Butterfly: Environment-Independent Physical-Layer Authentication for Passive RFID

JINSONG HAN, Institute of Cyberspace Research, College of Computer Science and Technology,Zhejiang University; Alibaba-Zhejiang University Joint Research Institute of Frontier Technologies, China
CHEN QIAN, University of California Santa Cruz, USA
YUQIN YANG, The School of Electronic and Information Engineering, Xi'an Jiaotong University, China
GE WANG*, The School of Electronic and Information Engineering, Xi'an Jiaotong University, China
HAN DING, The School of Electronic and Information Engineering, Xi'an Jiaotong University, China
XIN LI, University of California Santa Cruz, USA
KUI REN, Institute of Cyberspace Research, College of Computer Science and Technology, Zhejiang University, Alibaba-Zhejiang University Joint Research Institute of Frontier Technologies, China

RFID tag authentication is challenging because most commodity tags cannot run cryptographic algorithms. Prior research demonstrates that physical layer information based authentication is a promising solution, which uses special features from the physical backscatter signals from tags as their fingerprints. However, our recent studies show that existing physical-layer authentication may fail if feature collection and authentication are conducted in different locations, due to location-dependent noises, environmental factors, or reader hardware differences.

This paper presents a new physical layer authentication scheme, called Butterfly, which is resilient to environment and location changes. Butterfly utilizes a pair of adjacent tags as an identifier of each object. By using the difference between the RF signals of the two tags as their fingerprint, the environmental factors can be effectively canceled. Butterfly is fully compatible with commodity RFID systems and standards. We set up a prototype Butterfly using commodity readers, tags, and RF devices. Extensive experiments show that Butterfly achieves high authentication accuracy for substantially different environments and device changes.

CCS Concepts: • **Security and privacy → Mobile and wireless security**; • **Network security** → *Mobile and wireless security*;

Additional Key Words and Phrases: Internet of things; RFID; Device authentication

*This is the corresponding author

Authors' addresses: Jinsong Han, Institute of Cyberspace Research, College of Computer Science and Technology,Zhejiang University; Alibaba-Zhejiang University Joint Research Institute of Frontier Technologies, ROOM 410, CAO GUANGBIAO Building, ZHEJIANG UNIVERSITY, ZHEDA RD 38, Hangzhou, ZheJiang, 310027, China, hanjinsong@zju.edu.cn; Chen Qian, University of California Santa Cruz, USA, cqian12@ucsc.edu; Yuqin Yang, The School of Electronic and Information Engineering, Xi'an Jiaotong University, China, yangyuqin1992@stu.xjtu.edu.cn; Ge Wang, The School of Electronic and Information Engineering, Xi'an Jiaotong University, China, gewang.cs@gmail.com; Han Ding, The School of Electronic and Information Engineering, Xi'an Jiaotong University, China, dinghan@xjtu.edu.cn; Xin Li, University of California Santa Cruz, USA, xli178@ucsc.edu; Kui Ren, Institute of Cyberspace Research, College of Computer Science and Technology, Zhejiang University, Alibaba-Zhejiang University Joint Research Institute of Frontier Technologies, ROOM 205, KEGONG Building, ZHEJIANG UNIVERSITY, ZHEDA RD 38, Hangzhou, ZheJiang, 310027, China, kuiren@zju.edu.cn.

2474-9567/2018/12-ART166 $15.00
https://doi.org/10.1145/3287044

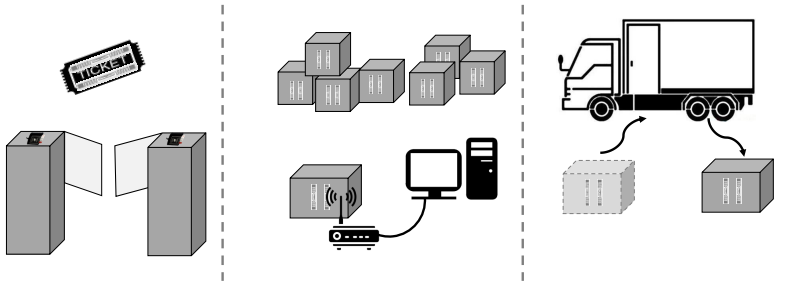


Fig. 1. Some typical use cases of tag authentication

ACM Reference Format:
Jinsong Han, Chen Qian, Yuqin Yang, Ge Wang, Han Ding, Xin Li, and Kui Ren. 2018. Butterfly: Environment-Independent Physical-Layer Authentication for Passive RFID. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 4, Article 166 (December 2018), 21 pages. https://doi.org/10.1145/3287044

1 INTRODUCTION

Radio Frequency IDentification (RFID) is a vital technology of Internet of Things (IoT) that has been widely used in crucial applications, such as identification, access control, E-payment, and object-tracking [8][28][27][22][23][17]. Passive RFID tags rely on backscatter for communication and exhibit several advantages, including low cost, small size, and battery-free design, in autonomous identification. In many applications such as entering fairs, museums, or theatres, passive RFID tags are used as passing tokens. In addition, logistic systems may use tag-labeled packages [11] for check-in and delivery tracking. However, RFID authentication in current applications only checks the ID numbers stored in tags, which leaves a fatal security flaw. Adversaries using standard readers can retrieve the ID and other legitimate information from a legitimate tag and forge another tag carrying the same ID. The forged tag can be used for *counterfeiting attacks*, such as being used as the token to enter an event.

Unfortunately, the limited computing capability of passive UHF RFID tags restricts the execution of cryptographic algorithms such as cryptographic hashing and encryption. In fact, most commodity off-the-shelf (COTS) passive tags do not support any cryptographic operation.[1] Hence existing network security solutions are impossible to apply on commodity passive tags. Even if cryptographic operations are available on tags, an attacker can still replicate one authorized tag to multiple ones, by stealing the keys or simply owning an authorized tag.

On the other hand, physical-layer tag authentication has been studied, which utilizes unique physical layer features from the backscatter signals of tags as their fingerprints [9][24][25]. The insight behind those solutions is that different tags show distinguishable features in their physical signals, called "fingerprints", due to manufacture imperfection. **The unique advantage of physical-layer authentication is that it verifies the physical existence of a device**, rather than just checking a shared digital key like the cryptographic methods. Physical-layer tag authentication does not need to modify existing RFID standards or replacing existing tags, hence are extremely attractive to existing RFID applications. It may also be combined with cryptographic based authentication to prevent the attackers from stealing the secret keys and reproducing tags using the keys. However, existing physical-layer authentication approaches are *environment-sensitive*. That is, the generated fingerprint is unstable under environment changes, resulting in more failures including both false positives and false negatives.

[1]To our knowledge, the only UHF passive tag that supports cryptographic functions is a recently announced NXP UCODE DNA RFID [1]. However, all related documents are for commercial purposes. There is no technical report or price. Hence we are unclear about its strengths, weaknesses, and trade-offs.

In fact, environment and device changes are very common in real scenarios. As shown in Fig. 1, considering three typical scenarios in practice:

1. Entrance check: An event or building may have different entrances, the manager should authenticate the pass of each passenger. In this case, different entrances may have different environments. Environmental factors such as walls, objects, and moving people as signal reflectors introduce unpredictable errors into physical-layer signal collections and hence lead to authentication failures.

2. Inventory management: The warehouse administrator should authenticate and check the identity of goods periodically. In this case, the goods are registered and authenticated using the same devices, while may be at different positions.

3. Package authentication: In logistic, the users always need to verify that the package is indeed the one registered at the place of departure. In this case, both the places and devices used for fingerprint-registration and authentication are different.

Therefore, generating fingerprints resilient to the environment and device changes is an essential requirement for physical-layer RFID authentication. Nevertheless, achieving this goal is challenging because environmental changes are unpredictable and ubiquitous in physical signals. Under such circumstance, RFID authentication may fail because of two reasons. a) The features extracted from a tag's physical signals in different environments yield inconsistent fingerprints, raising the false rejection rate (FRR) in authentication. b) The features are indistinguishable among different tags, or easy to be depressed by the incurred noisy signals, increasing the false acceptance rate (FAR) such that illegal tags might be accepted as valid ones.

To address the above issues, we design an environment-independent physical-layer RFID authentication scheme, called Butterfly. Instead of using a single tag, we propose to use a pair of adjacent tags for authentication. In particular, we calculate the *difference* between the two tags' physical layer signals as the fingerprint of this pair of tags. By utilizing the physical proximity of them, Butterfly effectively mitigates the noise caused by environment and device changes. In addition, Butterfly also extensively expands the feature space. As a result, the issues of being environment/device-sensitive and feature-indistinguishable are well addressed. Butterfly is fully compatible with commodity RFID systems, without any modification on the RFID hardware or standards. We implement a prototype of Butterfly using COTS RFID readers Impinj R420, an RF device USRP N210, and mainstream passive tags in the market, *e.g.*, Impinj E41-B, E41-C, and Alien 9640.

In this work, we do not consider *signal-replay attacks*, in which an attacker uses a high-end signal recorder and replayer to eavesdrop on valid tags and replay the exactly identical signal to the reader. Our solution is mainly used for applications where the profit from this attack is much less than the cost of signal replaying, such as event tickets. Current solutions to defend against signal replaying are also limited to special environments [19].

Our contributions are summarized as follows.

1. We propose a new physical layer fingerprint based RFID authentication scheme, called Butterfly, which employs a pair of tags for RFID authentication. Butterfly effectively mitigates the impact of environment and device changes on the fingerprint generation.

2. Butterfly is scalable by sufficiently expanding the feature space for generating distinguishable fingerprints. This is extremely important for large-scale RFID applications, where the legitimate tag pairs can be distinguished in terms of their fingerprints, while those invalid pairs can also be differentiated from the legitimate ones. We analyze the potential feature space for fingerprint generation and find that the number of pairs supported in one Butterfly system is quadratic larger than the state-of-art solutions. It infers that an attacker is more difficult to use a forged tag to pass the authentication.

3. Butterfly is completely compatible with existing RFID systems. It has no needs on modifying either the hardware or standards.

4. We implement a prototype Butterfly using commodity RFID devices and off-the-shelf USRP N210. The extensive experimental results show that Butterfly achieves high authentication accuracy, i.e.>95%, even if varying the environment or device.

In the rest of this paper, we first introduce some related works of Butterfly in Section 2. We then elaborate on the background and our observation in Section 3. We present our model and system design in Section 4 and 5. Finally, we evaluate Butterfly in Section 6 and 7. The security analysis of our system is discussed in Section 8. We conclude this work in Section 9.

2 RELATED WORKS

Prior works in RFID authentication fall into two categories: crypto-based and physical-layer approaches.

Crypto based approaches aim to utilize conventional cryptographic algorithms to perform the authentication. The basic idea is to allow each tag to share a secret key with the reader. The authentication is then a challenge-response interaction between the reader and tag. The reader will accept a tag as a valid one only if the tag can reply a cipher encrypted by a valid key. Song et al. [18] propose a symmetric key based key search scheme. Feldhofer *et al.* analyze the standardized cryptographic algorithms in RFID system [7]. Bruns *et al.* propose a method for cryptographically combining HF and UHF RFID Tag in [3]. And Poschmann *et al.* design a light-weight crypto algorithms for RFID system in [16]. Currently most encrypted tags work at the Low-Frequency (LF) spectrum in industry, such as Philips megamos RFID tag, NXP Hitag, and Hitag2 tags. However, due to the different communication mechanisms, the LF tags, which exchange data with the reader via circuits inductive coupling, usually support a read-range less than about 10 centimeters. Such short the range severely limited the application scope of those encrypted tags. Besides, crypto-based methods have several drawbacks. First, these methods cannot be implemented on main-stream COTS tags. Second, it cannot be adopted by COTS passive tags directly, due to the required modification on either the protocol or hardware. Third, if the secret keys are stolen, it is easy for adversaries to produce unlimited counterfeit tags. In contrast, counterfeiting physical-layer features of valid tags in Butterfly is extremely difficult, even if the features are known to the attacker. In addition, Butterfly can authenticate tags in a longer distance (1.5 meters in our experiments, but it can be extended by using more powerful reading and receiving devices, which is easy to operate in practice). Therefore, Butterfly would be an important alternative or supplementary for encrypted RFID communication.

Physical-layer authentication approaches are based on the hardware diversity of tags [4][10][19]. The imperfect manufacture procedure is the main reason to cause such diversity. The diversity of tags is usually presented by the difference in their physical layer signals. Periaswamy et al. [15] use the Minimum Power Response of RF signals as the fingerprint. However, extracting such a feature requires a specific device, *i.e.*, Voyantic Tag-formance Lite System. Zanetti et al. [25] extract the time interval error, average baseband power, and spectral feature as the fingerprint of tags. Although this work [25] achieves high authentication accuracy (99.6%), it still needs a costly and powerful spectrum analyzer for feature extraction. Geneprint [9] attempts to reduce the overhead in feature extraction. It calculates covariance (Cov) among two tags' square waves and Power Spectrum Density (PSD) of their signals as the fingerprint. As aforementioned, those fingerprint-based solutions suffer from environment changes. Even the change of tags' position, orientation, or transmission power will incur a non-trivial impact on their fingerprint generation and testing. On the contrary, Butterfly is resilient to environment changes yet guarantee high authentication accuracy.

3 BACKGROUND AND OBSERVATION

3.1 Background

A passive RFID system is usually composed of a reader with its antennas, a number of passive tags, and a back-end server. Figure 2 illustrates the communication procedure between the reader and a tag, which is specified by

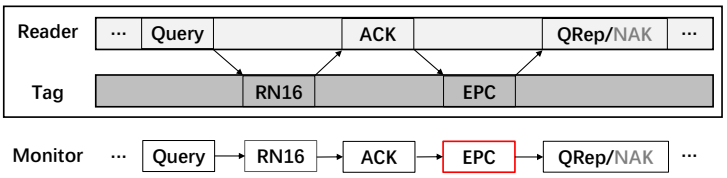


Fig. 2. EPC C1G2 protocal

Table 1. Accuracy under environment changes

Mehtod	(Cov,PSD)	ABP	TIE+ABP	SP
Accuracy	77.8%	15.92%	36.24%	37.6%

standard protocols, e.g. EPC Class 1 Generation 2 protocol [6]. Following this protocol, the reader sends a Query command to trigger an inventory round. Each tag under the reader's interrogation will select a time slot to reply with a random number RN16. The reader acknowledges the tag with the identical RN16. Once receiving this ACK, the tag will report its EPC code (ID) to the reader. The reader will check the validity of the received EPC code. If it is valid, the reader may send other commends for further interrogation, such as QueryRep. Otherwise, the reader terminates the interrogation by sending a NAK command.

3.2 Our Observation

In practice, the RF signal received by the reader's antenna is actually a hybrid one mixed by multiple signals. The backscattered signals travel along various paths, along which a certain number of reflections happen. When the environment changes, some reflections vary accordingly, affecting the essential parameters of signals, such as amplitude and phase. For instance, the work by Zanetti et al. [25] employs the average baseband power and spectral feature to generate fingerprints. However, these two features vary with the change of location and orientation of tags, and the transmission power of the reader. On the other hand, GenePrint [9] utilizes the power spectrum density (PSD) and covariance (Cov) as the tag's fingerprint. Similarly, these two features are also unstable upon the environment and device changes. As a result, certain errors are introduced to the signals received at the reader's antenna, yielding inconsistency to the fingerprints of tags. That is why the environment change severely influences the physical signal based fingerprint in prior works.

In order to demonstrate the impact of environment changes, we place a tag in two completely different rooms (Room1 and Room2) and collect the backscattered signals using a USRP based monitor. We keep the relative positions between the reader and monitor unchanged, while placing the tags at three randomly selected positions in the shared reading area of the reader and monitor. Fig. 3 plots the received signal by the monitor. We find that the environment has a strong impact on the signal strength of baseline and amplitude.

With such impact, prior works may not work well. We investigate the authentication accuracy of state-of-art works under environment changes in Table 1. In this table, the features include (Cov, PSD) used in GenePrint[9] as well as the time interval error (TIE), average baseband power (ABP), and spectral feature (SP) proposed by Zanetti *et al.* [25][26]. We find that, after changing the environment, the accuracy of all these features are less than 80%. Some of them are even lower than 40%. The results indicate that the features used as **fingerprints by existing physical-layer RFID authentications are not resilient to environment changes**.

4 MODEL AND MAIN IDEA OF BUTTERFLY

In this section, we analyze the received signal at the monitor and model the propagation process of RF waves. Figure 4 shows the system deployment of Butterfly. Instead of using a single tag, we utilize a pair of tags as a unity for authentication. Besides commercial RFID readers and tags, we utilize a USRP-based monitor to collect and record the RF signals transmitted between the reader and tags. In fact, the monitor plays a role like a listener,

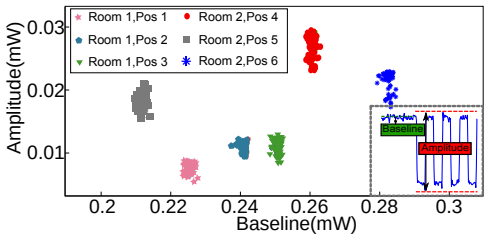


Fig. 3. Feature clusters of a tag at different locations

which does not disturb or interrupt the whole communication between the reader and tags. **Note that the monitor is not necessary in practice: a COTS reader also obtains the same data of signals, which is available if the manufactures provide APIs.** We then extract environment-independent features of tags from the signals received at the monitor.

The propagation process from the reader to the monitor can be divided into two phases. As shown in Fig. 5, one is from the RFID reader to the tag pair, and another is from the tag pair to the monitor. Both the two phases are vulnerable to the environment changes. We take the first phase as an example. The signals transmitted from the reader may bounce at static objects, such as walls, furniture, *etc.*. In addition, the moving objects, such as human beings and robots, will also introduce varying reflections to the tag pair. The line-of-sight signal superposes with those multipath signals. Therefore, the induced current (energy) among the tag pair varies in different environments. The situation is similar to the second phase. As a result, the received physical-layer signals are not consistent in variant environments. That is why existing authentication method cannot be perfectly adopted upon unstable environments.

To tackle the challenges raised by the environment or device changes, we propose a new physical layer authentication method to achieve trustworthy authentication for RFID tags. Our main idea is that if two adjacent tags are with a close in-between distance, they experience nearly the same impact from both the perspectives of environment changes and hardware (the reader and monitor). Based on this insight, we design our cancellation method to combat the changes of environments and devices. Suppose that these two tags are T_1 and T_2. In the monitored signals, their received signals are $P_t = [p^t(1), p^t(2), p^t(3)..., p^t(N)]$, where t =T_1 or T_2, and N is the number of samples. In theory, P^t is comprised of five components, *i.e.*, $P^t = \{C^t, F^t, N_G^t, N_E^t, N_D^t\}$, where C^t is a constant vector of the standard square wave pulse, F^t is a value representing the tag's inherent hardware feature, N_G^t is the White Gaussian Noise (WGN), N_E^t is the environmental noise, and N_D^t is the total noise introduced by all associated devices, including the reader and monitor, respectively.

$$\begin{aligned} P^{T_1} &= C^{T_1} + F^{T_1} + N_G^{T_1} + N_E^{T_1} + N_D^{T_1} \\ P^{T_2} &= C^{T_2} + F^{T_2} + N_G^{T_2} + N_E^{T_2} + N_D^{T_2}, \end{aligned} \tag{1}$$

The key idea to cope with the changing environment is computing the difference between P^{T_1} and P^{T_2} and thus canceling out common environmental factors in Eq. 1. Particularly, the difference is represented by all the differences between all pairs of corresponding elements in P^{T_1} and P^{T_2}. That is

$$\begin{aligned} &P^{T_2}(n) - P^{T_1}(n) = \\ &(C^{T_2}(n) - C^{T_1}(n)) + (F^{T_2}(n) - F^{T_1}(n)) + (N_G^{T_2}(n) - N_G^{T_1}(n)) + (N_E^{T_2}(n) - N_E^{T_1}(n)) + (N_D^{T_2}(n) - N_D^{T_1}(n)) \end{aligned} \tag{2}$$

where $n \in [1, N]$ is the index of the sample. From the two tags' perspective, at any given time, the devices for collecting their signals are identical. That is, $N_D^{T_2}(n) - N_D^{T_1}(n) \cong 0$. Furthermore, we can safely conjecture that the environment noise $N_E^{T_2}(n) - N_E^{T_1}(n) \cong 0$ when the two tags are sufficiently close to each other. This means they experience identical environment changes [20][21][14]. Meanwhile, $N_G^{T_1}$ and $N_G^{T_2}$ are the White Gaussian

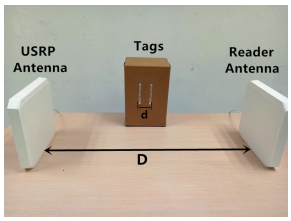


Fig. 4. System Deployment

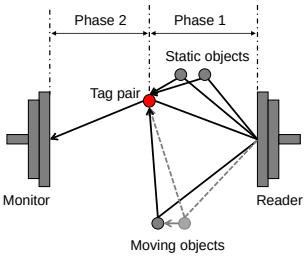


Fig. 5. The model of Butterfly

Noise (WGN). For these two components, we only know that their distributions follow the Gaussian distribution. However, we have no idea about the exact value of each sample point. So directly subtracting $N_G^{T_1}$ from $N_G^{T_2}$ (or vice versa) cannot effectively cancel the influence of WGN.

To deal with this problem, we adopt the wavelet analysis method to remove the interference of WGN on the signals. As we know, wavelet analysis can extract specific properties from the signals [2]. To our knowledge, WGN appears as random and high-frequency fluctuations on the received signals. On the contrary, the hardware features of each tag, *i.e.*, the square wave pulses and the tag inherent hardware features, are highly possible at low frequencies. So we decompose the signals into two parts, namely the high-frequency part and low-frequency part, by performing wavelet analysis and discarding the high-frequency portion, yet retaining the low-frequency part. Note that low-pass filter can also remove the high-frequency part. In our experiments, we find that both low-pass filter and WGN are effective in extracting features from the raw signals. The results do not show distinct differences. Hence we can also choose the appropriate low-pass filter here.

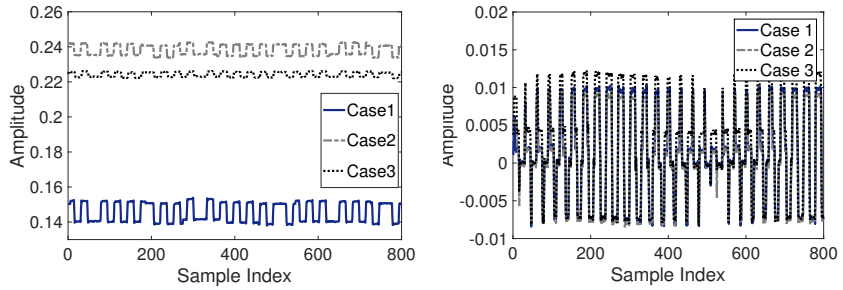
Combining all the analysis above, we have

$$s = diff(P^{T_2} - P^{T_1}) \approx (C^{T_2} - C^{T_1}) + (F^{T_2} - F^{T_1}), \tag{3}$$

where s denotes the signal segment after cancellation. To verify the effectiveness of the aforementioned noise cancellation method, we conduct two sets of experiments. One is to evaluate the performance of Butterfly in dealing with environment noises, while another focuses on checking the performance of device noise elimination. For the first experiment, we compare the tag signals collected in three cases: 1) Placing the tag pair in room 1 and collecting their signals. 2) Moving the entire systems into another room (room 2) and keeping the same deployment as case 1. 3) Keeping the deployment of the reader and monitor unchanged in room 2, but moving the tag pair to another position. Comparing the three cases, case 1 and 2 have different surrounding environments. While the tag pair has totally different line-of-sight propagation paths in case 2 and 3. We exhibit the raw data of one tag in case 1, 2 and 3 in Fig. 6(a). The results after performing our cancellation method are shown in Fig. 6(b). We find that though the raw data in the three cases are totally different, the results after the cancellation process are highly consistent, only with a slight difference.

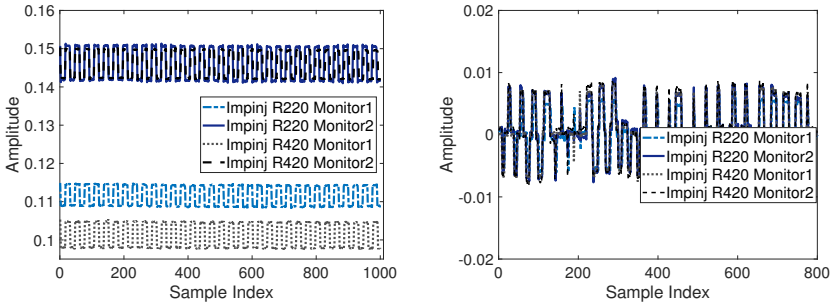
We also evaluate the performance of Butterfly in coping with device diversity. We utilize 2 readers (Impinj reader R220, Impinj reader R420) and 2 USRP N210 to simulate the scenario of device changes. Consequently, we have 4 combinations of readers and monitors. We collect the raw signals of a tag-pair using the devices of the four combinations and show the results in Fig. 7(a). We can observe that the signal varies significantly among the four combinations. On the other hand, we perform our difference based noise cancellation and plot the result in Fig. 7(b). The high coincidence among four curves exhibits excellent ability of our method in canceling the device noise.

The results demonstrate that our method is effective to eliminate the impact of environment changes and device diversity, enabling the environment-independent fingerprints for RFID tags.



(a) Before (b) After

Fig. 6. Environment change cancellation. a) The raw signals at different cases. b) The signals after environment changes cancellation.



(a) Before (b) After

Fig. 7. Device noise cancellation.a) The received signals by utilizing different devices. b) The signal after device noise cancellation

5 SYSTEM DESIGN

5.1 System Overview

As aforementioned in Section 4, Butterfly uses a pair of tags as an identifier. We define such a pair of tags as a tag-pair. A complete Butterfly system contains a commodity passive RFID reader, a monitor, and a group of tag-pairs.

Butterfly is comprised of three modules: signal collection, signal pre-processing, feature extraction and matching, as illustrated in Fig. 8. In the signal collection module, Butterfly utilizes a USRP-based monitor to record the whole communication process between the commercial reader and a tag-pair. The signal pre-processing module is designed for removing environment and device noises by selecting and subtracting appropriate signals. We further extract and store distinguishable features for each tag-pair in the signal extraction module. In the feature matching phase, Butterfly utilizes overlapped rates of processed signals to match this pair of tags against legitimate ones in the database for authentication.

5.2 Signal Collection

As illustrated in Fig. 4, the antennas of the monitor and the reader are placed in opposition to each other, with a distance D in-between. A tag-pair under authentication is placed between the two antennas to ensure that its two tags can communicate with the reader, and their backscattered signals can be received by the monitor.

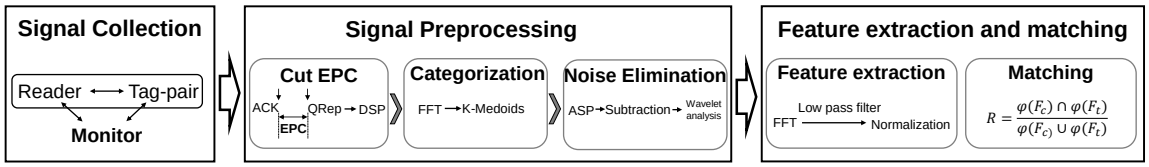


Fig. 8. Butterfly system design.

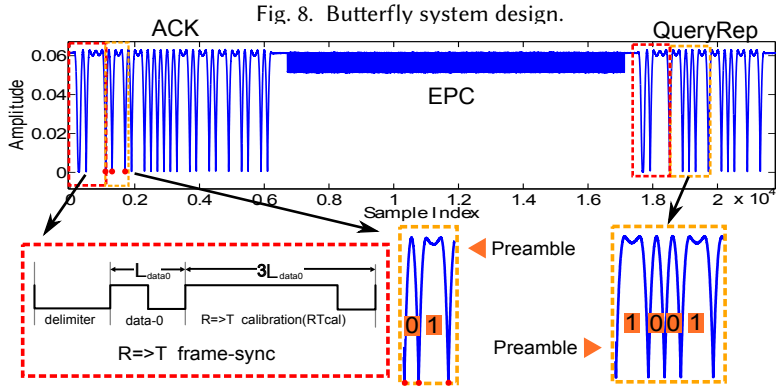


Fig. 9. The received signal at Monitor.

Meanwhile, we denote the distance between two tags in a tag-pair as d. In the following modules, we use the signal received at the monitor as the data source for signal processing and feature extraction.

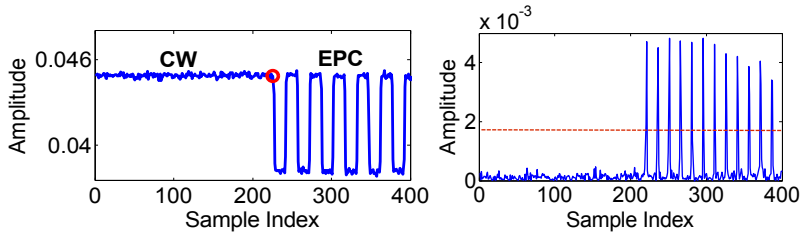
5.3 Signal Pre-processing

This module contains three processes, signal selection and segmentation, categorizing, and environmental noise cancellation.

5.3.1 Signal Selection and Segmentation. In this section, we aim to filter out the tags' backscattered signals from all the received signals. As aforementioned, the monitor records the whole communication process between the reader and a tag-pair. Among the recorded signals, we only need the backscattered signals from the tag-pair. As aforementioned in Sec. 3, a tag will response its RN16 and EPC during the inventory. As the random number RN16 will change every time the tag response its signals, we only select the tags' EPC segments as the signal source. Compared with RN16, tag's EPC is unique and identical, which is a good choice for authentication.

To obtain the pure EPC segments from the received signals, we should first filter out the reader's commands and other unnecessary segments, and cut out EPC segments. A straightforward method is to locate each EPC segment and decode it. However, doing so is time-consuming and error-prone. As shown in Fig. 9, compared with the reader's signals, the tag's signal is much weaker in terms of signal strength. As a result, localizing and decoding the EPC segments would be very inefficient. To tackle this problem, we transfer the task of finding tags' EPC segments to localizing specific reader's commands. Considering that the segments corresponding to the reader's commands are much powerful than those of tags, we can use such distinguishable segments to indirectly locate EPC segments. Following the specification in EPC C1G2 [6], an EPC segment appears between two sets of reader's commands, namely ACK and QUERY/ QREP /QADJ. As shown in Fig. 9, we locate these reader commands by recognizing their preambles, and cut out the signal segment in-between. We denote each segmented EPC signal part as p.

With the aforementioned process, we are able to filter the EPC segments of the tags from massive raw signals. However, the EPC signal intercepted via this indirect way includes not only the tag's EPC segment, but also the carrier wave (CW) transmitted by the reader. Hence we employ a mechanism called Determine Sample Point (DSP) to find out the real start point of tag's backscattered signals. DSP is based on the observation that the



(a) Raw signal (b) Locating the start point

Fig. 10. Effectiveness of DSP. a) The raw received signal of a tag. b) Locating the start point by calculating the difference between two adjacent samples.

amplitude of CW signal parts is relatively small and stable, while at the start (or end) point of EPC segments, the signal varies dramatically. We first select a small segment from the collected signal. Then we compute the difference between the adjacent sampling points, as formulated in Eq. 4. In this equation, we assume that the amplitude at the n-th sampling point is $p(n)$, and define a difference function δ.

$$\delta(n) = |p(n+1) - p(n)| \tag{4}$$

We locate the start point of EPC segment by setting a threshold σ, which is ρ times larger than the average value of the latter part of δ, *i.e.*,

$$\sigma = \rho \cdot \frac{\sum_{n=\lfloor N/2 \rfloor}^{N} \delta(n)}{N - \lfloor N/2 \rfloor} \tag{5}$$

where ρ is a coefficient which can be empirically determined. It can be chosen on each receiver. We exhibit the performance of DSP in Fig. 10. We find that at the start point of an EPC segment (marked in green in Fig. 10(b)) can be accurately and clearly localized.

5.3.2 Categorizing. To obtain the differences between tag 1 and 2, we should categorize each EPC segment and decide which tag it belongs. Intuitively, we can identify the segment by decoding it, like the process in commodity RFID readers. However, the USRP-based monitor does not provide this API. In addition, per-bit decoding in the signal is very complex and time-consuming. Therefore, we employ a hardware-characteristic-based tag categorization method. We exploit the difference in the backscatter link frequency (BLF) brought by the hardware diversity of the tags [20][9]. BLF is an inherent physical-layer signal characteristic of RFID tags, which is introduced by imperfection during manufacturing. It varies among different tags and relatively stable for one tag. BLF determines the response data rate of a tag, which can be extracted by frequency-related methods. So we perform Fast Fourier Transform (FFT) on each EPC segment. Then we employ a clustering method, namely K-Medoids, to classify two tags' EPC segments by analyzing their FFT results. In our prototype, we adopt two common statistical magnitudes, the variance (Var) and covariance (Cov) of the FFTed segments as the input of K-Medoids. The results are shown in Fig. 11. The x-axis and y-axis are the Var and Cov results of the processed signals of the two tags, respectively. We observe that the BLF-based characteristics can distinctly distinguish two tags' EPC segments. Note that though BLF-based method is good at telling two tags apart, it is not appropriate for authenticating large scale of tag population. That is because the BLF varying range for COTS passive tags is limited. For a large number of tags, there must be a lot of tags that own very similar BLF parameter. So we use EPC decoding in the multi-tag scenario. The decoding method has been introduced in the prior work [5]. After this step, we classify all the EPC segments into two categories, P^{T_1} and P^{T_2}, corresponding to tag 1 and 2, respectively.

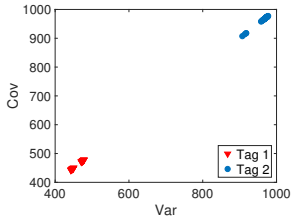
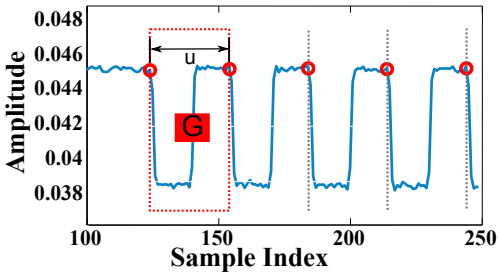
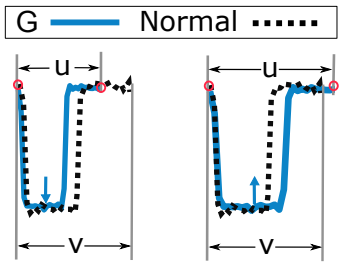


Fig. 11. Example of K-Medoids process. Two tags in a pair can be clustered by comparing the physical-layer features.

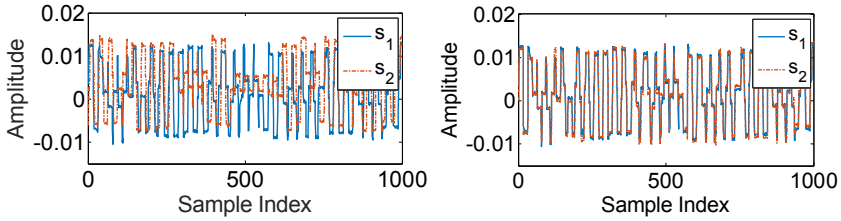


(a) segment



(b) abnormal waveforms

Fig. 12. Inconsistent signal caused by hardware.



(a) Before performing ASP

(b) After performing ASP

Fig. 13. Effectiveness of ASP.

5.3.3 Environmental Noise Cancellation. As aforementioned in Section. 4, we make a subtraction among the signals backscattered from the tag-pair. When performing the subtraction, an implicit assumption is that the involved signals should be collected in a transient period. In this way, the change of environments is negligible and hence the environment can be considered as stable. In Butterfly, we choose every two signals that are transmitted at adjacent time points. Since the communication between the RFID reader and tags is extremely fast (*i.e.*, a reader can read about 100∼120 times per second), the time duration between the two points is sufficiently short. We define the set of the final signal difference as S.

Our analysis in Section 4 implies that the difference between tags in one pair is able to cancel the environmental noise. However, in practice, we find that though the hardware characteristic is mostly stable, there are still some exceptions. As shown in Fig. 12, the number of sampling points in a waveform G may vary lightly when a tag transmits EPC segments. Butterfly will inevitably suffer from the gradually accumulated errors in the collected samples. We call such waveforms as *abnormal* ones. As a consequence, the feature extracted for fingerprint generation may not be identical, which introduces unpredictable errors.

To solve this problem, we propose an Align Sample Point (ASP) algorithm. According to our observation, the ratio of abnormal waveforms is very small, and such a waveform is shorter/longer than the normal ones. Here the normal waveform denotes the majority signal waveforms among all the received ones, which are supposed to be length-identical. We detail ASP in Algorithm 1. The basic idea of ASP is to extend/truncate a shorter/longer waveform such that its length is equal to that of normal ones.

The performance of ASP is shown in Fig. 13. We choose two signals, namely s_1 and s_2, in a set S. Note S contains all the results of subtractions (calculated using Eq. 3) of a tag-pair. We find that after performing the ASP algorithm, the two different curves perfectly matches, indicating the error caused by the instability of tags' hardware has been effectively amended.

ALGORITHM 1: Sample point selection.

Input: To be calibrated square wave, G;
The sampling point number of G, u;
The sampling point number of normal wave, v;
Output: Calibrated square wave, C.
$\epsilon = u - v$;
if $\epsilon = 0$ **then**
    return G;
end
$k = 0, i = 1$;
repeat
    $j = \lfloor k * u/|\epsilon| + u/(2 \cdot |\epsilon|) \rfloor$;
    if $\epsilon > 0$ **then**
        $C(i + k : 1 : j + k) = G(i : 1 : j)$;
        $p(j) = (G(j) + G(j + 1))/2$;
        $C(j + 1) = p(j)$;
    else
        $C(i - k : 1 : j - k - 1) = G(i : 1 : j - 1)$;
    end
until $k < |\epsilon|$;
$i = j + 1, k = k + 1$;
return C;

5.4 Feature Extraction and Matching

After the signal pre-processing, we obtain a set S containing the environment-noise-canceled EPC segments of a tag-pair. In this subsection, we aim to design efficient feature extraction and matching methods for Butterfly.

5.4.1 Feature Extraction. After the subtraction based noise elimination, we find that the signals are highly consistent on frequency, but not on amplitude. So we extract the features of the frequency domain by processing FFT on the subtracted results S. In Fig. 14, we show the FFTed segments of a tag-pair in three different cases mentioned in Sec. 4. It is obvious that although the entire trends of those segments are similar, there are still numerous tiny differences among them. To improve the authentication accuracy, we use a low pass filter to filter out the messy noises and figure out the trends. The low pass filter is selected experimentally and can be set per-device. Fig. 15 shows the result after performing the low pass filter. We can find that the segment in the three environments coincides much better. However, there is still some improvement space (marked in red square). We further normalize the segments to tackle such amplitude difference and achieve satisfied coincidence. Fig. 16 shows the normalized segments, which achieve excellent alignment among three cases. Thus, the above treatment allows the features of a tag-pair to be consistent in different environments. We also exhibit the FFTed results for different tag-pairs in Fig. 17. We can easily find significant differences between these three segments, indicating that our treatment provides Butterfly with efficient distinguishability among tag-pairs.

5.4.2 Matching. Matching is performed to compare a feature set under testing, denoted as F_t, to the feature set recorded in the check-in phase, denoted as F_c. We employ a simple but effective matching method. The idea behind our matching method is to check the overlapped rate between two tag-pairs' features. We define the rate

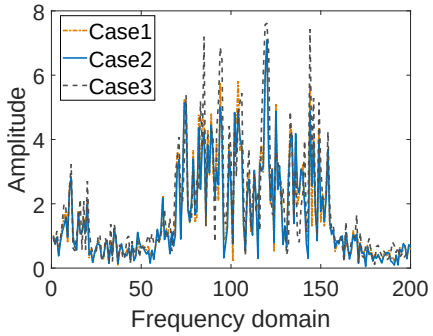


Fig. 14. After FFT

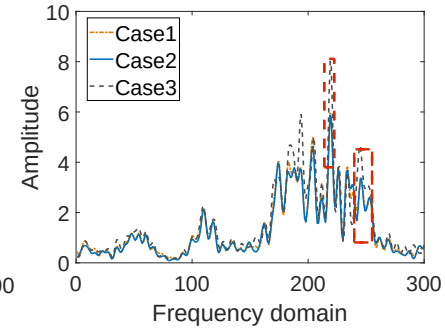


Fig. 15. After lowPass filter

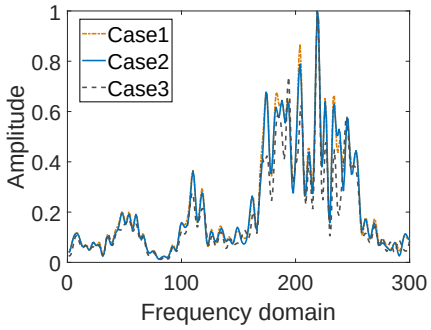


Fig. 16. After normalization

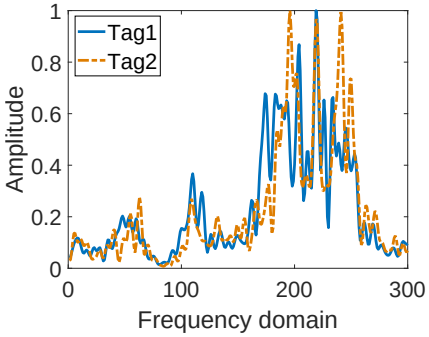


Fig. 17. Distinguishablity among tag-pair

as follows:

$$R = \frac{\varphi(F_c) \bigcap \varphi(F_t)}{\varphi(F_c) \bigcup \varphi(F_t)} \tag{6}$$

where R is the overlapped rate of F_c and F_t, and $\varphi(F(\cdot))$ represents the integral of signal $F(\cdot)$ along the frequency domain (x-axis). Obviously, if F_t matches F_c well, the overlapped rate R will approach 1. Otherwise, a low R indicates that there are greater differences between the two tag-pairs. We set a threshold Q for making a decision whether F_t matches F_c. We will specify how to select a proper Q in the next section.

6 IMPLEMENTATION

We implement a prototype of Butterfly using COTS RFID devices and monitor. Using this platform, we perform extensive experiments for evaluating the performance of Butterfly.

6.1 Experiment Setup

Hardware and software: As shown in Fig. 18 and 19, the prototype Butterfly contains commodity RFID devices, including one passive reader Impinj R220 and three groups of mainstream passive tags in the market (Impinj E41-B, Impinj E41-C, and Alien-9640). We use a USRP N210 plus an SBX daughterboard as the monitor. Both the reader and monitor are mounted with a Laird S9028PCL directional antenna with 8dBi.

We set the center frequency of both the reader and monitor as 924.38MHz. Note that Butterfly is applicable if the frequency is set to other frequencies within the RF spectrum specified in RFID standards.

Deployment: The deployment of Butterfly is shown in Fig. 4. The distance between the reader antenna and the monitor antenna is denoted as D. Note that D is adjustable based on the requirement of real applications. In our experiments, D ranges from 0.5m to 1.5m, which is suitable for most applications. We denote the distance between two tags in a tag-pair as d. We analyze the appropriate value of d with experiments and finally set it as

Fig. 18. Device in Butterfly

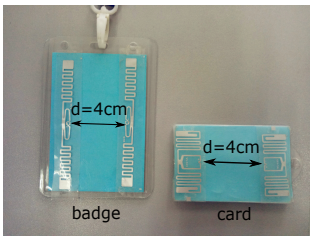


Fig. 19. Tag-pair in real applications

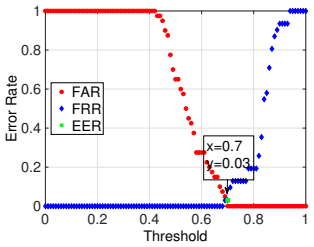


Fig. 20. Threshold selection

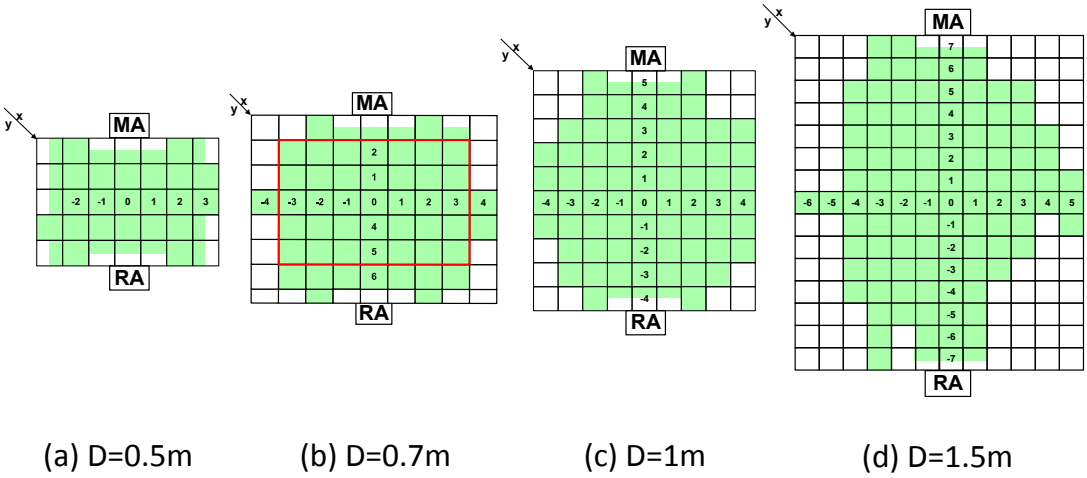


Fig. 21. Effective area

4cm. Both the monitor and reader have certain covering regions, in which these devices can effectively operate. We name the overlapped ones as *effective area*. We will specify how to determine it in the following sections.

6.2 Metrics and Methodology

Butterfly has the registration phase and authentication phase. At the registration phase, Butterfly extracts the features introduced and stores them in a database. At the authentication phase, Butterfly repeats the feature extraction procedure and compares them to the stored ones. Butterfly returns either 'Accept' or 'Reject'.

We evaluate both FRR and FAR of Butterfly. FRR is defined as the rate that **a legitimate tag is rejected by the authentication system and FAR is the rate that a counterfeited tag is accepted.** In particular, since the purpose of this work is to enhance the robustness of physical-layer authentication, we evaluate another metric *Accuracy*, defined as the rate that a tag is correctly matched to its fingerprint in the database.

7 EVALUATIONS

We evaluate the performance of Butterfly against four varying dimensions: the resilience to the environment change, device noise, tag diversity and tag's orientation. Before our evaluation, it is necessary to determine the core parameters of Butterfly.

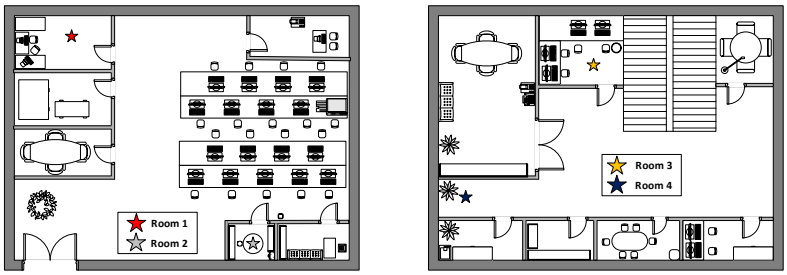


Fig. 22. Experiment environments

7.1 System Parameter Determination

7.1.1 Threshold Q. Feature matching in common applications relies on a threshold to accept or reject the testing sample. In our system, Butterfly utilizes a threshold, denoted as Q, for judging whether a testing fingerprint is valid or not. A good choice of Q requires balance: a stringent Q may reject valid tag-pairs due to the fingerprint mismatch, leading to high FRR for the authentication; for a low Q, on the other hand, different tag-pairs may be classified as the same one, raising FAR in the authentication. To minimize both FRR and FAR, we determine Q by observing the curves of FRR and FAR when shifting the value of Q, as shown in Fig. 20.

We notice that when Q=0.7, the false rates reach the Equal Error Rate (EER), where the FAR and FRR are equal with each other. At this point, FAR and FRR reach a balance. Therefore, we set $Q = 0.7$ in the following experiments. Note that in practice the administrator can select an appropriate Q based on real applications. For example, if security is more important, we may prefer lower FAR.

7.1.2 Outlining Effective Area. In subsection 6.1, we introduce the concept of effective area, within which the tags in a tag-pair can not only empowered by the reader, but also allow the monitor to record their signals. We aim to outline such an area for performing Butterfly. We take D = 0.5 m, 0.7 m, 1 m, and 1.5 m as examples, and divide the region between the reader and the monitor's antennas into small cells ($l \times w = 10cm \times 10cm$). We mark a cell with green if a tag-pair at that position meets the above two conditions. As shown in Fig. 21, between the Monitor Antenna (MA) and Reader Antenna (RA), we find that most cells are within the effective area. In addition, the effective area is mostly covered by the overlapping regions of two antennas' lobes. With this finding, we can easily determine the effective area in an unfamiliar environment by observing the position and direction of monitor and reader antennas. For simplicity, we conduct the following experiments in the area marked with the red square in Fig. 21(b).

We evaluate the performance of Butterfly in combating with environment changes. According to the application requirements in practice, we evaluate Butterfly in three cases: 1) Case 1: the tag-pair is authenticated at the *same position* with registration. A typical example is the entrance admission system. 2) Case 2: the tag-pair is authenticated at *different positions* in the *same room*. A typical example is the inventory management. 3) Case 3: The tag-pair is authenticated at *different positions* in a *different room*. A typical example is the package authentication in logistics.

We perform our experiments in four different rooms as shown in Fig. 22. Among them, room 1 is nearly empty, while other rooms are crowded with shelves, tables or furniture. Room 2 is in the same building as Room 1, while Room 3 and 4 are not. As shown in Fig. 21(b), we conduct our experiment in the 5×7 $10cm \times 10cm$ cells, which are marked in a red rectangle. The coordinate of each cell is expressed as $[x, y]$. We use 50 tag-pairs in our experiments and first register their features at the center of the effective area in room 1, *i.e.*,$[x, y]$=$[1, 0]$. Then we validate them at the center of each cell in Room 1~4.

Fig. 23. The accuracy of case 1 and 2

Fig. 24. The accuracy of case 3

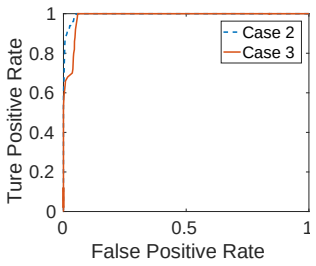


Fig. 25. The accuracy of case 3

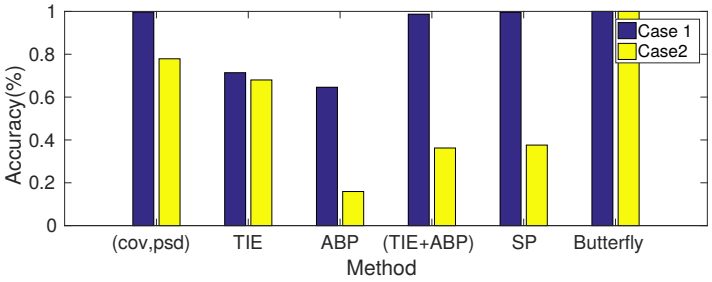


Fig. 26. Comparison between Butterfly and prior solutions in two cases

Fig. 23 exhibits the authentication accuracy in Case 1 and 2, and Fig. 24 shows the accuracy of Case 3. The results show that Butterfly can achieve high authentication accuracy, *i.e.*, >90%, even in Case 3 where both the rooms and positions are different between the check-in and testing phases. In some positions, the rate even approaches 100%. However, at a few positions, the accuracy is relatively low. Our observation is that the received signals at those positions are not quite clear due to the noise. Thus, the signal distortion introduced by the noise seems the dominant reason for the low authentication accuracy. We also exhibit the ROC curve of Butterfly in case 2 and 3 (as shown in Fig. 25). We find that Butterfly has a good performance in finding out illegitimate tag pair even with environment changes. This result indicates that Butterfly can effectively cope with the external environment changes to the tags' physical-layer signal, enabling highly-accurate authentication.

We also compare Butterfly with 5 feature extraction methods used by the state-of-the-art approaches, including the (Cov, PSD) feature used in GenePrint [9], time interval error, average baseband power, and spectral feature proposed by Zanetti *et al.* [25][26]. We check the authentication accuracy of the aforementioned 5 methods in case 1 and 2. In Fig. 26, we show the overall authentication accuracy of those 5 methods and Butterfly. The results reveal that environment changes impose the great impact on the authentication accuracy of the 5 existing methods. For example, using (Cov, PSD), GenePrint [9] achieves a very high accuracy (99.68%) if keeping the environment unchanged. However, once the environment around the tag changes, the accuracy drops sharply to 77.88%. Similarly, the other 4 methods present a low accuracy after changing the environment (< 70%). On the other hand, Butterfly demonstrates 100% authentication accuracy in unchanged environments. More importantly, Butterfly still retains high accuracy (96.7%) even if the environment changes. Therefore, Butterfly not only provides high accuracy for tag authentication, but also effectively eliminates the influence of the environment change.

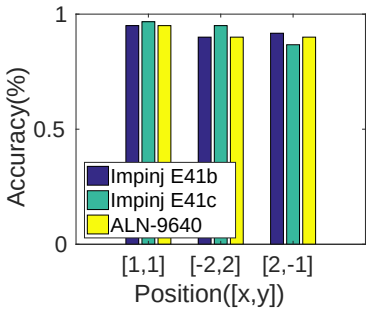


Fig. 27. The accuracy for different types of tags

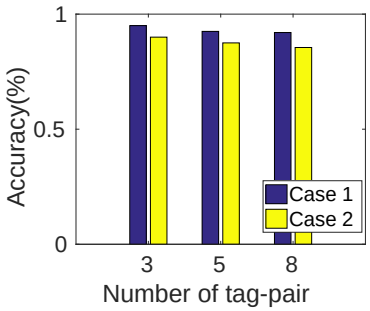


Fig. 28. The accuracy of multiple pairs

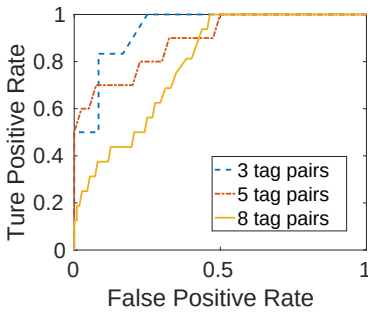


Fig. 29. The ROC curve of multiple pairs

Table 2. Accuracy after changing devices

	Room 2	Room 3	Room 4
Accuracy	98.5%	93.3%	91.5%

7.2 Device Diversity

In real applications, it is common that Butterfly uses one set of devices for fingerprints generation in the registration site, while using other sets of devices in different testing sites. To check the impact of device diversity, we use two sets of RFID devices, including the reader, monitor, and their antennas, to repeat the experiments with 40 tag-pairs. We first extract and record the fingerprints of tag-pairs in Room 1 at position $[x, y] = [1, 0]$ via one set of devices, and then conduct the authentication in Room 2/3/4 using a different set of devices. Hence both the environments and devices are changed. We report the overall authentication accuracy as well as FRR/FAR in Table 2. The high accuracy implies that the impact of the device diversity on Butterfly is trivial.

7.3 Tag Diversity

We further examine the influence of different tag types on Butterfly. We perform the experiment using three types of tags, respectively. For a tag-pair, we use two tags with the same type. For each type, we randomly form 10 tag-pairs. In each experiment trial, we place each tag-pair at $[x, y]$=[1,0] for registration. Then we move the tag-pair to three randomly selected positions, *i.e.*, $[x, y]$=[1,1], [-2,2], and [2,-1] for authentication. We plot the accuracy at the three positions in Fig. 27. The results show that all the three types of tags can achieve very high accuracy, which means Butterfly is a universal solution to mainstream passive RFID tags.

7.4 Authenticate Multiple Tags

As the application environments of passive RFID is mainly in retail, warehouse or places where a large amount of tags coexist, we conduct an experiment to evaluate the performance of Butterfly in the multiple-pairs scenario. We place 3, 5 and 8 pairs of tags inside the effective area, respectively. The authentication results in case 1 and 2 are shown in Fig. 28. We find that the accuracy decreases as the tag volume increases. In both case 1 and case 2, in the worst case the accuracy is still larger than 85%. We also exploit the ROC curve in multiple-pairs cases in Fig. 29. The results show that Butterfly has an acceptable performance in multiple-pairs cases. We further discuss the influence of tag volume in Section 9.

7.5 Impact of Angle Changes

Sometimes the orientation of tag-pairs varies in real applications. For example, when a staff member holds a tag-pair with different postures, the tag-pair changes its angle to the antenna of reader/monitor accordingly.

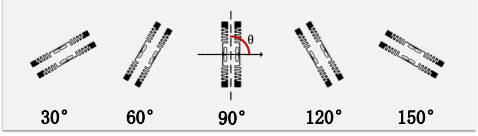


Fig. 30. Rotation of tag-pair

Table 3. The accuracy when tag pairs rotate

Angle(∘)	30	60	90	120	150
Accuracy(%)	91.7	96.7	100	95	93.3

To investigate the impact of such angle changes on Butterfly, we register 30 tag-pair when the two tags are perpendicular to the plane of the horizon and authenticate them after shifting the angle between each of tag-pair and the plane of the horizon to ±30° and ±60°, as shown in Fig. 30.

The average authentication accuracies are exhibited in Table 3. We find that when a clockwise or counter-clockwise rotation happens on a tag-pair, the authentication accuracy will slightly decline. But the overall accuracy still maintains at a high level. In the five angle settings, the average accuracy is 95.34%. Therefore, the orientation of tag pairs has little impact on Butterfly.

8 SECURITY ANALYSIS

We discuss the capability of Butterfly in defending against existing attacks as follows.

a) Tag-counterfeiting. Since the ID (EPC code) stored in a tag can be easily read by any standard readers, adversaries may simply write an overheard ID into a forged tag. More sophisticatedly, compromising attacker can fully retrieve the sensitive data, including the password or keys, stored in a legitimate tag and then duplicate the data to the forge tag. In this way, prior works based on crypto mechanisms could not distinguish the forged tag.

Butterfly identifies tag-pairs based on the physical-layer characteristics of tags, which is extremely hard to tamper. The physical-layer characteristic of each tag is determined in the manufacturing procedure, and varies among tags. Tags that are even produced by the same manufacturer will have distinguishable differences. Many existing physical-layer authentication methods successfully defend against counterfeiting attacks by using the physical-layer information based fingerprints. Compared with existing works that employ a single tag for authentication, Butterfly utilizes a pair of tags, which can extend the feature space and obviously increase the attack difficulty. If the feature space of single-tag authentication system is f, the feature space of Butterfly will be $C_f^1 \cdot C_f^1 = f^2$. We take Geneprint[9] as an example. Geneprint is a typical system for identifying the single tag. And it can achieve up to 99.68% identification accuracy for 150 RFID tags. In other words, the feature space of Geneprint is at least 150. While for Butterfly, the feature space will be $150^2 = 22500$, which is extremely larger than prior works.

b) Eavesdropping and replay attacks. Passive attackers usually eavesdrop on the communication channel between the reader and tags to retrieve sensitive information. Moreover, the attacker can record the signal and replay it later for deceiving the reader. Butterfly, together with most other physical-layer RFID authentication approaches, cannot thoroughly defend against such attacks. However, Butterfly can mitigate the impact of eavesdropping attacks by monitoring and limit the effective region. As aforementioned, signals backscattered from a tag-pair become unstable and the signal quality drastically decreases out of the effective area. Note performing replay attacks is much harder and more expensive than tag-counterfeiting.

c) Feature reconstruction attack. The principle of this attack is to forge or reconstruct the features of tag-pairs. If the attacker knows which parameters of the tag are involved in Butterfly, they may reconstruct and replicate the signals with emulators. However, it is not an easy task for attackers to obtain this information,

and both the device and emulations are very costly. The tag examiner may easily observe the existence of the emulators. An attacker may attempt to gain from each false positive or true negative result of Butterfly. In practice, the attacker will iteratively use counterfeited tags to try and expect that one of them can pass the authentication. In this way, the attacker may learn that some parameters can help to yield the false positive cases. However, infinite attempts will be prohibited if using Butterfly. When a negative result is obtained, the presenter of the tag pair will be further interrogated and verified using higher-level authentication method, such as being asked to report his/her personal ID, receipts, etc. The attacker will be penalized and pay a non-trivial cost for every true negative result. Thus, it is very costly and time-consuming to obtain and replicate the features of the tags in practice. In addition, Butterfly uses two tags instead of one tag to generate the fingerprint. Considering that reconstructing the feature of physical-layer signals is extremely difficult, such a tag-pair enhances the system security by increasing the attacking overhead, *i.e.*, reconstructing the features for two tags instead of merely one tag.

In a short summary, Butterfly is effective in preventing legitimate pairs from existing attacks.

9 DISCUSSION

The scalability of Butterfly. Butterfly can be extended to support multiple-pairs authentication. The only difference is that instead of utilizing physical-layer information to differentiate the two tags in a pair, we should decode each tag in those multiple pairs. The other signal processing modules of Butterfly can be reused without any modification. However, in the multiple-pairs scenario, every tag in the group should have a line-of-sight (LoS) propagation path to both the monitor and the reader, which slightly limits the application cases of Butterfly. Though there is such a limitation, we believe Butterfly can be easily applied in multiple-pairs scenarios for most testing sites where there is enough space for arranging tags such that they can meet the LoS requirement.

Different device choices of Butterfly. In fact, Butterfly can reduce the cost by utilizing only one transceiver device. There are two possible approaches: First, Butterfly can utilize an SDR-based reader to query the tags and collect the signals. In this implementation, the SDR device, e.g., USRP, works as a legitimate reader. Besides sending normal reader commands to tags, the SDR-based reader can also collect and record the responses from tags. In this way, only one transceiver device is sufficient for raw signal collection. Now this implementation has been applied in many existing researches. Note that the signal processing procedure of Butterfly is fully compatible with this implementation. Second, we can use the COTS reader as both the transmitter and receiver, if the manufacturer can release their APIs for retrieving raw signal data. That is because the source data we used as the input in our system is the raw received signals collected by the USRP at the receiver. For both the COTS reader and software-defined radio devices, their functions are actually similar in the components of Butterfly for signal acquiring. However, this implementation needs the supports from manufactures.

The cost of Butterfly. Instead of using one tag, Butterfly employs two tags as a unit for authentication, which will increase the cost. However, compared with one tag, the two-tag solution will make the authentication more practical and robust. Since the passive RFID tag is extremely cheap (several cents), the cost for adding another tag seems rewarding. Note Butterfly does not need to be deployed for every tag, but the tags that need special security concern, which may be a small population.

Environmental factors in practice. Our experiments are conducted in practical environments, where wireless signals like Wi-Fi[13][12], Bluetooth and FM radio co-exist. Therefore, Butterfly is robust and can be deployed in diverse environments. Besides interference, we also consider the cases that the tag-pair pasted on a metal surface or non-conductive material. We conduct experiments by placing the tag-pair on the metal surface. The authentication results are not good (< 20%) and the receiver may even not receive the responses from these tags. That is because the distance between the transmit-receiver devices and the tag-pair is extremely long for battery-free IoT devices. And the metal surface absorbs most RF energy and make the tag mute. To cope with this problem, we can adopt anti-metal tags, or increasing the transmission power of the reader.

10 CONCLUSION

In this paper, we present an environment-independent physical layer authentication scheme for passive RFID tags, called Butterfly. The main advantage of Butterfly is the resilience to environments, locations, and device changes, which are major problems in prior solutions. We implement a prototype Butterfly and conduct extensive experiments for evaluation. The results show that Butterfly is very effective and accurate in authentication (up to 96.7%). We also analyze the security of Butterfly from the perspectives of defending against existing attacks. From the analysis, we find that Butterfly outperforms prior solutions using physical-layer fingerprints. In particular, Butterfly is resilient to environment and device changes, while providing high authentication accuracy and much larger fingerprint space.

ACKNOWLEDGMENTS

This paper is partially supported by the NSFC Grant No. 61872285, 61772236, 61572396, 61802299 and Alibaba-Zhejiang University Joint Research Institute of Frontier Technologies. Chen Qian, and Xin Li were partially supported by National Science Foundation Grants CNS-1717948 and CNS-1750704.

REFERENCES

[1] NXP UCODE DNA RFID. https://www.nxp.com/docs/en/fact-sheet/UCODEDNATRACKLF.pdf.
[2] A. N. Akansu and R. A. Haddad. *Multiresolution Signal Decomposition: Transforms, Subbands, and Wavelets*. Academic press, 2001.
[3] L. Bruns and S. Chakraborty. Method for cryptographically combining hf and uhf rfid tags/smart cards to create a single multi-use credential, 2008.
[4] B. Danev, H. Luecken, S. Capkun, and K. El Defrawy. Attacks on physical-layer identification. In *In Proceedings of the third ACM conference on Wireless network security(WISEC)*. ACM, 2010.
[5] H. Ding, C. Qian, J. Han, G. Wang, Z. Jiang, J. Zhao, and W. Xi. Device-free detection of approach and departure behaviors using backscatter communication. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, pages 167–177. ACM, 2016.
[6] EPCglobal. Specification for RFID Air Interface EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHzÍC960 MHz, 2008.
[7] M. Feldhofer and J. Wolkerstorfer. Strong crypto for rfid tags - a comparison of low-power hardware implementations. In *In Proceedings of the IEEE International Symposium on Circuits and Systems*, 2007.
[8] G. Franceschetti and S. Stornelli. From the Physical Layer to Communication, Computing, Sensing and Control. In *Wireless Networks*, 2006.
[9] J. Han, C. Qian, P. Yang, D. Ma, Z. Jiang, W. Xi, and J. Zhao. Geneprint: Generic and accurate physical-layer identification for uhf rfid tags. *IEEE/ACM Transactions on Networking (TON)*, 24(2):846–858, 2016.
[10] Y. Hou, J. Ou, Y. Zheng, and M. Li. PLACE: Physical layer cardinality estimation for large-scale RFID systems. *IEEE/ACM transactions on networking*, 24(5):2702–2714, 2016.
[11] K. Koscher, A. Juels, V. Brajkovic, and T. Kohno. Epc rfid tag security weaknesses and defenses: Passport cards, enhanced drivers licenses, and beyond. In *In Proceedings of the ACM CCS*, 2009.
[12] Z. Li, Y. Xie, M. Li, and K. Jamieson. Recitation: Rehearsing wireless packet reception in software. In *Proceedings of ACM MobiCom*, 2015.
[13] Y. Liu and Z. Li. aleak: Privacy leakage through context-free wearable side-channel. In *Proceedings IEEE INFOCOM*, 2018.
[14] L. M. Ni, Y. Liu, Y. C. Lau, and A. P. Patil. LANDMARC: indoor location sensing using active RFID. *Wireless networks*, 10(6):701–710, 2004.
[15] S. C. G. Periaswamy, D. R. Thompson, and J. Di. Fingerprinting rfid tags. *IEEE Transactions on Dependable and Secure Computing*, 8(6):938–943, 2011.
[16] A. Poschmann, G. Leander, K. Schramm, and C. Paar. New light-weight crypto algorithms for rfid. In *In Proceedings of the IEEE International Symposium on Circuits and Systems*. IEEE, 2008.
[17] L. Shangguan, Z. Yang, A. X. Liu, Z. Zhou, and Y. Liu. STPP: Spatial-temporal phase profiling-based method for relative RFID tag localization. *IEEE/ACM Transactions on Networking*, 25(1):596–609, 2017.
[18] D. X. Song, D. Wagner, and A. Perrig. Practical techniques for searches on encrypted data. In *In Proceedings of the IEEE Symposium on Security and Privacy(S&P)*. IEEE, 2000.
[19] G. Wang, C. Qian, H. Cai, J. Han, H. Ding, and J. Zhao. Replay-resilient physical-layer authentication for battery-free iot devices. In *Proceedings of ACM Hotwireless*, 2017.

[20] G. Wang, C. Qian, J. Han, W. Xi, H. Ding, Z. Jiang, and J. Zhao. Verifiable smart packaging with passive rfid. In *In Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing*. ACM, 2016.

[21] J. Wang and D. Katabi. Dude, where ́s my card?: RFID positioning that works with multipath and non-line of sight. . In *In Proceedings of the ACM International Conference on the applications, technologies, architectures, and protocols for computer communication(SIGCOMM)*. ACM, 2013.

[22] L. Xie, Q. Li, C. Wang, X. Chen, and S. Lu. Exploring the gap between ideal and reality: An experimental study on continuous scanning with mobile reader in rfid systems. *IEEE Transactions on Mobile Computing*, 14(11):2272–2285, 2015.

[23] L. Xie, C. Wang, A. X. Liu, J. Sun, and S. Lu. Multi-touch in the air: Concurrent micromovement recognition using rf signals. *IEEE/ACM Transactions on Networking*, 26(1):231–244, 2018.

[24] L. Yang, Q. Lin, C. Duan, and Z. An. Analog On-tag Hashing: Selective Reading as Hash Primitives for COTS Gen2 RFID Systems. In *In Proceedings of IEEE MOBICOM*, 2017.

[25] D. Zanetti, B. Danev, et al. Physical-layer identification of UHF RFID tags. In *In Proceedings of the IEEE International Conference on Mobile Computing and Networking(MOBICOM)*. ACM, 2010.

[26] D. Zanetti, P. Sachs, and S. Capkun. On the practicality of UHF RFID fingerprinting: How real is the RFID tracking problem? In *Privacy Enhancing Technologies*. Springer, 2011.

[27] P. Zhang, J. Gummeson, and D. Ganesan. Blink: A high throughput link layer for backscatter communication. In *In Proceedings of the 10th international conference on Mobile systems, applications, and services*. ACM, 2012.

[28] Y. Zheng and M. Li. P-MTI: Physical-layer missing tag identification via compressive sensing. *IEEE/ACM Transactions on Networking (TON)*, 23(4):1356–1366, 2015.

Received May 2018; revised July 2018; accepted October 2018