Towards Replay-resilient RFID Authentication

Ge Wang [†‡], Haofan Cai [‡], Chen Qian [‡], Jinsong Han [*♯], Xin Li [‡], Han Ding [†], Jizhong Zhao [†]

[†]Xi'an Jiaotong University, Xi'an, China.
[‡] University of California, Santa Cruz, CA, USA.
[*]Institute of Cybersecurity Research, Zhejiang University, China.
[♯]ZJU-Alibaba Joint Cyber Security and Privacy Research Laboratory, China.

ABSTRACT

We provide the first solution to an important question, "how a physical-layer authentication method can defend against signal replay attacks". It was believed that if an attacker can replay the exact same reply signal of a legitimate authentication object (such as an RFID tag), any physical-layer authentication method will fail. This paper presents Hu-Fu, the first physical layer RFID authentication protocol that is resilient to the major attacks including tag counterfeiting, signal replay, signal compensation, and brute-force feature reply. Hu-Fu is built on two fundamental ideas, namely inductive coupling of two tags and signal randomization. Hu-Fu does not require any hardware or protocol modification on COTS passive tags and can be implemented with COTS devices. We implement a prototype of Hu-Fu and demonstrate that it is accurate and robust to device diversity and environmental changes, including locations, distance, and temperature. Hu-Fu provides a new direction of battery-free/low-power device authentication that enables numerous IoT applications.

CCS CONCEPTS

• **Security and privacy** → **Mobile and wireless security**;
• **Network security** → *Mobile and wireless security*;

KEYWORDS

Internet of things; RFID; Device authentication

MobiCom '18, October 29-November 2, 2018, New Delhi, India
© 2018 Association for Computing Machinery.
ACM ISBN 978-1-4503-5903-0/18/10...$15.00
https://doi.org/10.1145/3241539.3241541

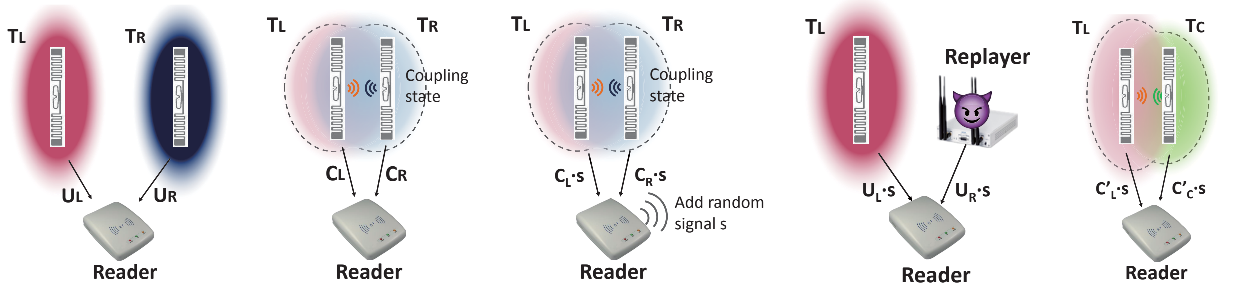
ACM Reference Format:
Ge Wang, Haofan Cai, Chen Qian, Jinsong Han, Xin Li, Han Ding, Jizhong Zhao. 2018. Towards Replay-resilient RFID Authentication. In *The 24th Annual International Conference on Mobile Computing and Networking (MobiCom '18), October 29 - November 2, 2018, New Delhi, India.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3241539.3241541

1 INTRODUCTION

Battery-free wireless communication, in particular passive RFID, is a promising solution of the Internet of Things (IoT), due to its energy efficiency and low cost [3, 10, 23, 24, 26, 28, 29, 33, 34, 36, 39]. In recent years, security issues of IoT devices have drawn increasing attentions. Among these issues, device authentication is one of the most important problems. IoT device authentication aims to validate whether a device is indeed the legitimate one which has been registered in the system. It is a crucial task in many applications such as the access control to an area or event, electronic payment, and tamper-evident packaging. However, the limited computing capability of battery-free devices restricts the execution of cryptographic algorithms such as hashing and encryption. In fact, commodity off-the-shelf (COTS) passive RFID tags do not support strong cryptographic operation and current UHF tags have no cryptographic capabilities. [1] Hence many classic security solutions are impossible to use on commodity passive tags. In addition, since a tag is simple and cheap, its memory may not be securely protected. If an attacker obtains the secret, it can easily produce unlimited counterfeits.

To this end, many researchers investigate to utilize physical-layer information of RFID tags for identification/authentication tasks [6][37][8][17]. Physical-layer identification methods are based on the fact that different tags may include hardware differences due to manufactural imperfection. Hence a tag can be verified using certain physical features and a

[1] To our knowledge, the only tag with a cryptographic function is the recently announced NXP UCODE DNA RFID [1]. However all related documents are for commercial purposes. Hence we are not clear about its cryptographic strategy, reliability, and other characteristics.



(a) Non-coupling

(b) Coupling makes the signal different

(c) Hu-Fu performs signal randomization

(d) Replaying U_R will be rejected

(e) Counterfeit can be detected

Figure 1: Utilize coupling state and signal randomization to defend against various attacks

counterfeited tag is unlikely to have highly similar physical features with the legitimate one [6][37][17]. However, it is known that physical-layer identification/authentication is vulnerable to several major attacks, and whether there exists a solution to defend against them was considered an "open question" [8].

Major attacks. We summarize four major attacks to physical layer authentication.

1. *Tag counterfeiting*; the attacker uses an unauthorized tag to let it carry the same ID of a legitimate tag.
2. *Signal replay*; the attacker eavesdrops the physical signals of a legitimate tag, captures them in a digital form, and then replays the exactly same signals towards the reader [7][8].
3. *Signal compensation*; the attacker obtains a signal that can pass the authentication, called a valid signal. Then during the authentication process, it compensates the current signal in the environment to become the valid signal [9].
4. *Brute-force feature replay*; Assuming the attacker knows the feature extraction algorithm and owns sufficiently many tags, it extracts the feature of every tag until getting one tag that presents a feature close enough to the legitimate tag [8].

All prior physical-layer identification methods mainly defend against tag counterfeiting, but are vulnerable to the remaining three attacks [7]. Traditional network protocols using a cryptographic nonce to defend against replay attacks but passive tags are obviously unable to use it. Signal and feature replay has been considered as an ultra-weapon to physical-layer authentication. A recent work [17] states "*To our knowledge, no existing work can effectively defend against such an attack (signal replay), including our work*". In [7] it states "*Signal replay makes the attacker frames almost indistinguishable from the genuine frames... Whether such impersonation detection (of signal or feature replay) is feasible, is an open question.*"

In this paper, we provide the first answer to such an open question, **a new direction of physical-layer authentication that is resilient the attacks listed above**. The proposed authentication method is called Hu-Fu.[2] Hu-Fu is based on two ideas. First, we observe the fact of *inductive coupling* of two adjacent tags [35][16] from real experiments, that if we place two tags in close positions (*e.g.*, in 2cm), the backscatter signal from either tag would be different from the signal by putting the tag alone. The coupling signal of a tag also depends on the other tag. Hence we use a tag, called the Retained Tag (or Left Tag) T_L, along with the reader as the authenticator. When an authenticatee, called the Right Tag T_R, is presented, T_R should be put to a position close to T_L and an inductive coupling state is created. The system validates whether the features from the physical signals of T_R and T_L are consistent to the signals collected previously using the legitimate tag T_R. As shown in Fig. 1(a), if T_L and T_R are separate, they will reply non-coupling signals U_L and U_R. However, if they are close enough, in Fig. 1(b) their signals will become C_L and C_R. The authentication features are extracted from C_L and C_R. The second idea, called *signal randomization* and introduced in a recent work [18], is to allow the reader sends a one-time random signal $s(t)$ that changes with time t. Then the backscatter signal C_R become $C_R \cdot s(t)$, which appears random to an eavesdropper who has no information of $s(t)$, shown in Fig. 1(c). The eavesdropper is even unable to tell whether a tag is transmitting or not. But the reader is able to remove $s(t)$ for decoding. Hu-Fu makes an attacker incapable to capture, replay, or compensate the signal or feature that can pass the authentication, because C_L and C_R are hidden. For example in Fig. 1(d), if an attacker records U_R by querying T_R using an unauthorized reader, even if it replays U_R, Hu-Fu will find the difference

[2] Hu-Fu, also called tiger tallies, were authentication seals used by ancient Chinese emperors to command and dispatch the army. The right piece was retained by the emperor and the left piece was issued to the general of the army. When a messenger sends a imperial command to the general, he must show the right tally that matches exactly to the left piece. Hu-Fu was famous for the tale of Lord Xinling in *The Records of the Grand Historian.*

between $< C_L, C_R >$ and $< U_L, U_R >$ and reject the replay. As in Fig. 1(e), since the attacker does not know C_R, the signal from a counterfeit C'_c will highly likely to be different from C_R and it cannot get accepted.

Both inductive coupling and signal randomization are essential components of Hu-Fu. They work together to block the access of attackers to valid signals and features from legitimate tags. Without inductive coupling, an attacker can easily get the reply signal from a legitimate tag by querying it using an unauthorized reader. Then the attacker replays it to the reader. Without signal randomization, the attacker can eavesdrop on C_L and C_R and try to use signal compensation or brute-force feature replay to re-build the signals.

Hu-Fu effectively protects the following information, which is the basis of the major attacks to physical-layer authentication. 1) The coupling signal of the pair of tags; 2) The feature of a legitimate tag, even though the attacker knows the feature extraction algorithm; 3) What signal can pass the authentication process. By cutting the source of these attacks, Hu-Fu effectively ensures the success of physical-layer authentication.

Hu-Fu is also cost-efficient. It does not require any change on COTS tags. A Hu-Fu reader can be built with COTS wireless devices. It is also easy if a vendor wants to change its readers to be compatible to Hu-Fu. The authentication time is fast (< 1.5sec).

The major contributions of Hu-Fu are as follows:

- Hu-Fu is the **first tag authentication solution** to defend against counterfeiting, signal replay, signal compensation, and feature replay attacks that is compatible to the standard protocol. It provides a new direction of battery-free/low-power IoT device authentication.
- Hu-Fu is robust to the device and environment diversity. It uses environment- and reader-independent features, hence it can accurately authenticate tags that are registered at different places.
- We implement a working prototype of Hu-Fu and conduct extensive experiments to demonstrate its security and reliability.

In the rest of this paper, we first present the overview of Hu-Fu in Section 2. We model and validate the inductive coupling of two tags in Section 3. In Section 4, we present the detailed system design. The security analysis of our system is discussed in Section 5. The prototype implement and evaluation of Hu-Fu are introduced in Section 6. The state-of-art RFID authentication methods and conclusion are discussed in Section 7 and 9.

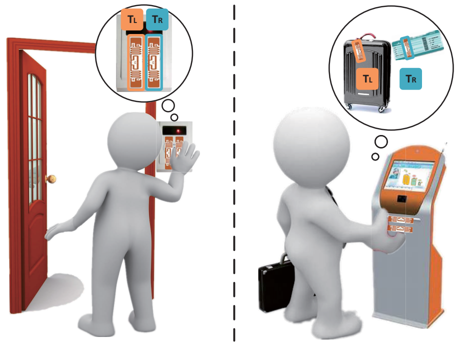


Figure 2: Two typical applications of Hu-Fu. Left: static scenario; Right: dynamic scenario

2 OVERVIEW

In this section we introduce the problem studied in this work, the system and security model, and the basic protocol work flow of Hu-Fu.

2.1 System and Security Model

Hu-Fu solves the following fundamental problem in an RFID system. Given a tag reply that reports a registered tag ID (EPC), the RFID system needs to decide whether the reply was from the authorized tag that has been registered with this ID, called a *legitimate tag*, or from an attacker who does not hold the legitimate tag. The tag reply from an attacker could be transmitted from a different tag that carries the registered ID, called a *counterfeit*, or from a powerful device that can replay any signal it has previously heard, called a *replayer*.

Depending on the application requirements, Hu-Fu may be utilized in two situations, namely static scenarios and dynamic scenarios. In a **static scenario**, a legitimate tag is registered at the *check-in site* and its physical-layer feature is collected by the system. Later it is verified at the same place for authentication. Such a scenario is useful for applications like access control. As shown in the left of Fig. 2, one tag is fixed at an entrance guard and acts as the Left Tag T_L. A first-time user registers her Right Tag at the entrance by placing it together with the Left Tag and letting the system record the physical feature under certain security control. Later when the user requests for entrance, she places her Right Tag again with the Left Tag and let the system verify it. A Left Tag can be paired with multiple Right Tags for different users. In a **dynamic scenario**, the *authentication site* where a tag is verified may be different from the check-in site. Such scenario is useful for applications such as a baggage claim system. As shown in the right of Fig. 2, a user checks in her luggage by letting the system record the physical feature of a pair of coupled tags. Then a tag is attached to the luggage, acting as the Left Tag. The user carries the Right Tag. Later at the destination of the trip, the system verifies the features

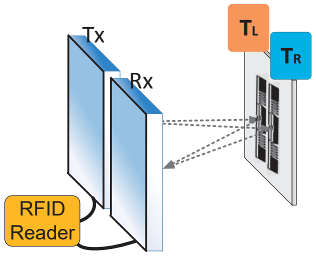


Figure 3: The deployment of Hu-Fu

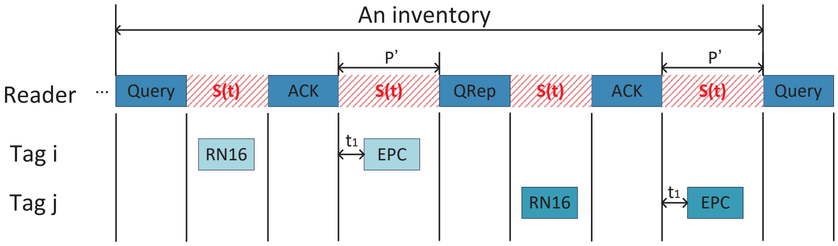


Figure 4: The design of Hu-Fu

of the pair of tags and authenticate the Right Tag presented by the user before allowing her to pick up the luggage.

Security Model. We assume a powerful attacker. It can eavesdrop on any communication between the legitimate reader and tags (attacker can also be a MIMO eavesdropper), record any signal, and replay the *identical* physical signal of prior communication to the reader, at any location including the check-in and authentication sites. However, it cannot obtain the tags' features by some active attacks at check-in and authentication sites, *e.g.*, using an unauthorized reader to query the legitimate tags. Attackers cannot block the communication channel between the legitimate reader and tags. In the dynamic scenario, the Left Tag cannot be accessed anywhere with an unauthorized reader. This assumption has been used in prior work such as [18], and it is reasonable as there are a few practical and commercial solutions that can detect and prevent active attacks, including shielding sleeves[25], RFID blocking wallets [18] and RFID reader detectors[11][22]. Right Tags do not have such a requirement. We further assume the attacker knows all authentication protocols and feature extraction algorithms.

Note that an attacker can gain from each false positive result of Hu-Fu, but it will also be penalized and pay non-trivial cost for every true negative result. When a negative result is obtained, the presenter of the right tag will be further interrogated and verified using next-level authentication method, such as being asked to show his/her personal ID, receipts, *etc.*. True negatives caused by attackers will hence be penalized. An attacker cannot try to use different counterfeited tags by infinitely many times and expect that one of them can pass Hu-Fu.

We mainly consider the four attacks presented in §1, namely 1) tag counterfeiting, 2) signal replay, 3) signal compensation, and 4) brute-force feature replay. The attacker is able to launch all of them. We focus on tag authentication and do not consider attacks that target on communication confidentiality, integrity, or availability.

To our knowledge, no prior work has considered such a powerful attacker and no prior work can defend against attacks 2), 3), and 4).

2.2 Workflow of Hu-Fu

As shown in Fig. 3, a Hu-Fu instance includes an RFID reader carrying two directional antennas.[3] The Left Tag T_L sits face to the reader and is fixed. We assume T_L cannot be destroyed, replaced, nor its communication channel to the reader can be blocked. The reader and T_L are together acting as the Hu-Fu authenticator. A tag as the 'authenticatee' is denoted as the Right Tag T_R. Hu-Fu has two phases, namely registration phase and authentication phase. Every legitimate tag j should have been registered to the system. To register a tag, it should be placed to a position in 2cm distance to T_L and become the Right Tag T_R. Certain features of the physical signals from T_L and T_R will be collected and stored in a back-end server associated with T_R's ID. Later if a tag claiming to be T_R is present and Hu-Fu needs to valid its authenticity, the tag will be putted to the place 2cm to T_L and become T_R. Their backscatter signals will be analyzed in order to verify that the features are consistent to the record of T_R stored at the back-end server. **A Left Tag can be paired with multiple Right Tags.**

The main idea of Hu-Fu is utilizing both the **inductive coupling** phenomenon between two adjacent tags and **signal randomization**. A passive tag can be modeled as a kind of coil. When a tag is powered by the reader, a current will flow inside the coil. As we all know, a steady current on a circular can generate a magnetic field around it [35][16], which may influence the current in adjacent circulars. That is why two close tags will inductive coupling with each other. In addition, due to the manufacturing imperfection, the inductive coupling phenomenons are not identical for different tag pairs. We utilize this characteristic of passive tags to perform authentication. Suppose tags T_L and T_R replies signals U_L and U_R respectively when they are not coupled. If they are in the coupling status, T_L and T_R's signals will become C_L and C_R respectively, whose features are used for authentication. Hence an attacker cannot get C_R by using an unauthorized

[3] We use a USRP-based Software Defined Radio (SDR) to build the reader. In fact, Hu-Fu utilizes the raw received signals as the feature source, which can also be captured by COTS readers. Hence we believe Hu-Fu can be easily implemented on COTS readers by a vendor [2].

reader to query T_R. However, it may still eavesdrop on C_L and C_R during the registration or authentication process.

Hu-Fu is able to hide C_L and C_R during the registration or authentication process. According to EPC C1G2 protocol [13], after transmitting commands, the reader will keep sending a constant carrier wave to supply energy to tag population. A tag will randomly choose a slot to reply. In our design, as shown in Fig. 4, instead of transmitting a constant carrier wave, we let the reader sends a one-time random signal $s(t)$ that changes with time t. Hence an attacker can only obtain $C_L \cdot s(t)$ and $C_R \cdot s(t)$ by eavesdropping on the registration/authentication process. The reader can easily extract and decode C_L and C_R since it knows $s(t)$. Since C_L and C_R are hidden, the attacker cannot extract the features from valid tags even if it knows the feature extraction algorithms. All attacks can be successfully defended by hiding both the valid signals and features. Note Hu-Fu does not need any hardware or protocol changes on COTS passive tags.

In addition, authenticating two tags as a unit is also helpful for extracting environment-independent features. For two tags that close with each other, the surrounding environments are very similar. This phenomenon can be applied in noise removal. Hu-Fu can effectively cope with environment diversity and achieve high accuracies in both static and dynamic scenarios.

3 MODEL AND VALIDATE TAG COUPLING

We show that *inductive coupling* introduces significant signal difference to RFID tags, by modeling and experimental validation.

The fundamental reason of inductive coupling is the electromagnetic induction. According to the Biot-Savart Law [35], a steady current on a circular can generate a magnetic field around it. We specific it by the model shown in Fig. 5. According to the physical property of the dipole-aerial design, each tag can be modeled as a circular loop [5] [35]. We set the origin point as the center of the circular of the Left Tag T_L. Let vector $\vec{d}$ denote the directional vector from the center of T_L's circular to that of the Right Tag T_R. When a reader inventories the pair of tags and induces a current I_1 on the circular of T_L, a magnetic field B_{21} will occur on T_R:

$$B_{21} = \frac{\mu_0}{4\pi} \oint_c \frac{I_1 d\vec{l} \times (\vec{d} - \vec{r})}{|\vec{d} - \vec{r}|^3}, \tag{1}$$

where $\vec{r}$ is the radius vector from the circular center of T_L to the differential element $d\vec{l}$ on the wire, the direction of $d\vec{l}$ is defined as the same with the conventional current I_1, and μ_0 is the magnetic constant. As a result, the magnetic filed B_{21} will introduce a magnetic flux Φ_{21} that go through T_R's loop. If the effective area of T_R's loop is S_2, the magnetic flux $\Phi_{21} = B_{21} \cdot S_2$. In this way, we can further measure the mutual inductance M_{21} between T_L and T_R:

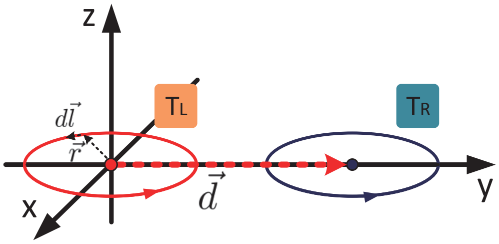


Figure 5: Model of two coupling tags

$$M_{21} = \frac{\Phi_{21}}{I_1} = \frac{\mu_0}{4\pi} \oint_c \frac{1}{|\vec{d} - \vec{r}|^2}. \tag{2}$$

According to Eq. 2, we find that the mutual inductance M_{21} is independent of the current in the circular of either T_L or T_R. It is only related to the relative position ($\vec{d}$) and the physical feature of the equivalent circular ($\vec{r}$).

In this way, we can divide the electromotive force E_2' to T_R into two parts: the internal electromotive force E_2 and the induced electromotive force E_{21}:

$$E_2' = E_2 + E_{21} = E_2 + (-N_2 \frac{d\Phi_{21}}{dt}), \tag{3}$$

where N_2 is the loop number of T_R, E_2 is the internal electromotive force of T_R in non-coupling case, and E_{21} represents the value that induced by the current in T_L's circular. As a result, the current I_2 on the circular of T_R in non-coupling case will change to I_2' accordingly:

$$I_2' = \frac{E_2'}{R_2} = \frac{E_2}{R_2} + \frac{E_{21}}{R_2} = I_2 - \frac{N_2}{R_2} \cdot \frac{d\Phi_{21}}{dt} \tag{4}$$

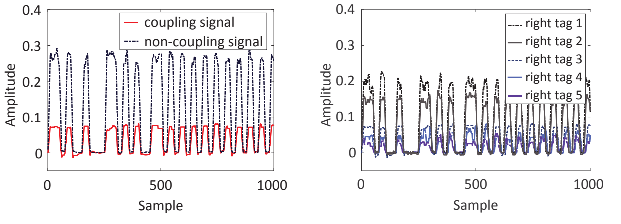
Considering Eq. 4 and 2, we have:

$$I_2' = I_2 - \frac{N_2}{R_2} \cdot \frac{dM_{21}}{dt} \cdot I_1. \tag{5}$$

In this way, we build a relationship between the influenced current I_2' in T_R with I_1 and I_2, as well as the physical features of itself (N_2, R_2, etc). Accordingly, the influenced current I_1' in T_L:

$$I_1' = I_1 - \frac{N_1}{R_1} \cdot \frac{dM_{12}}{dt} \cdot I_2. \tag{6}$$

Therefore when a pair of tags are put together, the coupled signal from either of them depends on the physical features of both tags. The coupled signals are different for different pairs of tags. If the attacker replaces one of them, the influenced current I_1'/I_2' will change. To verify this fact, we conduct two experiments. In the first experiment, we collect the non-coupling signal of T_L and then put a right tag T_R close to T_L with 2cm distance. As shown in Fig. 6(a), with the interference of the right tag, the coupling signal of T_L has obvious difference to the non-coupling one *in amplitude*. We then change the right tag to four other different ones. We do



(a) Coupling and non-coupling signals of T_L

(b) The coupling signals of T_L with different T_R

Figure 6: The inductive coupling phenomenon

not change any settings of the former experiment, including the parameters, environments and the tag's position. We show the coupling signal of the T_L in Fig. 6(b). We find that with the interference of different right tags, the coupling signals of the same left tag also have distinguishable differences in amplitude. Hence by querying T_L or T_R separately, the attacker cannot obtain the amplitude-based features that are used for authentication. Since the coupling signals are protected by randomization, the attacker is not able to obtain any valid signal or feature that can pass the authentication.

4 SYSTEM AND PROTOCOL DESIGN

To authenticate a tag presented to Hu-Fu, the system includes three modules to determine the result 'Accept' or 'Reject', namely signal collection, signal preprocessing, and feature extraction and comparison as shown in Fig. 7. The signal collection module aims to collect the signals from two coupling tags in a secure way with the reader. The signals are then processed to remove the random signal and environmental noise, in the signal preprocessing module. Finally, in feature extraction and comparison module, we propose two types of features, namely coupling feature and authentication feature, which are used for authenticating the tag and detect different kinds of attacks. Our design is compliable to the existing EPC protocol [13] and requires no change on passive tags.

4.1 Signal collection

In Hu-Fu the reader queries both the Left and Right Tags and then collects the backscatter signals from them. The deployment of Hu-Fu is shown in Fig. 3. We place the Tx and Rx antennas in a line. Both of them stand facing to the tag pair. In both the registration and authentication phases, Hu-Fu first collects the backscatter signal from T_L by keeping querying T_L for one second. Then T_R is placed within 2cm distance to T_L on the test board. Hu-Fu collects the backscatter signal from both T_L and T_R by keep querying them for another second.

To prevent attackers from eavesdropping and recording the coupling signals, the Hu-Fu reader sends a random signal instead of constant carrier waves during each tag response. As shown in Fig. 4, the reader transmits a random signal $s(t)$ instead of the carrier waves (cw). This mechanism has been introduced in RF-Cloak [18]. The authors of [18] have proved that this mechanism can overcome a single-antenna eavesdropper that uses the optimal decoder. For a MIMO eavesdropper, it may extract the coding of the legitimate tags. However, it is still not able to estimate the physical-layer features of each tag. The information it obtained is far from enough for recording, reconstructing and replying the original signals. We discuss it in Appendix A. Hence Hu-Fu can effectively prevent attackers from eavesdropping or recording the coupling signal. Without the knowledge about the coupling signal, attackers can hardly compensate uncoupling signals or find out a counterfeited tag that owns a similar hardware characteristic with the legitimate one.

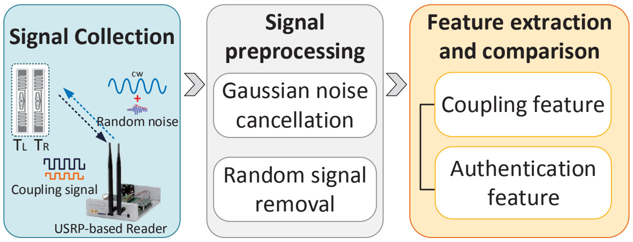


Figure 7: System design

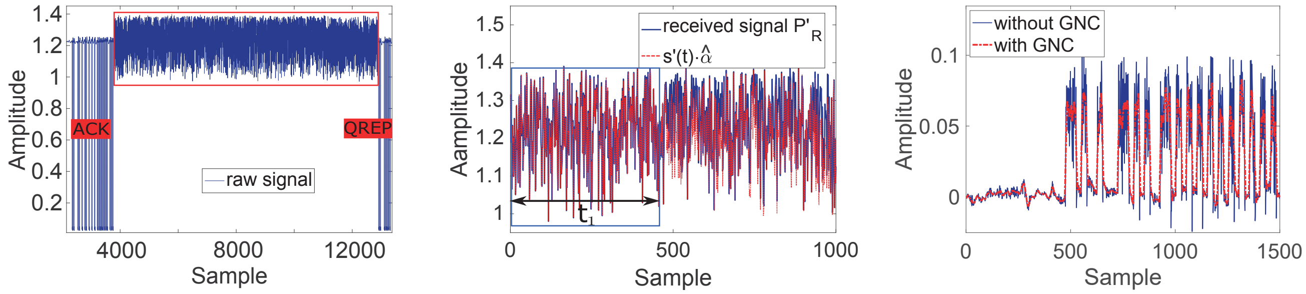
In our implementation, we use a USRP radio to achieve these tasks. The entire process can also be implemented on a COTS reader without introducing much complexity, if a vendor wants to.

Utilizing this mechanism, when a tag responds its data, the reader transmits a random signal $s(t)$ with the power of $P_R(t)$. We develop a model of the backscatter signal under such randomization using basic communication theory. Due to the space limitation, the detailed derivation is skipped. The received signal P'_R from a tag at the receiver of the reader R can be modeled as follows:

$$P'_R(t) = \gamma \cdot \gamma' \cdot h(R, T_i, T_j) \cdot s(t) \cdot x(t) + N_G, \tag{7}$$

where $h(R, T_i, T_j)$ is related to the hardware characteristics and relative positions of the reader R and two tags T_i and T_j,[4] γ and γ' are the attenuation parameters of the paths from the reader to tag and backwards, $x(t)$ is the original tag signal, and N_G is the Gaussian white noise introduced by devices. According to the EPC C1G2 protocol [13], we retrieve the tag's EPC signal segment by cutting out the signal between each valid *ACK* and its next command (usually *QueryREP*/*QueryAdj*/*Query*), and use it as the received signal P'_R.

[4] The detailed representation is $\frac{P_R \cdot G_{T_i} \cdot G_{Tx} \cdot |\Gamma_{T_i}|^2 \cdot \lambda^2}{16\pi^2 \cdot D^2} \cdot [G_{T_i} - \frac{N_i}{R_i} \cdot \frac{dM_{ij}}{dt} \cdot G_{T_j}]$ where G_{Tx} and G_{T_i} are the antenna gains of the reader and the tag T_i, Γ_{T_i} is the modified reflection coefficient, which is determined by the antenna resistance and reactance of both reader and the tag, D is the distance, and M_{ij} is the mutual inductance.



(a) Raw signal (b) Estimate $\hat{\alpha}$ (c) Random signal removed

Figure 8: Signal pre-processing. Due to signal overlaps, (b) and (c) are easier to read with colors.

4.2 Signal preprocessing

According to Eq. 7, we find that the received signal is influenced by many factors, including random signal, white noises and environment noises. To obtain the hardware-dependent features, we should first eliminate noises and remove the random signal $s(t)$. Hu-Fu processes the signal using two steps: Gaussian white noise cancellation and random signal removal.

Gaussian noise cancellation (GNC). Although we have no idea about the exact value of Gaussian white noise at a given time, the noise has a normal distribution in the time domain with an average value of zero, *i.e.*, $G_N \sim \mathcal{N}(0, \sigma^2)$. Hence we may employ a mean filter with a time window w to remove the Gaussian noise, *i.e.*:

$$P_1^*(t) = \text{MEAN}[P_R'(x)], x \in [t - w/2, t + w/2], \tag{8}$$

where t is the time point of a signal sample. The basic idea of the mean filter is that within a time window, the average value of Gaussian noise should be 0. While the other parts of signal P_R' are highly likely to be unchanged. Hence the signal P_1^* can be modeled as:

$$P_1^*(t) \approx \gamma \cdot \gamma' \cdot h(R, T_i, T_j) \cdot s(t) \cdot x(t). \tag{9}$$

Based on empirical experience, we choose the time window w as 10 samples, which is about half of a square wave.

Random signal removal. Then Hu-Fu removes the random signal that is used to hide the responses from tags. The inner structure of the reader (implemented by SDR in our prototype) is shown in Fig. 9 [20][4]. We generate a random signal $s'(t)$ in reader logic module and then send it instead of the constant carrier waves. However, before the SDR reader transmits $s'(t)$, it will put $s'(t)$ into an amplifier, *i.e.*, $s(t) = \alpha \cdot s'(t)$, where α represents the magnification times of the amplifier. In practice, we do not know the exact value of α and have no idea about the exact value of $s(t)$. That introduces a challenge in this step.

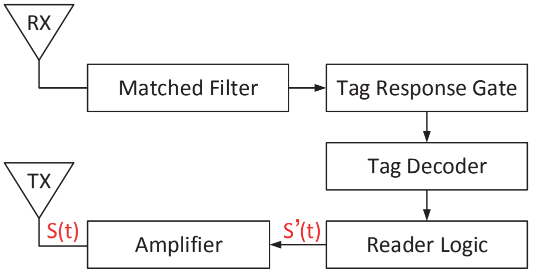


Figure 9: The structure of SDR reader

Fortunately, we find that after the reader finishes transmitting *ACK* commands, a tag will wait for a relatively stable time period t_1, before it starts to respond. As shown in Fig. 4, the tag will not start to transmit the EPC during time $[t_0, t_0+t_1]$, where t_0 is the time when the reader finishes transmitting its *ACK*. Hence the signal during time $[t_0, t_0 + t_1]$ can be expressed as follows:

$$P_R'(t) = \gamma^* \cdot h(R) \cdot s(t) + N_G, \tag{10}$$

where γ^* is the propagation parameter through the transmitting path, and $h(R)$ is only related to the reader hardware. After canceling the Gaussian white noise, we can estimate amplifier coefficient α as follows:

$$\hat{\alpha} = (P_R'(t) - N_G)/s'(t) = \gamma^* \cdot h(R) \cdot \alpha, \tag{11}$$

Utilizing the estimated amplifier parameter $\hat{\alpha}$, we can remove the random signal $s(t)$ for the signal samples collected after time $t_0 + t_1$, *i.e.*:

$$P_2^*(t) = P_1^*(t)/(\hat{\alpha} \cdot s'(t)), \tag{12}$$

Based on Eq. 9 and 12, $P_2^*(t)$ can be modeled as $\frac{\gamma \cdot \gamma'}{\gamma^*} \cdot \frac{h(R, T_i, T_j)}{h(R)} \cdot x(t)$. In practice, we can assume that the transmission channels stay unchanged in a very short time. As a result, the environment parameters, *i.e.*, $\gamma \cdot \gamma'/\gamma^*$, can be considered static when a tag responds its EPC, which costs just several microseconds. Even if the attacker can run the same preprocessing algorithm, it is not able to get $P_2^*(t)$ because it has no information of $s'(t)$.

In Fig. 8, we show an example of the preprocessing module. The raw data received at Rx is as shown in Fig. 8(a), the entire time between *ACK* and *QREP* (marked by a red rectangle) is covered by a random signal and the EPC signal can't be recognized. We zoom in the red rectangle and show the details in Fig. 8(b). The blue curve is the EPC signal, while the red dotted line is the estimated $s(t)$. We show in Fig. 8(c) the signal after removing the random signal, and find that we can recover the tag's EPC segment effectively. Canceling the Gaussian noise is very necessary, for the signal after GNC (the red curve) is much easier for decoding.

4.3 Feature extraction and comparison

To defend against different types of attacks, we propose to use two features in Hu-Fu, namely the *coupling feature* and *authentication feature*. The coupling feature is to determine whether the Left Tag is indeed coupling with another tag, while authentication feature aims to verify whether the Right Tag is the legitimate one. The coupling feature can be used to detect signal replay and the authentication feature is effective to detect tag counterfeiting. Note that both the two features are insensitive to the environment, *i.e.*, we can use them for tag authentication even if the registration phase and authentication phase happen at different locations.

Extracting the coupling feature. We first specify how to extract the coupling feature. In the signal collection module, Hu-Fu first collects the uncoupling signal of the Left Tag T_L and then records the coupling signals of both Left and Right Tags in the same situation. After pre-processing, let U_L denotes the signal of T_L in the non-coupling state, C_L and C_R denote the processed signals of T_L and T_R in the coupling state. Based on our model,

$$\begin{aligned} U_L(t) &= \frac{\gamma \cdot \gamma'}{\gamma^*} \cdot \frac{h(R, T_L)}{h(R)} \cdot x(t) \\ C_L(t) &= \frac{\gamma \cdot \gamma'}{\gamma^*} \cdot \frac{h(R, T_L, T_R)}{h(R)} \cdot x(t), \end{aligned} \tag{13}$$

where $h(R, T_L)$ represents the hardware characteristic parameters without inductive coupling, which can be modeled as $\frac{\lambda^2 \cdot G_{Tx} \cdot G_{T_L}^2 \cdot |\Gamma_{T_L}|^2}{16\pi^2 \cdot D_{R\to T_L}^2}$. We define the coupling feature as:

$$F_c = \frac{\int_{t_s}^{t_e} U_L dt}{\int_{t_s}^{t_e} C_L dt}, \tag{14}$$

where t_s and t_e are the start and end time of the tag's EPC segment. We detect them by finding the sudden rising/-falling edge of the received signal. F_c can be modeled as $\int_{t_s}^{t_e} G_{T_L} \cdot [G_{T_L} - \frac{N_L}{R_L} \cdot \frac{dM_{LR}}{dt} \cdot G_{T_R}]dt$ according to Eq. 13 and 14. We find that F_c is independent of the environment and reader hardware. In addition, F_c can be used to detect signal replay attack. If the attacker uses a signal replayer but not the actual Right Tag at present, the Left Tag will transmit a non-coupling signal. Under this circumstance, the coupling feature F_c will be close to 1. However, if there is indeed exist a correct Right Tag, the coupling feature F_c is much less than 1. We also validate that different Right Tags may introduce different hardware parameter $h(R, T_i, T_j)$. Hence the coupling feature F_c is also able to authenticate the right tag. We further introduce the authentication feature that enhances the accuracy of detecting a different Right Tag.

Extracting the authentication feature. The coupling feature F_c is used by Hu-Fu to determine whether the Left Tag T_L is indeed coupled with another Right Tag. If the attacker utilizes a counterfeited Right Tag, it is likely that F_c will be different. However, in some cases, Hu-Fu may observe similar F_c for different Right Tags. Hence we propose two metrics as the authentication feature. The first metric is defined as the specific value of energy spectrum of the Left and Right Tags, *i.e.*:

$$F_e = \frac{\int_{t_s}^{t_e} C_L dt}{\int_{t_s}^{t_e} C_R dt}, \tag{15}$$

Based on Eq. 13, F_e can be modeled as

$$F_e = \frac{h(T_L, T_R) \cdot \int_{t_s}^{t_e} x_L(t)dt}{\int_{t_s}^{t_e} x_R(t)dt},$$

where $h(T_L, T_R)$ is $\frac{G_{T_L} \cdot |\Gamma_{T_L}|^2}{G_{T_R} \cdot |\Gamma_{T_R}|^2} \cdot \frac{G_{T_L} - \frac{N_L}{R_L} \cdot \frac{dM_{LR}}{dt} \cdot G_{T_R}}{G_{T_R} - \frac{N_R}{R_R} \cdot \frac{dM_{RL}}{dt} \cdot G_{T_L}}$, only depending on the hardware characteristic of the two tags, and $x_L(t)$ and $x_R(t)$ are the data-dependent signal functions of the Left and Right Tags, respectively. We find that F_e is independent of the environment or reader. In addition to the hardware characteristics of T_L and T_R, F_e also takes the data-dependent signal functions $x(t)$ into consideration. However even though two Right Tags carry the same data, Hu-Fu will measure different values of the integral results (and hence different F_e), because the BLF of different tags is different. We will show that even if the attacker utilizes a counterfeited Right Tag that owns the same ID as the legitimate one, it cannot pass the authentication.

To further improve the authentication accuracy of Hu-Fu, we propose another authentication metric, namely Power Spectral Density (PSD). The PSD feature reflects the distribution of power into frequency components composing that signal [30]. The second authentication metric F_p is defined as:

$$F_p(T_i) = |\int_{t_s}^{t_e} e^{-j2\pi f_i t} C_i(t)dt|^2, \; i = \text{'}L\text{' or '}R\text{'}, \tag{16}$$

where f_L and f_R represent the corresponding frequencies of the Left and Right Tags. Hu-Fu calculates and records both $F_p(T_L)$ and $F_p(T_R)$ from each EPC segment of the two tags.

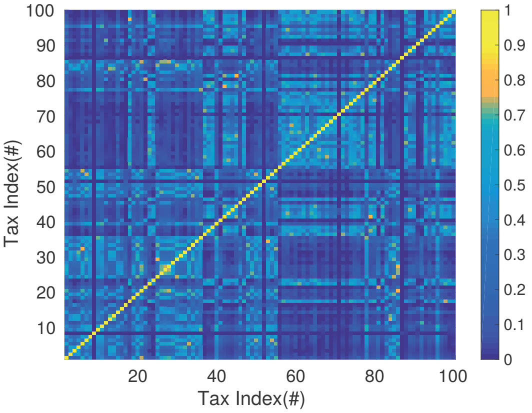


Figure 10: CORR among 100 tags

In practice, the surrounding moving objects may also introduce unpredictable errors. To tackle this problem, we pair each C_L and C_R that collected in an inventory round (as shown in Fig. 4), which have very adjacent reply time to calculate the authentication features.

We further define a vector $[F_e, F_p(T_L), F_p(T_R)]$. For an authenticatee tag, Hu-Fu calculates the *Cross Correlation Coefficient* (CORR) of the two authentication vectors collected at the registration and authentication phases.

Authentication logic. The authentication of a presented tag returns either 'Accept' or 'Reject'. If the coupling feature F_c is larger than a threshold ε determined by empirical results, Hu-Fu immediately returns 'Reject'. Otherwise, Hu-Fu calculates CORR of the two authentication vectors collected at the registration and authentication phases. If CORR is larger than another threshold ρ, Hu-Fu returns 'Accept'. Note the choice of both ε and ρ is **universal** in a system: each of them uses one single value for all tags in a Hu-Fu system. We do not need to determine them for each individual tag.

5 SECURITY ANALYSIS

In this section, we provide the detailed analysis on how Hu-Fu defends against the four major attacks, namely tag-counterfeiting, signal replay, signal compensation, and brute-force feature replay.

Tag counterfeiting. The attacker uses its own tag to carry the ID of a legitimate tag, and wants to get access to some region or resource. Most existing physical-layer authentication methods focus on solving this problem. By analysing the physical features from the signal from a tag, physical-layer authentication decides whether the presented tag has very similar features of the legitimate tag with the ID. To demonstrate that the feature used in Hu-Fu is unique and can be used for authentication purpose, we conduct the following experiments. We use 101 ALN-9840 tags, pick one tag as the Left Tag, and use the other 100 tags as the Right Tag. We calculate the feature CORR of all pairs among the 100 Right tags, which are coupled with the same Left tag under the same situation. As shown in Fig. 10, we find that 84% features have distinctly different features (CORR<0.5). Only 0.55% of the CORR values show similar features of two Right Tags (CORR>0.74, where 0.74 is the default value of threshold and can be set higher). We use other Right tags, which show similar results. Hence Hu-Fu can successfully detect counterfeited tags that carry the same ID but different physical features. One potential problem of defending against tag counterfeiting is that, if the registration and authentication happens in different environments, including location changes and dynamic moving objects. We will show Hu-Fu is robust to environmental changes in §6.3. An advanced tag counterfeiting attack is brute-force feature replay, which will be discussed later.

Signal replay attack. The attacker first eavesdrops on the backscatter communication of a legitimate tag, either during the registration/authentication period or using an unauthorized reader to query the tag. Then the attacker replays the identical signal to cheat the authenticator. Compared to tag counterfeiting, this attack requires a more powerful device at the attacker, which can replay signals. Existing methods are difficult in defending against signal replay. One unique advantage of Hu-Fu is that, even if an attacker can eavesdrop on all communication of a legitimate tag. None of these signals can pass Hu-Fu. The attacker can record the signal U_R of the legitimate tag in a non-coupling state, but U_R cannot pass Hu-Fu as shown in Fig. 1(d). It can also record the coupling signals $C_L \cdot s$ and $C_R \cdot s$ but replaying them does not work either, because next time the random signal is different. In addition, since simply replaying the signal will not make T_L in a coupling state, Hu-Fu can also detect signal replay if it finds T_L still transmits $U_L \cdot s$. Even if the attack may use both signal replay and a counterfeited tag, it still has no way to produce $C_L \cdot s$ and $C_R \cdot s$.

Signal compensation attack. In signal compensation, the attacker knows the signal that can pass the authentication, denoted as $\Im$. Assume the current signal in the environment is $\Im'$. The attacker can compensate the existing signal $\Im'$ to make it become $\Im$. Signal compensation might work if Hu-Fu is not protected by signal randomization. For example, the attacker eavesdrops on a prior registration or authentication of the legitimate tag and records C_L and C_R. Then it uses a faked tag and compensates any signal to make the signals be C_L and C_R. In Hu-Fu, C_L and C_R are protected by the one-time random signal s. The attacker can only get $C_L \cdot s$ and $C_R \cdot s$, which will fail to pass the next authentication because Hu-Fu will use another random signal. The attacker has no idea about the coupling signals, not to mention reconstructing them.

There is another reason that signal compensation to Hu-Fu is difficult. The RFID tags comply slotted-ALOHA-based

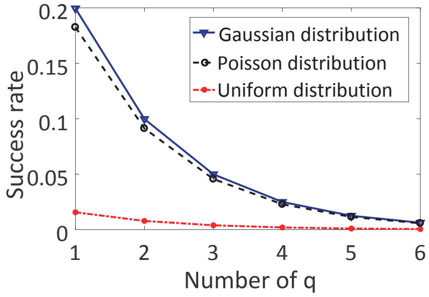


Figure 11: Success rate that the attacker hit the right start point in a slot

communication protocol [13]. Based on the protocol, after receiving the slot number, *i.e.*, 2^q, from the reader, tags will randomly select one slot to response. At that slot, a tag will wait for an uncertain time t_1 and then start to transmit the backscatter signal. According to the protocol [13], the range of t_1 is roughly from $184\mu s$ to $216\mu s$. In other words, the tag may start to respond at any time during the $32\mu s$. Because Hu-Fu transmits a random signal during tag's backscatter, attackers have to guess at which time point the tag will start to transmit. To discuss the success possibility of attackers to hit the right start point and reconstruct the coupling signal, we conduct a simulation. In fact, we have no idea about the exact probabilistic model of t_1. So we use three common models, namely Gaussian distribution, Poisson distribution and Uniform distribution, to simulate it. As shown in Fig. 11, the success probability goes down with the increased number of slots. However, even under the worst case, *i.e.*, there are only 2 slots ($q = 1$) in each inventory round and the values of t_1 follow a Gaussian distribution, the attackers only have less than 20% probability to compensate the signal to the expected one successively.

By combining the two reasons, Hu-Fu is resilient to the signal compensation attack.

Brute-force feature replay attack. Assuming the attacker knows the feature extraction algorithms and obtains sufficiently many tags, it extracts the feature of every tag until getting one tag that presents a feature close enough to the legitimate tag. Then that tag can be used as a strong counterfeit. Hu-Fu is also resilient to brute force attack. Since Hu-Fu randomizes the communication channel between the reader and the legitimate tags, the coupling signals are difficult to obtain. Hence the attacker does not know the valid features, even if the attacker knows the feature extraction algorithms. It is impossible to find an unknown feature from the tags owned by the attacker.

Tag tracking attack. Tag tracking does not target on the authenticity of an RFID system, but on the privacy. Hence as an authentication method, Hu-Fu does not need to be resilient to tag tracking, but it still worths discussion. Current COTS passive tags have no ability to protect their replies being eavesdropped by an attacker. The tag locations and moving trajectories can be tracked. In §6.2 we use experiments to show that a single-antenna eavesdropper is unable to decode any ID information from the signal that being covered by randomization. Hence Hu-Fu also improves the tag privacy.

6 IMPLEMENTATION AND EVALUATION

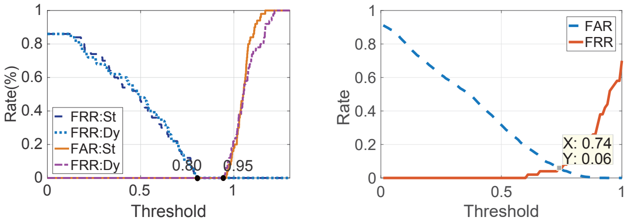
6.1 Prototype Implementation

We implement a prototype system of Hu-Fu with a USRP N210 equipped with an SBX daughter-board and two Laird S9028-PCL directional antennas. The center frequency of USRP-based SDR reader varies among [905MHz, 910MHz, 915MHz, 920MHz, 925MHz]. Note that in practice, we can randomly select center transmitting frequency from 902MHz to 928MHz. The sampling rate is 2MHz, and the transmission gain and receiving gain are both 25dB. The distance between the reader and tag pairs is 20cm. We have verified that most main-stream brands and models of passive RFID tags have the inductive coupling phenomenon and can be used in Hu-Fu, including ALN-9740, ImpinJ E41C/B, and Alien 964X. The prototype is compatible to the standard EPC Class 1 Generation 2 protocols (C1G2) [13]. In our experiments, we run the software components of Hu-Fu at a Dell desktop, which equips Intel Core i7-7700 CPU at 3.6 GHz and 16G memory.

As aforementioned, Hu-Fu has the registration phase and authentication phase. At the registration phase of a tag T_R, Hu-Fu collects the features introduced in § 4.3. Then the features are stored in a database running on a back-end server, indexed by the tag ID. At the authentication phase of the tag, Hu-Fu calculates its features and compared them to the stored features of the same tag ID. Hu-Fu returns either 'Accept' or 'Reject'.

6.2 Evaluation of Randomization

Methodology. We evaluate whether an attacker can obtain any useful information from Hu-Fu to conduct signal or feature replay attacks. Since tag replies will be covered by a one-time random signal, replaying the same signal will absolutely result in a 'Reject' because the random signal is different. We further ask an easier question to the attacker: whether it is able to decode or infer any bit from the tag replies covered by random signals. Note even if an attacker can decode the bits, it is still not able to conduct a successful reply attack. We conduct a set of experiments that use Hu-Fu to query 50 commercial tags in different models for 1000 times in total. The experiments are conducted in both static and dynamic scenarios. In static scenarios (St), registration and authentication happen at the same place. In dynamic



(a) Accuracy of determining coupling state (b) Accuracy of Hu-Fu in static scenarios (c) Accuracy of Hu-Fu in dynamic scenarios

Figure 12: Accuracy of Hu-Fu

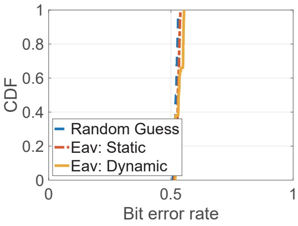


Figure 13: BER of an eavesdropper

scenarios (Dy), they happen in different places. We allow an eavesdropper to obtain the signal of the entire communication, which then tries to decode the signal by reading the rising and falling edges. We measure the Bit Error Rate (BER) of the eavesdropper.

Fig. 13 shows the cumulative distribution of the BER for the eavesdropper in St and Dy as well as the random guess (i.e., amplitude > 50% to 1 and ≤ 50% to 0). We find the BER for all three cases are extremely close to 50%, which implies they provide almost no information of the bits of tag replies. The average BER for St and Dy are 52.85% and 53.18%, with a standard deviation of 1.27% and 1.79%, respectively. The eavesdropper is not obviously better than a random guess.

On the other hand, the BER of Hu-Fu in all 100 experiments is always 0.

6.3 Evaluation of authentication quality

Methodology. We first evaluate the authentication accuracy of Hu-Fu in both static and dynamic scenarios. We define two accuracy metrics of physical-layer authentication, namely *False Accept Rate* (FAR) and *False Reject Rate* (FRR):

$$FAR = n_a/n_n; \ FRR = n_r/n_l$$

where n_n is the number of tests that use non-legitimate tags, n_a is the number of 'Accept' results among tests using non-legitimate tags, n_l is the number of tests that use legitimate tags, and n_r is the number of 'Reject' results among tests using legitimate tags. FRR is also equal to 1 - Recall. Note in practice, false acceptances are usually considered more harmful and critical than false rejections. It is because the users that are falsely rejected will usually go through other off-line and more reliable authentication processes, such as verifying their photo IDs or other certificates. On the other hand, false acceptance will allow an illegal user to get access to the protected area/objects. In addition to FAR and FRR, we use the *classification accuracy*, a metric that has been used by existing physical-layer identification methods [17, 37] for comparison. These experiments work as follows. Each method collects the testing features from a number of tags and classify each feature to one of the existing stored features that were from these tags. The accuracy is the rate of features that are correctly classified.

Table 1: Accuracy comparison

	Hu-Fu	[COV,PSD]	[TIE,ABP]	Spectral
St	95%	99%	96%	99.6%
Dy	90%	77.8%	36.24%	37.6%

Table 2: Hu-Fu accuracy with mobility

	Coupling state	Authentication
(FAR,FRR)	(0%, 0%)	(3.42%, 10%)

Note in the experiments, we give a huge advantage to the attacker by assuming the tag ID matching is always correct. However in actual cases since Hu-Fu hides the tag replies, the attacker has no information of the tag ID (see results in $6.2) if we can protect the Right Tag carefully from being queried by a malicious reader. **Hence even though the results show some level of FAR, the actual FAR of a practical attacker is still almost 0 if it has no information of the tag ID.**

Accuracy of determining a coupling tag. The first step of the authentication logic is to compare the coupling feature F_c with the threshold ε. Fig. 12(a) exhibits the FRR and FAR of Hu-Fu for determining the coupling state. Note that the FRR and FAR here are not calculated based on the final authentication results, but only the middle results for determining the coupling state of the Left Tag. We find that FAR and FRR in both St and Dy drop to 0 when ε is in the range of [0.8, 0.95]. This result is robust to different models of tags. Hence determining a coupling Left Tag is highly accurate. In other experiments, we set the threshold ε as 0.85.

Accuracy of Hu-Fu. After verifying the coupling state, Hu-Fu determines whether the CORR of authentication features that collected at registration and authentication phases is larger than the threshold ρ. It returns 'Accept' if CORR > ρ and 'Reject' otherwise. We show the FRR and FAR for static cases in Fig. 12(b) and for dynamic cases in Fig 12(c), by varying the threshold ρ. We find that when $\rho = 0.74$ in St, both the FAR and FRR are 6%. We set $\rho = 0.83$ to make FAR < 2% and allow 10% FRR. When $\rho = 0.62$ in Dy, both

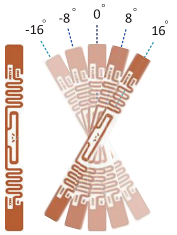


Figure 14: The intersection angle of two tags

the FAR and FRR are 4%. However, to make FAR < 2%, FRR may be a slightly higher than 10%.

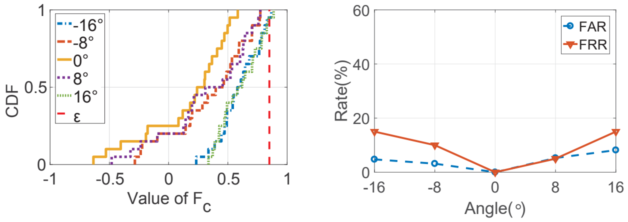
Comparison to existing methods. We compare Hu-Fu to existing physical-layer identification methods, including the COV and PSD method used in Geneprint [17], the time interval error (TIE), average baseband power (ABP), and spectral feature (SP) proposed by Zanetti *et al.* [37][38]. We perform these methods in both static and dynamic cases, and use a Bayesian classifier to classify 50 tags. We conduct multiple production experiments for every tag. The classification results are shown in Table 1. In St, all methods have high accuracy. Hu-Fu has a little lower accuracy than other methods. That is because signal processing, including the Gaussian noise and random signal removal, will more or less distort the tag's signals and introduce unpredictable errors in authentication. However, in Dy, only Hu-Fu can maintain a high accuracy and other methods are not resilient to environment changes. Note none of the prior methods can defend against reply attacks. Hu-Fu achieves an extra advantage of accuracy in Dy, because it can use a pair of tags to eliminate environmental factors.

Time cost of Hu-Fu. Hu-Fu is fast. In our experiments, all authentication decisions are made within 1.5 seconds. Existing work do not mention their authentication times. We believe that 1.5 seconds is an acceptable time for authentication applications.

6.4 Impact of environmental factors

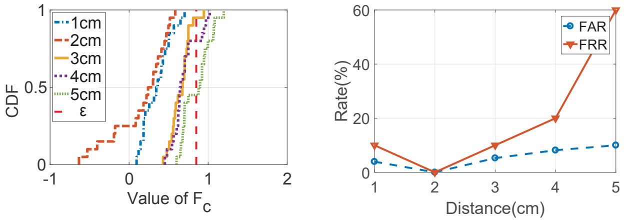
In this section, we evaluate the performance of Hu-Fu under the impacts of practical factors. Note that we do not alter the system threshold. Because we have no idea about the environmental factors at each moment.

In mobility environments. Moving persons and objects around the reader usually cause unstable signals due to multipath reflection [36]. To evaluate the robustness of Hu-Fu with moving objects, we conduct the experiments by allowing a person walking around the reader with a speed of 1 ∼ 2m/s. We first register 50 right tags in one place, and then authenticate them at another place. The results are shown in Table 2. We find that Hu-Fu still achieves 100% accuracy in determining a coupling Left Tag. The FAR and FRR of authentication the right tag do not increase much.



(a) CDF of F_c (b) Authentication accuracy

Figure 15: Accuracy by varying the angle



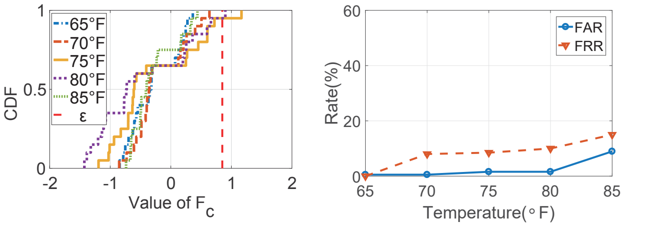
(a) CDF of F_c (b) Authentication accuracy

Figure 16: Accuracy by varying the distances

Varying tag angles. We evaluate the performance of Hu-Fu when the Right Tag is not fully parallel to the Left Tag. We define the intersection angle between Left and Right Tags as the angle between their antenna directions as shown in Fig. 14. The separation distance between two tags' centers is 2cm. We first collect the signals when the left tag is fully parallel to the right tags as the registration record, and then utilize the signals when the two tags have intersection angles as the authentication data. We exhibit the values of the coupling feature F_c for different angles in Fig. 15. The red dashed line is the threshold. When the angle is no more than ±8°, all F_c values are smaller than the threshold, which means the coupling determination is always correct. For tags that with ±16° intersection angles, Hu-Fu has a FAR of 5%. The authentication error rates are shown in Fig. 15(b). We find that the FARs are no more than 5% and the FRRs are no more than 10%, when the angle is between $-16°$ to 8°. According to the results, we can safely infer that an intersection angle smaller than about 8° may not impact the results significantly. Intersection angles larger than 8° are very obvious and easy to correct.

Varying tag distances. We evaluate whether the separation distance between the Left and Right Tags is a factor that may influence the authentication results. We use the records that the two tags have a $2cm$ separation distance as the registration data. Then we move the right tag with a separation distance from $1cm$ to $5cm$. Fig. 16(a) exhibits the CDF of coupling feature F_c by varying the distances. We find that the coupling features of tags with a distance smaller than $4cm$ are mostly smaller than the threshold ε. The authentication error rates are shown in Fig. 16(b), the FARs for 1cm to 3cm distances are all smaller than 10%. Hence by slightly moving the Right Tag, the results are still reliable.

Varying the temperature. The outside temperature may change the hardware characteristic of the RFID tag and make its signals distort. In this set of experiments, we will discuss the impact of temperature on the system's performance. We first collect registration data at $18.3^\circ C$ ($65^\circ F$) and then heat the room to conduct authentication at $21.1^\circ C$ ($70^\circ F$), $23.9^\circ C$ ($75^\circ F$), $26.7^\circ C$ ($80^\circ F$), and $29.4^\circ C$ ($85^\circ F$), respectively. As shown in Fig. 17, most coupling states can be accurately determined when the temperature changes. The authentication FAR and FRR for different temperatures $\leq 80^\circ F$ are extremely low ($\leq$ 1.5% and $\leq$ 10%), but increase for $\leq 85^\circ F$. As long as the system operator keeps the temperature $\leq 80^\circ F$, Hu-Fu has stable accuracy.



(a) CDF of F_c

(b) Authentication accuracy

Figure 17: Accuracy by varying the temperature

7 RELATED WORK

Recent effort has been made to authenticating RFID tags. Most existing solutions fall into two categories: crypto-based and physical-layer approaches.

Crypto-based approaches aim to utilize conventional cryptographic algorithms to perform the authentication. After allowing each tag to share a secret key with the reader, the reader will accept a tag as a valid one only if the tag can replay a cipher depending on the secret [12, 14, 15, 21, 31]. However, Crypto-based methods suffer from several drawbacks. First, it is difficult for these methods to be implemented on COTS passive tags as they are commonly with a need of changing the current industrial standards and introducing non-trivial financial cost and labor cost. To our knowledge, the only tag claimed with a cryptographic function is the NXP UCODE DNA RFID [1], but its price is much higher than COTS tags ($67,000 for 77K tags, not available for purchase under 77K tags). Its performance and actual security level are unclear to the public, because there is no report from its users. Using tags with a cryptographic function may have several limitations. First, the current main-stream COTS tags need to be replaced, which introduce non-trivial financial cost and labor cost. Second, the process of storing secret key on tags may also be vulnerable to some eavesdropping and active attacks. Third, if the secret keys are stolen, it will be easy for attackers to produce unlimited counterfeit tags. In contrast, Hu-Fu does not need to modify the protocol or substitute the deployed tags. In addition, it is infeasible for an attacker to produce many counterfeits that can pass the authentication. Our conclusion is, even if on-chip cryptographic passive tags would be available in future, Hu-Fu still has its unique advantages.

Physical-layer identification approaches leverage the hardware diversity of tags [6, 17, 19, 32, 37] caused by manufactural imperfection. Danev *et al.* [6] show the feasibility of using the physical-layer information to detect cloned or counterfeit RFID tag. Zanetti *et al.* [6] further propose physical-layer identification of UHF RFID using the time interval error (TIE), average baseband power (ABP) and spectral feature as the fingerprints. Periaswamy *et al.* [27] use a specific device to extract the Minimum Power Response of RF signals as the fingerprint. Geneprint [17] utilizes the covariance among the square waves of two tags' signals as the fingerprint, which reduces the cost of feature extraction. These methods name themselves as 'identification' rather than 'authentication' and they are not robust against the signal-replay, brute force, and signal compensation attacks [7]. Physical-layer identification has also been investigated for other wireless devices such as 802.11 and 802.15.4 [8], but there is no effective solution for the attacks mentioned in §1. RF-Cloak [18] is a recent solution that protests tags from eavesdropping. It the first work to introduces signal randomization. However, it mainly focuses on providing confidentiality and does not validate tag authenticity.

8 DISCUSSION

A crucial concern is that whether an attacker can model the interactions between legitimate tags if he could obtain their uncoupling signals. Our answer is that modeling and reconstructing the coupling signals of the legitimate tags are extremely difficult. There are two reasons: 1) As aforementioned in Section. 2.1, we assume the Left tag is always under higher security protection. Hence the attacker cannot access the uncoupling signals of the Left tag. Only obtaining the uncoupling signal of the Right tag is not enough to infer their interactions. 2) There remains a huge gap between molding the interaction of a tag pair and obtaining their uncoupling signals. Due to the complexity of indoor environments, both the signal collection and reply are vulnerable to the environment changes. Even if the attacker can extract the corresponding characteristics of the Right tags, they are not able to infer the environment variation at the current moment. During the authentication process, the signal from the Left tag includes environment factors and an attacker is difficult to create the coupling signals of both Left and Right tags.

9 CONCLUSIONS

Hu-Fu is a physical layer authentication method for battery-free IoT devices, in particular, passive RFID tags. Hu-Fu is the first solution that is resilient to a number of major attacks to physical layer authentication, including tag counterfeiting, signal replay, signal compensation, and brute-force feature reply. We design Hu-Fu with two essential ideas, namely inductive coupling and signal randomization. We provide a complete security analysis of the resiliency to these attacks. We build a prototype of Hu-Fu and conduct extensive experiments to show that Hu-Fu can achieve reliable accuracy under environmental changes.

10 ACKNOWLEDGMENT

This work was partially supported by National Basic Research Program of China (973 Program) under Grant No 2015CB351705, NSFC Grant No. 61572396, 61751211, 61772413, National Science and Technology Major Project of the Ministry of Science and Technology of China JZ- 20150910 and Alibaba-Zhejiang University Joint Research Institute of Frontier Technologies. Haofan Cai, Chen Qian, and Xin Li were partially supported by National Science Foundation Grants CNS-1717948 and CNS-1750704.

APPENDIX

A RESISTANCE TO MIMO ATTACKERS

At check-in site, an attacker first eavesdrops with n antennas. The received signals $y_1(t)$, $y_2(t)$, ..., $y_n(t)$ on each of its n antennas can be modeled as follows:

$$Y(t) = [\Gamma_{ra} + \Gamma_{ta} \cdot \gamma_{rt} \cdot h(R, T_i, T_j) \cdot x(t)] \cdot s(t), \tag{17}$$

where $Y(t) = [y_1(t), y_2(t), ..., y_n(t)]^T$, and $\Gamma_{ra} = [\gamma_{r1}, \gamma_{r2}, ..., \gamma_{rn}]^T$, $\Gamma_{ta} = [\gamma_{t1}, \gamma_{t2}, ..., \gamma_{rn}]^T$. Here γ_{rn}, γ_{tn} and γ_{rt} are the transmitting parameters through wireless channels from reader to the n-th eavesdropper's antenna, the tag to the n-th eavesdropper's antenna and the reader to the tag, respectively. As specifies in [18], the eavesdropper can eliminate the random signal $s(t)$ by dividing two received signals at two antennas i and j, *i.e.*,

$$\frac{y_i(t)}{y_j(t)} = \frac{\gamma_{ri} + \gamma_{ti} \cdot \gamma_{rt} \cdot h(R, T_i, T_j) \cdot x(t)}{\gamma_{rj} + \gamma_{tj} \cdot \gamma_{rt} \cdot h(R, T_i, T_j) \cdot x(t)}, \tag{18}$$

where $x(t)$ is the data of the tag. It has two states, namely *off* and *on*. We can further model $x(t)$ as:

$$x(t) = \begin{cases} 0, & state\ is\ off \\ A_t, & state\ is\ on \end{cases} \tag{19}$$

where A_t is the amplitude of the *on* state, which is related to the hardware characteristic of the tag. It can be a value larger or smaller than the state of *off*. The eavesdropper can decode the data of the tag by comparing the ratio of $y_i(t)/y_j(t)$. When the state is off, the ratio is γ_{ri}/γ_{rj}, or it is $\frac{\gamma_{ri}+\gamma_{ti}\cdot\gamma_{rt}\cdot h(R,T_i,T_j)\cdot A_t}{\gamma_{rj}+\gamma_{tj}\cdot\gamma_{rt}\cdot h(R,T_i,T_j)\cdot A_t}$.

To reconstruct the right coupling signals at authentication site, the attacker should transmit a well-calculated signal $y'(t)$:

$$y'(t) = \frac{(\gamma'_{tr})^2}{\gamma'_{ar}} \cdot h(R', T_i, T_j) \cdot x(t) \tag{20}$$

where γ'_{tr} and γ'_{ar} are the transmitting parameters from the position the tag should at to the reader and the attacker to the reader. Since the reader we used in authentication site maybe different with the one in check-in site, the hardware characteristic $h(R', T_i, T_j)$ maybe not identical to the previous one, *i.e.*, $h(R, T_i, T_j)$. [5] .

Observing the received signals $y_i(t)$ of the MIMO attacker in Eq. 17 and the coding it obtains in Eq. 18, we find that the attacker is extremely hard to retrieve the original physical-layer feature, *e.g.*, $h(R, T_i, T_j) \cdot A_t$, of the legitimate tags. They should first estimate each transmitting parameter Γ_{ra}, Γ_{ta}, γ_{rt} accurately. Then at the authentication site, it should estimate the hardware characteristic $h(R', T_i, T_j)$ and the channel parameter γ'_{rt} and γ'_{ar} in real time. Since the attacker cannot block the communication channel between the Left tag and the reader, he has to estimate and imitate the changing channel between the reader and the position the Right tag should be. Or Hu-Fu will not cancel the environment difference between the reconstructing signals and the one sent by the Left tag. In fact, it is a difficult task to accurately calculate and estimate all these communication channel parameters. There are two reasons: First, the communication channel is very vulnerable to the changing of surrounding environments. The difficulty for MIMO attacker to estimate the channel parameters is no easy than that of the single-antenna attacker. And in our experiment, we have verified that Hu-Fu can successfully defend against a single-antenna attacker. Secondly, Hu-Fu randomly changes the center transmitting frequency of the reader, which may also change the channel parameters frequently. That is because signals at different frequencies have different wavelengths, which are highly related to the line-of-sight transmitting, reflections and other propagation phenomenons. As a result, a MIMO attacker can only obtain the coding of the legitimate tags. It is still very difficult for him to retrieve, reconstruct and reply the physical-layer signals of the legitimate tags.

[5] As mentioned in Section. 4.2, the detailed representation of $h(R, T_i, T_j)$ is $\frac{P_R \cdot G_{T_i} \cdot G_{Tx} \cdot |\Gamma_{T_i}|^2 \cdot \lambda^2}{16\pi^2 \cdot D^2} \cdot [G_{T_i} - \frac{N_i}{R_i} \cdot \frac{dM_{ij}}{dt} \cdot G_{T_j}]$. We find that in authentication site, the reader antenna's gain G_{Tx}, power P_R and the distance between reader and tags D maybe not identical to the ones in check-in site.

REFERENCES

[1] [n. d.]. NXP UCODE DNA RFID. https://www.nxp.com/docs/en/fact-sheet/UCODEDNATRACKLF.pdf.

[2] [n. d.]. ThinkMagic Evaluation Kit. http://www.thingmagic.com/rfid-developers-kits.

[3] Fadel Adib, Zachary Kabelac, and Dina Katabi. 2015. Multi-person localization via RF body reflections. In *Proceedings of USENIX NSDI*.

[4] Michael Buettner and David Wetherall. 2011. A software radio-based UHF RFID reader for PHY/MAC experimentation. In *RFID (RFID), 2011 IEEE International Conference on*. IEEE, 134–141.

[5] Xiaosheng Chen, Feng Lu, and T Ye Terry. 2010. The “weak spots" in stacked UHF RFID tags in NFC applications. In *Proceedings of IEEE RFID*.

[6] Boris Danev, Thomas S Heydt-Benjamin, and Srdjan Capkun. 2009. Physical-layer Identification of RFID Devices.. In *Usenix Security Symposium*. 199–214.

[7] Boris Danev, Heinrich Luecken, Srdjan Capkun, and Karim El Defrawy. 2010. Attacks on physical-layer identification. In *Proceedings of the third ACM conference on Wireless network security*. ACM, 89–98.

[8] Boris Danev, Davide Zanetti, and Srdjan Capkun. 2012. On physical-layer identification of wireless devices. *ACM Computing Surveys (CSUR)* 45, 1 (2012), 6.

[9] Boris D. Danev. 2011. *Physical-Layer Identification of Wireless Devices*. Doctoral Thesis, ETHZ.

[10] Han Ding, Jinsong Han, Alex X. Liu, Jizhong Zhao, Panlong Yang, Wei Xi, and Zhiping Jiang. 2015. Human object estimation via backscattered radio frequency signal. In *Proceedings of IEEE INFOCOM*.

[11] Han Ding, Jinsong Han, Yanyong Zhang, Fu Xiao, Wei Xi, Ge Wang, and Zhiping Jiang. 2018. Preventing Unauthorized Access on Passive Tags. In *Proceedings of IEEE INFOCOM*.

[12] Daniel Engels, Markku-Juhani O Saarinen, Peter Schweitzer, and Eric M Smith. 2011. The Hummingbird-2 lightweight authenticated encryption algorithm. In *International Workshop on Radio Frequency Identification: Security and Privacy Issues*. Springer, 19–31.

[13] EPCglobal. 2005. EPC^{TM} radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860 MHz–960 MHz.

[14] Martin Feldhofer. 2007. Comparison of low-power implementations of Trivium and Grain. In *The State of the Art of Stream Ciphers, Workshop Record*. 236–246.

[15] Martin Feldhofer and Johannes Wolkerstorfer. 2007. Strong crypto for RFID tags-a comparison of low-power hardware implementations. In *Circuits and Systems, 2007. ISCAS 2007. IEEE International Symposium on*. IEEE, 1839–1842.

[16] Jinsong Han, Chen Qian, Xing Wang, Dan Ma, Jizhong Zhao, Wei Xi, Zhiping Jiang, and Zhi Wang. 2016. Twins: Device-free object tracking using passive tags. *IEEE/ACM Transactions on Networking (TON)* 24, 3 (2016), 1605–1617.

[17] J. Han, C. Qian, P. Yang, D. Ma, Z. Jiang, W. Xi, and J. Zhao. 2016. GenePrint: Generic and accurate physical-layer identification for UHF RFID tags. *IEEE/ACM Transactions on Networking (TON)* (2016).

[18] Haitham Hassanieh, Jue Wang, Dina Katabi, and Tadayoshi Kohno. 2015. Securing RFIDs by randomizing the modulation and channel. In *Proceedings of USENIX NSDI*.

[19] Yuxiao Hou, Jiajue Ou, Yuanqing Zheng, and Mo Li. 2016. PLACE: Physical layer cardinality estimation for large-scale RFID systems. *IEEE/ACM transactions on networking* 24, 5 (2016), 2702–2714.

[20] Nikos Kargas, Fanis Mavromatis, and Aggelos Bletsas. 2015. Fully-coherent reader with commodity SDR for Gen2 FM0 and computational RFID. *IEEE Wireless Communications Letters* 4, 6 (2015), 617–620.

[21] Yudai Komori, Kazuya Sakai, and Satoshi Fukumoto. 2018. Fast and secure tag authentication in large-scale RFID systems using skip graphs. *Computer Communications* 116 (2018), 77–89.

[22] K. Koscher, A. Juels, V. Brajkovic, and T. Kohno. 2009. EPC RFID Tag Security Weaknesses and Defenses: Passport Cards, Enhanced Drivers Licenses, and Beyond. In *Proceedings of ACM CCS*.

[23] Zhenjiang Li, Yaxiong Xie, Mo Li, and Kyle Jamieson. 2015. Recitation: Rehearsing wireless packet reception in software. In *Proceedings of ACM MOBICOM*.

[24] Tianci Liu, Lei Yang, Qiongzheng Lin, Yi Guo, and Yunhao Liu. 2014. Anchor-free backscatter positioning for RFID tags with high accuracy. In *Proceedings of IEEE INFOCOM*.

[25] N. Marquardt and A. Taylor. 2009. RFID Reader Detector and Tilt-Sensitive RFID Tag. In *Proceedings of ACM CHI*.

[26] Jiajue Ou, Mo Li, and Yuanqing Zheng. 2015. Come and be served. In *Proceedings of ACM MOBICOM*.

[27] Senthilkumar Chinnappa Gounder Periaswamy, Dale R Thompson, and Jia Di. 2011. Fingerprinting RFID tags. *IEEE Transactions on Dependable and Secure Computing* 8, 6 (2011), 938–943.

[28] C. Qian, H. Ngan, Y. Liu, and L. M. Ni. 2011. Cardinality Estimation for Large-scale RFID Systems. *IEEE Transactions on Parallel and Distributed Systems* (2011).

[29] Longfei Shangguan, Zimu Zhou, Xiaolong Zheng, Lei Yang, Yunhao Liu, and Jinsong Han. 2015. Shopminer: Mining customer shopping behavior in physical clothing stores with COTS RFID devices. In *Proceedings of ACM SenSys*.

[30] Petre Stoica, Randolph L Moses, et al. 2005. *Spectral analysis of signals*. Vol. 1. Pearson Prentice Hall Upper Saddle River, NJ.

[31] Min-Te Sun, Kazuya Sakai, Wei-Shinn Ku, Ten H Lai, and Athanasios V Vasilakos. 2016. Private and secure tag access for large-scale RFID systems. *IEEE Transactions on Dependable and Secure Computing* 13, 6 (2016), 657–671.

[32] Ge Wang, Chen Qian, Haofan Cai, Jinsong Han, Han Ding, and Jizhong Zhao. 2017. Replay-resilient Physical-layer Authentication for Battery-free IoT Devices. In *Proceedings of ACM Hotwireless*.

[33] Ge Wang, Chen Qian, Jinsong Han, Wei Xi, Han Ding, Zhiping Jiang, and Jizhong Zhao. 2016. Verifiable smart packaging with passive RFID. In *Proceedings of ACM Ubicomp*.

[34] Jue Wang and Dina Katabi. 2013. Dude, where's my card?: RFID positioning that works with multipath and non-line of sight. In *Proceedings of ACM SIGCOMM*.

[35] Roald K Wangsness. 1986. Electromagnetic fields. *Wiley-VCH* (1986), 608.

[36] Lei Yang, Yekui Chen, XiangYang Li, Chaowei Xiao, Mo Li, and Yunhao Liu. 2014. Tagoram: Real-time tracking of mobile RFID tags to high precision using COTS devices. In *Proceedings of ACM MOBICOM*.

[37] Davide Zanetti, Boris Danev, et al. 2010. Physical-layer identification of UHF RFID tags. In *Proceedings of ACM MOBICOM*.

[38] Davide Zanetti, Pascal Sachs, and Srdjan Capkun. 2011. On the practicality of UHF RFID fingerprinting: How real is the RFID tracking problem?. In *International Symposium on Privacy Enhancing Technologies Symposium*. Springer, 97–116.

[39] Y. Zheng, M. Li, and C. Qian. 2011. PET: Probabilistic Estimating Tree for Large-Scale RFID Estimation. In *Proceedings of IEEE ICDCS*.