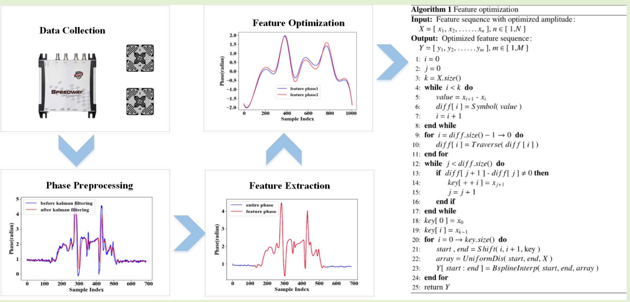
An Enhanced Secure Authentication Scheme With One More Tag for RFID Systems

He Xu, Xianzhen Yin, Feng Zhu, and Peng Li, *Member, IEEE*

***Abstract*—Currently, Radio Frequency Identification (RFID) is one of the key technologies to realize the Internet of Things (IoT), which is widely used in our daily life. However, there are some security threats such as impersonation attack, replay attack in existed RFID systems. In addition, most physical-layer authentication methods for RFID systems are mainly to authenticate tags without authenticating the user. In this paper, we present the design and implementation of Au-Hota, a system that can authenticate the tag and the user simultaneously, and can resist replaying attack and impersonation attack that cannot be solved by most physical-layer methods. Our idea is to assign a unique identifier to the user based on the inductive coupling between two adjacent tags. When the user draws the identity identifier on the tag, different identity identifiers correspond to unique phase features so that simultaneous authentication of the tag and the user can be achieved under the premise of ensuring security. The system is fully compatible with Ultra High Frequency (UHF) RFID systems without any modification. We implement a prototype of the system and conduct extensive experiments to evaluate performance. Our results demonstrate that the system has good authentication performance.**



Algorithm 1 Feature optimization

```
Input: Feature sequence with optimized amplitude:
  $X = [\, x_1, x_2, \ldots\ldots x_n \,], n \in [\, 1, N \,]$
Output: Optimized feature sequence:
  $Y = [\, y_1, y_2, \ldots\ldots y_m \,], m \in [\, 1, M \,]$
$i = 0$
$j = 0$
$k = X.size()$
while $i < k$ do
    $value = x_{i+1} - x_i$
    $diff[\, i \,] = Symbol(\, value \,)$
    $i = i + 1$
end while
for $i = diff.size() - 1 \rightarrow 0$ do
    $diff[\, i \,] = Traverse(\, diff\,[\, i \,]\,)$
end for
while $j < diff.size()$ do
    if $diff[\, j+1 \,] - diff[\, j \,] \neq 0$ then
        $key[\, ++i \,] = x_{j+1}$
        $j = j + 1$
    end if
end while
$key[\, 0 \,] = x_0$
$key[\, i \,] = x_{k-1}$
for $i = 0 \rightarrow key.size()$ do
    $start\,, end = Shift(\, i, i+1, \text{key} \,)$
    $array = UniformDis(\, start, end, X \,)$
    $Y[\, start : end \,] = BsplineInterp(\, start, end, array \,)$
end for
return $Y$
```

***Index Terms*—Impersonation attack, replay attack, RFID, user authentication.**

I. Introduction

RADIO Frequency Identification (RFID) is an essential part of the Internet of Things (IoT). It has now been widely used in access control system, warehouse management system, and traceability and tracking systems [1]–[4]. Compared with other technologies, RFID has irreplaceable advantages, mainly represented by lower energy consumption and low cost [5]–[8]. However, because tags use backscatter to communicate with the reader, some security problems will be encountered during the communication process. For example, when using an access control system, an attacker can use a particular device to eavesdrop on the tag signal, to crack it, and to write the decrypted data into the illegal tag. The attacker can pass the system authentication by using the illegal tag. In view of the RFID systems' hidden dangers, researchers begin to research on RFID security issues.

Commercial Off-The-Shelf (COTS) tags have limited storage and computing capabilities, and it is not feasible to use encryption algorithms. Some tags with strong storage and computing capabilities, such as NXP UCODE DNA RFID, are expensive so that it will bring cost pressure to RFID systems' applications, which are not conducive to large-scale use and will make tags lose the advantage of low price. Even if the encryption algorithm is used in tags, the attacker still has the possibility of cracking the tag.

Some researchers begin to use physical layer methods to authenticate tags [9]–[12], mainly using the difference of internal hardware characteristics of different tags in the

Manuscript received March 20, 2021; accepted April 27, 2021. Date of publication May 4, 2021; date of current version July 30, 2021. This work was supported in part by the National Key Research and Development Program of China under Grant 2019YFB2103003; in part by the National Natural Science Foundation of China under Grant 61602261, Grant 61872196, Grant 61872194, and Grant 61902196; in part by the Scientific and Technological Support Project of Jiangsu Province under Grant BE2019740, Grant BK20200753, and Grant 20KJB520001; in part by the Major Natural Science Research Projects in Colleges and Universities of Jiangsu Province under Grant 18KJA520008; in part by the Six Talent Peaks Project of Jiangsu Province under Grant RJFW-111; in part by the Postgraduate Research and Practice Innovation Program of Jiangsu Province under Grant SJKY19_0761, Grant SJKY19_0759, and Grant KYCX20_0759; and in part by the 1311 Talent Plan of the Nanjing University of Posts and Telecommunications (NUPT). The associate editor coordinating the review of this article and approving it for publication was Dr. Qammer H. Abbasi. *(Corresponding authors: He Xu; Peng Li.)*

He Xu and Peng Li are with the School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China, and also with the Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210023, China (e-mail: xuhe@njupt.edu.cn; lipeng@njupt.edu.cn).

Xianzhen Yin and Feng Zhu are with the School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China.

Digital Object Identifier 10.1109/JSEN.2021.3077575

manufacturing process and extracting tag physical-layer information. For example, Phase and Received Signal Strength Indicator (RSSI) can be used to authenticate tags. Compared with running the encryption algorithm in the tag, the tag authentication method based on the physical layer does not have any requirements on the tag's performance. It is suitable for all common tags. However, most physical-layer authentication methods are mainly to authenticate tags without authenticating the user holding the tag. When an attacker finds the tag lost by a legitimate user, it will perform impersonation attack on the system. In addition, the attacker can use special equipment to eavesdrop on the signal in the authentication of the legitimate user and replay attack on the system.

Aiming at the security problems that the above existing methods have not solved, we design Au-Hota that can authenticate the tag and the user holding the tag. It can not only resist common attacks but also resist replaying attack and impersonation attack simultaneously. Au-Hota realizes the tag and the user's simultaneous authentication by extracting the phase features of two adjacent tags. Since two tags are placed close together, inductive coupling will affect the signals of two tags and change phases. We can determine whether it is replay attack during the authentication by analyzing the phase curve of the fixed tag. During the authentication, the user needs to draw the assigned unique identity identifier on the tag to be authenticated with his finger. Then the system classifies the phase curve of the tag to determine the legitimacy of the tag and the user's identity. The equipment used in Au-Hota is common, the Ultra High Frequency (UHF) reader is Impinj R420, and the tag is Impinj H47.

The contributions of this paper are as follows:

(1) We design a new physical-layer RFID authentication system(Au-Hota) that can authenticate tags and users simultaneously, and the authentication strengths the RFID systems' security. The system can resist both replay attack and impersonation attack.

(2) We implement the system and evaluate its performance through many experiments. The experimental results show that the system has higher authentication performance.

(3) Au-Hota is fully compatible with the existing RFID systems without any changes to the RFID hardware systems, and the equipment used is common.

In the rest of the paper, Section II is the overview of Au-Hota. Section III introduces the principles that affect the phase change of tags. In addition, the detailed design of Au-Hota is descripted in Section IV, and Section V evaluates the system's performance. Section VI gives the comparison with other tag authentication methods. The related work is given in Section VII, and Section VIII is the discussion and conclusion.

II. Overview

This section introduces the system workflow, the design of identity identifiers, and system application scenarios.

A. System Introduction

Workflow of Au-Hota: Figure 1 is the system model. UHF RFID reader is connected to the directional antenna. Tag area is divided into two parts. One part is for the fixed tag, which we call the left tag T_L, and the other part is where the tag to be authenticated is placed, which is called the right tag T_R. When users use Au-Hota, they need to register in advance. During the registration, the system will save the user's tag ID and assign the user a unique identity identifier, such as a capital letter 'Z'. After completing the registration, the user needs to stand at the position designated by the system, to place the tag on the right tag area and to use the finger to draw the assigned unique identifier on T_R. The system first judges whether the ID of T_R is legal. If it is legal, it will match the collected phase curves of T_L and T_R with the fingerprint database and judge whether the identity identifier is correct according to the matching result of the right tag's phase curve. Through the matching result of T_L, we can determine whether it is replay attack. Au-Hota can ensure that the RFID tag and the user holding the tag are authenticated at the same time.

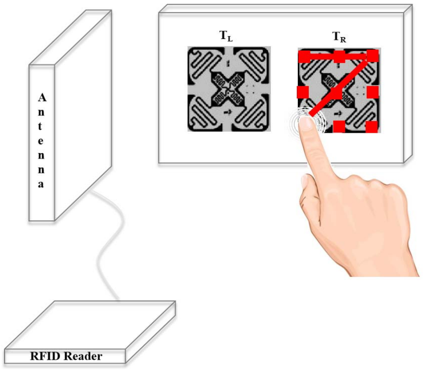


Fig. 1. Au-Hota system model.

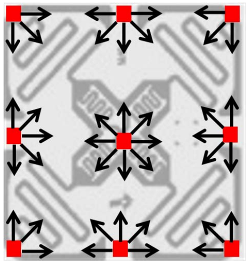


Fig. 2. The sliding direction of the finger on each marked point of T_R.

Identity identifier: To ensure the accuracy of system authentication, we mark 9 points on T_R, as shown in Figure 2. The user's finger can only slide between every two marked points. We call the sliding distance between every two points as the distance of the finger sliding once, which is called one step. If the identity identifier is only one step, there can be 40 types of identity identifiers. If the identity identifier has two steps, there are 40^2 types of identifiers. If there are 3 steps, there are 40^3. If it is n steps, there are 40^n. Therefore, Au-Hota can provide enough identity identifiers to meet the needs of large-scale applications of the system. We use those identity identifiers as user IDs.

B. Attack Types

Au-Hota can resist multiple attack types. This paper mainly discusses replay attack, counterfeiting attack, impersonation attack and brute-force attack.

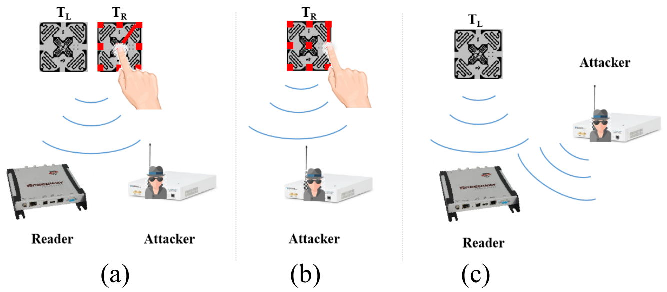
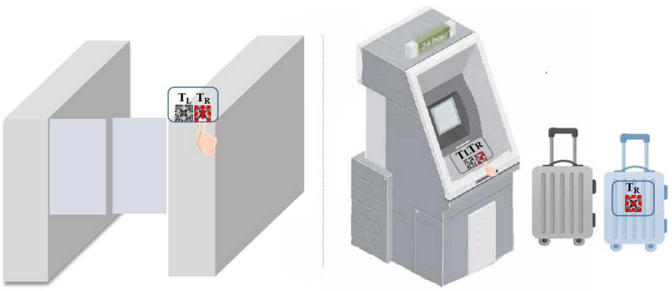


Fig. 3. Sketch maps of two types of replaying attack. (a) The attacker eavesdrops on the entire authentication; (b) The signal of T_R is collected by the attacker; (c) System is under replay attack.



(a)Checking Exhibition Ticket (b) Baggage Claim

Fig. 4. Two typical application scenarios.

Replay attack: We mainly analyze two types of replay attack [13], [14], one is for the attacker to use special equipment to eavesdrop on the signal of the entire authentication in Figure 3(a). The other is that the attacker obtaining T_R and user ID collect the signal of T_R in Figure 3(b). The attacker obtains the authentication signal in either of these two ways, replaying the signal in Au-Hota, as shown in Figure 3(c).

Counterfeiting attack: The legal tag's data is acquired by the attacker and is written to the illegal tag, which is used to try to pass the system authentication.

Impersonation attack: It is possible to lose the legal tag when using it. If the lost tag is picked up by an attacker, the attacker will use it to attack the system and cause security risks.

Brute-force attack: After the attacker has mastered the method of extracting features by the system, the attacker spends enough time and money to find an illegal tag with the same features as the legal tag, using the found illegal tag to attack the system.

C. Application Scenarios

Au-Hota can be applied in many scenarios in daily life, especially in scenarios where RFID tags and user identity authentication are required simultaneously. This section mainly introduces the application of the system in checking exhibition ticket and baggage claim.

Checking exhibition ticket: Participants need to register their identity before participating in the exhibition. The organizer will assign a right tag T_R and a unique identity identifier to the participants. When these participants arrive at the exhibition entrance, they need to place T_R at the right tag placement place on the entrance gate, and T_L is adjacent to T_R, as shown in Figure 4(a). Participant stands in the verification area and uses a finger to draw the unique user ID assigned by the organizer on the right tag. If the verification is passed, the gate will be opened, and participant can enter the exhibition. Au-Hota is used for checking tickets at the exhibition, and the secure design of the system can improve the security of the exhibition.

Baggage claim: Passengers consign their baggage at the place of departure. The staff assigns the left tag T_L and user ID to the passenger and the right tag T_R is placed on the baggage. When arriving at the destination, acquiring the right tag of the luggage and placing it in the authentication area together with the left tag for authentication, the passenger needs to draw the user ID on T_R with his finger. After passing the authentication, the passenger can take the luggage, as shown in Figure 4(b). According to related statistics, there are more than 20 million luggage errors every year, and airlines need to compensate hundreds of millions of RMB each year. The application of Au-Hota can effectively reduce the number of baggage errors and reduce airlines' economic burden.

III. Principles Analysis

We analyze the tag phase change in Au-Hota from the perspective of principle, mainly analyzing two kinds of coupling in the system and the user's influence on the tag phase.

A. Two Kinds of Coupling

Radiative coupling: After being activated through radiative coupling, the tag returns relevant information such as the Electronic Production Code (EPC), RSSI, and phase of the tag to the reader by backscattering signals. The tag phase is affected by the distance between the reader and the tag. The relationship between phase and distance can be expressed by the following formula [15]:

$$\theta = (\frac{4\pi d}{\lambda} + \Delta\theta) \bmod 2\pi \tag{1}$$

where d is the distance between the reader and the tag, λ is the wavelength, and $\Delta\theta$ is the total influence of the reader and the tag circuit on the tag phase.

Inductive coupling: When a tag is activated, the internally generated current flowing in the loop part of the antenna creates a magnetic field around it, which affects the surrounding tags. We refer to this effect as inductive coupling between two adjacent tags. When two tags are placed in close proximity, both radiative and inductive coupling are present. RF-Mehndi [21] and Hu-Fu [22] are designed both based on the inductive coupling between tags. To verify the inductive coupling, we do some experiments between two tags and the experimental results are shown in Figure 5. When T_L and T_R are read respectively, Phase1 and Phase2 in the figure's blue points are 3.5 radians and 2.3 radians. When two tags are placed in close distance, phases become 4.0 radians and 1.5 radians, as shown in the red points corresponding to Phase1 and Phase2. Experiments show that the inductive coupling between two tags will affect the tag phase.

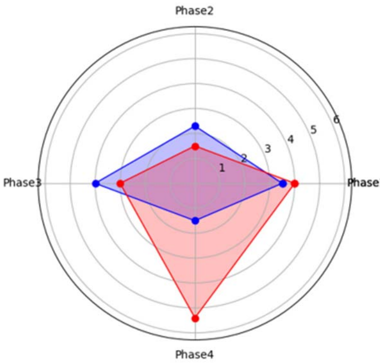
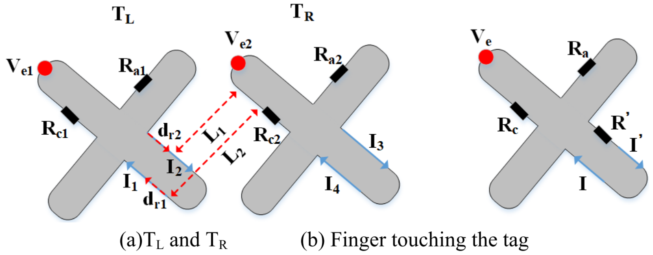


Fig. 5. The influence of inductive coupling and finger touching T_R on the tag phase.



(a)T_L and T_R (b) Finger touching the tag

Fig. 6. Structure of tags when placed statically and touched by a finger.

To further analyze the influence of inductive coupling on the phase, we simplified the tag's structure. The tag is mainly composed of tag chip impedance, tag antenna impedance, and the electromotive force produced by the reader radiative coupling, as shown in Figure 6(a). I_1 and I_2 are the equal magnitude but opposite direction. In the case of only T_L, the magnetic flux generated by the current of T_L cancels each other. When T_R is placed 6mm away from T_L, T_L and T_R will generate magnetic flux to each other, which affects the current on the tag, thereby changing the phase of the two tags. Take T_L affecting T_R as an example to illustrate the principle. First of all, according to Biot-Savart law, the magnetic flux generated by the current of T_L on T_R can be expressed as:

$$\Delta\Phi = (\mathrm{B}_1 - \mathrm{B}_2)\cdot S = \frac{\mu_0 S}{4\pi}\left(\int_0^R \frac{I_1 L_1 dr_1}{L_1^3} - \int_0^R \frac{I_2 L_2 dr_2}{L_2^3}\right) \quad (2)$$

where μ_0 is the vacuum permeability, B_1 and B_2 are the magnetic fields produced by I_1 and I_2 on T_R, L_1 and L_2 are the distance between two tags, d_{r1} and d_{r2} are differential elements, and S is the effective annular area in T_R, as shown in Figure 6(a). The magnetic flux generated in T_R will bring about additional induced current. Therefore the total current can be expressed as:

$$I_R = I + \frac{M}{R_{c2} + R_{a2}} \cdot \frac{d\Delta\phi}{dt} \quad (3)$$

where M is the number of loops in T_R, I is the current in T_R, and R_{c2} and R_{a2} are the chip and antenna resistances in T_R, respectively. The current in T_R changes under the influence of T_L, so the phase of T_R is changed.

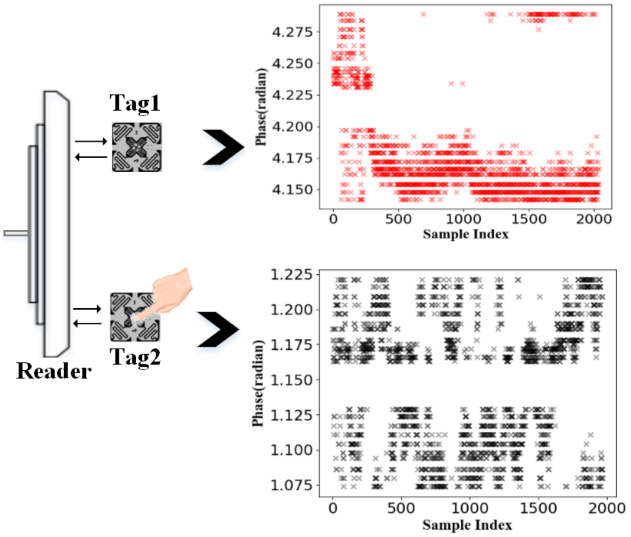


Fig. 7. Validation experiments.

B. User Influence

When the user draws the identity identifier, the finger impedance and finger motion will affect the tag phase. We analyze the influence process from the perspective of principle.

Finger Impedance: Our body can also be regarded as an equivalent resistance and capacitance [16]. The effective impedance used in Au-Hota is the local area at the end of the limb, i.e. the finger. Since biometric features of the finger are simple, the impedance on the finger is also stable [22]. RF-Mehndi is the introduction of impedance on the finger to achieve authenticating a person. We have done some experiments to verify the finger impedance.

We conduct two types of experiments on individual tag, fingerless touch and finger touch, and collect phases of the tag in both cases. In Figure 7, the tag phase is distributed on both sides of the 4.22 radian when there is no finger touch. When the tag is touched by a finger, the tag phase changes to 1.14 radians. We validate finger impedance through tag phase change.

Touching T_R with the user's finger is equivalent to introduce a new resistance in the circuit of the tag, as shown in Figure 6(b). The introduced resistance will change the tag's current, affect the coupling reaction between two tags, and thus change the phase of two tags. The Phase3 and Phase4 corresponding to the blue points in Figure 5 are the phases of T_L and T_R without finger touch, and the phase are 4.0 radians and 1.5 radians, respectively. Phase3 and Phase4 corresponding to the red points are the phases of two tags when the finger touches T_R, and the phase are 3.0 radians and 5.4 radians.

Finger motion: When the user draws the identity identifier, the finger's movement will change the phase of two tags. Before user authentication in Au-Hota, the propagation distances of the two tags are d_1 and d_2. The propagation path will be changed by the finger motion when the user is authenticating, as shown in Figure 8. We do not consider the influence of tags and reader circuits on the phase. The calculation methods for T_L and T_R are the same, and the phase

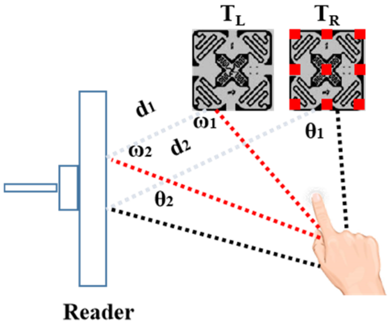
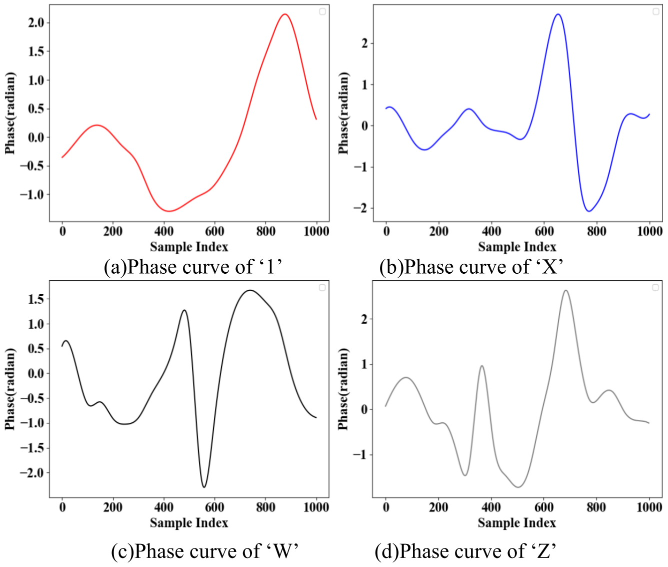


Fig. 8. Finger movement on the tag.



(a)Phase curve of ‘1’ (b)Phase curve of ‘X’

(c)Phase curve of ‘W’ (d)Phase curve of ‘Z’

Fig. 9. When a finger draws the user ID on T_R, the phase of T_R changes.

calculation formula for T_R is as follows:

$$\theta = \frac{4\pi d_1(\sin\theta_1 + \sin\theta_2)}{\lambda \sin(\theta_1 + \theta_2)} \% 2\pi \tag{4}$$

When the user draws different identity identifiers on T_R, different feature phase curves can be obtained due to the introduction of different finger impedance and finger movement trajectories. We draw four identity identifiers ‘1’, ‘X’, ‘W’ and ‘Z’ on T_R, and the corresponding phase curves are shown in Figure 9.

IV. System Design

Au-Hota can authenticate tags and user identities simultaneously and can ensure the security of the authentication. Au-Hota architecture consists of four modules: data collection, phase preprocessing, feature extraction and optimization, and secure authentication, as shown in Figure 10.

During the data collection, the reader collects the phase data of two tags and then transmits it to the background system to provide data sources for subsequent processing. The purpose of phase preprocessing is to eliminate the impact of data jumps and noise on the data. Feature extraction is to extract the phase curve of T_L and T_R when the user's finger draws the identity identifier on T_R. Feature optimization improves the accuracy of authentication and processes phase into data can be identified and processed easily by the system. Authentication is to make a judgment whether the user and tag are legal. We only introduce the three modules of phase preprocessing, feature extraction and optimization, and secure authentication in the following analysis.

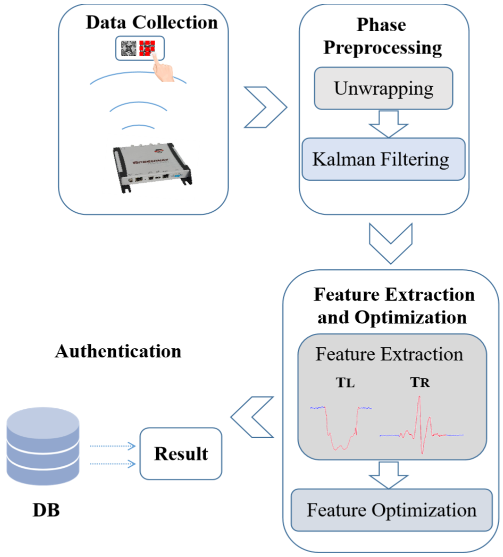


Fig. 10. Au-Hota system architecture.

A. Phase Preprocessing

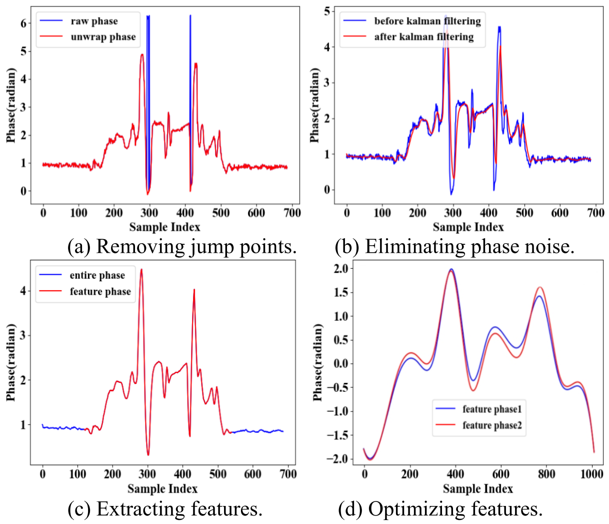
The data processed by the system is the tag phase, which is a periodic function [3], [8], [17] with a range of 0 to 2π. In experiments, it is found that tag phase sometimes jumps directly from 0 to 2π or 2π to 0. In order to resolve phase jump points, we use the phase unwrapping method. Besides, the tag phase is susceptible to environmental noise. We use the Kalman filter to filter the phase noise.

Phase unwrapping: The phase jump will seriously affect the authentication accuracy of the system. Using the phase unwrapping algorithm can eliminate the phase curve's jump point and improve the authentication performance of the system. The algorithm determines whether the current phase is plus or minus an integer multiple of 2π by the phase difference between adjacent phases. The specific formula is as follows:

$$\theta_0' = \theta_0, \quad \theta_i' = \theta_i + 2\pi \sum_{k=1}^{k} \Delta\eta_{k,k-1} \tag{5}$$

Among them, the value of $\Delta\eta_{k,k-1}$ is determined by phase difference of the adjacent phases and can be 0, -1, 1 according to the range of the phase difference value. The phase curve processed by the unwrapping algorithm is shown in Figure 11 (a), which can remove jump points on the phase curve, and make the phase curve become a continuously changing curve.

Kalman filtering: We use the Kalman filter [18] to deal with phase noise. The algorithm's core idea is to get the optimal phase at the current moment based on the phase at the current moment and the predicted phase and error at the



(a) Removing jump points. (b) Eliminating phase noise.

(c) Extracting features. (d) Optimizing features.

Fig. 11. Processing and optimizing phase features.

last moment, and then predict the phase at the next moment. The formula for calculating the optimal phase at the current moment is as follows:

$$\psi_{\text{i}} = \psi_{\text{i}-1} + (\varphi_i - \psi_{\text{i-1}}) \cdot \text{K}_{\text{i}} \tag{6}$$

where ψ_i is the optimal phase at the current moment, ψ_{i-1} is the optimal value at the last moment, which is the predicted value at the current moment, φ_i is the phase at the current moment, and K_{i} is the Kalman gain at the current moment. Kalman gain needs to be updated continuously, the update process is as follows:

$$\text{K}_{\text{i+1}} = \frac{\lambda_{\text{i+1}}}{\lambda_{\text{i+1}} + \tau}, \quad \lambda_{\text{i+1}} = (1 - \text{K}_{\text{i}}) \cdot \lambda_{\text{i}} \tag{7}$$

where λ is the predicted mean square error, and τ is a fixed constant. The phase curve processing result is shown in Figure 11(b). The Kalman filter can make the phase curve contour clearer, getting rid of the influence of noise.

B. Feature Extraction and Optimization

The phase curves of T_{L} and T_{R} need to be extracted from tag phases collected by the reader when the user's finger draws the identity identifier on T_{R}. The extracted phase curve is used as the unique phase feature corresponding to the user ID. To ensure that Au-Hota has a higher authentication accuracy rate, we have optimized the phase features.

Feature extraction: The variation trends of the phase curves of two tags during the authentication are as follows. First, before the user draws the user ID, the phase curves of T_{L} and T_{R} tend to be stable; during the period of drawing the user ID, the phase curves vary significantly; finally, when the user finishes drawing the user ID, phase curves of two tags are always a straight line. We use the changing rule of the phase sliding window size to 30, and compare each sliding window variance with the set variance threshold to determine the starting point and ending point of the feature. T_{L}'s sliding window variance threshold is set to 0.3, and T_{R}'s threshold is set to 0.1. The red curve in Figure 11(c) is the unique phase feature corresponding to the user ID.

Feature optimization: During the authentication, the finger's sliding speed on T_{R} cannot be guaranteed to be the same every time. Different sliding speeds will produce phase curves with different lengths and amplitudes. In order to solve this problem, we propose a feature optimization method, which optimizes the feature corresponding to the same identity identifier into a curve with basically the same amplitude and length.

We first take the mean for every 30 samples, then uniformly distribute the abscissa corresponding to the samples and use the B-spline interpolation algorithm to smooth the curve, and divide the difference by the standard deviation of the smoothed samples:

$$X'(t) = [X(t) - \mu]/\sigma \tag{8}$$

where μ and σ is the mean and the standard deviation of the smoothed samples, respectively. The above method can handle the amplitude of the phase curve. We use feature optimization algorithm (Algorithm 1) to solve the length of the phase curve. The central idea is to process the curve based on the standard phase curve.

First, we search critical points of the phase curve (start point, end point, crests, and troughs), and then segment the phase curve according to two critical points each time.

Algorithm 1 Feature Optimization

```
Input: Feature sequence with optimized amplitude:
  $X = [x_1, x_2, \ldots\ldots x_n], n \in [1, N]$
Output: Optimized feature sequence:
  $Y = [y_1, y_2, \ldots\ldots y_n], m \in [1, M]$
$i = 0$
$j = 0$
$k = X.size()$
while $i < k$ do
    $value = x_{i+1} - xi$
    $diff\ [i] = Symbol\ value$
    $i = i + 1$
endwhile
for $i = diff.size() - 1 \rightarrow 0$ do
    $diff\ [i] = Traverse\ [diff\ [\ i\ ]\ )$
end for
while$j < diff.size()$ do
    if $diff[j+1] - diff[j] \neq 0$ then
        $key[++i] = x_{j+1}$
        $j = j + 1$
    end if
end while
$key[0] = x_0$
$key[i] = x_{k-1}$
for $i = 0 \rightarrow key.size()$ do
    $start,\ end = Shift\ (i, i+1,$key)
    $array = UniformDis(start, end, X)$
    $Y[start : end] = Bsplinelnterp(start, end, array)$
end for
return $Y$
```

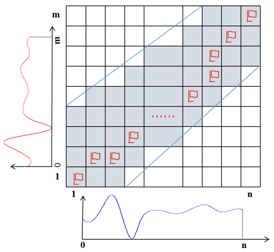


Fig. 12. Au-Hota system uses fast-DTW algorithm to compare the similarity of two phase.

Each curve is mapped to the standard curve's corresponding position according to two critical points, being used uniform distribution and B-spline interpolation method to normalize the length of this curve. Finally, the phase curve that has almost the same trend and constant length can be obtained. In regard to finding crests and troughs of the phase curve, we perform the first-order difference processing on the phase curve, use the sign operation to obtain the positive and negative feature curves conditions of the first derivative, and then perform the first-order difference processing on the symbol array, so as to accurately determine crests and troughs of the phase curve. Figure 11(d) shows two phase feature curves corresponding to the same identity identifier with different sliding speeds. It can be seen from the figure that the optimized curves are basically the same in amplitude and length. The authentication module entered the optimized data can improve the accuracy of system authentication.

C. Secure Authentication

The feature that Au-Hota needs to be classified is the phase curve that changes with time. The best way to solve this problem is the K-Nearest Neighbor (KNN) and dynamic time warping algorithm (DTW). DTW is mainly used in speech recognition [18], but DTW's time complexity is $O(N^2)$, which will degrade the system's authentication performance. We use the KNN classification algorithm and improved DTW algorithm, which is called fast-DTW algorithm [19], to reduce DTW algorithm's time and space complexity. The fast-DTW algorithm optimizes the performance of DTW from two aspects. On the one hand, the search space is restricted to the shadow area, reducing the number of spatial searches. On the other hand, an abstract method is used to determine the shortest path of the two feature curves in the shadow area, as shown in Figure 12. In order to further improve the accuracy of Au-Hota, we optimize the input data of the fast-DTW algorithm, as explained in the next section.

V. Implementation and Evaluation

We use COTS RFID readers and tags to implement Au-Hota and perform experiments to evaluate the performance of the system.

A. System Implementation

Hardware and software: As shown in Figure 13(c), Au-Hota uses Impinj R420 UHF reader connecting the VIKITEK VA094 directional antenna with an antenna gain of 9dBi. The tag used by the system is the common Impinj H47 tag, and the operating frequency of the entire system is 920.625MHz.

Au-Hota system software is developed by Java, using LLRP (Low-Level Reader Protocol) to communicate with the UHF RFID reader. Through the Ethernet interface, the reader can transmit these data of two tags to the client that verifies T_R's ID and the identity of user holding T_R as well as determines whether it is replay attack. The software can run on Intel Core i7-9700F CPU at 3.6 GHz and 8GB memory.

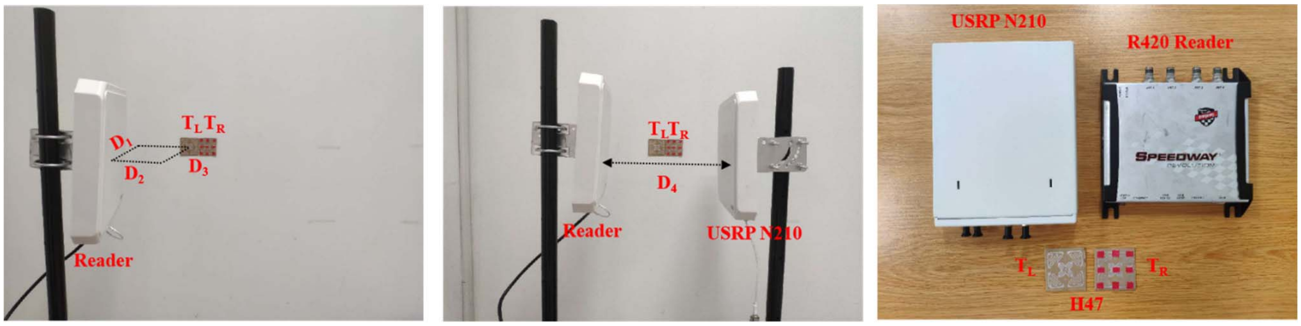
Deployment: To further evaluate the system's performance, we conduct extensive experiments. Figure 13(a) shows the specific experimental deployment, and the directional antenna is connected to the reader. Two H47 tags are used in experiments, where one as the left tag T_L and the other as the right tag T_R. The vertical distance D_1 between the center of the directional antenna and the T_L's center is 30cm, and the horizontal distance D_2 is 15cm. In order to ensure that T_L and T_R have an obvious coupling reaction, we make the distance D_3 between the two tags as small as possible, which is 6mm.

The deployment to verify the system's performance against replay attack is shown in Figure 13(b). USRP N210 equipped with the SBX daughter board is connected to a directional antenna and aligned horizontally with the reader. D_4 between the reader and USRP N210 is 25cm. Besides, the distance between USRP N210 and two tags is equivalent to the reader.

B. Secure Analysis

This section sets forth the security of Au-Hota and analyzes in detail how the system resists attacking from attackers. These attacks analyzed include replay attack, counterfeiting attack, impersonation attack, and brute-force attack.

Replay attack: Attackers need to use special equipment such as the USRP N210 to approach the system in a short distance to eavesdrop on signals. The entire authentication of Au-Hota occurs in a close scenario, which can reduce the risk of eavesdropping. It is supposed that the attacker eavesdrops on an individual legal authentication in Au-Hota and attempts to pass the authentication by replaying the signal. Because the UHF reader uses the ALOHA anti-collision algorithm, the system will not only receive the replay signal S_R of the attacker, but also the signal S_L of T_L in the system when the attacker replays the signal. Therefore the final T_L's signal is S_L+S_{RL} (S_{RL} is the replayed T_L's signal). By comparing T_L's signal S_{RL} under legal authentication, the classification algorithm can quickly and accurately identify this authentication as replay attack. Also, if the attacker obtains the legal T_R and acquires the identity identifier of the legal user, USRP N210 is designed as a UHF RFID reader. Making his finger draw the legal user's identity identifier on T_R, the attacker replays the T_R's signal by exploiting the designed reader to collect T_R's signal in Au-Hota. This kind of replay attack still cannot pass the authentication. If only T_R's signal is replayed, T_L will not react with T_R, which gets constant T_L's signal obviously different from the signal under legal authentication, so the system can identify this authentication as replay attack with high accuracy.



(a) To verify Au-Hota (b)To verify against replaying attack (c) Equipment included in Au-Hota

Fig. 13. Experimental deployments and equipment to evaluate the performance of Au-Hota.

Counterfeiting attack: In most existing physical layer-based authentication systems [11], [20]–[22], this kind of attack can be solved and Au-Hota can also resist counterfeiting attack. By analyzing T_R's phase curve, even if the ID of T_R is legal, it still fails to pass the authentication.

Impersonation attack: Most physical layer authentication systems cannot solve this attack. RF-Mehndi [21] is the first and only system that can resist this attack. By introducing human biological features, it can solve security issues due to tag loss. For this attack, Au-Hota proposes a solution to assign a unique ID to each legitimate user. During the authentication, the user needs to draw his unique ID on the T_R with his finger. The system realizes user identity authentication by analyzing the phase curve of T_R. Although there is a risk of losing the identity identifier, this method is still an excellent way to solve the impersonation attack.

Brute-force attack: Au-Hota can resist brute-force attack that is very time-consuming. The attacker needs to invest a significant amount of time and energy, and the probability of cracking is very low. Mastering the system's feature extraction and feature optimization methods and finding a tag that is similar in signal features to the legal T_R from a large number of tags, an attacker performing counterfeiting still fails to pass the authentication. Because the attacker cannot pass the authentication without knowing the user ID, even if the user ID is obtained, the classification algorithm adopted by Au-Hota will compare the difference with the legal tag.

C. Graphics Evaluation of Performance

We evaluate the overall performance and security of Au-Hota through many experiments. Evaluation indexes are false recognition rate (FAR) and rejection rate (FRR). The results show that the system has high authentication accuracy and can resist most attacks.

Overall performance of Au-Hota: To evaluate the authentication's overall performance, we invite 9 volunteers who are assigned 9 right tags and 9 unique IDs, which are shown in Figure 14. Each volunteer carries out 100 authentications, and these results are given in Figure 15. In Figure 15 we can see that Au-Hota has a higher authentication accuracy. The accuracy can reach 95.6%. Among them, the accuracy of H2, H3, and H8 in the authentication can reach 100%, which shows that the system has good performance. On account of the high symmetry of the H47 tag, user IDs 'Z' and '⊾' corresponding to H6 and H7 are very similar, so the accuracy is reduced. The FAR and FRR of H6 and H7 are 5.0%, 4.0% and 4.0%, 6.0%, respectively. Although the accuracy has been reduced, it can still be maintained above 90.0%. In practical application, Au-Hota can provide abundant IDs, which can completely avoid the situation of similar IDs.

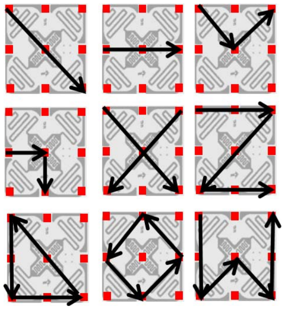


Fig. 14. 9 user IDs used in the experiment.

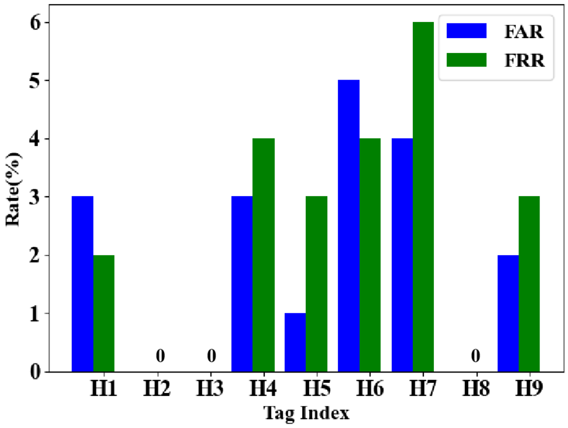


Fig. 15. Overall performance of Au-Hota.

Resisting replay attack: Two types of replay attack are analyzed in the paper. One is to eavesdrop on the signal during the entire legal authentication and the other is to collect T_R's signal where the finger draws the identity identifier on T_R. For the first type of replay attack, we eavesdrop on the signals in different legal authentication 10 times, and then replay each signal 100 times. Figure 16 shows that the system's

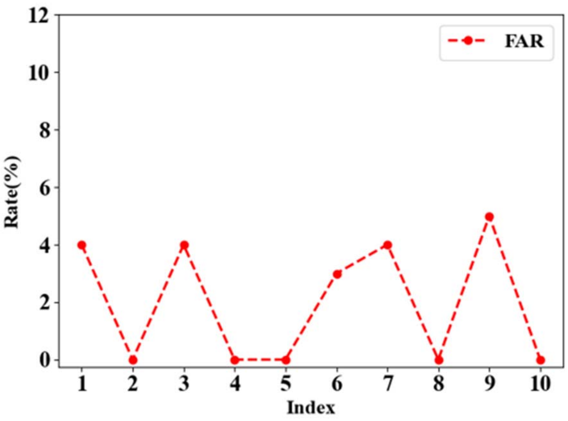


Fig. 16. Performance of resisting replay attack.

accuracy against replay attack is 98%, of which the second, fourth, fifth, eighth and tenth signals reach 100%. We collect 10 signals from T_R for the second replay attack and replay each T_R signal 100 times. In this case, T_L's phase curve approaches a straight line, compared with the curve under legal authentication, which has obvious difference. Therefore the recognition accuracy is 100%.

D. Influence Factors of Au-Hota

During the authentication of Au-Hota, the extracted feature is the tag phase that is mainly affected by distance, angle, and environment. Combined with the actual situation of Au-Hota, this section mainly analyzes the three influencing factors of distance, environment, and finger sliding speed.

Distance: The tag phase is closely related to the distance, so we verify the influence of distance on the system. There are two main types of distance involved in Au-Hota, one is the distance between the reader and tags, and the other is the distance between the user and tags. Since the position of the reader and tags are determined in the system, which will not affect the tag phase. To verify the influence of the distance between the user and tags on the system authentication accuracy, we have prepared 3 training sets with distances of 30cm, 40cm and 50cm.

In the test period, volunteers keep varying the distance to the tag from 10cm to 70cm, changing 10cm each time. The test result is shown in Figure 17. It can be seen from the figure that the authentication distance with higher system accuracy is 30cm to 60cm, and the best authentication distance is 40cm. In actually, the system determines the authentication distance between the user and tags, which can effectively eliminate the influence of distance on the system's accuracy.

Environment: Moving people or objects in the environment will cause the tag's phase to be affected by the multipath signal [8]. Au-Hota is a short-range authentication that can reduce the impact of the environment on the accuracy. We register the identity of volunteers in room 1, and volunteers perform identity authentication in room 2. The authentication result show that the system's accuracy is 94.4% under the circumstances of environmental changes in Figure 18.

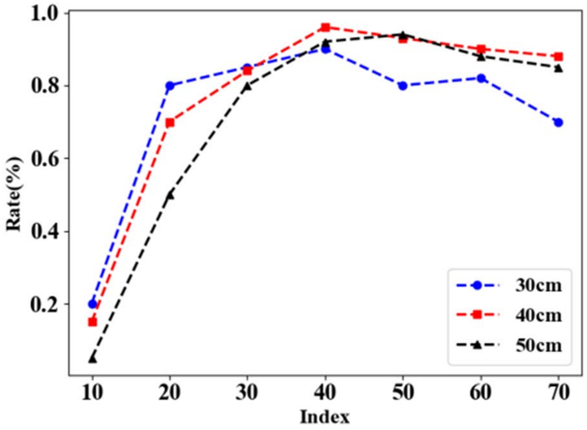


Fig. 17. Accuracy at different distances.

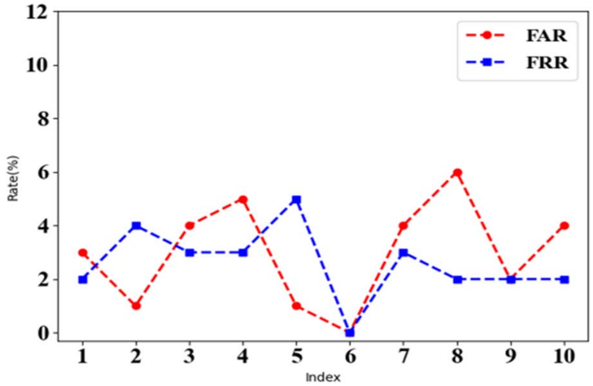


Fig. 18. The performance of Au-Hota when the environment varies.

TABLE I
THE PERFORMANCE OF AU-HOTA UNDER DIFFERENT SLIDING SPEEDS

Results	1 seconds	3 seconds	5 seconds
(FAR,FRR)	(5.0%,3.0%)	(3.0%,1.0%)	(4.0%,3.0%)

Finger sliding speed: The sliding speed of the finger on T_R cannot be guaranteed to be constant. Different sliding speeds will result in different amplitude and length of the phase curve. Au-Hota uses feature optimization to solve this problem. We require volunteers to slide at 1s, 3s, and 5s, respectively and conduct experiments. The experimental results are shown in Table I. Even if the sliding speed is different, the accuracy of Au-Hota can still be maintained above 90%. Besides, the best sliding speed for system certification is 3s.

VI. COMPARISON

We compare Au-Hota with other tag authentication methods achieved by Butterfly [12], Hu-Fu [22] and RF-Mehndi [21]. The comparison results are shown in Table II. Butterfly can achieve the accuracy of 96.7% for tag authentication, but is only resistant to counterfeiting attack, not replay or impersonation attack. Hu-Fu is more resistant to replay attack than Butterfly, and has the accuracy of 95%, but is limited to authenticating tags, not people, i.e. it is not resistant to impersonation attack. RF-Mehndi introduces human biomet-

TABLE II
COMPARISON WITH OTHER METHODS

Methods	Counterfeiting attack	Reply attack	Impersonation attack	Accuracy
Butterfly	Yes	No	No	96.7%
Hu-Fu	Yes	Yes	No	95.0%
RF-Mehndi	Yes	No	Yes	95.0%
Au-Hota	Yes	Yes	Yes	95.6%

rics to authenticate people and achieves 95% accuracy, but this authentication method is not resistant to replay attack. However, our proposed method not only resists common attack methods such as counterfeiting attack and replay attack, but also achieves authentication of people with the accuracy of 95.6%. Thus, compared to other recently existing authentication methods, Au-Hota enables simultaneous authentication of tags and the user and is resistant to a wide range of attacks with a high accuracy.

VII. Related Work

There are mainly two kinds of methods for authenticating RFID tags. One is based on encryption. The other is a method based on the physical layer authentication.

The encryption-based method uses traditional encryption technology to authenticate the tag. Only when the tag provides the reader with the correct password can the tag pass the authentication [23]–[27]. This authentication method is impossible for ordinary tags, and it requires tags with certain storage and computing capabilities. Meanwhile, the communication protocol between the reader and the tag needs to be modified, which is time-consuming and laborious. When an attacker obtains the authentication password and modifies the tag to the legal tag to perform counterfeit attack on the system, these encryption-based methods cannot resist this attack.

Considering these shortcomings of encryption-based methods, researchers begin to use physical layer methods to authenticate tags. Periaswamy *et al.* [9] realize the tag authentication by extracting the tag signal's minimum power. Danev *et al.* [10] authenticate tags by analyzing the interval error (TIE), average baseband power (ABP), and power spectrum features of RN16 preamble signal. Geneprint[11] takes the covariance (Cov) and power spectral density (PSD) of the RN16 preamble signal as features, which can be very convenient for tag authentication. To eliminate the environment's influence on the authentication, Butterfly [12] separates the EPC signal of two tags and authenticates the tag by analyzing the frequency domain features of the EPC signal difference between two tags. Resisting replay attack, Hu-Fu [22] adds a random signal during the communication between the reader and tags and extracts the power spectral density (PSD) and energy spectrum of two tag signals as features of authentication. RF-Mehndi [21] introduces human biological features, authenticating both the tag and the tag holder. All the above methods have a common flaw that the system cannot resist replay attack and impersonation attack simultaneously.

Some studies use machine learning to identify human motion [28] and detect skin hydration level [29], and Au-Hota feeds the extracted physical layer features of the tag into a machine learning model that not only authenticates the tag, but also resists both replay and impersonation attack. Equipment used in Au-Hota is COTS devices, and there is no need to make any changes to the UHF RFID systems.

VIII. Discussion and Conclusion

The Au-Hota system has four advantages for large-scale applications. Firstly, the equipment employed is commonly UHF equipment and is compatible with existing systems without the need to make any changes. Secondly, Au-Hota can be used on a large scale as RFID tags are available at a low price. Thirdly, it is simple to deploy, requiring only the deployment of the reader and tags, which is less complex. Fourthly, the system can be deployed in any noisy environment and has high authentication accuracy.

We conduct experiments to verify the system's performance. Firstly, the overall performance of the system is evaluated. Then, the performance of the system against various attacks is evaluated. Finally, various factors that affect the performance are analyzed. The experimental results show that Au-Hota maintains a high performance against a variety of security attacks.

Au-Hota can authenticate both tags and the user, which is the first method that not only can resist the common attacks but also replay attack and impersonation attack. The feature extracted by Au-Hota is the tag phase that is closely related to the inductive coupling between two tags and the identification identifier drawn on the tag by the finger. In the future work, we will realize the scheme integrated with existed RFID-based door system to enhance the system's security.

References

[1] Y. Zheng and M. Li, "P-MTI: Physical-layer missing tag identification via compressive sensing," *IEEE/ACM Trans. Netw.*, vol. 23, no. 4, pp. 1356–1366, Aug. 2015.

[2] L. Xie, Q. Li, C. Wang, X. Chen, and S. Lu, "Exploring the gap between ideal and reality: An experimental study on continuous scanning with mobile reader in RFID systems," *IEEE Trans. Mobile Comput.*, vol. 14, no. 11, pp. 2272–2285, Nov. 2015.

[3] L. Xie, C. Wang, A. X. Liu, J. Sun, and S. Lu, "Multi-touch in the air: Concurrent micromovement recognition using RF signals," *IEEE/ACM Trans. Netw.*, vol. 26, no. 1, pp. 231–244, Feb. 2018.

[4] L. Shangguan, Z. Yang, A. X. Liu, Z. Zhou, and Y. Liu, "STPP: Spatial-temporal phase profiling-based method for relative RFID tag localization," *IEEE/ACM Trans. Netw.*, vol. 25, no. 1, pp. 596–609, Feb. 2017.

[5] H. Ding *et al.*, "Human object estimation via backscattered radio frequency signal," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Hong Kong, Apr. 2015, pp. 1652–1660.

[6] T. Liu, L. Yang, Q. Lin, Y. Guo, and Y. Liu, "Anchor-free backscatter positioning for RFID tags with high accuracy," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Toronto, ON, Canada, Apr. 2014, pp. 379–387.

[7] L. Shangguan, Z. Zhou, X. Zheng, L. Yang, Y. Liu, and J. Han, "ShopMiner: Mining customer shopping behavior in physical clothing stores with COTS RFID devices," in *Proc. 13th ACM Conf. Embedded Netw. Sensor Syst.*, Seoul, South Korea, Nov. 2015, pp. 113–125.

[8] L. Yang, Y. Chen, X.-Y. Li, C. Xiao, M. Li, and Y. Liu, "Tagoram: Real-time tracking of mobile RFID tags to high precision using COTS devices," in *Proc. 20th Annu. Int. Conf. Mobile Comput. Netw.*, Honolulu, HI, USA, Sep. 2014, pp. 237–248.

[9] S. C. G. Periaswamy, D. R. Thompson, and J. Di, "Fingerprinting RFID tags," *IEEE Trans. Dependable Secure Comput.*, vol. 8, no. 6, pp. 938–943, Dec. 2011.

[10] B. Danev, T. S. Heydtbenjamin, and S. Capkun, "Physical-layer identification of RFID Devices," in *Proc. 18th Conf. USENIX Secur. Symp.*, Montreal, QC, Canada, Aug. 2009, pp. 199–214.

[11] J. Han *et al.*, "GenePrint: Generic and accurate physical-layer identification for UHF RFID tags," *IEEE/ACM Trans. Netw.*, vol. 24, no. 2, pp. 846–858, Apr. 2016.

[12] J. Han *et al.*, "Butterfly: Environment-independent physical-layer authentication for passive RFID," *Proc. ACM Interact., Mobile, Wearable Ubiquitous Technol.*, vol. 2, no. 4, pp. 1–21, Dec. 2018.

[13] B. Danev, H. Luecken, S. Capkun, and K. El Defrawy, "Attacks on physical-layer identification," in *Proc. 3rd ACM Conf. Wireless Netw. Secur. (WiSec)*, Piscataway, NJ, USA, Jul. 2010, pp. 89–98.

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

[15] *Speedway Revolution Reader Application Note: Low LevelUser Data Support*, Impinj, Seattle, WA, USA, 2010. [Online]. Available: https://support.impinj.com/hc/en-us/articles/202755318-Application-Note-Low-Level-User-Data-Support

[16] S. Pradhan, E. Chai, K. Sundaresan, L. Qiu, M. A. Khojastepour, and S. Rangarajan, "RIO: A pervasive RFID-based touch gesture interface," in *Proc. 23rd Annu. Int. Conf. Mobile Comput. Netw.*, Salt Lake City, UT, USA, Oct. 2017, pp. 261–274.

[17] J. Han *et al.*, "CBID: A customer behavior identification system using passive tags," *IEEE/ACM Trans. Netw.*, vol. 24, no. 5, pp. 2885–2898, Oct. 2016.

[18] Z. Luo, W. Wang, J. Qu, T. Jiang, and Q. Zhang, "ShieldScatter: Improving IoT security with backscatter assistance," in *Proc. 16th ACM Conf. Embedded Netw. Sensor Syst.*, Shenzhen, China, Nov. 2018, pp. 185–198.

[19] S. Salvador and P. Chan, "Toward accurate dynamic time warping in linear time and space," *Intell. Data Anal.*, vol. 11, no. 5, pp. 561–580, Oct. 2007.

[20] H. Ding *et al.*, "Preventing unauthorized access on passive tags," *IEEE Trans. Mobile Comput.*, Honolulu, HI, USA, Apr. 2018, pp. 1115–1123.

[21] C. Zhao *et al.*, "RF-Mehndi: A fingertip profiled RF identifier," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Paris, France, Apr. 2019, pp. 1513–1521.

[22] G. Wang *et al.*, "Hu-Fu: Replay-resilient RFID authentication," *IEEE/ACM Trans. Netw.*, vol. 28, no. 2, pp. 547–560, Apr. 2020.

[23] T. Li, W. Luo, Z. Mo, and S. G. Chen, "Privacy-preserving RFID authentication based on cryptographical encoding," in *Proc. 31st IEEE INFOCOM Workshops*, Orlando, FL, USA, Mar. 2012, pp. 2174–2182.

[24] D. Engels, M. O. Saarinen, P. Schweitzer, and E. M. Smith, "The hummingbird-2 lightweight authenticated encryption algorithm," in *Proc. 7th Int. Conf. Workshop. RFID. Secur. Privacy*, Amherst, MA, USA, Jun. 2011, pp. 19–31.

[25] M. Feldhofer and J. Wolkerstorfer, "Strong crypto for RFID tags—A comparison of low-power hardware implementations," in *Proc. IEEE Int. Symp. Circuits Syst.*, Baton Rouge, Louisiana, LA, USA, May 2007, pp. 1839–1842.

[26] M.-T. Sun, K. Sakai, W.-S. Ku, T. H. Lai, and A. V. Vasilakos, "Private and secure tag access for large-scale RFID systems," *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 6, pp. 657–671, Nov. 2016.

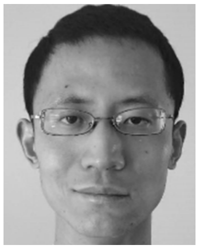
[27] Y. Komori, K. Sakai, and S. Fukumoto, "Fast and secure tag authentication in large-scale RFID systems using skip graphs," *Comput. Commun.*, vol. 116, pp. 77–89, Jan. 2018.

[28] W. Taylor, S. A. Shah, K. Dashtipour, A. Zahid, Q. H. Abbasi, and M. A. Imran, "An intelligent non-invasive real-time human activity recognition system for next-generation healthcare," *IEEE Sensors J.*, vol. 20, no. 9, pp. 2653–2672, May 2020.

[29] S. Liaqat, K. Dashtipour, K. Arshad, and N. Ramzan, "Non invasive skin hydration level detection using machine learning," *Electronics*, vol. 9, no. 7, pp. 1086–1095, Jul. 2020.

He Xu received the M.Eng. and Ph.D. degrees in information network from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 2009 and 2012, respectively. He is currently an Associate Professor and a Master Supervisor with the School of Computer Science, Nanjing University of Posts and Telecommunications. His main research interest includes the Internet of Things (IoT) technology and applications. He is a member of the CCF.

Xianzhen Yin was born in 1994. He is currently pursuing the master's degree with the School of Computer Science, Nanjing University of Posts and Telecommunications. His main research interests include RFID security and the IoT technology and application.



Feng Zhu received the B.S. degree in computer science from Nanjing University, China, in 2009, and the Ph.D. degree in computer science from Florida International University, USA, in 2014. He is currently an Assistant Professor with the School of Computer Science, Nanjing University of Posts and Telecommunications. His main research interests include networks security and the IoT security, and operating systems security.

Peng Li (Member, IEEE) received the Ph.D. degree in computer science and technology from the Nanjing University of Posts and Telecommunications, Nanjing, China, in 2013. He is currently a Professor and a Master Supervisor with the School of Computer Science, Nanjing University of Posts and Telecommunications. He has presided over ten national, provincial and ministerial projects. His main research interests include computer communication networks, wireless sensor networks, and information security. He is a member of the CCF and the IEEE Communications Society.