Replay-resilient Physical-layer Authentication for Battery-free IoT Devices

Ge Wang†, Chen Qian*, Haofan Cai*, Jinsong Han†, Han Ding†, Jizhong Zhao†
†Xi'an Jiaotong University, China, * University of California Santa Cruz, California, USA
[gewang.cs,dinghanxjtu]@gmail.com,[hanjinsong,zjz]@xjtu.edu.cn,[cqian12,hcai10]@ucsc.edu

ABSTRACT

On battery-free IoT devices such as passive RFID tags, it is extremely difficult, if not impossible, to run cryptographic algorithms. Hence physical-layer identification methods are proposed to validate the authenticity of passive tags. However no existing physical-layer authentication method of RFID tags that can defend against the signal replay attack. This paper presents Hu-Fu, a new direction and the first solution of physical layer authentication that is resilient to the signal replay attack, based on the fact of inductive coupling of two adjacent tags. We present the theoretical model and system workflow. Experiments based on our implementation using commodity devices show that Hu-Fu is effective for physical-layer authentication.

KEYWORDS

Internet of things; RFID; Device authentication

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. 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 any cryptographic operation. Hence many existing network security solutions are impossible to use on commodity passive tags.

One of the most important security task of IoT is device authentication. The task aims to validate whether a device is indeed the legitimate one which was registered in the system. It is a crucial task in many applications such as passes to an area or event, electronic payment, and tamper-evident packaging. One approach towards device authentication is to use physical-layer information [10][2][5]. Physical-layer identification works based on the fact that different devices may include hardware differences due to manufactural imperfection. Hence a counterfeited device is unlikely to have high similarity in certain physical features to the legitimate one [10][5].

In this work we use passive tags as an example to study physical-layer device authentication of battery-free IoT devices. Though physical-layer identification can effectively defend against tag counterfeiting, it is vulnerable to the signal replay attack, in which the attacker eavesdrop the physical signals of the legitimate tag, capture them in a digital form, and then replay the exactly same signals towards the reader [2]. This attack may require high-end wireless signal analyzers and generator. However, there is no existing solution to defend against this attack for COTS passive tags. Traditional network protocols using cryptographic nonce to defend against replay attacks but passive tags obviously has no ability to use it. Signal replay has been considered as an ultra-weapon to physical-layer authentication. The authors of [5] state that "*To our knowledge, no existing work can effectively defend against such an attack (signal replay), including our work*". RF-Cloak [6] is a recent solution that protests tags from eavesdropping without any change to COTS tags. RF-Cloak mainly focuses on providing confidentiality and does not validate tag authenticity.

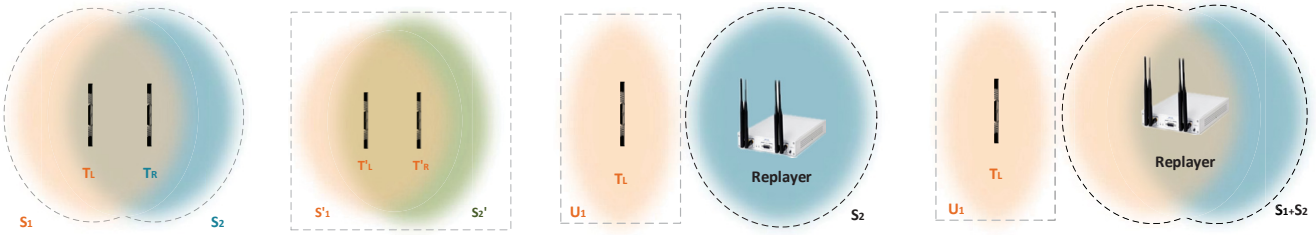
We present **a new direction of physical-layer authentication that is resilient to signal replaying**. Our idea is based on the fact of inductive coupling of two adjacent tags [9]. We observe, from real experiments, that if we place two tags in close positions (*e.g.*, in 2cm distance), the backscatter signal from either tag, say x, would be different from the signal by putting x alone, due to inductive coupling. The coupling signal of x also depend on another tag y. 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 Authentication Tag (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 just 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, shown as the signal S_1 from T_L and S_2 from T_R in Fig. 1(a).

This authentication method, called Hu-Fu,[1] is resilient to both tag counterfeiting and signal replaying. If a counterfeited

HotWireless'17, October 16, 2017, Snowbird, UT, USA

ACM ISBN 978-1-4503-5140-9/17/10...$15.00
https://doi.org/10.1145/3127882.3127887

[1] 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*.



(a) Two tags in coupling state (b) A counterfeited tag T'_R can be detected as it transmit a different signal S'_2 (c) A signal replayer transmits S_2 will be detected as T_L still transmit non-coupling signal (d) A signal replayer transmits S_1 and S_2 will also be detected as T_L still transmit non-coupling signal

Figure 1: Utilize coupling state of two tags to defend against signal replay attacks

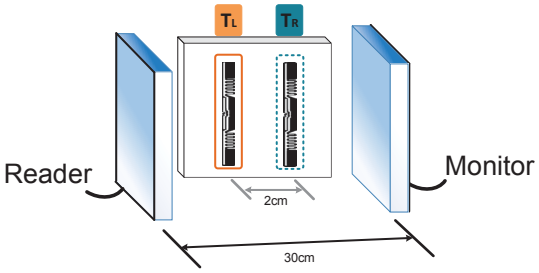


Figure 2: Overview

tag carrying the same ID of T_R is presented, it will transmit a different physical signal S'_2 compared to S_2 as in Fig. 1(b), which can be detected by the system. If an attacker use a signal replayer to replay S_2, as in Fig. 1(c), T_R will not enter the coupling state and hence transmit signal U_1, which is different to S_1. This attack can again be detected. In a more sophisticated attack, the attacker replays both S_1 and S_2 but it cannot stop R_L to transmit U_1, which again help the reader to detect such attack as in Fig. 1(d). Note we assume R_L is put into a safe place and anyone who wants to block the transmission of R_L will be immediately detected.

Hu-Fu is the first solution of replay-resilient authentication for passive tags. It does not require hardware changes on COTS tags and provides a new direction of battery-free/low-power IoT device authentication.

In the rest of this paper we will state the physical-layer authentication problem and system model in Section 2. We present the model of tag coupling in Section 3 and the system design in Section 4. We use preliminary experimental results to valid our idea in Section 5 and conclude this work in Section 6.

2 PROBLEM STATEMENT

We state the physical-layer authentication problem as follows. Hu-Fu validates whether a tag reporting a certain ID is indeed the legitimate tag with this ID that was registered in the system. Hu-Fu applies no change to the current passive RFID protocol and only requires the tag to ordinarily response to reader queries.

As shown in Fig. 2, a Hu-Fu instance includes a COTS RFID reader and a USRP-based monitor.[2] The Left Tag T_L sits between the reader and monitor and is fixed. We assume T_L cannot be destroyed, replaced, nor its signal can be blocked. The reader, monitor, and T_L are together acting as the Hu-Fu authenticator. A tag y as the authenticatee is denoted as the Right Tag T_R. Every legitimate tag y should have been registered to the system. To register a tag y, 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 stored in a backend server associated with y's ID. Later if a tag claiming to be y is present and Hu-Fu needs to valid its authenticity, the tag will be put 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 y stored at the backend server.

Note a Left Tag T_L can be paired to arbitrarily many tags. Hence each Hu-Fu instance only needs one Left Tag. Moreover, it is possible that the entire system needs multiple Hu-Fu instances. For example, a protected area may have multiple entrances. A supply chain may include multiple relay stations or inspection sites. In these cases, a Hu-Fu instance should be install in every entrance/station. For each legitimate tag, its physical features with the Left Tag of all instances should be stored.

We assume a very powerful attacker. It can eavesdrop any communication between the reader and T_L/T_R, record any communication, and replay the physical signal of prior communication to the reader. However, it cannot block the channel between the reader and T_L. We mainly consider two attacks: 1) Tag counterfeiting; the attacker forges a tag with the same ID to a legitimate tag and wants to use the counterfeited tag to cheat Hu-Fu. 2) Signal replay; the attacker records the communication between the reader and a legitimate tag and replays the exactly same signal to cheat the reader. We focus on tag authentication and do not consider attacks that target on communication confidentiality, integrity, or availability.

[2]We introduce a USRP monitor simply because COTS readers provide no API to analyze the amplitude and phase of received signals. Technically Hu-Fu can be implemented without the USRP.

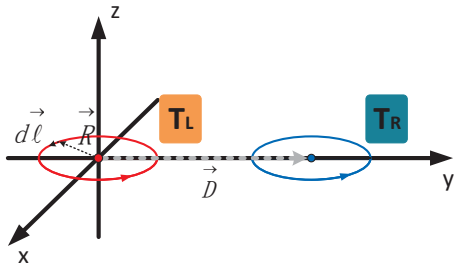


Figure 3: Model of two coupling tags

3 MODEL OF TAG COUPLING

In this section, we present a model of the coupling signal of a pair of tags T_L and T_R, which will be used as the theoretical basis of the system design of Hu-Fu.

In near-field communication, the interaction between two adjacent passive tags is called *inductive coupling*. The reason of inductive coupling is the electromagnetic induction. According to the Biot-Savart Law [9], a steady current on a circular can generate a magnetic field around it. We specific it by the model shown in Fig. 3. According to the physical property of the dipole-arial design, each tag can be modeled as a circular loop [1] [9]. We set the origin point as the center of the circular of the Left Tag T_L. And vector $\vec{D}$ denotes the directional vector from the center of T_L's circular to the circular center of the Right Tag T_R. When a reader inventories the pair of tags and induce 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 Φ_{21} can be written as:

$$\Phi_{21} = B_{21} \cdot S_2. \tag{2}$$

In this way, we can further measure the mutual inductance M_{21} between T_L and T_R:

$$M_{21} = \frac{\Phi_{21}}{I_1} = \frac{\mu_0}{4\pi} \oint_c \frac{1}{|\vec{D} - \vec{R}|^2}. \tag{3}$$

According to Eq. 3, we find that the mutual inductance M_{21} has nothing to do with the current in circular of either T_L or T_R. It is only related to the relative position ($\vec{D}$) and some 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}:

$$E_2' = E_2 + E_{21} = E_2 + (-N_2 \frac{d\Phi_{21}}{dt}), \tag{4}$$

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

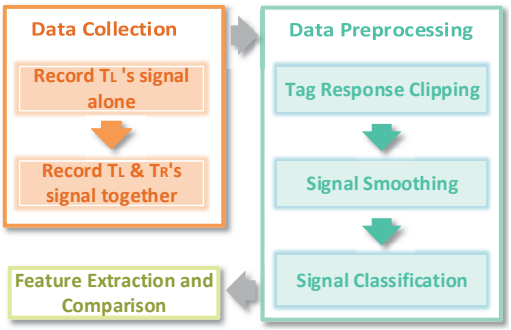


Figure 4: System workflow

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:

$$I_2' = \frac{E_2'}{R_2} = \frac{E_2}{R_2} + \frac{E_{21}}{R_2} = I_2 - \frac{N_2}{R_2} \cdot \frac{d\Phi_{21}}{dt} \tag{5}$$

Considering Eq. 5 and 3 simultaneously, we have:

$$I_2' = I_2 - \frac{N_2}{R_2} \cdot \frac{dM_{21}}{dt} \cdot I_1. \tag{6}$$

In this way, we build a relationship between the influenced current I_2' in T_R with the conventional current I_1 in T_L. In addition, the influenced current I_2' in T_R is also effected by the physical features of itself (N_2, R_2, etc). Accordingly, the influenced current I_1' in T_L is also related to the current in T_R, *i.e.*:

$$I_1' = I_1 - \frac{N_1}{R_1} \cdot \frac{dM_{12}}{dt} \cdot I_2. \tag{7}$$

In other words, when a pair of tags are put together, they will "lay a brand" on each other and the reader will receive a unique signal from each of them. If the attacker replaces one of them, the influenced current I_1'/I_2' will change. By detecting the change, Hu-Fu may determine that the tag T_R at present is not a legitimate one. Furthermore, by analyzing the conventional current I_1' on the protected tag T_L, we will find out whether it is in the state of inductive coupling.

4 SYSTEM DESIGN

To authenticate a tag presented to Hu-Fu, the system includes three stages, namely data collection, data preprocessing, and feature extraction and comparison as shown in Fig. 4.

4.1 Data collection

In a Hu-Fu instance, the reader queries the tags T_L and T_R, and the monitor passively listens to their communication. We only utilize the signals collected by the monitor, which contains both the command signal from the reader and the backscatter signals from the tags. As shown in Fig. 4, we put the monitor's antenna and reader's antenna face to face. The tags are placed on a test board between the two antennas. In both the registration and authentication cases, Hu-Fu first collects the backscatter signal from T_L by keep 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.

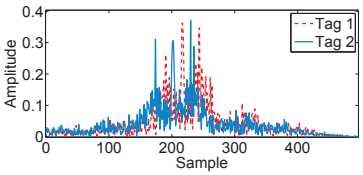


Figure 5: The FFT distribution of two tags

At each time of registration or authentication, the signal of T_L needs to be collected and analyzed. It is because the environment changes may cause signal changes at different points of time. The environment factors will be canceled using the newly collected signals every time.

4.2 Data preprocessing

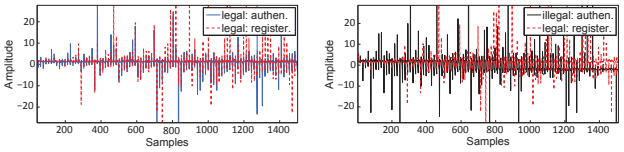
Note that the signal collected by the monitor includes reader queries and tag replies. Hence data preprocessing is necessary to determine which segment of signal belongs to which device. As shown in Fig. 4, data preprocessing consists of three steps, namely tag response clipping, signal smoothing, and signal classification.

Hu-Fu first cuts out the tag responses from the entire signal data. We utilize the method introduced in [8][3]. The basic idea is to detect the energy-intensity signals transmitted by the reader, and cut out the signal segment between commands 'ACK' and 'QREP', which are known as the front and the end of a tag's EPC signal. In this way, we can find out the tag responses effectively and accurately.

After obtaining the tag signals, we smooth the received raw signal by low-pass filtering and signal smoothing tool. Then Hu-Fu classifies these signals to the two tags T_L and T_R. To achieve this goal, Hu-Fu tries to separate the signals from the two tags apart by analyzing their physical layer features. It is known that different tags, even in the same model and type, are likely to be different in their Backscatter Link Frequency (BLF). This characteristic has also been widely verified in existing research [5][7]. To this end, we give up the traditional decoding method (decode the EPC by telling '0'/'1' bit one by one), which is very time-consuming and error-prone. Instead, we utilize the BLF feature of each tag. To extract the BLF feature, we calculate the Fast Fourier Transform (FFT) distribution of the tag response signals. As shown in Fig. 5, the FFT distribution of two different tags are stable, evidently different, and easy to separate. Hence Hu-Fu classifies the received signals by comparing their FFT distribution.

4.3 Feature extraction and comparison

In Section 3, we find that the currents of the two tags may influence each other when they are in the coupling state. The change of the conventional current in a tag's circular will trigger the change of signal power. Let $\vec{U_1}$ denote the the vector of signal power samples of T_L in the the non-coupling state, $\vec{S_1}$ denote the vector of signal power samples of T_L in the coupling state, and $\vec{S_2}$ denote the vector of signal power samples of T_R in the coupling state. To detect this change, we propose two features, namely the *inter-tag feature* $\vec{F_T}$ and



(a) Legitimate tag T_R (b) Counterfeited tag T'_R

Figure 6: The performance of $\vec{F_T}$

coupling feature $\vec{F_C}$. They are defined as follows:

$$\vec{F_T} = [\frac{s_{1,1}}{s_{2,1}}, \frac{s_{1,2}}{s_{2,2}}, ..., \frac{s_{1,n}}{s_{2,n}}], \vec{F_C} = [\frac{u_{1,1}}{s_{1,1}}, \frac{u_{1,2}}{s_{1,2}}, ..., \frac{u_{1,n}}{s_{1,n}}] \quad (8)$$

where $s_{1,i}$, $s_{2,i}$, and $u_{1,i}$, is the i-th element of $\vec{S_1}$, $\vec{S_2}$, and $\vec{U_1}$ respectively. To remove the common noise of signal samples, we choose a simple but effective method, *i.e.*, divide the two signal power samples. $\vec{F_T}$ aims to measure the relative energy distribution between two tags, characterize the unique physical feature at the moment of inductive coupling of T_L and T_R. In addition, since $\vec{F_T}$ is related to the time sequence of each signal, it is also good at extracting the tags' BLF and EPC code.

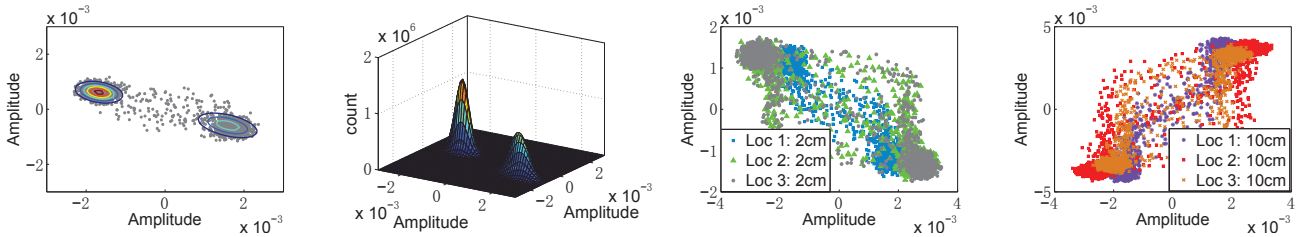
Defend against tag counterfeiting. It can be used to detect the tag counterfeiting attack by comparing the value of $\vec{F_T}$ stored at the backend server and $\vec{F_T}$ collected at the moment of authentication. To compare two vectors of $\vec{F_T}$ and $\vec{F'_T}$, we take the similarity identifier G, defined as the average value of $g_i = \frac{|f_i - f'_i|}{|f_i| + |f'_i|}$, where f_i and f'_i is the i-th element of $\vec{F_T}$ and $\vec{F'_T}$ respectively. If the presented tag is legitimate, G is like to be close to 0. If the attacker uses a counterfeited tag, G will be much larger than 0. Hence the value of G can be used to detect counterfeiting.

Defend against signal replay. If an attacker eavesdrops the communication process of the legitimate tags and replay the exactly same signals of T_L and T_R in coupling state, Hu-Fu will obtain a similar feature $\vec{F_T}$. Note that at this time, T_L is either alone or coupled with another tag different from T_R. Hence T_L will transmit backscatter signal different from the coupled signal with T_R. In either case, the monitor will hear extra signal from T_L other than the replayed coupling signals of T_L and T_R. Hence the attack can also be detected.

The feature $\vec{F_C}$ is to quantify whether T_L is a good tag to use as the authenticator in Hu-Fu. $\vec{F_C}$ basically compares the signal power of T_L in the coupling state and non-coupling state. We use $\vec{F_C}$ to select qualified tags for T_L. Experimental results show that most commodity tags are actually qualified.

5 IMPLEMENTATION AND EXPERIMENTS

We implement a prototype system of Hu-Fu using COTS devices: an ImpinJ Speedway R420 RFID reader, two Laird S9028PCL directional antennas and a USRP N210 monitor. We use a mainstream UHF passive RFID tags, ImpinJ E41C. The prototype uses the standard EPC Class 1 Generation 2 protocols (C1G2) [4]. In our experiments, we run the data processing software at a Lenovo PC, which equips Intel Celeron CPU G530 at 2.4 GHz and 2G memory.



(a) $\vec{F_C}$ of T_L in registration (b) Frequency of elements in $\vec{F_C}$ (c) $\vec{F_C}$ of coupling state (d) $\vec{F_C}$ of non-coupling state

Figure 7: The results related to $\vec{F_C}$

We conduct two sets of experiments to study the two features proposed in Section 4: the inter-tag feature $\vec{F_T}$ and coupling feature $\vec{F_C}$.

We choose a pair of tags as the pair of retained tag T_L and legitimate tag T_R. We conduct the registration process of the two tags in one room and the authentication process in another room. We use different rooms to simulate environment changes, but in practice most authentication processes will be in a same room of registration. Hence our experiment setup is tougher than practice. We show the feature vector $\vec{F_T}$ in Fig. 6(a) for the two processes. In general $\vec{F_T}$ in the two cases are quite similar with a few high-value outliers due to small denominators. Note we show 1500 elements which only include a few outliers. The similarity identifier $G = 0.4535$. We also use another tag as the counterfeited tag T'_R and show the results of $\vec{F_T}$ in Fig. 6(b). The two vectors are significantly different and the similarity identifier $G = 0.8427$. We have try various tags as the legitimate ones and counterfeited ones using 20 randomly picked tags. For legitimate cases G is always smaller than 0.5 and for counterfeited cases G is always higher than 0.7. Hence there is a quite big margin between the two cases. indicating that G is a robust feature for authentication.

We evaluate the coupling feature $\vec{F_C}$ of T_L and show that T_L's signal is different from the coupling signal. In Fig. 7(a), the x axis is the values of elements of $\vec{U_1}$, and the y axis is the values of elements of $\vec{S_1}$. The cotangent angle $\cot\theta$ ($\cot\theta = x/y$) of these points is the elements of $\vec{F_C}$. We show $\vec{F_C}$ in 3D in Fig. 7(b) where the height is the frequency distribution of elements of $\vec{F_C}$. We find that U_1 and S_1 are very different with $\cot\theta$ around -2.85. Hence for this T_L, its coupling signal can be distinguished from its non-coupling signal. We vary different tags and get similar results for every of them.

To simulate the signal reply attack, we put T_R with a 10cm distance to T_L to simulate a signal replayer. We also conduct the experiments in three different rooms by placing T_L and T_R with in 2cm and in the coupling state. We show the results of $\vec{F_C}$ in Fig. 7(c). $\cot\theta$ is almost the same for coupling state in the three locations. However, if we separate the two tags by 10cm, the results of $\vec{F_C}$ in Fig. 7(d) show that the value of $\cot\theta$ is almost equal to 1, indicating U_1 is similar to S_1. Hence Hu-Fu is sensitive if T_L transmits U_1 instead of S_1.

6 CONCLUSION AND FUTURE WORK

We propose the first solution of physical layer authentication that is resilient to the signal replay attack, for battery-free IoT devices, in particular, passive RFID tags. In future we will find a more sophisticated and robust feature to detect tag counterfeiting and signal replaying. We will also provide a complete security analysis against more possible attacks to tag authenticity. We will conduct extensive experiments to validate the effectiveness of Hu-Fu.

7 ACKNOWLEDGMENT

This work was supported in part by National Basic Research Program of China (973 Program) under Grant No. 2015CB351705, NSFC Grant No.61190112, 61325013, 61572396, 61402359, China 863 Grant 2013AA014601, and National Science and Technology Major Project of the Ministry of Science and Technology of China JZ-20150910. Chen Qian is supported by National Science Foundation grants CNS-1701681 and CNS-1717948. We thank the valuable comments from anonymous reviewers.

REFERENCES

[1] 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*.
[2] Boris Danev, Davide Zanetti, and Srdjan Capkun. 2012. On physical-layer identification of wireless devices. *ACM Computing Survey* (2012).
[3] Han Ding, Chen Qian, Jinsong Han, Ge Wang, Zhiping Jiang, Jizhong Zhao, and Wei Xi. 2016. Device-free detection of approach and departure behaviors using backscatter communication. In *Proceedings of ACM Ubicomp*.
[4] EPCglobal. 2005. *EPC^{TM}* radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860 MHz–960 MHz. (2005).
[5] 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* (2016).
[6] Haitham Hassanieh, Jue Wang, Dina Katabi, and Tadayoshi Kohno. 2015. Securing RFIDs by randomizing the modulation and channel. In *Proceedings of USENIX NSDI*.
[7] Jiajue Ou, Mo Li, and Yuanqing Zheng. 2015. Come and be served. In *Proceedings of ACM MOBICOM*.
[8] 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*.
[9] Roald K Wangsness. 1986. Electromagnetic fields. *Wiley-VCH* (1986), 608.
[10] Davide Zanetti, Boris Danev, and Srdjan Capkun. 2010. Physical-layer identification of UHF RFID tags. In *Proceedings of ACM MOBICOM*.