' privacy and how those can be used for cloning detection in RFID-enabled supply chains?

3. EXPERIMENTAL SETUP AND DATA

In this section, we first describe our signal acquisition and antenna setup. We then detail the different types of experiments we performed and present the collected datasets.

3.1 Acquisition and Antenna Setup

The communication between RFID readers and tags is half-duplex. A reader transmits commands and data to a tag by modulating an RF signal. The tag replies to the reader using a backscattered signal modulated by modifying the reflection coefficient of its antenna. Figure 1 shows a sample reader's challenge and subsequent tag's response.

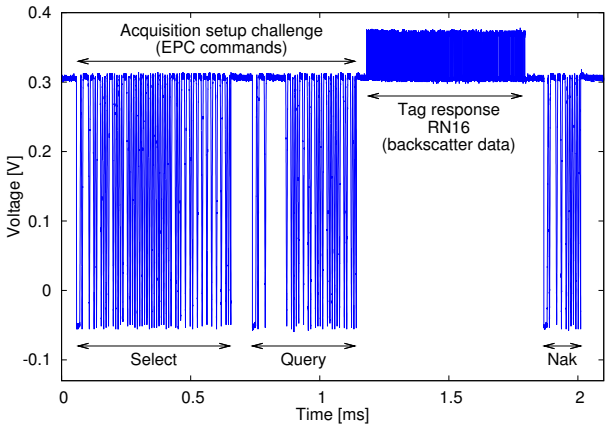

Figure 1: Acquisition setup challenge and tag response.

Our acquisition setup is shown in Figure 2: it consists of a transmitter and a receiver and uses a bistatic antenna configuration to minimize leakage from the transmitter to the receiver (i.e., one antenna for the transmitter and a second one for the receiver). The chosen antennas are circularly polarized, which allows our acquisition setup to power up (and then communicate with) a tag minimizing the impact of the tag orientation.

Our transmitter is composed of an arbitrary waveform generator which outputs commands and data at the baseband frequency according to the pulse-interval encoding (PIE) and phase-reversal amplitude shift keying (PR-ASK) modulation (as detailed into the EPC C1G2 specification [18]), and of a mixer that upmixes the baseband signal to the chosen carrier frequency. After the final amplification stage and considering the antenna gain, the nominal transmission power is 29 dBm. The chosen carrier frequency is 866.7 MHz (corresponding to channel 6, band 2, of the ETSI EN 302 208 regulations [20], which define 10 channels of 200 KHz @ 2W ERP between 865.6 and 867.6 MHz). Commands and data are loaded into the arbitrary waveform generator as sequences of samples with sampling rate and resolution equal to 600 KS/s and 12 bits, respectively.

Our receiver is based on a direct-conversion I/Q demodulator [15] and two analog to digital converters (ADC). The phase of the tag reflection (i.e., the backscatter signal) is not predictable or controllable, as it varies with the distance to the tag; the I/Q demodulator allows the reception of a backscatter signal regardless of the distance to the tag. To finally acquire the tag backscatter signal, we convert it into the digital domain using two ADCs with sampling rate of 1 GS/s and 8-bit resolution.

The positions of the transmitting and receiving antennas and of the tags that we considered in our experiments are shown in Figure 3. The acquisition antennas are placed vertically (z-axis) one above the other, at 0.5 m and 1 m from the ground, respectively. In their nominal position, the tags are positioned equidistantly between the two antennas along the z-axis, centered on the antennas on the x-axis, and at a distance of 0.8 m. The tag nominal position is therefore (0, 0.8, 0.75).

3.2 Performed Experiments

Our experiments are based on the interaction between a reader and a tag population that is used for inventorying purposes as de-

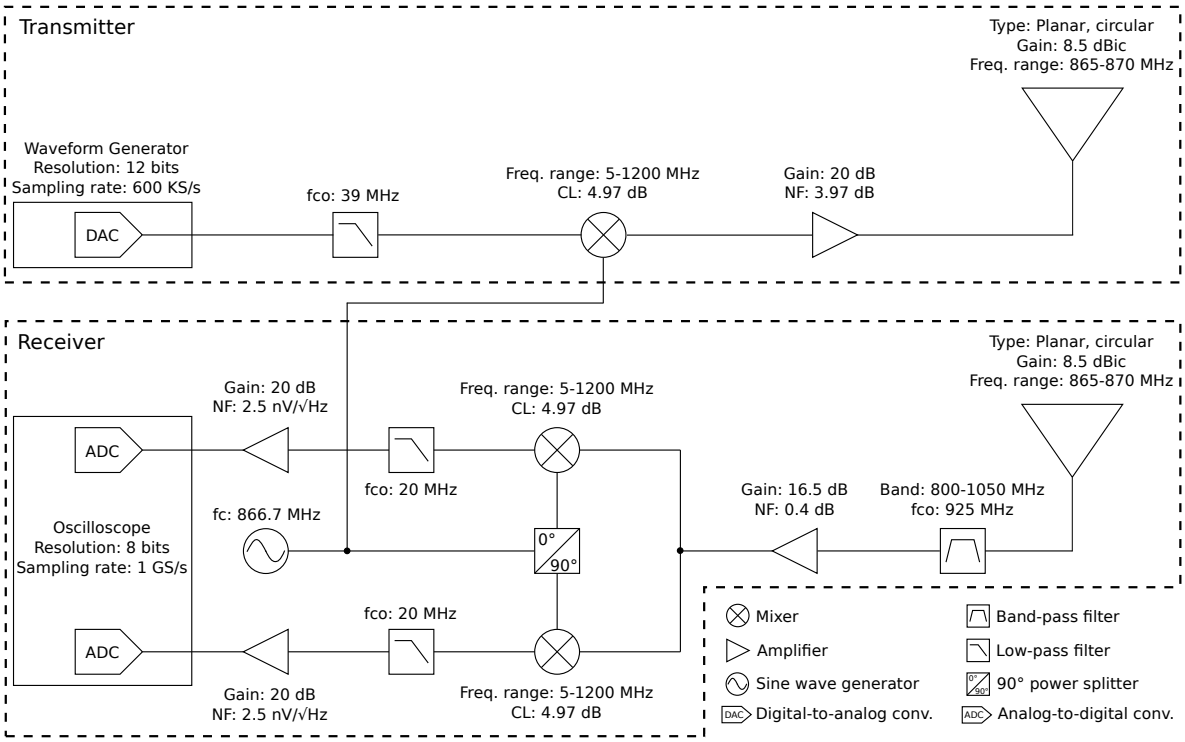

Figure 2: Block diagram of our acquisition setup.

fined in the EPC C1G2 specification [18]. The communication sequence between a reader and a tag with no collisions is shown in Figure 4. The reader challenges the tag with a set of commands to select a particular tag population (*Select*), to initiate an inventory round (*Query*), and to request the transmission of a tag's identification (EPC) number (*Ack*). The tag replies first with an RN16 packet (after the reader's Query) and then with an EPC packet (after the reader's Ack). We extracted signal features (fingerprints) from the tags' replies, more specifically from the fixed preamble of the

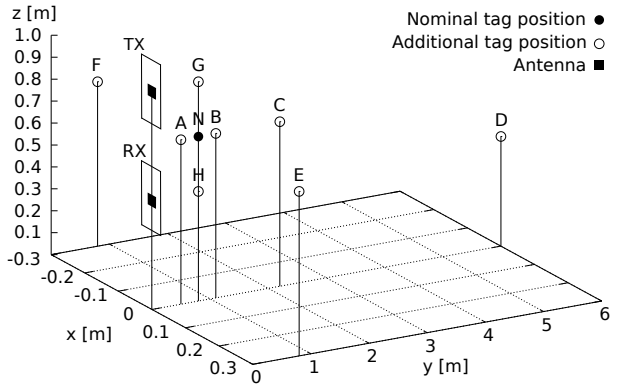

Figure 3: Considered positions of the acquisition antennas and of the tags. In our experiments, acquisition antennas (TX and RX) are fixed, while tag responses are acquired from different tag locations (A-H and N).

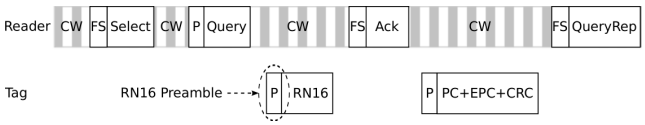

Figure 4: EPC inventory sequence. P, FS, and CW stand for preamble, frame-sync, and continuous wave respectively.

RN16 packet[1]. This was done to not introduce any data-dependent bias in our identification, since the RN16 preamble is fixed for all tags.

Our tag population is composed of 70 tags of 3 different models and manufactures: ALN9540, AD833, and UPM Dogbone. Tags from the same model were taken from the same roll. The selected models present differences in the embedded integrated circuits, antenna sizes and materials, and applications[2].

For all the tags in our tag population, we collected the preambles of RN16 reply packets. In our experiments, we varied tag positions (Figure 3) as well as challenged tags at different power levels and to backscatter data at different link frequency.

According to the EPC C1G2 specification [18], the reader can specify the backscatter link frequency (BLF, i.e., the tag data rate) through a parameter called *TRcal*; Table 1 shows the selected TRcal times for our experiments and their corresponding BLF, frequency tolerances, and frequency variations during backscatter according to the EPC C1G2 specification. We note that the relatively large BLF tolerance and variation during backscatter may represent a distinguishing factor between different tags. We expect the varia-

[1]RN16 packets are transmitted by the tags as a part of the anti-collision protocol that is used during tag inventorying [18].
[2]Datasheets can be found online [3–5].

tion in BLF tolerance and variation during backscatter to be higher when tags are requested to backscatter at an out-of-specification BLF, since the manufacturers mainly focus on tag responses within the specified frequency range. Therefore, in order to increase the possibility of finding distinguishing characteristics, we challenged tags with out-of-specification TRcal times. For this experiment, we selected subsets of tags from all three tag models. The acquisition setup was configured as detailed in Section 3.1 and tags were placed at the nominal position (Figure 3 and Table 2 – configuration 0).

For a subset of tags of one model, we acquired the preamble of the RN16 packet by challenging tags to backscatter at one selected link frequency, but varying the position of the tags, the tag orientation, and the transmission power of our acquisition setup for a total of 10 different configurations (summarized in Table 2 – configurations 1 to 10). For the tag position, we considered location points that are representative of the tag being on the right, left, closer to the reader antennas, and further away to the reader antennas. Therefore, we run four experiments by varying the tag distance (y-axis) to the antennas (between 0.5 and 6 m), two experiments by varying the tag vertical position (z-axis, between 0.5 and 1 m), and two experiments by varying the tag lateral position (x-axis, between -0.3 and 0.3 m). For tag orientation, we run one experiment by rotating the tag by 90° with respect to the y-axis. In terms of transmission power, we run one experiment by decreasing it by a factor of 4 (from 29 to 23 dBm). Although several other tag orientations and transmission powers could be explored, those will only affect the amount of power transferred from the reader to the tag and viceversa. The considered location points already represent different cases of power transfer.

3.3 Collected Data

Using our setup, we performed the experiments described in Section 3.2 and collected RN16 preambles. Each collected RN16 preamble is a fixed sequence of 16 data-0 symbols, which, according to the selected tag encoding scheme (i.e., Miller encoding with 4 subcarrier [18]), corresponds to 64 square wave cycles (duty cycle equal to 50%). In Table 3, we summarize the data that we collected, represented in a form of datasets.

Dataset 1 contains tag responses from 50 different ALN9540 tags. For each tag and one selected TRcal (equal to 15 μs), we collected 100 RN16 preambles. This dataset is used in Section 5.2 to evaluate the identification and classification accuracies of the proposed physical-layer identification techniques (detailed in Section 4) for a population composed of same model, same manufacturer tags. Dataset 2 contains tag responses from 10 different ALN9540 tags (randomly selected among the 50 tags used for dataset 1). For each tag and for 10 different configurations (Table 2, configurations 1 to 10), we collected 100 RN16 preambles, for a total of 1000 RN16 preambles per tag. This dataset is used in Section 5.3 to estimate the stability of the proposed techniques with respect to different configurations of tag position, orientation, and transmission power. Datasets 3, 4, and 5 contain tag responses from 3 models, 10 tags for each model. For each tag and for each of the six selected TRcal (Table 1), we collected 100 RN16 preambles, for a total of 600 RN16 preambles per tag. These datasets are used in Section 5.4 to analyze the classification accuracy between different tag models and within each model, as well as to validate the accuracy of the proposed techniques for different TRcal values.

Data collection was performed over two weeks, one tag at the time, 100 RN16 preamble acquisitions in a row, in a indoor, RF noisy environment with active Wi-fi, GSM, and Bluetooth networks and with other objects nearby. Between two acquisitions, tags are powered-down and considered fully discharged[3]. Unless otherwise indicated, acquisition setup and tags were in the nominal configuration (i.e., Table 2 – configuration 0). In order to speed up the acquisition process, we shortened the aforementioned inventorying sequence as shown in Figure 1: the considered acquisition sequence is only composed of *Select* and *Query* commands as reader challenge and the RN16 packet as tag response (i.e., the tag's identification (EPC) number is not requested and therefore not acquired). Within our setup, a single RN16 preamble acquisition takes 10 ms (including challenge, tag response, and discharge time of the tag).

Table 1: Selected TRcal times and related backscatter link frequencies (BLF), BLF tolerances, and BLF variations.

TRcal [μs]	BLF [KHz]	Freq. tolerance	Freq. variation during backscatter
15[1]	1422	-	-
17[1]	1255	-	-
33.3	640	+/- 15%	+/- 2.5%
83.3	256	+/- 10%	+/- 2.5%
225	95	+/- 5%	+/- 2.5%
250[1]	85.3	-	-

[1] Those TRcal values are out-of-specification, therefore the given BLF are only estimated.

Table 2: Varied parameters for the different configurations.

Config.	Tag position Fig. 3	Tag position (x,y,z)-axis [m]	Tag orientation	TX power [dBm]
0	N	(0, 0.8, 0.75)	0°	29
1	A	(0, 0.5, 0.75)	0°	29
2	B	(0, 1.1, 0.75)	0°	29
3	C	(0, 2.2, 0.75)	0°	29
4	D	(0, 6, 0.5)	0°	32[1]
5	E	(0.3, 0.8, 0.75)	0°	29
6	F	(-0.3, 0.8, 0.75)	0°	29
7	G	(0, 0.8, 1)	0°	29
8	H	(0, 0.8, 0.5)	0°	29
9	N	(0, 0.8, 0.75)	90°	29
10	N	(0, 0.8, 0.75)	0°	23

[1] Due to the larger distance (6 m) between tags and antennas in this configuration, in order to power up the tags the transmission power is increased by a factor of 2.

4. FEATURE EXTRACTION AND MATCHING

The goal of the fingerprinting features is to obtain distinctive fingerprints from the signals collected in the proposed experiments. Here, we detail the extraction and matching procedures of two types of features: time domain features (Section 4.1) and spectral PCA features (Section 4.2). The feature extraction is based on the fixed RN16 preamble in order to avoid any data-dependent bias in our evaluation.

[3]According to the EPC C1G2 specification [18], the maximum fall time for the reader power-down RF envelope is 0.5 ms and the reader shall remain powered off for at least 1 ms before powering up again. After the tag response, we provide a 2 ms discharge time where no RF signals are transmitted to the tag.

Table 3: Collected data.

Dataset	Model	# tags	# acquired RN16 preambles per tag and TRcal	Considered TRcal	Considered configurations	Total # acquired RN16 preambles per tag
1	ALN9540	50	100	1 (15)	1	100
2	ALN9540	10	100	1 (15)	10	1000
3	ALN9540	10	100	6 (15, 17, ..., 250)	1	600
4	AD833	10	100	6 (15, 17, ..., 250)	1	600
5	Dogbone	10	100	6 (15, 17, ..., 250)	1	600

4.1 Time Domain Features

In this section, we describe the extraction and matching procedures for fingerprinting features in the time domain, namely the time interval error (TIE) and the average baseband power ($\bar{P}_B$). We also investigated the use of additional timing features, such as the signal rise and fall times and the time from the reader's transmission to the tag's response. These timing features, however, performed poorly in both classification and identification, hence in this work we focus on the time interval error and the average baseband power from the time domain characteristics.

4.1.1 Time Interval Error

The time interval error (TIE) measures how far each active edge of the clock varies from its ideal position. To measure the TIE, the ideal edges must be known or estimated. Figure 5 shows part of the RN16 preamble of an UHF RFID tag and the time interval error computed by using a fixed reference clock on a number of consecutive clock cycles. We observe a constant increase of TIE, i.e., constant first derivative ∂_{TIE}. We therefore define ∂_{TIE} as a feature for fingerprinting UHF RFID tags. In fact, in our particular case, the ∂_{TIE} is proportional to the tag backscatter link frequency.

Since the TIE measurements demonstrated precise and stable behavior, i.e., no significant outliers, we used a standard linear least square fitting algorithm (LSF) to determine ∂_{TIE}. More precisely, we fit a line $y = a \cdot x + b$ to the set of TIE points $\{(x_i, y_i) : i \in \{1, ..., C\}\}$, by minimizing the least square error. Here C is the number of clock cycles used to fit the line, x_i is the index of the clock cycle, and y_i is the TIE at clock cycle i. The ∂_{TIE} is the fitted line coefficient a.

For each cycle i, we computed TIE_i with respect to the 10% of the cycle step height, i.e., at $0.1 \cdot (A_i - B_i) + B_i$, where B_i and A_i are the average low-state amplitude and the average high-state amplitude of the baseband signal for cycle i, respectively (Figure 5). For more accurate approximation of ∂_{TIE} we used all (64) clock cycles in the preamble part of the tag response.

It should be noted that the notions of time interval error and ∂_{TIE} are close to the notion of clock offset and clock skew as in [26, 34]. The difference resides in the communication layer used for measurement. We measured the time interval error on the physical-layer signal, while in [26, 34], the clock offset/skew was derived from timestamps available at upper-layer protocols (e.g., TCP). Such timestamp information however is not available in EPC RFID communication and therefore cannot be used.

4.1.2 Average Baseband Power

We define the average baseband power $\bar{P}_B$ as the average power of an acquired RN16 preamble. The average is computed by considering each cycle in the acquired baseband signal such as $\bar{P}_B = \frac{1}{C} \cdot \sum_{i=1}^{C} P_{B,i}$, where C is the number of clock cycles and the average baseband power for a cycle i is $P_{B,i} = \frac{1}{2} \cdot (A_i - B_i)^2$.

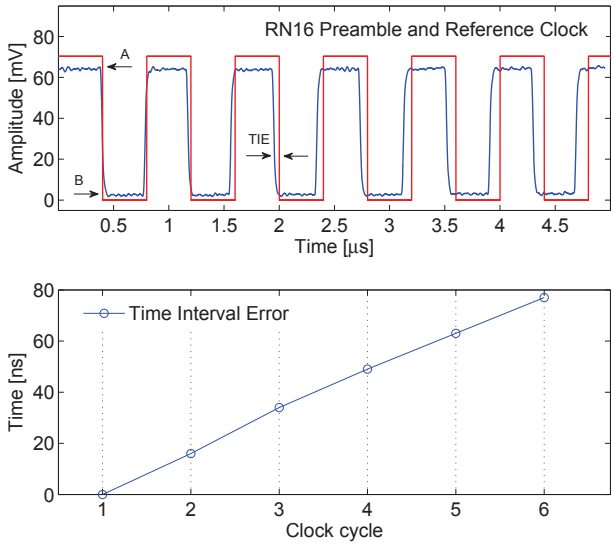

Figure 5: The preamble of the tag response and its corresponding time interval error (TIE) with respect to a reference clock. The TIE is the difference between the edges of the tag signal and the reference clock. We observe a linear increase of TIE.

The average baseband power relates to the backscatter power transferred from the tag to the reader during data modulation, i.e., when the tag modulates the RF carrier from A to B and vice-versa (Figure 5). The modulation backscatter power is given, among other parameters, by the reflection coefficients of the tag antenna, which are determined by the input impedance of the tag antenna and the input impedance of the RF port of the tag embedded integrated circuit [22].

4.1.3 Feature Combination and Matching

Given that the ∂_{TIE} and the average baseband power $\bar{P}_B$ are 1-dimensional features, for the purposes of classification and identification we also combine them in a 2-dimensional feature vector $[\partial_{TIE}, \bar{P}_B]$. We denote this feature combination as $(\partial_{TIE}, \bar{P}_B)$.

For evaluation, reference and testing device fingerprints are built from a number N of acquired RN16 preambles. Each device fingerprint is the value of a selected feature, ∂_{TIE}, $\bar{P}_B$, or $(\partial_{TIE}, \bar{P}_B)$, averaged over N. For matching two fingerprints, i.e., computing the similarity score between reference and testing fingerprints, we used Euclidean distance.

4.2 Spectral Features

Statistical spectral features for identification were initially proposed in [12, 13]. We used the feature extraction and matching

methods described in [12]. Here, we briefly discuss them for completeness. First, we separated the RN16 preamble of each collected sampled signal into single clock cycles and then computed the spectral features for each of those clock cycles. The final fingerprint of each RN16 preamble was formed by computing the average of the spectral features of all single clock cycles. This procedure is similar to the computation of ∂_{TIE}, where we used a linear regression over all clock cycles in the RN16 preamble. The advantage of this approach is that it allowed us to work on low dimensional data which is suitable for standard PCA analysis as opposed to [12].

5. PERFORMANCE RESULTS

In this section, we present the evaluation of the classification and identification accuracies obtained by using each one of the four proposed features, i.e., ∂_{TIE}, $\bar{P}_B$, $(\partial_{TIE}, \bar{P}_B)$, and spectral features. First, we review the metrics that we used to evaluate the classification and identification accuracy. Then, we elaborate on the achieved results and summarize the main outcomes of our experimental analysis.

5.1 Evaluation Metrics

We evaluate our feature accuracy in terms of classification and threshold-based identity verification. We also compute the entropy of the probability distribution of selected features.

For evaluation of the classification capabilities of our features, we adopt the classification success rate metric. We compute it as follows. Each individual tag (or tag model) is considered as a separate class. A reference fingerprint of each class is then computed and stored. During classification, unknown testing fingerprints are assigned to one of the classes according to the k-Nearest Neighbor rule[4]. The percentage of correctly assigned testing fingerprints to their respective classes is our classification success rate.

For identity verification (identification), we adopted the Equal Error Rate (EER) as a single metric since it is a widely agreed metric for evaluating such systems [9]. We estimate the EER as follows. We compute the similarity score between all testing and reference fingerprints from all tags. We then separate these scores in two categories: genuine and imposter. The genuine category includes all scores from matching two fingerprints from the same tag. The imposter category contains all scores from comparing two fingerprints from different tags. Given that each score represents the similarity between two fingerprints (identities), we compute the rate of falsely rejected and falsely accepted tags using a threshold score value. The scores from the genuine category that are above this threshold indicate the number of false rejects or the False Reject Rate (FRR), while the scores from the imposter category that are below the threshold indicate the number of the false accepts or the False Accept Rate (FAR). The EER is the error rate where both FAR and FRR are equal. The value of the threshold at the EER is our threshold T for an accept/reject decision.

For our 1-dimensional features, we compute the entropy of the corresponding probability distribution in order to show how many bits of information are contained within that distribution. To compute the entropy, we consider bins of width equal to the average variance of the features in the dataset and count the number of fingerprints that fall in the different bins. We then apply the standard entropy formula [42]. We note that for higher dimensional features, computing the entropy can be misleading due to the small size of our dataset and the curse of dimensionality [8].

[4]It should be noted that more sophisticated classifiers can be devised such as Support Vector Machines (SVM) and Probabilistic Neural Networks (PNN) [8]. Due to more complicated training procedures, we do not consider them in the present work.

Table 4: ALN9540 - Classification accuracy - 50 tags.

Feature	Class. Succ. Rate (%)	Entropy [bits] (empirical)	(theory)
∂_{TIE}	71.4 (69.7; 73.0)	5.84	7.08
$\bar{P}_B$	43.2 (38.6; 47.7)	4.57	6.02
$(\partial_{TIE}, \bar{P}_B)$	98.7 (98.0; 99.4)	-	-
Spectral	99.6 (99.3; 99.9)	-	-

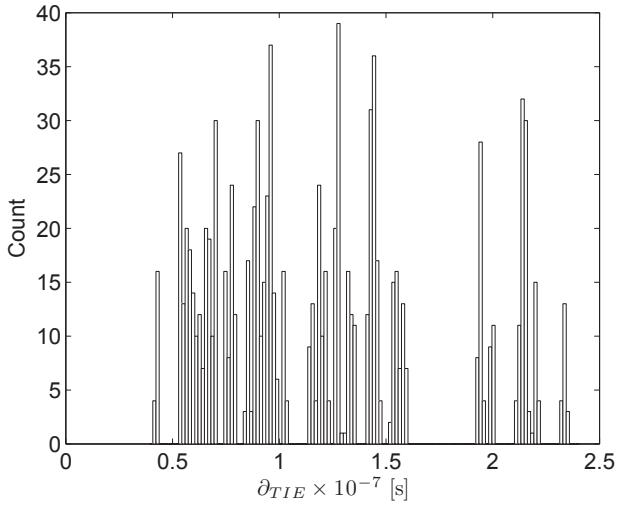

Figure 6: Distribution of ∂_{TIE} for the 50 identical ALN9540 tags in a form of histogram. The total of 1000 fingerprints (20 per tag for $N = 5$) are used to fill in the histogram bins.

5.2 Recognition Accuracy

In this section, we analyze the accuracy of our proposed features for classification and threshold-based identity verification (identification). For accuracy estimation, we used dataset 1 (Table 3) which contains 5000 RN16 preamble acquisitions from 50 identical (same model and manufacturer) tags. We used a 5-fold cross validation [8] in order to validate the error rates. For each tag (100 acquisitions), the set was split in 5 independent folds; one fold (20 acquisitions) was used for training and the remaining four folds (80 acquisitions) were used to form the testing device fingerprints. The training and testing data were thus separated.

Table 4 shows the classification success rates and confidence intervals for the proposed features. The number of acquisitions that were used to build a device fingerprint was fixed to 5 ($N = 5$) and classification was performed with the 3-Nearest Neighbor rule[5]. The ∂_{TIE} achieves an accuracy of approximately 71%.

Given that the classification accuracy is dependent on the number of evaluated tags, we estimated the entropy in bits from the empirical distribution of ∂_{TIE} obtained from our investigation over 50 tags (Figure 6). Additionally, we computed its theoretical maximum, i.e., the maximum number of information bits that could be

[5]Typical choices for k are 1, 3, 5, and 7. In our case, $k = 3$ provided a good benchmark given that the estimated accuracy showed higher variance for $k = 1$ and did not significantly improve for $k \geq 5$.

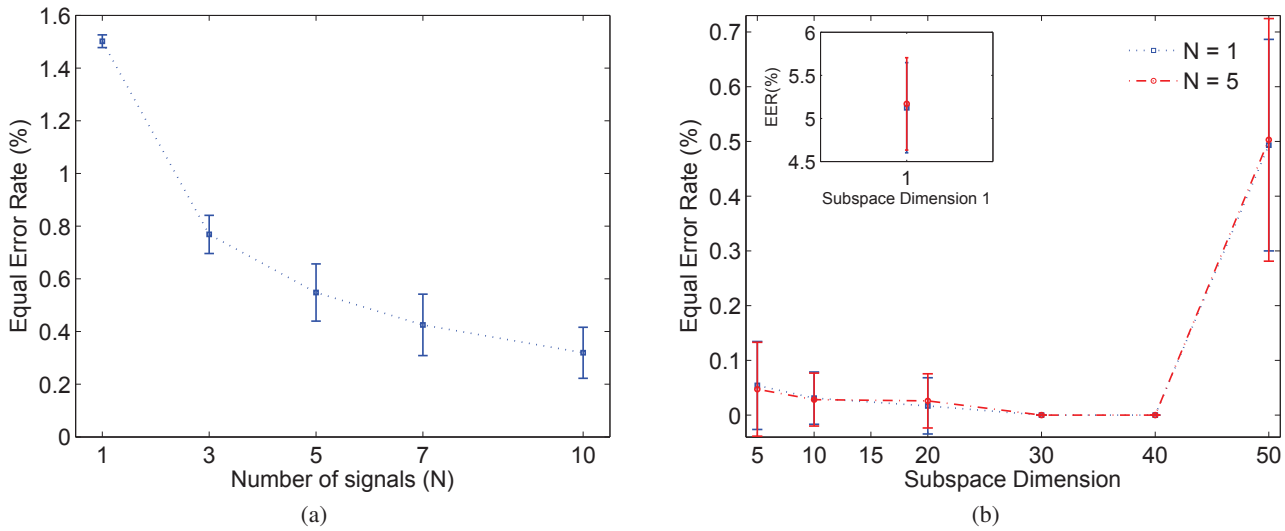

Figure 7: Identification accuracy of (a) the $(\partial_{TIE}, \bar{P}_B)$ feature for different number of RN16 preambles (signals) N used to build the fingerprints and (b) the spectral features for different N and subspace dimensions. The computation is performed on the 50 identical (same manufacturer and model) tags.

learned from ∂_{TIE}, with respect to the empirical distribution and the maximal allowed backscatter link frequency (BLF) tolerance as defined in the EPC C1G2 specification [18]. The entropy results based on the empirical distribution suggest that we could learn 5.84 bits of information about an UHF RFID tag (Table 4). The entropy depends only on the variations of ∂_{TIE}, which relate to the BLF tolerances. Considering the ∂_{TIE} distribution (Figure 6), we observe a BLF tolerance of $\pm 14.01\%$ around a mean BLF of approx. 1400 KHz (for the considered TRcal, we estimated a BLF equal to 1422 KHz, Table 1). Given this measured tolerance, the maximum possible entropy would be 7.08 bits[6]. If considering the maximal allowed BLF tolerance as defined in the EPC C1G2 specification, i.e., $\pm 22\%$ for BLF equal to 320 KHz, the maximum possible entropy would be 9.86 bits. Although this last result seemed very promising, we could not observe such a large tolerance within our tag population. We later further show that ∂_{TIE} is stable across different locations and distances to the reader of up to 6 meters. The implications of these results are discussed in Section 6.

The average baseband power ($\bar{P}_B$) feature shows a significantly lower accuracy on its own, but performs well when combined with ∂_{TIE} (98.7%). The empirical entropy is 4.57 bits and the maximum entropy 6.02 bits[7]. This shows that there is much less uncertainty in the baseband power compared to ∂_{TIE}. The spectral features score the highest classification success rate of 99.6%. Those results motivated us to explore the accuracy of the two most discriminative features, i.e., the combined $(\partial_{TIE}, \bar{P}_B)$ and the spectral features, in the case of tag identity verification (identification).

For the combined $(\partial_{TIE}, \bar{P}_B)$ feature we varied the number of acquired RN16 preambles N over which we average to obtain the testing device fingerprint. The reference device fingerprint is obtained by averaging over all acquisitions in the training set (20 acquisitions). The results of the analysis for $N = 1, 3, 5, 10$ acquisitions are shown in Figure 7(a). The Equal Error Rate (EER) gradually decreases with higher averaging factor N reaching an EER = 0.5% approximately. This means that by using these combined features, our system can verify the identity of individual identical tags with an accuracy of 99.5% (genuine accepts), while allowing 0.5% of false rejects. For the EER estimation, we approximated the genuine and imposter score distributions. For example, in the case of $N = 5$, each fold contains 4 fingerprints, for a total of 16 testing fingerprints (4 folds). For 50 tags, this results in 800 genuine and 39200 imposter matching scores.

For the spectral features we varied two parameters, the number of RN16 preambles N and the dimensionality of the PCA subspace. As shown in Figure 7(b), the averaging factor N does not have an effect as opposed to the subspace dimensionality. The most discriminative subspaces are to be found in subspaces with dimensionality 5 to 40. For dimensionality 30 and 40, the EER = 0%. Higher dimensionality subspaces degrade the accuracy, most probably due to noisy eigenvector components. While this result demonstrates the discriminant capabilities of the spectral features, a larger dataset of hundreds of tags is required in order to have a more accurate estimate of the EER.

In summary, we observe that a combination of only 2 features, i.e., ∂_{TIE} and the average baseband power $\bar{P}_B$, provides high identification accuracy in terms of EER. The spectral features further decrease the EER to 0%.

5.3 Feature Stability

In the previous section, we have analyzed the classification and identification accuracies of our proposed features. This allows us to have a benchmark for estimating the stability of those features with respect to different configurations of tag position, orientation, and transmission power (Table 2). In this section, we evaluate:

1. The stability of the proposed features to different configurations by using datasets 1 and 2 (Table 3). First, we extract the reference fingerprints from dataset 1 (which contains RN16 preambles from 50 tags) for the same set of 10 tags deployed to collect dataset 2. Then, we compute the testing fingerprints from all the different configurations and

[6]The maximum possible entropy is achieved when the probability distribution of ∂_{TIE} is assumed to be uniform [23].

[7]The maximum possible entropy according to the standard specification could not be computed because no tolerances on the baseband power are included.

Table 5: Feature stability - ALN9540 - 10 tags

Feature	Classification Success Rate (%) Nominal configuration	Different configurations	Reduced sampling rate (100 MS/s)
∂_{TIE}	99.8 (99.5; 100)	96.4 (95.01; 97.86)	99.88 (99.49; 100)
$\bar{P}_B$	64.6 (56.9; 72.3)	15.92 (14.49; 17.35)	60.25 (54.28; 66.22)
$(\partial_{TIE}, \bar{P}_B)$	100 (100; 100)	36.24 (26.73; 45.75)	100 (100; 100)
Spectral	100 (100; 100)	37.6 (18.5; 56.8)	100 (100; 100)

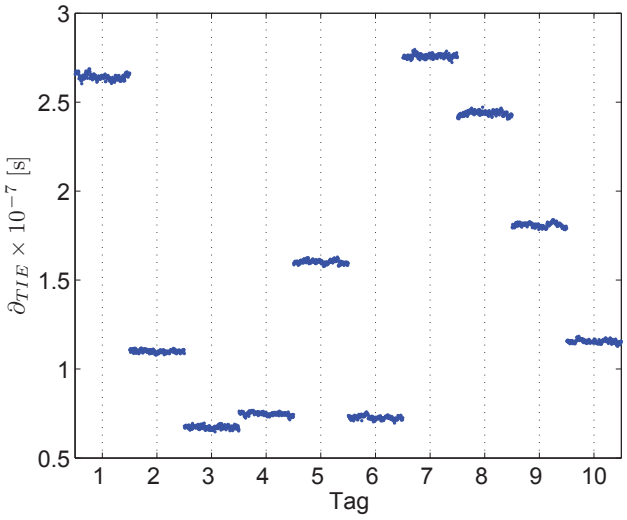

Figure 8: Visualization of ∂_{TIE} of 10 randomly selected ALN9540 tags. 220 fingerprints (11 configurations x 20 fingerprints) are displayed for each tag ($N = 5$). ∂_{TIE} is stable across all configurations.

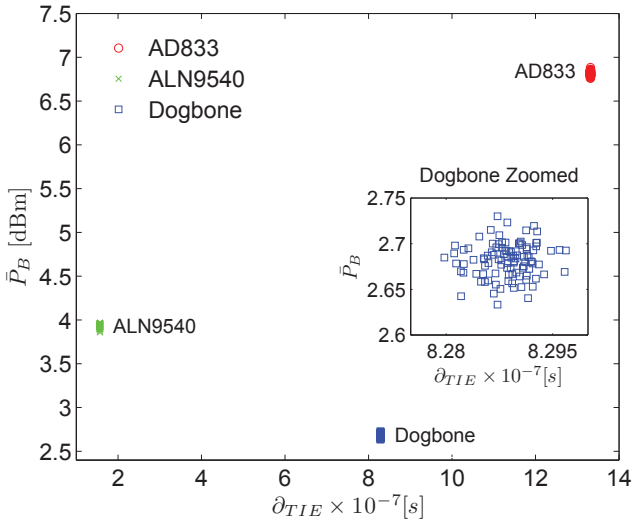

Figure 9: The fingerprints of the 3 models (AD833, Dogbone, and ALN9540) clustered in separate regions by using ∂_{TIE} and the average baseband power $\bar{P}_B$.

tags in dataset 2, and classify them to the reference fingerprints. The classification success rate of this analysis is compared to the classification success rate for the selected 10 tags computed from dataset 1 (i.e., in the nominal configuration, Table 2 – configuration 0).

2. The stability of the proposed features to a reduced sampling rate. First, we downsample by a factor of 10, i.e., from the nominal sampling rate of 1 GS/s to 100 MS/s, the collected signals in dataset 1 for the same set of 10 tags deployed to collect dataset 2. Then, we extract the reference and testing fingerprints from the downsampled signals and evaluate the classification accuracy. The classification success rate of this analysis is compared to the classification success rate for the selected 10 tags computed from dataset 1 (i.e., at 1 GS/s).

For all the proposed features, Table 5 compares the classification success rates and confidence intervals for the selected tags in the nominal configuration with the rates of the stability analysis for different configurations and reduced sampling rate (for this analysis, N was set to 5).

The obtained results demonstrate that the ∂_{TIE} feature is stable across all configurations. Figure 8 visually illustrates ∂_{TIE} for the selected 10 tags. For each tag, the figure shows all 220 fingerprints ($N = 5$) from the 11 configurations in Table 2 (20 fingerprints for each configuration). Very small variability can be observed.

On the negative side, the average baseband power, the combination of time interval error and average baseband power, and the spectral features significantly reduced their corresponding discriminant capabilities. This result shows that while those features in the considered signals are unique within a fixed tag position, orientation, or transmission power, they change across different configurations of these parameters. We discuss the impact of these limitations on applications in Section 6.

Considering the stability of the proposed features to a lower sampling rate, the obtained results demonstrate that our features are stable when reducing the sampling rate from 1 GS/s to 100 MS/s. We discuss the impact of this result in Section 5.5.

5.4 Accuracy on Different Models

In this section, we present accuracy results on our 3 different models (datasets 3-5). We analyze the classification accuracy between the models (model distinction) and within each model. We also validate the accuracy of our features for different TRcal values.

In terms of the ability to classify different models, all features perform equally well with a success rate of 100%. For the time domain features this is due to the good discriminant capabilities of both ∂_{TIE} and $\bar{P}_B$, which show perfect and distant boundaries between the three models. This is visualized for these two features in Figure 9. Given the stability results (Section 5.3), the ∂_{TIE} feature is also a good candidate for model distinction independently of the location and distance to the reader. We acknowledge, however, that we need to consider a larger set of models in order to more precisely estimate the classification accuracy across models and possibly compute the entropy (Section 5.2).

The ability of the proposed features to distinguish devices within the same model for different TRcal is summarized in Tables 6(a), 6(b), and 6(c). The ∂_{TIE} feature shows on average an accuracy of 80-100% for the selected TRcal, i.e., between 8 and 10 tags are correctly classified within each model. We observe that the accuracy is higher compared to the analysis on the 50 tags (Table 4). This is most likely due to the smaller tag set used in this analysis. Nevertheless, this result clearly shows that the time interval error can equally be exploited on different models.

The average baseband power ($\bar{P}_B$) feature varies depending on the model. While its accuracy is comparable for Dogbone and ALN9540, it is very high on AD833 (90-100%). In line with the results in Section 5.2, the combined feature ($\partial_{TIE}, \bar{P}_B$) shows high classification accuracy on each model. The spectral features also perform very well irrespective of the model. This result shows that our proposed features work on different models of UHF RFID tags.

We note that, although in some case out-of-specification TRcal times lead to a more accurate classification, it is not possible to generalize this for all combinations of models and features. Similarly, no generalization can be done on the relationship between classification accuracy and TRcal length.

5.5 Discussion

The results of our work show that we can learn approx. 6 bits of information about an UHF RFID tag by only observing the time interval error (TIE). This information can be extracted independently of the tag position (distances up to 6 meters), orientation, or transmission power. The stability of the TIE across different configurations is due to the origin of TIE variability, namely the tag local oscillator.

For more accurate identification of individual tags, we observed other physical characteristics such as average baseband power and spectral features. We demonstrated that a combination of only two physical-layer parameters, i.e., TIE and average baseband power, can accurately identify same model and manufacturer tags with EER = 0.5%. The spectral features further decrease the EER to 0%. We acknowledge that a larger dataset of hundreds to thousand devices is required to give a better estimate of the operational EER. The main drawback of the above features is their instability to tag position, orientation, and transmission power. In contrast to the TIE, the average baseband power and spectral features are bound to particular tag antenna reflection characteristics, which themselves are sensitive to position, orientation, and transmission power. Future work is needed to better quantify these effects and propose appropriate measures. Moreover, the impact of other factors like temperature variation, different acquisition setups, and tag motion needs to be quantified.

In addition to identification accuracy, the design specification of an identification system will usually include requirements for computational speed and system cost [9]. Computational speed refers to how fast an identification system makes the accept/reject decisions, which affects the scalability of the system from small populations to large populations. Our techniques obtain high accuracies by using a minimum of one (for spectral features) and a maximum of 5 (for the ($\partial_{TIE}, \bar{P}_B$) feature) RN16 preambles. A RN16 preamble is acquired in 10 ms (Section 3.3). Therefore, considering data processing (i.e., the feature extraction process) as negligible[8], our techniques can process between 20 and 100 tags/s. We note that the RN16 preamble acquisition time can be reduced as the backscatter link frequency increases. For TRcal equal to 15 μs, we can reduce this time by half, doubling the acquisition speed.

In physical-layer identification the quality of the obtained fingerprints and the computational speed are related to the system cost. In our acquisition setup, the cost is mainly affected by the acquisition of the RN16 preambles (operated by an oscilloscope), which requires a sampling rate of 1 GS/s. However, we showed that is possible to reduce this sampling rate to 100 MS/s with no impacts on the identification accuracy. This allows us to lower the system cost by deploying less expensive acquisition setups that use for example USRP platforms [6].

[8]The time length of the RN16 preamble for TRcal equal to 15 μs is about 48 μs, which at a sampling rate of 100 MS/s makes the number of samples to process equal to 4800. Considering the relatively short length and size of this digital signal, we assume the process time as negligible when compared to the acquisition time.

Table 6: Classification accuracy - 3 models.

(a) AD833 - Classification Success Rate (%) - 10 tags.

	TRcal [μs]					
Feature	15	17	33.3	83.3	225	250
∂_{TIE}	72.5	79.6	70.9	84.5	89.4	76
$\bar{P}_B$	99.9	99.0	100	98.1	94.9	100
($\partial_{TIE}, \bar{P}_B$)	99.9	99.6	100	99.8	98.5	98.5
Spectral	100	100	99.9	100	100.0	99

(b) Dogbone - Classification Success Rate (%) - 10 tags.

	TRcal [μs]					
Feature	15	17	33.3	83.3	225	250
∂_{TIE}	72.4	73.0	75.8	81.3	71.9	75.1
$\bar{P}_B$	53	87.5	72.5	62	77.9	66.1
($\partial_{TIE}, \bar{P}_B$)	93	100	99	94.6	97.4	92.1
Spectral	96.9	100	100	97.8	98.3	96.8

(c) ALN9540 - Classification Success Rate (%) - 10 tags.

	TRcal [μs]					
Feature	15	17	33.3	83.3	225	250
∂_{TIE}	99.6	85.5	87.1	86	53.5	59.3
$\bar{P}_B$	72.6	92.4	80.4	80.1	94.4	87.4
($\partial_{TIE}, \bar{P}_B$)	100	92.9	100	100	95.6	83.4
Spectral	100	97.8	100	100	99	96.5

6. IMPLICATIONS OF UHF RFID TAG IDENTIFICATION

In this section, we discuss the implications of our physical-layer identification and classification techniques on the privacy of tag holders and the application of those techniques to cloning detection in RFID-enabled supply chains.

6.1 Breaking Tag Holder Privacy

RFID technology has raised a number of privacy concerns in many different applications, especially when considering consumer privacy [29]. A person carrying several tags – attached to various objects like books, passport, medicine, medical devices, and clothes – can be subject to clandestine tracking by any reader in the read range of those tags. Although some objects may be only temporarily with a person (e.g., a shopping bag), others may be carried

for a longer time (e.g., a book) or even permanently (e.g., medical devices), allowing clandestine tracking over wider time periods.

Although solutions that prevent a (clandestine) reader to communicate with tags at the physical layer exist (e.g., by "killing" tags or by putting them to "sleep", or by using Faraday cages, active jammers, or "clipped" tags [32]), the provided privacy comes at the price of tag functionality. Several solutions that guarantee both privacy against clandestine tracking and tag functionality have been proposed [44]. Those mainly exploit tag identification number pseudonymity by means of cryptographic techniques like public-key algorithms, symmetric-key primitives, pseudo-random number generators, and hash functions [7, 14, 16, 35]. However, the proposed solutions consider protection measures on the upper (logical) layers; physical-layer identification techniques can invalidate those protection measures by identifying devices on the physical communication layer.

In a scenario in which the target person carries several tags, a relatively low identification accuracy (per tag) may be enough to break privacy: besides the fact that privacy can be compromised by having only weak evidence of someone being at a certain place, combining the identification information from several tags will significantly reduce a person's privacy. Our TIE-based technique provides $b = 5.84$ bits of information for each tag, i.e, when individually considered, a maximum of $n = \lfloor 2^b \rfloor$ tags can be uniquely identified. As a consequence, a set composed of k tags can be uniquely identified among other $\binom{n+k-1}{k} = \frac{(n+k-1)!}{k!(n-1)!}$ sets, which provides more information and leads to a more accurate identification. For example, a set composed of 5 tags can be uniquely identified among other $6 \cdot 10^6$ sets (corresponding to 22.5 bits of information), while a set of 10 tags among other $2 \cdot 10^{11}$ sets (corresponding to 37.6 bits of information). It is clear that the identification of a person carrying several tags will be possible with a very high accuracy[9].

Therefore, our TIE-based technique allows, in fact, people profiling and clandestine tracking: an attacker only needs to profile the target once, i.e., to extract and store for each of the tags in the target's set the corresponding timing feature ∂_{TIE}, and then track it by following the set of tags. As mentioned in previous sections, identification through our TIE-based technique can be achieved independently of the location and distance to the reader from up to 6 meters, which facilitates clandestine tracking.

Defining countermeasures against unauthorized physical-layer identifications is an open issue that, given our results, needs to be addressed.

6.2 Cloning Detection in RFID-enabled Supply Chains

Within RFID-enabled supply chains, each product is equipped with an RFID tag containing a unique identifier (ID). Through an RFID infrastructure (e.g., the EPCglobal network [19]), supply chain partners can record, store, and share information associated with those IDs, and use it to automate and speed-up processes. Tag cloning may facilitate the injection of counterfeit products into legal RFID-enabled supply chains: by carrying tags containing IDs of genuine products, clones will be recognized as genuine by the RFID infrastructure (unless human inspection is performed).

Current solutions for RFID-enabled supply chains, like the aforementioned EPCglobal architecture, do not provide effective anti-cloning measures [28]. In the past years, several solutions have been proposed (e.g., [10, 14, 16, 28, 36]), but due to the limited resources and cost constraints of passive UHF RFID tags for supply chain applications, a standardizable anti-cloning mechanism is still under investigation.

Physical-layer identification provides means to detect counterfeit products by creating physical-layer fingerprints that bind the RFID tag to the claimed identity (fingerprints could then be stored in a database, e.g., maintained by the tag manufacturer, for later comparisons).

In a scenario where pallets of tagged products pass through an RFID portal for physical-layer identification, the large amount of products that need to be identified in a short time would require a high computational speed. Additionally, tagged products can be placed anywhere on a pallet and interfere with each other during wireless communication (e.g., by signal superposition or signal diffraction due to product packaging); fingerprints would then be required to be particularly stable. Moreover, identification accuracy should be particularly high: the time spent in verifying false positives will slow down the supply chain processes.

Similarly to the pallet-scenario, a physical-layer identification system for a scenario in which tagged products move over a conveyor belt would require a high computational speed and accuracy. Differently, tagged products may pass one at a time and at a fixed position through the RFID portal, reducing interferences and allowing fingerprints to be sensitive to tags' position.

Although our work shows that identifying tags with high accuracy (EER=0%) and computational speed (100 tags/s) is feasible using spectral features, our spectral-based technique is not suitable for the pallet-scenario due to its sensitivity to tags' position. Such a technique may be, however, suitable for the conveyor-scenario, where tags are identified one at a time and at a fixed position.

In summary, we show that cloning detection in RFID-enabled supply chains is feasible under certain conditions. We note that finding a highly-accurate, position-insensitive identification technique is an open issue. Similarly, security threats (and possible countermeasures) against such cloning detection systems need to be explored.

7. RELATED WORK

Physical-layer fingerprinting (identification) has been investigated on a number of hardware platforms including RFID [12, 38, 40, 41]. To the best of our knowledge, only Periaswamy et al. [38] considered identification of UHF RFID tags. The authors proposed a method to enable ownership transfer of UHF RFID tags using the minimum power response of tags as a physical-layer fingerprint. The authors considered a small set of 8 tags from 2 models and only showed visual evidence that UHF tags can be distinguished; feature stability was also not considered[10]. In comparison to the above works, our work is the first to show the existence of stable physical-layer fingerprints for distinguishing UHF RFID tags and to provide empirical and theoretical bounds about their accuracy. In addition, we validate the applicability of existing HF RFID identification techniques to UHF RFID.

In the context of HF RFID, Danev et al. [12] studied and evaluated the feasibility of using physical-layer identification to detect cloned or counterfeit HF RFID smart cards and electronic passports. The authors proposed statistical spectral features as physical-layer fingerprints. Experimental results on 50 identical smart cards

[9]The accuracy may be additionally increased by considering sets of tags composed of different tag models and manufacturers.

[10]The minimum power response provides tag's energy-harvesting information and it is usually indicated at a specified frequency and distance [45]. This implies that it varies with the distance, which makes the proposed technique working only at a fixed location. Additionally, reflective environments cause significant variations in the minimum power response [37], which may further limit the proposed technique to controlled environments.

showed an EER of 2.43% from close proximity. Similarly, Romero et al. [40] demonstrated that the magnitude and phase at selected frequencies allow fingerprinting different models of HF RFID tags. The authors validated their technique on 4 different models. Recently, the same authors extended their technique to enable identification of same model and manufacturer transponders [41]. The above works considered inductive coupled HF RFID tags and the proposed features work from close proximity.

Besides the mentioned works on RFID devices, physical-layer fingerprinting has been explored on different platforms such as VHF [43, 47], Bluetooth [24], IEEE 802.11 [11, 26, 48], and 802.15.4 (ZigBee) [13, 39]. Our proposed TIE-based feature is close to the notion of clock offset/skew proposed in [34] for fingerprinting network hosts. The difference resides in the communication layer used for measurement. We measure the time interval error at the physical layer, while in [34], the clock offset and skew are derived from timestamps in upper-layer protocols (e.g., TCP).

Here follows a brief description of other related works. Shaw and Kinsner [43] proposed to identify radio transmitters used in violation of regulations by extracting and modeling the radio transmitter (turn-on) transient for classification. Ureten and Serinken [47] used the same feature (but different feature extraction and classification methods) to identify VHF radio transmitters. Ellis and Serinken [17] studied the feasibility of visually identifying VHF radio transmitters based on amplitude and phase information contained in the transmitter transient. Hall et al. studied and evaluated radio fingerprinting for intrusion detection in both IEEE 802.11 [24] and Bluetooth [25] networks, while the amplitude and phase envelops of the transmitter transient have been used by Ureten and Serinken [48] to fingerprint IEEE 802.11b devices. Rasmussen and Čapkun [39] demonstrated the feasibility of device fingerprinting of wireless sensor nodes and discussed the implication of fingerprinting on detecting wormhole, Sybil, and cloning attacks. Brik et al. [11] considered variances in the modulation errors to fingerprint IEEE 802.11 devices, while Danev and Čapkun [13] investigated the identification of identical IEEE 802.15.4 wireless sensor nodes using temporal and spectral features of the transmitter transient.

8. CONCLUSION

In this work, we studied physical-layer identification of passive UHF RFID tags. We collected signals from a population of 70 tags using a purpose-built reader and we analyzed time domain and spectral features of the collected signals. We showed that, using time domain features, UHF RFID tags can be classified, independently of the location and distance to the reader (tested up to 6 meters), with an accuracy of approx. 71%. Additionally, we showed that is possible to uniquely identify a maximum of approx. 2^6 UHF RFID tags independently of the population size. These results show that breaking privacy at different locations and distances is possible, especially when target users carry several tags. We further showed that, in controlled environments, UHF RFID tags can be uniquely identified based on their signal spectral features with an Equal Error Rate of 0%. This result shows that cloning detection in RFID-enabled supply chains is feasible under certain conditions. The countermeasures against unauthorized physical-layer identifications remain an open problem.

9. REFERENCES

[1] http://www.icao.int/.

[2] http://www.avoine.net/rfid/index.html.

[3] http://www.alientechnology.com/.

[4] http://www.upmrfid.com/.

[5] http://www.rfid.averydennison.com/.

[6] http://www.ettus.com/.

[7] BERBAIN, C., BILLET, O., ETROG, J., AND GILBERT, H. An efficient forward private RFID protocol. In *Proc. ACM Conference on Computer and Communications Security* (2009), pp. 43–53.

[8] BISHOP, C. *Pattern Recognition and Machine Learning*. Springer, 2006.

[9] BOLLE, R., CONNELL, J., PANKANTI, S., RATHA, N., AND SENIOR, A. *Guide to Biometrics*. Springer, 2003.

[10] BOLOTNYY, L., AND ROBINS, G. Physically unclonable function-based security and privacy in RFID systems. In *Proc. IEEE International Conference on Pervasive Computing and Communications* (2007).

[11] BRIK, V., BANERJEE, S., GRUTESER, M., AND OH, S. Wireless device identification with radiometric signatures. In *Proc. ACM International Conference on Mobile Computing and Networking* (2008).

[12] DANEV, B., HEYDT-BENJAMIN, T. S., AND ČAPKUN, S. Physical-layer identification of RFID devices. In *Proc. USENIX Security Symposium* (2009).

[13] DANEV, B., AND ČAPKUN, S. Transient-based identification of wireless sensor nodes. In *Proc. ACM/IEEE Conference on Information Processing in Sensor Networks* (2009).

[14] DIMITRIOU, T. A lightweight RFID protocol to protect against traceability and cloning attacks. In *Proc. International ICST Conference on Security and Privacy in Communication Networks* (2005).

[15] DOBKIN, D. M. *The RF in RFID: Passive UHF RFID in Practice*. Newnes, 2007.

[16] DUC, D. N., PARK, J., LEE, H., AND KIM, K. Enhancing security of EPCglobal Gen-2 RFID tag against traceability and cloning. In *Proc. Symposium on Cryptography and Information Security* (2006).

[17] ELLIS, K., AND SERINKEN, N. Characteristics of radio transmitter fingerprints. *Radio Science 36* (2001), 585–597.

[18] EPCGLOBAL. UHF Class 1 Gen 2 Standard v. 1.2.0. Standard, 2008.

[19] EPCGLOBAL. *The EPCglobal Architecture Framework v. 1.3*, 2009.

[20] ETSI. *ETSI EN 302 208-1*, 2006.

[21] FELDHOFER, M., DOMINIKUS, S., AND WOLKERSTORFER, J. Strong authentication for RFID systems using the AES algorithm. In *Proc. Workshop on Cryptographic Hardware and Embedded Systems* (2004), vol. 3156 of *LNCS*, pp. 357–370.

[22] GRIFFIN, J. D., AND DURGIN, G. D. Complete link budgets for backscatter-radio and RFID systems. *IEEE Antennas and Propagation Magazine 51* (2009), 11–25.

[23] GUIASU, S., AND SHENITZER, A. The principle of maximum entropy. *The Mathematical Intelligencer 7* (1985), 42–48.

[24] HALL, J., BARBEAU, M., AND KRANAKIS, E. Enhancing intrusion detection in wireless networks using radio frequency fingerprinting. In *Proc. Communications, Internet, and Information Technology* (2004).

[25] HALL, J., BARBEAU, M., AND KRANAKIS, E. Detecting rogue devices in Bluetooth networks using radio frequency fingerprinting. In *Proc. IASTED International Conference on Communications and Computer Networks* (2006).

[26] JANA, S., AND KASERA, S. K. On fast and accurate detection of unauthorized wireless access points using clock skews. In *Proc. ACM International Conference on Mobile Computing and Networking* (2008).

[27] JUELS, A. Minimalist cryptography for low-cost RFID tags. In *Proc. International Conference on Security in Communication Networks* (2004), vol. 3352 of *LNCS*, pp. 149–164.

[28] JUELS, A. Strengthening EPC tags against cloning. Manuscript, 2005.

[29] JUELS, A. RFID security and privacy: A research survey. *IEEE Journal on Selected Areas in Communications 24*, 2 (2006).

[30] JUELS, A., PAPPU, R., AND PARNO, B. Unidirectional key distribution across time and space with applications to RFID security. In *Proc. USENIX Security Symposium* (2008).

[31] JUELS, A., RIVEST, R., AND SZYDLO, M. The blocker tag: Selective blocking of RFID tags for consumer privacy. In *Proc. ACM Conference on Computer and Communications Security* (2003).

[32] KARJOTH, G., AND MOSKOWITZ, P. A. Disabling RFID tags with visible confirmation: clipped tags are silenced. In *Proc. ACM Workshop on Privacy in the Electronic Society* (2005).

[33] KERSCHBAUM, F., AND SORNIOTTI, A. RFID-based supply chain partner authentication and key agreement. In *Proc. ACM Conference on Wireless Network Security* (2009).

[34] KOHNO, T., BROIDO, A., AND CLAFFY, K. Remote physical device fingerprinting. *IEEE Transactions on Dependable and Secure Computing 2*, 2 (2005).

[35] LEE, Y. K., BATINA, L., SINGELÉE, D., AND VERBAUWHEDE, I. Low-cost untraceable authentication protocols for RFID. In *Proc. ACM Conference on Wireless Network Security* (2010).

[36] LEHTONEN, M., MICHAHELLES, F., AND FLEISCH, E. How to detect cloned tags in a reliable way from incomplete RFID traces. In *Proc. IEEE International Conference on RFID* (2009).

[37] NIKKARI, M., BJORNINEN, T., SYDANHEIMO, L., UKKONEN, L., ELSHERBENI, A., YANG, F., AND KIVIKOSKI, M. Performance of a passive UHF RFID tag in reflective environment. In *Proc. IEEE Antennas and Propagation Society International Symposium* (2008).

[38] PERIASWAMY, S. C. G., THOMPSON, D., AND DI, J. Ownership transfer of RFID tags based on electronic fingerprint. In *Proc. International Conference on Security and Management* (2008).

[39] RASMUSSEN, K., AND ČAPKUN, S. Implications of radio fingerprinting on the security of sensor networks. In *Proc. International ICST Conference on Security and Privacy in Communication Networks* (2007).

[40] ROMERO, H. P., REMLEY, K. A., WILLIAMS, D. F., AND WANG, C.-M. Electromagnetic measurements for counterfeit detection of radio frequency identification cards. *IEEE Transactions on Microwave Theory and Techniques 57*, 5 (2009), 1383–1387.

[41] ROMERO, H. P., REMLEY, K. A., WILLIAMS, D. F., WANG, C.-M., AND BROWN, T. X. Identifying RF identification cards from measurements of resonance and carrier harmonics. *Online manuscript* (2010).

[42] SHANNON, C. A mathematical theory of communication. *The Bell System Technical Journal 27* (1948), 379–423.

[43] SHAW, D., AND KINSNER, W. Multifractal modeling of radio transmitter transients for classification. In *Proc. IEEE Conference on Communications, Power and Computing* (1997).

[44] SPIEKERMANN, S., AND EVDOKIMOV, S. Privacy enhancing technologies for RFID - A critical investigation of state of the art research. In *Proc. IEEE Privacy and Security* (2009).

[45] SYDANHEIMOL, L., NUMMELA, J., UKKONEN, L., MCVAY, J., HOORFAR, A., AND KIVIKOSKI, M. Characterization of passive UHF RFID tag performance. *IEEE Antennas and Propagation Magazine 50*, 3 (2008), 207–212.

[46] TIPPENHAUER, N. O., RASMUSSEN, K. B., PÖPPER, C., AND ČAPKUN, S. Attacks on public WLAN-based positioning. In *Proc. ACM/USENIX International Conference on Mobile Systems, Applications and Services* (2009).

[47] URETEN, O., AND SERINKEN, N. Detection of radio transmitter turn-on transients. In *Electronic Letters* (2007), vol. 35, pp. 1996–1997.

[48] URETEN, O., AND SERINKEN, N. Wireless security through RF fingerprinting. *Canadian Journal of Electrical and Computer Engineering 32*, 1 (Winter 2007).

[49] VAJDA, I., AND BUTTYÁN, L. Lightweight authentication protocols for low-cost RFID tags. In *Proc. Workshop on Security in Ubiquitous Computing* (2003).

[50] WANG, B., OMATU, S., AND ABE, T. Identification of the defective transmission devices using the wavelet transform. *IEEE Transactions on Pattern Analysis and Machine Intelligence 27*, 6 (2005), 696–710.

[51] WILLIAMS, B. *Intelligent Transport Systems Standards*. Artech House Publishers, 2008.