Adaptive Trust Management for Soft Authentication and Progressive Authorization Relying on Physical Layer Attributes

He Fang, *Student Member, IEEE,* Xianbin Wang, *Fellow, IEEE,* and Lajos Hanzo, *Fellow, IEEE*

***Abstract*—Conventional authentication mechanisms routinely used for validating communication devices are facing significant challenges. This is mainly due to their reliance on both 'spoofable' digital credentials and static binary characteristic, and inevitable misdetection in physical layer authentication using time-varying attributes, leading to the cascading risks of security and trust. To circumvent these impediments, we develop an adaptive trust management based soft authentication and progressive authorization scheme by intelligently exploiting the time-varying communication link-related attribute of the transmitter to improve wireless security. First of all, the trust relationship between the transmitter and receiver is established based on the evaluation of selected physical layer attribute for fast authentication and multiple-level authorization. Through the designed trust model, the transmitter is authorized by the specific level of services/resources corresponding to its trust level, so that soft security is achieved. To dynamically update the trust level of the transmitter, we propose an online conformal prediction-based adaptive trust adjustment algorithm relying on the real-time validation of its attribute estimates at the receiver, thus resulting in progressive authorization. The performance of our scheme is theoretically analyzed in terms of its individual risk and individual satisfaction. Our simulation results demonstrate that the proposed scheme significantly improves the security performance and robustness in time-varying environments, and performs better than the static binary authentication scheme and existing physical layer authentication benchmarker.**

***Index Terms*—Physical layer attributes, authentication and authorization, trust management, online conformal prediction, risk assessment, satisfaction evaluation**

I. INTRODUCTION

INNOVATIONS in wireless communications and Internet technologies during last few decades have brought about not only radically new applications, but also significantly increased security challenges imposed on the legitimate users owing to the rapidly improving capability of adversaries. To be specific, due to the broadcast nature of radio signal propagation, owing to the intermittent nature of communications as well as the complex dynamic network environments encountered, wireless communications are vulnerable to spoofing attacks [1]–[3]. A spoofer may intercept the transmissions between legitimate devices and imitate them to obtain illegal benefits from networks/systems, while counterfeiting authorized identities for fraud or other malicious purposes.

Although key-based cryptographic techniques [4]–[7] have been widely used for authentication, they face increasing challenges in securing wireless communications. Differentiating devices with the aid of digital credentials cannot be readily achieved when the diverse attributes of communication devices are disregarded, thus leading to a high risk of undetected spoofing attacks [8]. Furthermore, the conventional key-based cryptographic techniques are static in time and binary in nature, where the devices either pass the security check or fail by a one-time authentication. These security schemes cannot help in detecting/preventing spoofers after the initial authentication has been completed. Although repeated authentication may theoretically be achieved with the aid of key-based cryptographic techniques by repeatedly logging into the server/system, the excessive latencies and computational overhead are particularly undesirable for delay-sensitive communications as well as for devices having limited battery lifetime and computational capability, such as the Internet-of-Thing (IoT) devices [1]–[3].

Physical layer security techniques [8]–[15] provide alternative authentication methods relying on the uniquely random link-related attributes, as exemplified by the channel impulse response (CIR) [2], carrier frequency offset (CFO) [11], and received signal strength (RSS) [8], just to name a few, which are difficult for malicious devices to impersonate and predict. Although they have obvious advantages including the low computational requirement, low network overhead and modest energy consumption, most of the physical layer authentication schemes based on the classic hypothesis test are also static in the time-domain, as exemplified by [10]–[13]. Hence, they tend to be unsuitable for providing continuous identification. A kernel machine learning-based physical layer authentication scheme is proposed in our previous work of [2] through tracking multiple time-varying attributes to provide lasting protection for legitimate links. However, the above schemes constitute binary admit/reject solutions as well as rely on separate authentication and authorization, hence resulting in latent loopholes for spoofing attacks because of the potential misdetection events in physical layer authentication. Once an adversary passed the authentication by spoofing a legitimate device, the corresponding information/services/resources in the system will be leaked to this adversary. Furthermore, these

H. Fang and X. Wang are with the Department of Electrical and Computer Engineering, Western University, London, ON N6A 5B9, Canada (emails: hfang42@uwo.ca, xianbin.wang@uwo.ca).

L. Hanzo is with the School of Electronics and Computer Science, University of Southampton, Southampton SO17 1BJ, U.K (email: lh@ecs.soton.ac.uk).

L. Hanzo would like to acknowledge the financial support of the Engineering and Physical Sciences Research Council projects EP/Noo4558/1, EP/PO34284/1, COALESCE, of the Royal Society's Global Challenges Research Fund Grant as well as of the European Research Council's Advanced Fellow Grant QuantCom.

binary-type solutions fail to provide differentiated levels of access control.

To overcome these challenges, the concept of *soft authentication and progressive authorization* is extremely beneficial for holistic system optimization in dynamic communication environments. The soft security solution provides a fast authentication and multiple-level authorization, while the progressive approach achieves continuous identification to enhance the security by multiple-step validation of the physical layer attribute observations. Through such scheme, the threats and uncertainties caused by adversaries as well as the cascading risks in security and trust can be evaluated and controlled in real time. In achieving this, the decision-making in high layer is also required for modelling the soft authentication and progressive authorization as well as for security enhancement.

Trust management processes symbolic representations of trustworthiness in support of a decision-making process, which has been widely studied in dealing with security problems [16]–[24]. However, the conventional trust management approaches are usually used for modelling the trust relationships among authenticated users/devices for supporting cooperations in wireless networks. In this paper, we focus our attention on proposing an adaptive trust management approach by evaluating the attribute estimation of the transmitter to establish the trust relationship between transceiver for authentication and to provide metric for authorization. Through exploring the adaptive trust management, our radical solution provides fast authentication and dynamic multiple-level authorization, thus resulting in soft and progressive security. More importantly, our scheme moves further away from the classical mechanisms, since it quests a holistic system design of unified authentication and authorization based on the continuous evaluation of time-varying physical layer attribute, which requires new wireless radio technologies. Hence, the machine learning techniques [1], [2] are studied in this paper for adaptive trust management through classifying the time-varying attribute estimates of the transmitter.

In the unsupervised machine learning techniques of [25]–[28], an assumption is usually made for the classification between normal and abnormal events that normal events are those that occur frequently and anomalous events occur rarely. This leads to a high false alarm rate in physical layer authentication, since those rare attribute observations may be deemed to be from the Spoofer. Therefore, the family of supervised learning techniques is invoked for the classification of the time-varying physical layer attribute estimates, which may be from legitimate devices and (or) adversaries. However, most of the existing supervised machine learning techniques have a limited capability to update the trustworthiness of an authenticating transmitter because of the lack of information on how close their predictions are to the real observations. These motivate us to explore the conformal prediction technique of [29]–[31], where a valid measurement of each individual prediction is provided along with a confidence value based on the learning algorithms. More importantly, by invoking the online machine learning technique of [32], [33], the associated real-time classification results can be used for adaptive trust management, thus improving the security performance in time-varying communication scenarios.

In a nutshell, our online conformal prediction-based adaptive trust management approach provides differentiated levels of continuous protection for legitimate communications. Such approach evaluates the trustworthiness of an authenticating transmitter using its physical layer attribute dynamically, thereafter the corresponding level of services/resources is authorized to the transmitter according to its trust level. Furthermore, it integrates authentication and authorization for achieving seamless and holistic system optimization, thus leaving fewer loopholes open for spoofing attacks. Specifically, the contributions of this paper are summarized as follows:

1) To achieve the soft security, we design a trust model for evaluating the trustworthiness of an authenticating transmitter relying on physical layer attribute without requiring its statistical properties. This model achieves fast authentication and provides metric for multiple-level authorization to deal with the threats caused by adversaries and to control the risks of being attacked;

2) An online conformal prediction-based adaptive trust adjustment algorithm is proposed for real-time validation of transmitter and for dynamically updating the trust model developed. Therefore, our scheme becomes capable of adapting to time-varying environments for security enhancement;

3) Our simulation results demonstrate that the proposed scheme describes a soft access control and continuous procedure of authentication, thereby providing reliable adaptive protection for legitimate communication links. We also demonstrate the superiority of our scheme over the static binary authentication scheme and our an exiting physical layer authentication scheme.

The rest of this paper is organized as follows. In Section II, the system model used in this paper is presented. In Section III, we propose our online conformal prediction-based adaptive trust management scheme for achieving soft authentication and progressive authorization using physical layer attribute. The security performance analysis of our scheme is also presented in Section III, while our simulation results are discussed in Section IV. Finally, Section V concludes the paper.

Notations: In this paper, scalars are denoted by italic letters, while vectors are respectively denoted by bold-face letters. False alarm (FA) represents an event when the receiver wrongly believes that the legitimate transmitter is an adversary, while misdetection (MD) is an event when the receiver wrongly identifies the adversary as a legitimate device. Table I shows the notations of this paper.

II. SYSTEM MODEL AND PROBLEM FORMULATION

As shown in Fig. 1, we commence by characterizing the attack model in a time-varying environment, where Alice and Bob represent a pair of legitimate devices and aim for communicating in the presence of a Spoofer, who tries to impersonate Alice and hence to access the system. More explicitly, the Spoofer not only tries to intercept Alice's transmission, but also to imitate her for obtaining illegal benefits from Bob. The

TABLE I
NOTATIONS IN THIS PAPER

Notations	Definitions
H_A	Attribute estimate collected from Alice.
H_O	Attribute estimate collected from Alice or the Spoofer.
t	Time instant of physical layer authentication.
$\mathcal{F}$	Trust value of relationship $\{Bob : Transmitter, Alice\}$.
N	Number of authorization levels.
R_{ind}	Individual risk of our scheme.
S_{ind}	Individual satisfaction of our scheme.
Ψ_0	Scenario that the transmitter is the Spoofer.
Ψ_1	Scenario that the transmitter is Alice.
Γ	Conformal predictor.
y	Label of an attribute estimate.
Z	Set of training samples in conformal predictor.
Y	Predicted set of conformal predictor.
ϵ	Significance level of conformal predictor.
$1-\epsilon$	Confidence level on the predicted set Y.
e	Error made by the conformal predictor.
A	Nonconformity measure function.
α	Nonconformity score.
p	p-value of the conformal predictor.
θ	Validation result of the attribute estimates.
L	Number of training samples.

Spoofer also tries to counterfeit authorized identities for fraud or other malicious purposes. The aggregated spoofing channel (i.e. the physical channel spanning from the Spoofer to Bob, as well as the hardware and analog components involved) is assumed to be independent of the main channel between Alice and Bob. Therefore, it is hard for the Spoofer to predict and clone Alice's physical layer attributes, such as her channel impulse response (CIR) [2], carrier frequency offset (CFO) [11], and received signal strength (RSS) [8]. In this paper, only one physical layer attribute is utilized for authentication and authorization.

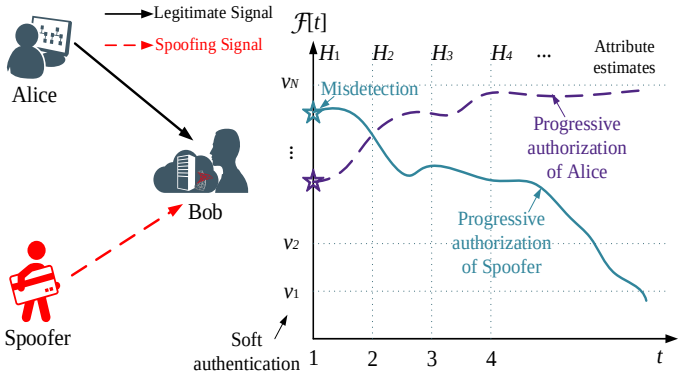

Fig. 1. Soft authentication and progressive authorization system between Alice and Bob using a physical layer attribute continuously. The authentication and authorization mechanisms secure the legitimate communications through confirming the identities of all devices and their right access to the authorized resources, data and services.

At the beginning of communication between Alice and Bob, existing security schemes have been used to establish initial authentication between them explicitly. Indeed, it is reasonable to expect that the devices have to be registered before joining the communication system, which is a basic prerequisite of physical layer authentication schemes [10]–[13]. L estimates of the selected physical layer attribute of Alice can be obtained during the established initial authentication phase, which are denoted as

$$H_{A1}, H_{A2}, ..., H_{AL}, \tag{1}$$

where each H_{Al} represents an attribute estimate collected from Alice, $l \in \{1, 2, ..., L\}$ is an estimation time index, and L is the number of estimates during the established initial authentication phase. The major objective of physical layer authentication is to verify that the information received is from a legitimate device (i.e. Alice) by exploiting the difference between the estimates $H_{A1}, H_{A2}, ..., H_{AL}$ and new estimates of the selected attribute arriving from the transmitter (i.e. Alice or the Spoofer) during the subsequent communication stages. The new attribute estimates are denoted as H_{Ot}, explicitly showing the time instants of physical layer authentication $t = 1, 2, 3, ...$ Due to the dynamic nature of the environment encountered, the attribute estimates H_{Ot} are likely to be time-varying. Explicitly, the new attribute estimates H_{Ot} may have arrived from Alice or the Spoofer, and the validation of these estimates has to identify whether they are from Alice or the Spoofer. Moreover, the physical layer authentication starts at time instant $t = 1$ by identifying the estimate H_{O1}, which is arranged to be the $(L+1)$-st attribute estimate, because we have had L estimates of Alice collected during the initial authentication phase. Then, the physical layer authentication at time instant $t = 1$ is formulated as

$$\Delta H_{O1} = f(H_{A1}, H_{A2}, ..., H_{AL}, H_{O1}), \tag{2}$$

where $f(\cdot)$ represents a function that quantifies the difference between the estimates $H_{A1}, H_{A2}, ..., H_{AL}$ and H_{O1}. The nonconformity measure of [35] will be applied in our scheme for characterizing this difference (see Section III-A). If the difference ΔH_{Ot} is small enough, the signal is deemed to be coming from Alice, otherwise, from the Spoofer. We assume that the attribute estimation noises of Alice and the Spoofer are independent and identically distributed, which may caused by the measurement errors, channel noises, interferences in the wireless communication environment, and so on.

In order to achieve security enhancement, this paper focuses on proposing a novel adaptive trust management approach for achieving soft authentication and progressive authorization in dynamic communication environments. To be more specific, our soft security solution provides prompt authentication and multiple-level authorization, while the progressive approach enhances the security by multiple-step validation of the time-varying physical layer attribute considered. The varying threats and uncertainties caused by the Spoofer and the cascading risks in security can be evaluated and controlled in real time by our scheme. Furthermore, various levels of protection can be provided for legitimate communications.

We characterize the trust relationship between the transmitter (i.e. Alice or the Spoofer) and Bob for the sake of evaluating the trustworthiness of the transmitter as follows:

Definition 1: The trust level of the relationship $\{Bob : Transmitter, Alice\}$ at time t is defined as the probability that the transmitter is deemed to be Alice in Bob's point of view by identifying the selected physical layer attribute, which is represented as

$$\mathcal{F}[t] = \Pr\{Bob : Transmitter, Alice\} \in [0, 1]. \tag{3}$$

We can observe from Definition 1 that Bob has full trust in the transmitter when $\mathcal{F}[t] = 1$, and Bob totally distrusts the transmitter if $\mathcal{F}[t] = 0$. Then the new concept of multiple-level authorization is developed, where we have N classes of security services/resources, denoted as $\{\Phi_0, \Phi_1, ..., \Phi_{N-1}\}$. The multiple-level authorization classes satisfy $\Phi_0 \subset \Phi_1 \subset ... \subset \Phi_{N-1}$, where Φ_{N-1} represents the highest level of authorization, while Φ_1 is the lowest one. Moreover, Φ_0 represents failed authentication and access denial for Bob. Our soft authentication and progressive authorization scheme can be formulated relying on thresholds $\nu_1, \nu_2, ..., \nu_{N-1}$ obeying

$$\begin{cases} \Phi_0: & \mathcal{F}[t] \in [\nu_0, \nu_1] \\ \Phi_1: & \mathcal{F}[t] \in (\nu_1, \nu_2] \\ & \vdots \\ \Phi_{N-1}: & \mathcal{F}[t] \in (\nu_{N-1}, \nu_N] \end{cases}, \tag{4}$$

where the thresholds satisfy $0 = \nu_0 < \nu_1 < \nu_2 < \cdots < \nu_{N-1} < \nu_N = 1$.

As shown in Fig. 1, upon assuming the estimation range of the selected physical layer attribute as $[-a, a]$, we design the soft authentication and progressive authorization process based on the trust level $\mathcal{F}[t]$ by evaluating the estimates of the selected attribute H_{Ot} as follows:

Soft authentication: We set the initial trust level of the relationship $\{Bob : Transmitter, Alice\}$ relying on the physical layer attribute estimate H_{O1} at time instant $t = 1$ according to the authentication of (2) as

$$\mathcal{F}[1] = 1 - \Delta H_{O1}. \tag{5}$$

If the initial trust level satisfies $\mathcal{F}[1] \in (\nu_n, \nu_{n+1}]$, the transmitter is allowed to access the services/resources associated with the n-th level of authorization, namely at Φ_n, $n \in \{0, 1, ..., N-1\}$. In contrast to the conventional hypothesis testing-based physical layer authentication schemes [10]–[13], our soft authentication solution does not require any knowledge of the statical properties of the attribute selected and neither does it require the derivation of optimal thresholds for hypothesis testing. These simplifications lead to prompt authentication via (4), but the lack of having an optimal threshold may lead to an increased misdetection rate during the soft authentication of (5). Fortunately, both the multiple-level authorization and following progressive authorization designed for our scheme are capable of enhancing the security by authorizing the corresponding class of security services and resources according to the trust level $\mathcal{F}$ as well as through the multiple-step validation of the physical layer attribute selected.

Progressive authorization: Given estimates of the selected physical layer attribute $H_{Ot} \in [-a, a]$ at time instants $t = 2, 3, 4, ...$, the trust level $\mathcal{F}$ should be updated to control the individual risk and individual satisfaction, which is formulated as

$$\mathcal{F}(H_{Ot}, \mathcal{F}[t-1]): \ [-a, a] \times [0, 1] \quad \rightarrow \quad [0, 1], \tag{6}$$

where the individual risk and individual satisfaction are given in Definitions 2 and 3, respectively. Our progressive solution provides security enhancement by validating the transmitter continuously for ensuring that the security risks caused by inevitable misdetection during the soft authentication can be evaluated by the proposed trust management approach as well as carefully controlled by the judicious adjustment of the authorization level via (4).

Upon denoting the scenarios when the signal is from the Spoofer and from Alice by Ψ_0 and Ψ_1, respectively, we define the individual risk and individual satisfaction of our scheme as:

Definition 2: The individual risk level of our soft authentication and progressive authorization scheme at time t is formulated as

$$R_{\text{ind}}[t] = \sum_{n=1}^{N-1} r_n \cdot \Pr(\mathcal{F}[t] \in (\nu_n, \nu_{n+1}] \mid \Psi_0), \tag{7}$$

where r_n is Bob's degree of loss or damage, if the system assigns the authorization level Φ_n to the Spoofer.

Definition 3: The individual satisfaction level of our soft authentication and progressive authorization scheme at time t is given by

$$S_{\text{ind}}[t] = \sum_{n=1}^{N-1} s_n \cdot \Pr(\mathcal{F}[t] \in (\nu_n, \nu_{n+1}] \mid \Psi_1), \tag{8}$$

where s_n denotes Alice's degree of satisfaction at the authorization level Φ_n.

According to Definitions 2 and 3, the individual risk quantifies the potential loss of Bob if the Spoofer is granted authentication, while the individual satisfaction level quantifies the utility of services/resources granted to Alice by Bob. Note that we have $P_{\text{MD}} = R_{\text{ind}}$ and $P_{\text{FA}} = 1 - S_{\text{ind}}$ in the conventional binary authentication associated with $N = 2$ and $r_1 = s_1 = 1$, where P_{MD} and P_{FA} represent the misdetection rate and false alarm rate, respectively. Furthermore, we can observe from (7) and (8) that there is a trade-off between the individual risk and individual satisfaction level associated with the thresholds $\nu_1, \nu_2, ..., \nu_{N-1}$. If the thresholds are set too low, Bob will suffer from a higher individual risk, because the Spoofer may more easily succeed in imitating Alice and accessing a higher authorization level, but Alice will access more valuable services/resources to achieve a higher level of individual satisfaction. By contrast, if they are set too high, our scheme may suffer from a low individual satisfaction level because of the lower authorization level Alice has, although Bob will experience a lower risk level. In the specific communication scenarios requiring high security protection, the thresholds of our scheme can be increased for reducing the risk caused by the Spoofer during the soft authentication stage.

Remark 1. The designed trust model provides an efficient metric for multiple-level authorization and for coping with the uncertainty and uncontrollability caused by the Spoofer. In contrast to the conventional physical layer authentication schemes [10]–[12], which minimize the misdetection rate while guaranteeing the false alarm rate, we focus our attention on enhancing security by updating the trust level $\mathcal{F}[t]$ based on the validation of the attribute estimates H_{Ot} continuously.

Hence, we will propose an adaptive trust adjustment algorithm to achieve soft authentication and progressive authentication in next section.

III. ONLINE CONFORMAL PREDICTION-BASED ADAPTIVE TRUST MANAGEMENT

In order to adaptively update the trust level $\mathcal{F}$ for soft authentication and progressive authorization, we explore the online conformal prediction technique for classifying the new collected estimates of the physical layer attribute used, i.e. $H_{Ot}, t = 1, 2, 3, ...$, which are time-varying and imperfectly estimated. Through developing an adaptive trust adjustment algorithm based on the confidence of prediction results, security enhancement can be achieved by multiple-step validation of the selected attribute and by appropriately adjusting authorization level in real time.

A. Conformal Predictor for Classification of Physical Layer Attribute Estimates

To classify the new attribute estimates, we explore the conformal prediction technique in this subsection, which is a method conceived for providing valid measures of confidence for individual predictions by machine learning algorithms [34]. One of the main advantages of a conformal predictor is that it can guarantee that the probability of making erroneous predictions is the same as a pre-defined significance level (apart from some statistical fluctuations) [30]. Let us denote the initial training set as $\{z_1, z_2, ..., z_L\} = \{(H_{A1}, 1), (H_{A2}, 1), ..., (H_{AL}, 1)\}$. In general, each training sample z_l contains an attribute estimate in the set $[-a, a]$ and a label of $y_l \in \{0, 1\}$. The label '0' indicates that the attribute estimate is from the Spoofer, while label '1' indicates that it is from Alice. The set of training inputs is denoted by $\mathcal{Z} = [-a, a] \times \{0, 1\}$.

Given a new sample having the observed attribute H_{O1} and a defined *significance level* of $\epsilon \in [0, 1]$, a conformal predictor outputs a predicted set of $Y_{L+1}^{\epsilon} \subseteq \{0, 1\}$ for the unknown label y_{L+1}. Note that H_{O1} is arranged to be $L+1$-th attribute estimate because of the L estimates of Alice collected during the initial authentication phase. The complementary value of $(1 - \epsilon)$ is called *confidence level*. We will always consider nested prediction sets $Y_{L+1}^{\epsilon_1} \subseteq Y_{L+1}^{\epsilon_2}$ when $\epsilon_1 \geq \epsilon_2$. The conformal predictor is formulated as a measurable function

$$\begin{aligned} \Gamma: \quad \mathcal{Z}^* \times [-a, a] \times [0, 1] \quad &\rightarrow \quad \{\emptyset, \{0\}, \{1\}, \{0, 1\}\} \\ z_1, z_2, ..., z_L, \ H_{O1}, \ \epsilon \quad &\rightarrow \quad Y_{L+1}^{\epsilon}, \end{aligned} \tag{9}$$

where $(z_1, z_2, ..., z_L) \in \mathcal{Z}^*$.

The predicted set is valid at the specified significance level ϵ in the sense that the probability of an error satisfies

$$\Pr(y_{L+1} \notin Y_{L+1}^{\epsilon}) \leq \epsilon, \tag{10}$$

under the randomness assumption [34]. That is to say, we have more than $(1-\epsilon)$ confidence in the predicted set Y_{L+1}^{ϵ}. Let us take $\epsilon = 0.1$ as an example, we know that the probability that a prediction set includes the true label is at least 90%. Whether Γ makes an error on the $L+1$-th trial can be represented by 1 and by 0 in case of no error as

$$e_{L+1}^{\epsilon} = \begin{cases} 1, \ \text{if } y_{L+1} \notin Y_{L+1}^{\epsilon} \\ 0, \ \text{otherwise} \end{cases}. \tag{11}$$

The basic idea of conformal prediction is to estimate the p-value for $y \in \{0, 1\}$, denoted as p_y, and to exclude those labels from the predicted set, which satisfy $p_y < \epsilon$. This p-value indicates how different a sample is from a set of training samples, and the higher the p-value, the better this sample fits the group of other samples. In order to obtain the p-value, we apply the nonconformity measure of [35] for estimate H_{O1} as

$$A_{L+1} : \mathcal{Z}^* \times \mathcal{Z} \rightarrow \Re. \tag{12}$$

Then the nonconformity score, which measures how different a sample z_l is from other samples in the set $\{z_1, z_2, ..., z_L, z_{L+1}\}$ [35], can be defined as

$$\alpha_l : A_{L+1}(\{z_1, z_2, ..., z_{l-1}, z_{l+1}, ..., z_L, z_{L+1}\}, z_l) \tag{13}$$

for each sample z_l in $\{z_1, z_2, ..., z_L, z_{L+1}\}$. We can observe from (13) that z_{L+1} depends on an unknown y_{L+1}, so that the nonconformity score α_l relies on a variable $y \in \{0, 1\}$, which is a possible label for the new observation of the selected physical layer attribute H_{O1}. The nonconformity scores are based on the output of a classical underlying predictor, as exemplified by the ridge regression technique of [36], the k-nearest neighbours method of [37] and the autoregressive moving average solution of [38].

Then the p-value of z_{L+1} with different y in set $\{0, 1\}$ can be estimated as the ratio of the nonconformity scores $\alpha_1, \alpha_2, ..., \alpha_L$ that are at least as large as α_{L+1}, which is given as

$$p_{y,L+1} = \frac{|\ \{l = 1, 2, ..., L : \alpha_l \geq \alpha_{L+1}\}\ |}{L}, \tag{14}$$

where $|\ \cdot\ |$ represents the number of samples in the set $\{z_1, z_2, ..., z_L\}$ satisfying $\alpha_l \geq \alpha_{L+1}$ [34]. The predicted set is formed by estimating the p-value for each sample having a nonconformity score, and by adding those samples associated with p-value$\geq \epsilon$, which is formulated as

$$Y_{L+1}^{\epsilon} = \{y : y \in \{0, 1\}, p_{y,L+1} \geq \epsilon\}. \tag{15}$$

Remark 2. Given the conformal predictor developed, the estimates of the selected physical layer attribute can be classified. Then the trust level $\mathcal{F}[t]$ can be adaptively adjusted depending on the classification results and the confidence level $(1-\epsilon)$ in real-time for progressive authorization, which will be explored in next subsection.

B. Adaptive Trust Adjustment Based on Online Machine Learning

In order to dynamically update the trust level $\mathcal{F}$ based on the validation results of estimates $H_{Ot}, t = 1, 2, 3, ...$ in this subsection, we propose an online conformal prediction-based adaptive trust adjustment algorithm. In online learning, the samples $z_{L+t} = (H_{Ot}, y_{L+t}), t = 1, 2, 3, ...$, are presented one by one. We observe the attribute estimate H_{Ot} and

predict its label y_{L+t} for each time, and then we move on to the next attribute estimate. After obtaining the label of each physical layer attribute estimate, the training set $\{z_1, z_2, ..., z_L\}$ is updated by incorporating it and its label, as well as by removing the decorrelated historical training estimates. This is because the physical layer attribute used may become gradually uncorrelated after a period of time. Hence, the training set is also time-varying for maintaining its capability of adapting to the dynamic environment. Note that the attribute estimate at time instant t, namely H_{Ot}, is arranged to represent the $(L+t)$-th trial in the online conformal predictor due to having L initial training samples used at the beginning of physical layer authentication.

This algorithm focuses on validating the collected attribute estimates of the transmitter, i.e. $H_{Ot}, t = 1, 2, 3, ...$, thereby to dynamically update the trust level $\mathcal{F}$ relying on the real-time classification results of H_{Ot}, so that progressive authentication associated with multiple-level authorization can be achieved. To be more specific, according to Definition 1, if Bob observes that the attribute estimate H_{Ot} is classified to be from Alice, the trust level $\mathcal{F}$ will be increased, otherwise it will be decreased. In this way, our trust model becomes robust even if an inaccurate classification occurs during the learning process. At the same time, the risk of a misdetection taking place during the soft authentication stage can be controlled by authorizing the corresponding class of security services/resources according to the trust level $\mathcal{F}[t]$ and by multiple-step validation.

According to the results in [34], the confidence predictor Γ is exactly valid if for each ϵ, $e_1^\epsilon, e_2^\epsilon, ...$ is a sequence of independent Bernoulli-distributed random variables. Unfortunately, the notion of exact validity is vacuous for confidence predictors, since no confidence predictor is exactly valid [34]. A modification of conformal predictors is developed in [35], named smooth conformal predictor $\Gamma^{\rm sm}$, by redefining p-value as

$$p_{y,L+t}^{\rm sm} = \frac{\mid \{l : \alpha_l > \alpha_{L+t}\} \mid + \eta \mid \{l : \alpha_l = \alpha_{L+t}\} \mid}{L+t-1}, \quad (16)$$

where l ranges over $\{1, 2, ..., L+t-1\}$ and η is generated randomly from the uniform distribution on $[0, 1]$. Then, we have the following Lemma:

Lemma 1 [35]: Given any significance level ϵ, the output of the smooth conformal predictor $\Gamma^{\rm sm}$ satisfies

$$\lim_{t\to\infty} \wp_t = 1 - \epsilon, \quad (17)$$

where $\wp_t$ is denoted as the prediction accuracy of the proposed online conformal predictor at time instant t. It is formulated as

$$\wp_t = \frac{\mid \{i = 1, 2, ..., t-1 : e_i^\epsilon = 0\} \mid}{t-1}. \quad (18)$$

Based on the above analysis, the validation result of the online conformal predictor at time instant t associated with dynamically updating the trust level $\mathcal{F}$ is designed as

$$\theta_t = \begin{cases} -(1-\epsilon), & \text{if } Y_{L+t}^\epsilon = \{0\} \\ 1-\epsilon, & \text{if } Y_{L+t}^\epsilon = \{1\} \\ 0, & \text{otherwise} \end{cases}. \quad (19)$$

In this equation, $(1-\epsilon)$ represents our confidence in the prediction set $Y_{L+t}^\epsilon = \{1\}$, namely that the attribute estimate collected is from Alice at time instant t. By contrast, $-(1-\epsilon)$ quantizes the opposite of our confidence in the prediction set $Y_{L+t}^\epsilon = \{0\}$, namely that the collected attribute estimate is deemed to be from the Spoofer at time instant t. We set the validation result for updating the trust level $\mathcal{F}[t]$ as $\theta_t = 0$ in the cases of $Y_{L+t}^\epsilon = \{0, 1\}$ and $Y_{L+t}^\epsilon = \emptyset$, since the prediction results are invalid for authentication and authorization. It is plausible that if $Y_{L+t}^\epsilon = \{0, 1\}$ or $Y_{L+t}^\epsilon = \emptyset$, we can just shift our attention to other confidence levels, especially to specific confidence levels ϵ for which Y_{L+t}^ϵ is a singleton. Although the empirical error rate of the online conformal predictor approaches ϵ in our wireless communication scenarios, we set the validation result in (19) according to the confidence concerning the prediction results. This is because our scheme requires multiple-step validation of the transmitter, thus resulting in a robust performance as a benefit of the progressive authorization process.

Then the trust level $\mathcal{F}$ at time instant t can be obtained by Definition 1 and (6), which is updated as

$$\mathcal{F}[t] = \frac{\rho\mathcal{F}[t-1] + \theta_t}{\rho+1} = \frac{\rho^{t-1}\mathcal{F}[1] + \sum_{i=2}^{t} \rho^{t-i}(\rho+1)^{i-2}\theta_i}{(\rho+1)^{t-1}}, \quad (20)$$

where $\rho \in (0, 1]$ is the forgetting factor. Note that the forgetting factor should be chosen according to the specific application scenario. Upon using this forgetting factor in the trust management, the closer validation results will have a higher influence on the trust level $\mathcal{F}$. It is observed from (20) that $(1-\epsilon) \in [0, 1]$, $-(1-\epsilon) \in [-1, 0]$, $\mathcal{F}[1] \in [0, 1]$, and $\mathcal{F}[t-1] \in [0, 1]$. Upon setting $\mathcal{F}[t] \leq 0$ to 0, we have $\mathcal{F}[t] \in [0, 1]$. In summary, the adaptive trust adjustment procedure conceived for soft authentication and progressive authorization is summarized in Algorithm 1.

Remark 3. In Algorithm 1, Bob authenticates the transmitter (Alice or the Spoofer) through an adaptive process based on the classification of the physical layer attribute estimates. Once the transmitter is believed to be the Spoofer, i.e. its trust level $\mathcal{F}$ is lower than ν_1, the communication session will be terminated by Bob, otherwise, our scheme will be operated until the end of their communications. This algorithm describes a soft authentication and progressive authorization process, which supports prompt connection and enhanced security for legitimate devices.

C. Security Performance Analysis

According to Algorithm 1 and the proposed scheme, we can formulate the following theorems:

Theorem 1: In the case of $\nu_1 \geq (\rho + \epsilon - 1)/(\rho + 1)$ and $s_n = r_n, n = 1, 2, ..., N-1$, the individual risk and individual satisfaction of our scheme at time instant t satisfy

$$\wp[t] R_{\rm ind}[t] = (1 - \wp[t]) S_{\rm ind}[t]. \quad (21)$$

Proof: Please see Appendix A.

Theorem 2: In our soft authentication and progressive authorization scheme, the individual risk at time instant t satisfies

$$(1 - \wp[t]) R_{\rm ind}[t-1] \leq R_{\rm ind}[t] < 1 - \wp[t] \quad (22)$$

Algorithm 1 Online conformal prediction-based adaptive trust adjustment

Given initial training set $\{z_1, z_2, ..., z_L\}$ and significance level ϵ;
1. ***Soft authentication:***
1.1 obtain the initial trust level $\mathcal{F}[1]$ via (5);
1.2 **if** $\mathcal{F}[1] \in (\nu_n, \nu_{n+1}]$, $n \in \{1, 2, ..., N-1\}$
1.3 authorize this transmitter with Φ_n and go to Step 2;
1.4 **else**
1.5 authenticate this transmitter as the Spoofer and go to Step 3;
1.6 **end if**
2. ***Progressive authorization:***
2.1 update training set by $\{z_1, z_2, ..., z_L\} + (H_{O1}, y_{L+1}) - z_1$;
2.2 **for** authentication time instants $t = 2, 3, 4, ...$
2.3 collect new physical layer attribute estimate H_{Ot};
2.4 obtain value $p^{\text{sm}}_{y,L+t}$ and predicted set Y^{ϵ}_{L+t} via (16) and (15), respectively;
2.5 obtain validation result θ_t via (19), and then update trust level $\mathcal{F}[t]$ via (20);
2.6 **if** $\mathcal{F}[t] \in (\nu_n, \nu_{n+1}]$, $n \in \{1, 2, ..., N-1\}$
2.7 authorize this transmitter with Φ_n;
2.8 **else**
2.9 terminate the communication with this transmitter and go to Step 3;
2.10 **end if**
2.11 update training set as $\{z_t, z_{t+1}, ..., z_{L+t-1}\} + (H_{Ot}, y_{L+t}) - z_t$;
2.12 **end for**
3. **END**

under the condition $\nu_1 \geq (\rho+\epsilon-1)/(\rho+1)$ and $\nu_{N-1} \leq 1-\epsilon$.
Proof: Please see Appendix B.

Theorem 3: In our soft authentication and progressive authorization scheme, the individual satisfaction at time instant t obeys

$$\wp[t] S_{\text{ind}}[t-1] \leq S_{\text{ind}}[t] < \wp[t] \tag{23}$$

under the condition $\nu_1 \geq (\rho+\epsilon-1)/(\rho+1)$ and $\nu_{N-1} \leq 1-\epsilon$.
Proof: Please see Appendix C.

Corollary 1: When t is large enough, the individual risk and individual satisfaction of our scheme at time instant t satisfy

$$(1-\epsilon) R_{\text{ind}}[t] \approx \epsilon S_{\text{ind}}[t], \tag{24}$$

under conditions $\nu_1 \geq (\rho+\epsilon-1)/(\rho+1)$ and $s_n = r_n, n = 1, 2, ..., N-1$.
Proof: Please see Appendix D.

We can observe from Theorems 1-3 that the individual satisfaction and individual risk of our scheme depend both on the dynamic trust level $\mathcal{F}[t]$ as well as on the prediction accuracy $\wp[t]$, which rely on the real-time validation results of the selected time-varying attribute. It is observed from Theorems 2 and 3 that our scheme evaluates the physical layer attribute used, thereby promptly adjusting the trust model, so that the individual risk can be dramatically reduced within a short time. Given the specific distribution of the attribute estimates used in our scheme, the closed-form expressions of the $R_{\text{ind}}[t]$ and of the $S_{\text{ind}}[t]$ can be obtained.

Case study: In order to characterize the performance of our soft authentication and progressive authorization, we study a special case assuming that the specific physical layer attribute of Alice and that of the Spoofer obey the classic Gaussian distribution with means of μ_1 and μ_2 as well as with variances of σ_1^2 and σ_2^2, respectively, and setting $N = 3$ and $\rho = 1$. Then we can obtain the following results:

Corollary 2: The closed-form expressions of the individual risk and individual satisfaction of our scheme at time instant $t = 1$ can be formulated, respectively, as

$$\begin{aligned} R_{\text{ind}}[1] = \frac{r_1}{\sqrt{\pi}} [& \int_{\frac{\mu_1-\mu_2+2a(1-\nu_2)}{\sigma_2\sqrt{2}}}^{\frac{\mu_1-\mu_2+2a(1-\nu_1)}{\sigma_2\sqrt{2}}} \exp(-x^2) \mathrm{d}x \\ & + \int_{\frac{\mu_1-\mu_2-2a(1-\nu_1)}{\sigma_2\sqrt{2}}}^{\frac{\mu_1-\mu_2-2a(1-\nu_2)}{\sigma_2\sqrt{2}}} \exp(-x^2) \mathrm{d}x] \\ & + \frac{r_2}{\sqrt{\pi}} \int_{\frac{\mu_1-\mu_2-2a(1-\nu_2)}{\sigma_2\sqrt{2}}}^{\frac{\mu_1-\mu_2+2a(1-\nu_2)}{\sigma_2\sqrt{2}}} \exp(-x^2) \mathrm{d}x \end{aligned} \tag{25}$$

and

$$\begin{aligned} S_{\text{ind}}[1] = s_1 [& \text{erf}(\frac{\sqrt{2}a(1-\nu_1)}{\sigma_1}) - \text{erf}(\frac{\sqrt{2}a(1-\nu_2)}{\sigma_1})] \\ & + s_2 \text{erf}(\frac{\sqrt{2}a(1-\nu_2)}{\sigma_1}), \end{aligned} \tag{26}$$

where $\text{erf}(\cdot)$ is the error function.
Proof: Please see Appendix E.

Corollary 3: The closed-form expressions of the individual risk and individual satisfaction of our scheme at time instant $t = 2, 3, 4, ...$ can be obtained based on the results of Corollary 2, respectively, as

$$\begin{aligned} R_{\text{ind}}[t] = & r_1 (1 - \wp[t]) \Pr(\mathcal{F}[t-1] \in (2\nu_1 - 1 + \epsilon, 2\nu_2 - 1 + \epsilon]) \\ & + r_2 (1 - \wp[t]) \Pr(\mathcal{F}[t-1] \in (2\nu_2 - 1 + \epsilon, 1]) \end{aligned} \tag{27}$$

and

$$\begin{aligned} S_{\text{ind}}[t] = & s_1 \wp[t] \Pr(\mathcal{F}[t-1] \in (2\nu_1 - 1 + \epsilon, 2\nu_2 - 1 + \epsilon]) \\ & + s_2 \wp[t] \Pr(\mathcal{F}[t-1] \in (2\nu_2 - 1 + \epsilon, 1]) \end{aligned} \tag{28}$$

under condition $\nu_1 \geq \epsilon/2$.
Proof: Please see Appendix F.

Corollary 4: Based on the results of Corollaries 2 and 3, the solution of the following problem does exist.

$$\begin{aligned} & (\nu_1, \nu_2) = \arg\max S_{\text{ind}}[t], \\ & \text{s.t. } R_{\text{ind}}[t] \leq \delta, 0 < \nu_1 < \nu_2 < 1, \end{aligned} \tag{29}$$

where δ denotes maximum tolerate individual risk invoked for controlling the risk in our soft authentication and progressive authorization process.
Proof: Please see Appendix G.

Remark 4. Corollaries 2 and 3 give the closed-form expressions of the individual risk and individual satisfaction in the soft authentication phase (i.e. $t = 1$) and in the following phases (namely $t = 2, 3, 4, ...$), respectively. It is observed from Corollary 2 that the required soft security is achieved

by setting multiple authorization levels, thus the risk of a misdetection can be carefully controlled by configuring this device for a low authorization level.

Remark 5. As we can observe from above Theorems and Corollaries that the individual risk and individual satisfaction depend on the thresholds $\nu_1, \nu_2, ..., \nu_{N-1}$. Most of the conventional physical layer authentication techniques determine the threshold of the authentication system based on the Neyman-Pearson criterion [2], [8], [11], which minimizes the misdetection rate subject to a maximum tolerable constraint on the false alarm rate. However, these schemes constitute binary authentication solutions, which are unsuitable for achieving the soft authentication and progressive authorization. More importantly, for a communication system, the thresholds can be flexibly determined to meet the requirement of security.

IV. SIMULATION RESULTS

In order to evaluate the performance of our soft authentication and progressive authorization scheme, we provide simulation results in this section by utilizing both carrier frequency offset (CFO) and received signal strength indicator (RSSI). Firstly, the training process and our results characterizing the proposed online conformal predictor are presented. Then we characterize the performance of our soft authentication solution by studying the trade-off between individual satisfaction level vs. individual risk level during the soft authentication stage. A scenario is studied for characterizing the security performance and robustness of our progressive authorization solution, where a misdetection event occurs during the soft authentication stage or the Spoofer imitates Alice after the soft authentication. Compared to the static binary authentication scheme and the kernel machine learning-based authentication scheme of [2], the superiority of our scheme is highlighted.

A. Online Conformal Prediction Results

In order to achieve soft authentication and progressive authorization, we utilize both the CFO [11] and RSSI [39] for the validation of our scheme. The observations of the CFO seen in Fig. 2 (a) and those of the RSSI seen in Fig. 3 (a) used for training and testing of our scheme are collected from the implementation-oriented contributions of [11] and [39], respectively. In a little more detail, the authors of [11] built a software-defined radio platform based on the Universal Software Radio Peripheral to capture the real CFO data. The system implemented comprises two transmitters (i.e. Alice and the Spoofer) and one receiver (Bob) operating at a carrier frequency of 2.47 GHz. Furthermore, the authors of [39] collected data throughout three different measurement campaigns, seven days combined and spread across two summer seasons. The measurements were carried out in an approximate range of 0-100 m at points which were approximately 10 m apart from each other at 9 different parts of the orchard described in [39] along five directions, namely along, across, 30°, 45°, and 60° with respect to the tree rows. As shown in Fig. 1 and the system model, the Spoofer can be viewed as the second transmitter, who is located in a third location (i.e. more than a wave length away from Alice) and tries to imitate Alice for

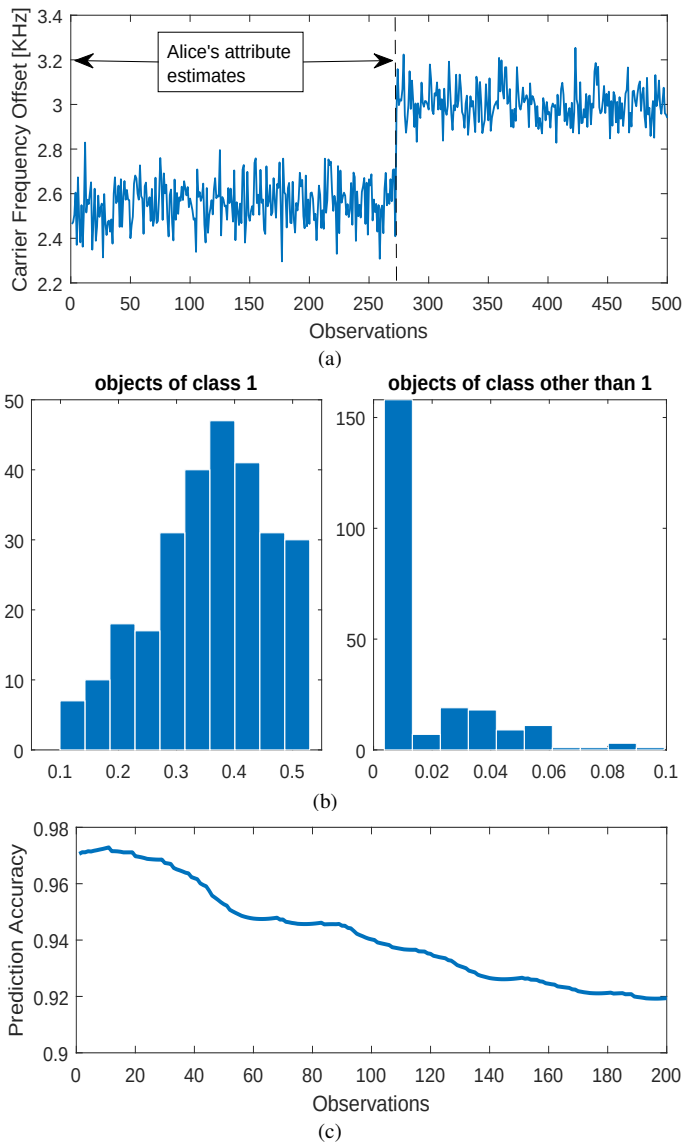

Fig. 2. Performance of the proposed online conformal predictor relying on CFO. (a) Carrier frequency offset (CFO) observations of Alice for training, and CFO observations of both Alice and the Spoofer for testing in our scheme. (b) p-value for case $y = 1$, i.e. the CFO estimate is from Alice. (c) Accuracy of our online conformal predictor by utilizing CFO observations.

gleaning illegal advantages from Bob. Hence, the CFO and RSSI estimates of the Spoofer are also collected for testing in the simulation.

Given the initial training set $\{z_1, z_2, ..., z_L\}$, $L = 40$, and the significance level of $\epsilon = 0.1$, we train and test the proposed online conformal predictor by utilizing the collected observations of the CFO. Note that only Alice's CFO observations are used for training, i.e. the first 40 samples in Fig. 2 (a), and the CFO observations of both Alice and the Spoofer are utilized for testing the prediction accuracy of the proposed scheme based on the online conformal predictor. The distribution of the smoothened p-values recorded for $y = 1$ (i.e. the CFO observations are from Alice) is given in Fig. 2 (b), which is used to form the predicted set of (15). To be more specific, the x-axis represents the p-values, while the y-axis is the number of CFO observations. When the p-value is below the

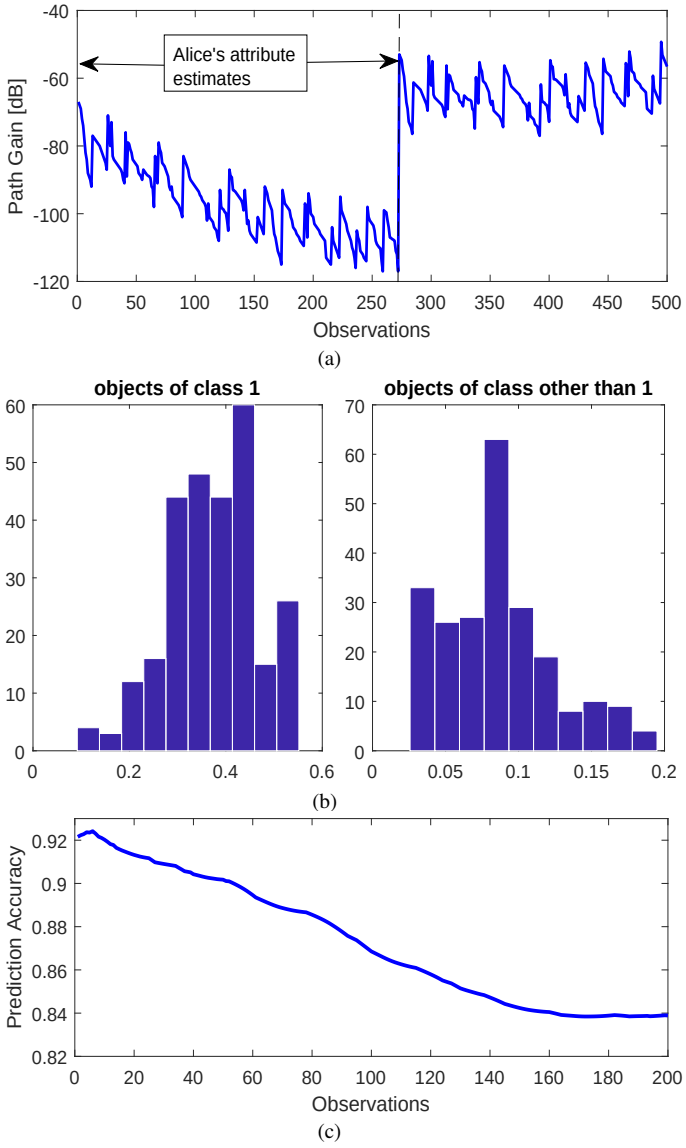

Fig. 3. Performance of the proposed online conformal predictor relying on RSSI. (a) Received signal strength indicator (RSSI) observations of Alice for training, and RSSI observations of both Alice and the Spoofer for testing in our scheme. (b) p-value for case $y = 1$, i.e. the RSSI estimate is from Alice. (c) Accuracy of our online conformal predictor by utilizing RSSI observations.

significance level ϵ, the class (either 0 or 1) will be removed from the predicted set Y_t^{ϵ}. Then we have a confidence level of 0.9 concerning the predicted set. More importantly, Fig. 2 (c) characterizes the prediction accuracy of the proposed online conformal predictor relying on new CFO observations, i.e. $\wp_t$. We can observe from Fig. 2 (c) that the prediction accuracy values concerning new CFO observations are all higher than 0.9. The reason for this trend is that the proposed conformal predictor keeps the error rate below the significance level ϵ.

Similarly, only Alice's RSSI observations are used for training, i.e. the first 40 samples in Fig. 3 (a), and the RSSI observations of both Alice and the Spoofer are utilized for testing in the online conformal predictor. Fig. 3 (b) and (c) characterize the online conformal prediction results relying on the RSSI observations by setting the significance level of $\epsilon = 0.2$, where (b) presents the p-values for the class of $y = 1$, and (c) demonstrates the prediction accuracy of our scheme concerning new RSSI observations. It is observed from Fig. 3 (c) that the prediction accuracy concerning new observations is higher than 0.8.

B. Performance of Our Soft Authentication and Progressive Authorization Scheme

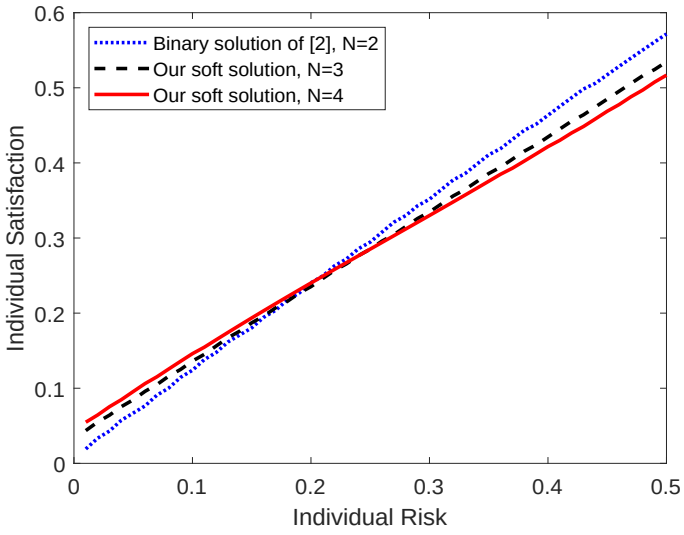

Fig. 4. Performance of our soft authentication solution: Individual satisfaction vs. threshold of individual risk for the numbers of authorization levels $N = 2$, $N = 3$, and $N = 4$ based on the results of Fig. 2. Case $N = 2$ is the binary authentication scheme of [2] while cases $N = 3$ and $N = 4$ represent the proposed soft solution in this paper.

Fig. 4 characterizes the individual satisfaction vs. the individual risk with respect to the number of authorization levels of $N = 2$, $N = 3$, and $N = 4$ by utilizing CFO of Fig. 2. We can observe from Fig. 4 that upon increasing the individual risk threshold, namely δ, the individual satisfaction values increase in all cases. The reason for this trend is that there is a trade-off between the individual risk and individual satisfaction as demonstrated by the analytical results of Section III-C. Furthermore, when the threshold of the individual risk is lower than 0.2, the individual satisfaction value of the scenario associated with $N = 4$ is the highest, while that of $N = 2$ is the lowest. It is because that using multiple authorization levels in our scheme helps to access services/resources quickly when the threshold of individual risk is low, i.e. the security requirement is high.

Then we study the scenario when a misdetection event occurs during the soft authentication stage or when the Spoofer attacks Alice after the soft authentication stage. In Fig. 5, we characterize the performance of our progressive authorization scheme by utilizing the CFO (see Fig. 2) with respect to the forgetting factors of $\rho = 0.8$, $\rho = 0.6$ and $\rho = 0.4$ compared to that of the static binary authentication scheme. In this figure, we set the number of authorization levels to $N = 3$ in our scheme, while the classification of the services/resources is given by Φ_0, Φ_1, and Φ_2. We can observe from Fig. 5 that the individual risk values of our scheme decrease in all cases upon increasing the number of observations (i.e. the

estimates of CFO) of the transmitter. The reason for this trend is that if Bob observes that the CFO is in nonconformity with the training samples of Alice, the trustworthiness of this transmitter will be decreased. Thereafter the authorization level will be reduced to Φ_0 within a short time. However, in the static binary authentication scheme, the individual risk value will not be decreased, leading to substantial losses in this scenario. This demonstrates that the static binary authentication scheme fails to deal with the scenario, when a misdetection occurs during the soft authentication phase or the Spoofer attacks the authorized device after the soft authentication stage. It also demonstrates the superiority of our scheme after soft authentication by providing additional protection. Additionally, it can be observed from Fig. 5 that the individual risk of our scheme associated with the forgetting factor of $\rho = 0.8$ is higher than that of $\rho = 0.6$ and $\rho = 0.4$. The risk level associated with $\rho = 0.4$ is the lowest in these three cases. This is because the historical observations of Alice's CFO have more substantial effects on the adaptive trust adjustment system in the case $\rho = 0.8$, so that the trust level $\mathcal{F}$ is reduced slower than that of the forgetting factors of $\rho = 0.6$ and $\rho = 0.4$.

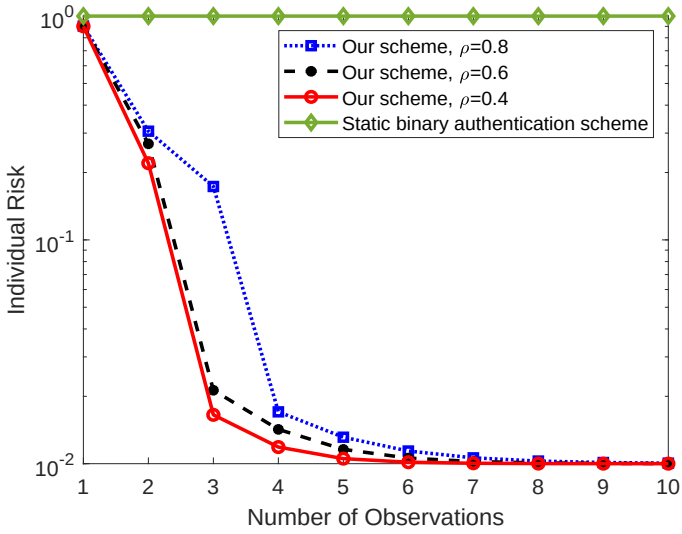

Fig. 5. Performance of our progressive authorization solution for the forgetting factors of $\rho = 0.8$, $\rho = 0.6$ and $\rho = 0.4$ benchmarked against the static binary authentication scheme.

In Fig. 6, we characterize the security performance of our scheme for $N = 3$, $N = 4$ and $N = 5$ authorization levels to show the effects of N on our scheme in the scenario that a misdetection event occurs in the soft authentication stage or the Spoofer attacks the authorized device after the soft authentication stage. Some transient observations (from 3 to 5 observations) are added to show the robustness of our scheme, which represent the prediction errors in the proposed online conformal predictor, and are mainly caused by the imperfect estimates and variations of the CFO, noisy observations, as well as owing to the dynamic behaviors of the Spoofer. It can be observed from Fig. 6 that the individual risk value of our scheme recorded for $N = 3$ decreases quicker than in the other cases in Stage 1. The reason for this trend is that

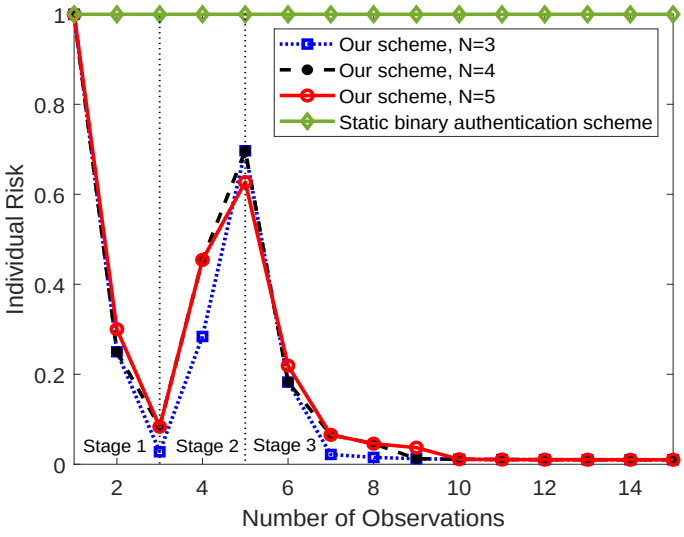

Fig. 6. Security performance and robustness of our progressive authorization solution parameterized by the number of authorization levels $N = 3$, $N = 4$ and $N = 5$. There are some transient observations (in Stage 2) in the progressive authorization process.

when the CFO estimates are identified by Bob to be from the Spoofer, the authorization of the transmitter in the $N = 3$ scenario will be reduced to the lowest level more quickly. By contrast, the case of $N = 5$ needs more time (observations) to achieve a low individual risk. Furthermore, the performance of our scheme recorded for $N = 3$ suffers from the lowest robustness, although the individual risk level of this scenario decreases more quickly than in the other cases in Stage 1. To be specific, the risk level of $N = 3$ decays fastest in Stage 1 (before 3 observations), while it increases fastest in Stage 2 (from 3 to 5 observations). In Stage 3, it decreases fastest in all cases. This indicates that our scheme having a lower number of authorization levels is less robust, but it achieves a reduced individual risk more quickly in the scenario that a misdetection event occurs in the soft authentication stage or the Spoofer attacks Alice after the soft authentication stage.

Fig. 7 characterizes the individual satisfaction comparison results of our progressive authorization process and the kernel machine learning-based physical layer authentication process of [2]. In this figure, we consider a scenario that false alarm events occur during the authentication process because of the imperfect estimates and variations of the CFO, as seen from 6 to 8 observations. It is observed from Fig. 7 that the individual satisfaction level of our scheme is a bit lower than that of the physical layer authentication process of [2] for less than 6 CFO observations. This is because of the specific nature of the trust management approach used in the proposed scheme, where the individual satisfaction level depends on the trust level between Alice and Bob. However, once a false alarm event occurs during the authentication process, the individual satisfaction value of the authentication process of [2] tends to 0, because the communication session between Alice and Bob is terminated by Bob. By contrast, the proposed progressive authorization scheme exhibits its robustness in term of tolerating a few false alarms. In conclusion, both Fig.

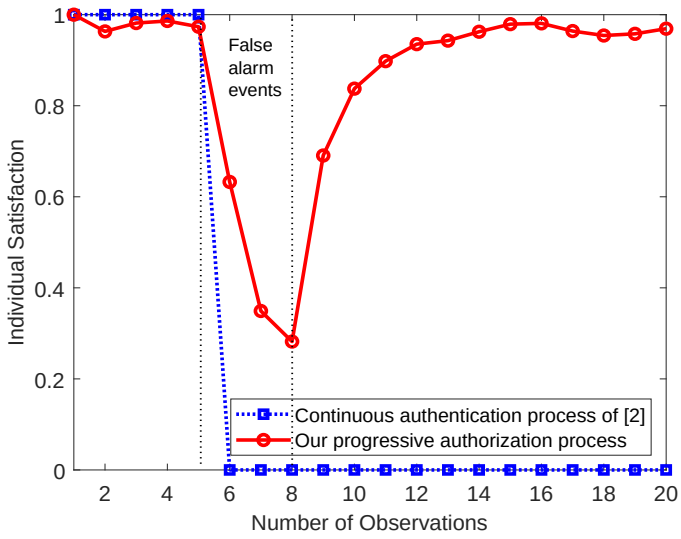

Fig. 7. Individual satisfaction comparison results of our scheme and the physical layer authentication scheme of [2] in the scenario that false alarms happen during the authentication process.

4 and Fig. 7 demonstrate that the proposed soft authentication and progressive authorization scheme performs better than the kernel machine learning-based authentication scheme of [2] when the threshold of individual risk is low or when false alarm events occur during the authentication process, hence resulting in a faster access and higher robustness.

V. CONCLUSIONS

In this paper, we proposed a soft authentication and progressive authorization scheme based on the trust management to achieve security enhancement by evaluating the physical layer attribute estimates. A trust model was firstly designed for evaluating the trustworthiness of the relationship between transmitter and receiver, and for supporting a multiple-level authorization. Then a conformal predictor was developed for classifying the estimates of the physical layer attribute selected, which are used for characterizing the trustworthiness of the transmitter. We proposed an adaptive algorithm based on online machine learning to update the trust management in real time. The simulation results characterized the benefits of our scheme, demonstrating its superiority over the static binary authentication scheme and the exiting physical layer authentication scheme benchmarker.

APPENDIX A
THE PROOF OF THEOREM 1

According to Definitions 2 and 3, and the proposed adaptive trust management approach of (20), the individual risk and individual satisfaction at time instant t can be expressed as (30) and (31), respectively. Given the condition $\nu_1 \geq (\rho + \epsilon - 1)/(\rho + 1)$, we can obtain

$$\Pr(\mathcal{F}[t-1] \in (\frac{\nu_n(\rho+1)+1-\epsilon}{\rho}, \frac{\nu_{n+1}(\rho+1)+1-\epsilon}{\rho}]) = 0, \quad (32)$$

since $0 < \nu_1 < \nu_2 < \cdots < \nu_N = 1$ and $(\nu_n(\rho+1)+1-\epsilon)/\rho \geq 1$.

Then the individual risk and individual satisfaction at time instant t can be rewritten as

$$R_{\text{ind}}[t] = (1-\wp[t]) \sum_{n=1}^{N-1} s_n \Pr(\mathcal{F}[t-1] \in (\frac{\nu_n(\rho+1)-1+\epsilon}{\rho}, \frac{\nu_{n+1}(\rho+1)-1+\epsilon}{\rho}]) \quad (33)$$

and

$$S_{\text{ind}}[t] = \wp[t] \sum_{n=1}^{N-1} s_n \Pr(\mathcal{F}[t-1] \in (\frac{\nu_n(\rho+1)-1+\epsilon}{\rho}, \frac{\nu_{n+1}(\rho+1)-1+\epsilon}{\rho}]) \quad (34)$$

under the condition of $s_n = r_n$. Therefore, the individual risk and individual satisfaction of our scheme at time instant t satisfy (21). □

APPENDIX B
THE PROOF OF THEOREM 2

According to Definition 2 and the proposed adaptive trust management approach of (20) as well as the results of Theorem 1, the individual risk at time instant t can be expressed as

$$R_{\text{ind}}[t] = (1-\wp[t]) \sum_{n=1}^{N-1} r_n \Pr(\mathcal{F}[t-1] \in (\frac{\nu_n(\rho+1)-1+\epsilon}{\rho}, \frac{\nu_{n+1}(\rho+1)-1+\epsilon}{\rho}]) \quad (35)$$

under the conditions $\nu_1 \geq (\rho+\epsilon-1)/(\rho+1)$ and $\nu_{N-1} \leq 1-\epsilon$. Then we have

$$\frac{\nu_n(\rho+1)-(1-\epsilon)}{\rho} \leq \nu_n, \ n = 1, 2, ..., N-1, \quad (36)$$

and

$$\Pr(\mathcal{F}[t-1] \in (\frac{\nu_{N-1}(\rho+1)-1+\epsilon}{\rho}, \frac{(\rho+1)-1+\epsilon}{\rho}]) \geq \Pr(\mathcal{F}[t-1] \in (\nu_{N-1}, 1]). \quad (37)$$

Hence, the following result is obtained.

$$R_{\text{ind}}[t] \geq (1-\wp[t]) R_{\text{ind}}[t-1]. \quad (38)$$

Furthermore, due to

$$\sum_{n=1}^{N-1} \Pr(\mathcal{F}[t-1] \in (\frac{\nu_n(\rho+1)-1+\epsilon}{\rho}, \frac{\nu_{n+1}(\rho+1)-1+\epsilon}{\rho}]) \leq 1, \quad (39)$$

we have

$$(1-\wp[t]) \sum_{n=1}^{N-1} r_n \Pr(\mathcal{F}[t-1] \in (\frac{\nu_n(\rho+1)-1+\epsilon}{\rho}, \frac{\nu_{n+1}(\rho+1)-1+\epsilon}{\rho}]) < (1-\wp[t]). \quad (40)$$

Hence, the individual risk at time instant t satisfies (22) in our scheme. □

$$R_{\rm ind}[t] = \sum_{n=1}^{N-1} r_n \cdot \Pr(\mathcal{F}[t-1] \in (\frac{\nu_n(\rho+1)-\theta_t}{\rho}, \frac{\nu_{n+1}(\rho+1)-\theta_t}{\rho}] \mid \Psi_0)$$
$$= \sum_{n=1}^{N-1} r_n \cdot \{\Pr(\mathcal{F}[t-1] \in (\frac{\nu_n(\rho+1)+1-\epsilon}{\rho}, \frac{\nu_{n+1}(\rho+1)+1-\epsilon}{\rho}])\wp[t]$$
$$+ \Pr(\mathcal{F}[t-1] \in (\frac{\nu_n(\rho+1)-1+\epsilon}{\rho}, \frac{\nu_{n+1}(\rho+1)-1+\epsilon}{\rho}])(1-\wp[t])\}. \quad (30)$$

$$S_{\rm ind}[t] = \sum_{n=1}^{N-1} s_n \cdot \Pr(\mathcal{F}[t-1] \in (\frac{\nu_n(\rho+1)-\theta_t}{\rho}, \frac{\nu_{n+1}(\rho+1)-\theta_t}{\rho}] \mid \Psi_1)$$
$$= \sum_{n=1}^{N-1} s_n \cdot \{\Pr(\mathcal{F}[t-1] \in (\frac{\nu_n(\rho+1)-1+\epsilon}{\rho}, \frac{\nu_{n+1}(\rho+1)-1+\epsilon}{\rho}])\wp[t]$$
$$+\Pr(\mathcal{F}[t-1] \in (\frac{\nu_n(\rho+1)+1-\epsilon}{\rho}, \frac{\nu_{n+1}(\rho+1)+1-\epsilon}{\rho}])(1-\wp[t])\}. \quad (31)$$

APPENDIX C
THE PROOF OF THEOREM 3

Similar to the proof of Theorem 2 in Appendix B, given the conditions $\nu_1 \geq (\rho+\epsilon-1)/(\rho+1)$ and $\nu_{N-1} < 1-\epsilon$, the individual satisfaction at time instant t is shown in (30). Based on the results of (34) and (37), as well as $0 \leq s_1 < s_2 < \cdots < s_{N-1} \leq 1$, we have

$$S_{\rm ind}[t] \geq \wp[t] S_{\rm ind}[t-1]. \quad (41)$$

Given the result of (39), the following inequality is satisfied

$$\wp[t] \sum_{n=1}^{N-1} s_n \Pr(\mathcal{F}[t-1] \in (\frac{\nu_n(\rho+1)-1+\epsilon}{\rho}, \frac{\nu_{n+1}(\rho+1)-1+\epsilon}{\rho}]) < \wp[t]. \quad (42)$$

Therefore, the individual satisfaction at time instant t satisfies (23) in our scheme. □

APPENDIX D
THE PROOF OF COROLLARY 1

According to Lemma 1, when t is large enough, the empirical prediction accuracy of the online conformal predictor obeys

$$\wp_t \approx 1-\epsilon \quad (43)$$

according to (17). Hence, the result of Corollary 1 can be obtained directly based on (21) and (43). □

APPENDIX E
THE PROOF OF COROLLARY 2

In this case study, we assume that the attribute observations of Alice and that of Spoofer obey Gaussian distribution with means μ_1 and μ_2 and variances σ_1^2 and σ_2^2, respectively, as well as set $N=3$ and $\rho=1$. We formulate $\mathcal{F}[1] = |H_A - H_{O1}|/2a$ where H_A is the average of $H_{A1}, H_{A2}, ..., H_{AL}$, and $|H_A - H_1|/2a$ normalizes the range of difference ΔH_{O1} in (2) to the limited set $[0,1]$. Then the individual risk and individual satisfaction at time instant $t=1$ can be given as (44) and (45), respectively. Therefore, the closed-forms of individual risk and individual satisfaction of our scheme at time instant $t=1$ are shown in (25) and (26), respectively. □

APPENDIX F
THE PROOF OF COROLLARY 3

In this case study, the individual risk and individual satisfaction at time instant $t=2,3,4,...$ can be obtained based on the results of Theorems 1-3 and Corollary 2 as

$$R_{\rm ind}[t] = \sum_{n=1}^{2} r_n \Pr(\frac{\mathcal{F}[t-1]+\theta_t}{2} \in (\nu_n, \nu_{n+1}] \mid \Psi_0)$$
$$= (1-\wp[t]) r_1 \Pr(\mathcal{F}[t-1] \in (2\nu_1 - 1 + \epsilon, 2\nu_2 - 1 + \epsilon])$$
$$+(1-\wp[t]) r_2 \Pr(\mathcal{F}[t-1] \in (2\nu_2 - 1 + \epsilon, 1])$$
$$+\wp[t] r_1 \Pr(\mathcal{F}[t-1] \in (2\nu_1 + 1 - \epsilon, 2\nu_2 + 1 - \epsilon])$$
$$+\wp[t] r_2 \Pr(\mathcal{F}[t-1] \in (2\nu_2 + 1 - \epsilon, 3 - \epsilon]) \quad (46)$$

and

$$S_{\rm ind}[t] = \sum_{n=1}^{2} s_n \Pr(\frac{\mathcal{F}[t-1]+\theta_t}{2} \in (\nu_n, \nu_{n+1}] \mid \Psi_1)$$
$$= \wp[t] s_1 \Pr(\mathcal{F}[t-1] \in (2\nu_1 - 1 + \epsilon, 2\nu_2 - 1 + \epsilon])$$
$$+\wp[t] s_2 \Pr(\mathcal{F}[t-1] \in (2\nu_2 - 1 + \epsilon, 1])$$
$$+(1-\wp[t]) s_1 \Pr(\mathcal{F}[t-1] \in (2\nu_1 + 1 - \epsilon, 2\nu_2 + 1 - \epsilon])$$
$$+(1-\wp[t]) s_2 \Pr(\mathcal{F}[t-1] \in (2\nu_2 + 1 - \epsilon, 3 - \epsilon]). \quad (47)$$

According to the derived $R_{\rm ind}[1]$ and $S_{\rm ind}[1]$ in (25) and (26), respectively, the the individual risk and individual satisfaction of our scheme at time instant $t=2,3,4,...$ are given as (27) and (28), respectively, under condition $\nu_1 \geq \epsilon/2$. □

APPENDIX G
THE PROOF OF COROLLARY 4

Given the problem of (29), we let $R_{\rm ind}[t] = \delta$, since there is a trade-off between the individual risk and individual sat-

$$
\begin{aligned}
R_{\rm ind}[1] &= r_1 \Pr(\mathcal{F}[1] \in (\nu_1, \nu_2] \mid \Psi_0) + r_2 \Pr(\mathcal{F}[1] \in (\nu_2, 1] \mid \Psi_0) \\
&= r_1 \Pr(|H_A - H_{O1}| \in [2a(1-\nu_2), 2a(1-\nu_1)) \mid \Psi_0) + r_2 \Pr(|H_A - H_{O1}| \in [0, 2a(1-\nu_2)) \mid \Psi_0) \\
&= \frac{1}{2} r_1 [\mathrm{erf}(\frac{H_A + 2a(1-\nu_1) - \mu_2}{\sigma_2 \sqrt{2}}) - \mathrm{erf}(\frac{H_A + 2a(1-\nu_2) - \mu_2}{\sigma_2 \sqrt{2}}) + \mathrm{erf}(\frac{H_A - 2a(1-\nu_2) - \mu_2}{\sigma_2 \sqrt{2}}) \\
&\quad - \mathrm{erf}(\frac{H_A - 2a(1-\nu_1) - \mu_2}{\sigma_2 \sqrt{2}})] + \frac{1}{2} r_2 [\mathrm{erf}(\frac{H_A + 2a(1-\nu_2) - \mu_2}{\sigma_2 \sqrt{2}}) - \mathrm{erf}(\frac{H_A - 2a(1-\nu_2) - \mu_2}{\sigma_2 \sqrt{2}})] \\
&= \frac{1}{2} r_1 [\mathrm{erf}(\frac{\mu_1 - \mu_2 + 2a(1-\nu_1)}{\sigma_2 \sqrt{2}}) - \mathrm{erf}(\frac{\mu_1 - \mu_2 + 2a(1-\nu_2)}{\sigma_2 \sqrt{2}}) + \mathrm{erf}(\frac{\mu_1 - \mu_2 - 2a(1-\nu_2)}{\sigma_2 \sqrt{2}}) \\
&\quad - \mathrm{erf}(\frac{\mu_1 - \mu_2 - 2a(1-\nu_1)}{\sigma_2 \sqrt{2}})] + \frac{1}{2} r_2 [\mathrm{erf}(\frac{\mu_1 - \mu_2 + 2a(1-\nu_2)}{\sigma_2 \sqrt{2}}) - \mathrm{erf}(\frac{\mu_1 - \mu_2 - 2a(1-\nu_2)}{\sigma_2 \sqrt{2}})]. \qquad (44)
\end{aligned}
$$

$$
\begin{aligned}
S_{\rm ind}[1] &= s_1 \Pr(\mathcal{F}[1] \in (\nu_1, \nu_2] \mid \Psi_1) + s_2 \Pr(\mathcal{F}[1] \in (\nu_2, 1] \mid \Psi_1) \\
&= s_1 \Pr(|H_A - H_{O1}| \in [2a(1-\nu_2), 2a(1-\nu_1)) \mid \Psi_1) + s_2 \Pr(|H_A - H_{O1}| \in [0, 2a(1-\nu_2)) \mid \Psi_1) \\
&= \frac{1}{2} s_1 [\mathrm{erf}(\frac{H_A + 2a(1-\nu_1) - \mu_1}{\sigma_1 \sqrt{2}}) - \mathrm{erf}(\frac{H_A + 2a(1-\nu_2) - \mu_1}{\sigma_1 \sqrt{2}}) + \mathrm{erf}(\frac{H_A - 2a(1-\nu_2) - \mu_1}{\sigma_1 \sqrt{2}}) \\
&\quad - \mathrm{erf}(\frac{H_A - 2a(1-\nu_1) - \mu_1}{\sigma_1 \sqrt{2}})] + \frac{1}{2} s_2 [\mathrm{erf}(\frac{H_A + 2a(1-\nu_2) - \mu_1}{\sigma_1 \sqrt{2}}) - \mathrm{erf}(\frac{H_A - 2a(1-\nu_2) - \mu_1}{\sigma_1 \sqrt{2}})] \\
&= s_1 [\mathrm{erf}(\frac{2a(1-\nu_1)}{\sigma_1 \sqrt{2}}) - \mathrm{erf}(\frac{2a(1-\nu_2)}{\sigma_1 \sqrt{2}})] + s_2 \mathrm{erf}(\frac{2a(1-\nu_2)}{\sigma_1 \sqrt{2}}). \qquad (45)
\end{aligned}
$$

isfaction associated with the thresholds ν_1, ν_2. The maximum $S_{\rm ind}[t]$ can only be achieved when $R_{\rm ind}[t] = \delta$. Hence, we have

$$
\begin{aligned}
&(1 - \wp[t]) r_1 \Pr(\mathcal{F}[t-1] \in (2\nu_1 - 1 + \epsilon, 2\nu_2 - 1 + \epsilon]) \\
&\quad + (1 - \wp[t]) r_2 \Pr(\mathcal{F}[t-1] \in (2\nu_2 - 1 + \epsilon, 1]) = \delta \qquad (48) \\
&\Rightarrow \nu_2 = g(\nu_1), \qquad (49)
\end{aligned}
$$

where $g(\cdot)$ is the function of ν_2 in terms of ν_1. Then the problem of (29) can be rewritten as

$$
\begin{aligned}
\nu_1 = \arg\max \{ &\wp[t] s_1 \Pr(\mathcal{F}[t-1] \in (2\nu_1 - 1 + \epsilon, 2g(\nu_1) \\
&- 1 + \epsilon]) + \wp[t] s_2 \Pr(\mathcal{F}[t-1] \in (2g(\nu_1) - 1 + \epsilon, 1])\}. \qquad (50)
\end{aligned}
$$

Therefore, the solution of problem (29) does indeed exist because the righthand side of (50) is a continuous function in terms of ν_1 based on the closed-form expression of individual satisfaction of (28). □

REFERENCES

[1] H. Fang, X. Wang, and S. Tomasin, "Machine learning for intelligent authentication in 5G-and-beyond wireless networks," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 55-61, 2019.

[2] H. Fang, X. Wang, and L. Hanzo, "Learning-aided physical layer authentication as an intelligent process," *IEEE Trans. Commun.*, vol. 67, no. 3, pp. 2260-2273, 2019.

[3] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727-1765, 2016.

[4] M. Iwamoto, K. Ohta, and J. Shikata, "Security formalizations and their relationships for encryption and key agreement in information-theoretic cryptography," *IEEE Trans. Inf. Theory*, vol. 64, no. 1, pp. 654-685, 2018.

[5] Y. Chen, "Fully incrementing visual cryptography from a succinct non-monotonic structure," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 5, pp. 1082-1091, 2017.

[6] Y. Ren, J.-C. Chen, J.-C. Chin, and Y.-C. Tseng, "Design and analysis of the key management mechanism in evolved multimedia broadcast/multicast service," *IEEE Trans. Wireless Commun.*, vol. 15, no. 12, pp. 8463-8476, 2016.

[7] J. Ning, J. Xu, K. Liang, F. Zhang, and E.-C. Chang, "Passive attacks against searchable encryption," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 3, pp. 789-802, 2019.

[8] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: current challenges and future developments," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 152-158, 2016.

[9] H. Fang, L. Xu, and X. Wang, "Coordinated multiple-relays based physical-layer security improvement: a single-leader multiple-followers Stackelberg game scheme," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 1, pp. 197-209, 2018.

[10] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 56-62, 2010.

[11] W. Hou, X. Wang, J. Chouinard, and A. Refaey, "Physical layer authentication for mobile systems with time-varying carrier frequency offsets," *IEEE Trans. Commun.*, vol. 62, no. 5, pp. 1658-1667, 2014.

[12] X. Duan and X. Wang, "Authentication handover and privacy protection in 5G HetNets using software-defined networking," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 28-35, 2015.

[13] X. Wang, F. J. Liu, D. Fan, H. Tang, and P. C. Mason, "Continuous physical layer authentication using a novel adaptive OFDM system," in *Proc. IEEE International Conference on Communications (ICC)*, 2011.

[14] H.-M. Wang, T.-X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1204-1219, 2016.

[15] D. Wang, B. Bai, W. Chen, and Z. Han, "Secure green communication via untrusted two-way relaying: a physical layer approach," *IEEE Trans. Commun.*, vol. 64, no. 5, pp. 1861-1874, 2016.

[16] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile Adhoc networks: a survey," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 2, pp. 279-295, 2012.

[17] Y. L. Sun, W. Yu, Z. Han, and K. J. Ray Liu, "Information theoretic framework of trust modeling and evaluation for Ad Hoc networks," *IEEE J. Sel. Areas Commn.*, vol. 24, no. 2, pp. 305-316, 2006.

[18] Z. Movahedi, Z. Hosseini, F. Bayan, and G. Pujolle, "Trust-distortion resistant trust management frameworks on mobile Ad Hoc networks: a survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1287-1309, 2016.

[19] X. Fan, L. Liu, M. Li, and Z. Su, "GroupTrust: dependable trust management," *IEEE Trans. Parallel Distrib.*, vol. 28, no. 4, pp. 1076-1090, 2017.

[20] C. Zhu, J. J. P. C. Rodrigues, V. C. M. Leung, L. Shu, and L. T. Yang, "Trust-based communication for the industrial internet of things," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 16-22, 2018.

[21] P. Zhang, Y. Kong, and M. Zhou, "A domain partition-based trust model for unreliable clouds," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2167-2178, 2018.

[22] H. Fang, L. Xu, and X. Huang, "Self-adaptive trust management based on game theory in fuzzy large-scale networks," *Soft Computing*, vol. 21, no. 4, pp. 907-921, 2017.

[23] M. Zhao, J. Y. Ryu, J. Lee, T. Q. S. Quek, and S. Feng, "Exploiting trust degree for multiple-antenna user cooperation," *IEEE Trans. Wireless Commun.*, vol. 16, no. 8, pp. 4908-4923, 2017.

[24] L. Yao, Y. Man, Z. Huang, J. Deng, and X. Wang, "Secure routing based on social similarity in opportunistic networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 594-605, 2016.

[25] T. C. Silva and L. Zhao, "Machine learning in complex networks," Springer Cham Heidelberg New York Dordrecht London, pp. 71-82, 2016.

[26] H. Yang, Q. Yao, A. Yu, Y. Lee, and J. Zhang, "Resource assignment based on dynamic fuzzy clustering in elastic optical networks with multi-core fibers," *IEEE Trans. Commun.*, vol. 67, no. 5, pp. 3457-3469, 2019.

[27] M. Gharbieh, A. Bader, H. ElSawy, H.-C. Yang, M.-S. Alouini, and A. Adinoyi, "Self-organized scheduling request for uplink 5G networks: A D2D clustering approach," *IEEE Trans. Commun.*, vol. 67, no. 2, pp. 1197-1209, 2019.

[28] O. Ibidunmoye, A.-R. Rezaie, and E. Elmroth, "Adaptive anomaly detection in performance metric streams," *IEEE Trans. Netw. Service Manag.*, vol. 15, no. 1, pp. 217-231, 2018.

[29] R. Laxhammar and G. Falkman, "Online learning and sequential anomaly detection in trajectories," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 36, no. 6, pp. 1158-1173, 2014.

[30] M. Dashevskiy and Z. Luo, "Network traffic demand prediction with confidence," in *Proc. 2008 IEEE Global Telecommunications Conference (GLOBECOM)*, 2008.

[31] A. Lambrou, H. Papadopoulos, and A. Gammerman, "Reliable confidence measures for medical diagnosis with evolutionary algorithms," *IEEE Trans. Inf. Technol. Biomed.*, vol. 15, no. 1, pp. 93-99, 2011.

[32] X. Lu, F. Yin, C. Liu, and M. Huang, "Online spatiotemporal extreme learning machine for complex time-varying distributed parameter systems," *IEEE Trans. Ind. Informat.*, vol. 13, no. 4, pp. 1753-1762, 2017.

[33] S. Scardapane, D. Comminiello, M. Scarpiniti, and A. Uncini, "Online sequential extreme learning machine with kernels," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 26, no. 9, pp. 2214-2220, 2015.

[34] V. Vovk, A. Gammerman, and G. Shafer, "Algorithmic learning in a random world," New York, NS, USA: Springer-Verlag, Inc., 2005.

[35] G. Rhafer and V. Vovk, "A tutorial on conformal prediction," *J. Mach. Learn. Res.*, vol. 9, pp. 371-421, 2008.

[36] J. Zhang, Z. Wang, X. Zheng, L. Guan, and C. Y. Chung, "Locally weighted ridge regression for power system online sensitivity identification considering data collinearity," *IEEE Trans. Power Syst.*, vol. 33, no. 2, pp. 1624-1634, 2018.

[37] S. S. Mullick, S. Datta, and S. Das, "Adaptive learning-based k-nearest neighbor classifiers with resilience to class imbalance," *IEEE Trans. Neural Netw. Learn. Syst.*, doi: 10.1109/TNNLS.2018.2812279, 2018.

[38] E. Isufi, A. Loukas, A. Simonetto, and G. Leus, "Autoregressive moving average graph filtering," *IEEE Trans. Signal Process.*, vol. 65, no. 2, pp. 274-288, 2017.

[39] P. Abouzar, D. G. Michelson, and M. Hamdi, "RSSI-based distributed self-localization for wireless sensor networks used in precision agriculture," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6638-6650, 2016.

He Fang is a Ph.D. candidate at the Department of Electrical and Computer Engineering, Western University, Canada. She received her B.Sc. and Ph.D. degrees in Applied Mathematics from Fujian Normal University, China, in 2012 and 2018, respectively. Her research interests include intelligent security provisioning, machine learning, as well as distributed optimization and collaboration techniques.

One focus of her current research is on the development of new machine-learning enabled authentication schemes through utilization of time-varying wireless environment for security enhancement. She is also working on distributed security management in IoT and blockchain systems under practical network constraints.

Dr. Xianbin Wang (S'98-M'99-SM'06-F'17) is a Professor and Tier 1 Canada Research Chair at Western University, Canada. He received his Ph.D. degree in electrical and computer engineering from National University of Singapore in 2001.

Prior to joining Western, he was with Communications Research Centre Canada (CRC) as a Research Scientist/Senior Research Scientist between July 2002 and Dec. 2007. From Jan. 2001 to July 2002, he was a system designer at STMicroelectronics. His current research interests include 5G and beyond, Internet-of-Things, communications security, machine learning and intelligent communications. Dr. Wang has over 400 peer-reviewed journal and conference papers, in addition to 30 granted and pending patents and several standard contributions.

Dr. Wang is a Fellow of Canadian Academy of Engineering, a Fellow of Engineering Institute of Canada, a Fellow of IEEE and an IEEE Distinguished Lecturer. He has received many awards and recognitions, including Canada Research Chair, CRC Presidents Excellence Award, Canadian Federal Government Public Service Award, Ontario Early Researcher Award and six IEEE Best Paper Awards. He currently serves as an Editor/Associate Editor for IEEE Transactions on Communications, IEEE Transactions on Broadcasting, and IEEE Transactions on Vehicular Technology. He was also an Associate Editor for IEEE Transactions on Wireless Communications between 2007 and 2011, and IEEE Wireless Communications Letters between 2011 and 2016. He was involved in many IEEE conferences including GLOBECOM, ICC, VTC, PIMRC, WCNC and CWIT, in different roles such as symposium chair, tutorial instructor, track chair, session chair and TPC co-chair. Dr. Wang is currently serving as the Chair of ComSoc SPCE Technical Committee and a member of IEEE Fellow Committee.

Lajos Hanzo (http://www-mobile.ecs.soton.ac.uk, https://en.wikipedia.org/wiki/Lajos_Hanzo) FREng, FIEEE, FIET, Fellow of EURASIP, DSc received his degree in electronics in 1976 and his doctorate in 1983. In 2009 he was awarded an honorary doctorate by the Technical University of Budapest and in 2015 by the University of Edinburgh. In 2016 he was admitted to the Hungarian Academy of Science. During his 40-year career in telecommunications he has held various research and academic posts in Hungary, Germany and the UK. Since 1986 he has been with the School of Electronics and Computer Science, University of Southampton, UK, where he holds the chair in telecommunications. He has successfully supervised 119 PhD students, co-authored 18 John Wiley/IEEE Press books on mobile radio communications totalling in excess of 10 000 pages, published 1900+ research contributions at IEEE Xplore, acted both as TPC and General Chair of IEEE conferences, presented keynote lectures and has been awarded a number of distinctions. Currently he is directing an academic research team, working on a range of research projects in the field of wireless multimedia communications sponsored by industry, the Engineering and Physical Sciences Research Council (EPSRC) UK, the European Research Council's Advanced Fellow Grant and the Royal Society's Wolfson Research Merit Award. He is an enthusiastic supporter of industrial and academic liaison and he offers a range of industrial courses. He is also a Governor of the IEEE ComSoc and VTS. During 2008 - 2012 he was the Editor-in-Chief of the IEEE Press and a Chaired Professor also at Tsinghua University, Beijing. For further information on research in progress and associated publications please refer to http://www-mobile.ecs.soton.ac.uk