Learning-Aided Physical Layer Authentication as an Intelligent Process

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

(Invited Paper)

***Abstract*—Performance of the existing physical layer authentication schemes could be severely affected by the imperfect estimates and variations of the communication link attributes used. The commonly adopted static hypothesis testing for physical layer authentication faces significant challenges in time-varying communication channels due to the changing propagation and interference conditions, which are typically unknown at the design stage. To circumvent this impediment, we propose an adaptive physical layer authentication scheme based on machine-learning as an intelligent process to learn and utilize the complex time-varying environment, and hence to improve the reliability and robustness of physical layer authentication. Explicitly, a physical layer attribute fusion model based on a kernel machine is designed for dealing with multiple attributes without requiring the knowledge of their statistical properties. By modeling the physical layer authentication as a linear system, the proposed technique directly reduces the authentication scope from a combined N-dimensional feature space to a single-dimensional (scalar) space, hence leading to reduced authentication complexity. By formulating the learning (training) objective of the physical layer authentication as a convex problem, an adaptive algorithm based on kernel least-mean-square is then proposed as an intelligent process to learn and track the variations of multiple attributes, and therefore to enhance the authentication performance. Both the convergence and the authentication performance of the proposed intelligent authentication process are theoretically analyzed. Our simulations demonstrate that our solution significantly improves the authentication performance in time-varying environments.**

***Index Terms*—Intelligent Authentication, Multiple Physical Layer Attributes, Kernel Machine, Adaptive Algorithm**

I. Introduction

DUE to the *open broadcast nature* of radio signal propagation, as well as owing to using *standardized transmission schemes* and *intermittent communications*, wireless communication systems are extremely vulnerable to interception and spoofing attacks. First of all, the open broadcast nature of wireless medium facilitates the reception of radio signals by any illegitimate receiver within the coverage of the transmitter [1]. Secondly, the standardized transmission and conventional security schemes of wireless networks make interception and eavesdropping fairly straightforward [2], [3]. Moreover, the "on-off" and sporadic transmissions of low cost wireless devices, especially the significantly growing number of Internet-of-Things (IoT) devices, provide abundant opportunities to adversaries for spoofing attacks. Therefore, the enhancement of authentication schemes is of paramount importance for wireless communication systems, especially in the light of the ongoing convergence between the wireless infrastructure and vertical industrial applications enabled by IoT.

A. Comparison of Conventional and Physical Authentication Techniques

Although digital key-based cryptographic techniques [4]–[6] have been widely used both for communication security and authentication, they may fall short of the desired performance in many emerging scenarios. One fundamental weakness of the digital credentials based on conventional cryptography is that detecting compromised security keys cannot be readily achieved, since the inherent physical attributes of communication devices and users are disregarded [1]. Given the rapidly growing computational capability of low-cost devices, it is becoming more and more feasible to crack the security key from the intercepted signals of standardized and static security protocols. Furthermore, conventional cryptographic techniques also require appropriate key management procedures to generate, distribute, refresh and revoke digital security keys, which may result in excessive latencies in large-scale networks. Indeed, this latency may become intolerable for delay-sensitive communications, such as networked control and vehicular communications. The computational overhead of digital key-based cryptographic methods is also particularly undesirable for devices, which have limited battery lifetime and computational capability, such as IoT sensors.

To overcome these challenges, an alternative approach of authenticating a user (transmitter) is to exploit the physical layer attributes of communication links. Such analog-domain attributes are inherently related to the unique imperfection of communicating devices and to the corresponding environment, which are hard to impersonate and predict. These physical layer attributes include the channel impulse response (CIR) [7], received signal strength indicator (RSSI) [8], carrier frequency offset (CFO) [9]–[11], in-phase-quadrature-phase imbalance

The work of H. Fang and X. Wang was supported by Natural Sciences and Engineering Research Council of Canada under Discovery Grant RGPIN-2018-06254, CREATE Program in Communications Security, Privacy and Cyberethics (grant number 432280-2013), and Department of National Defence under grant DGDND-2018-00018. The work of L. Hanzo was supported by EPSRC projects EP/Noo4558/1, EP/PO34284/1 as well as of the European Research Council's Advanced Fellow Grant QuantCom. (Corresponding author: Xianbin Wang)

H. Fang and X. Wang are with the Department of Electrical and Computer Engineering, The University of Western Ontario, London, ON N6A 5B9, Canada. Email: 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.

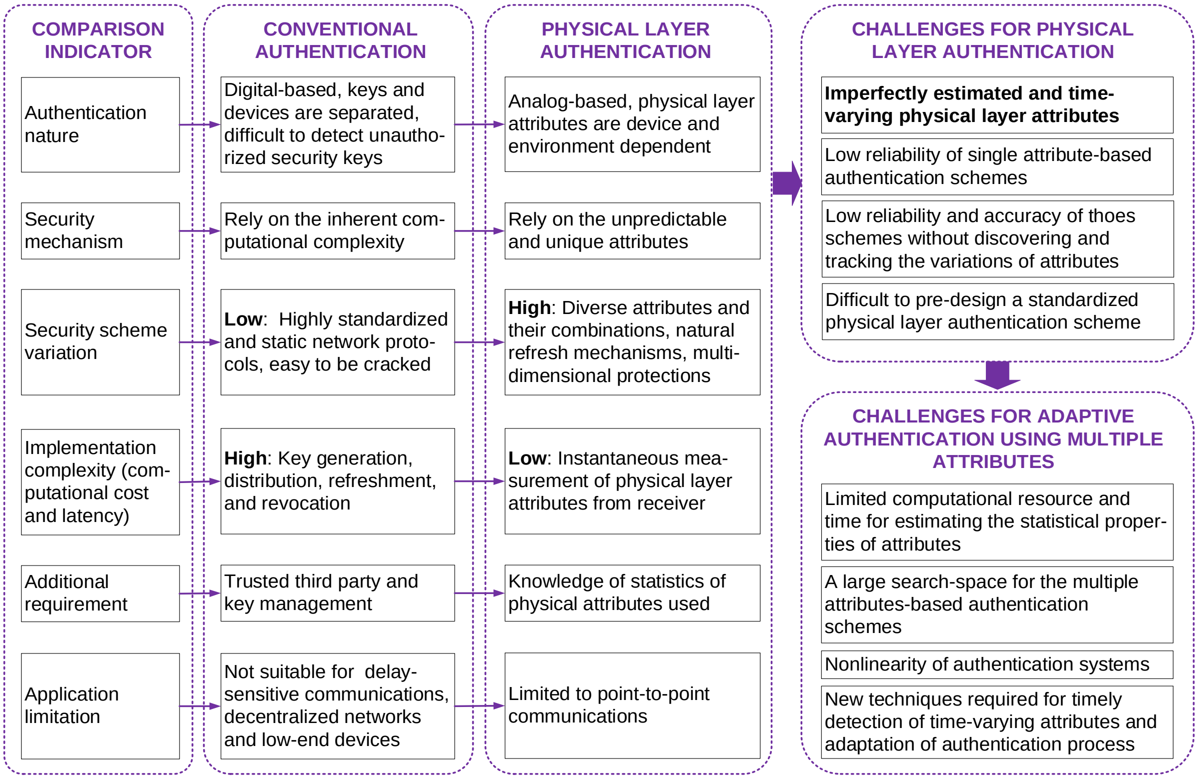
COMPARISON INDICATOR
Authentication nature
Security mechanism
Security scheme variation
Implementation complexity (computational cost and latency)
Additional requirement
Application limitation
CONVENTIONAL AUTHENTICATION
Digital-based, keys and devices are separated, difficult to detect unauthorized security keys
Rely on the inherent computational complexity
Low: Highly standardized and static network protocols, easy to be cracked
High: Key generation, distribution, refreshment, and revocation
Trusted third party and key management
Not suitable for delay-sensitive communications, decentralized networks and low-end devices
PHYSICAL LAYER AUTHENTICATION
Analog-based, physical layer attributes are device and environment dependent
Rely on the unpredictable and unique attributes
High: Diverse attributes and their combinations, natural refresh mechanisms, multi-dimensional protections
Low: Instantaneous measurement of physical layer attributes from receiver
Knowledge of statistics of physical attributes used
Limited to point-to-point communications
CHALLENGES FOR PHYSICAL LAYER AUTHENTICATION
Imperfectly estimated and time-varying physical layer attributes
Low reliability of single attribute-based authentication schemes
Low reliability and accuracy of thoes schemes without discovering and tracking the variations of attributes
Difficult to pre-design a standardized physical layer authentication scheme
CHALLENGES FOR ADAPTIVE AUTHENTICATION USING MULTIPLE ATTRIBUTES
Limited computational resource and time for estimating the statistical properties of attributes
A large search-space for the multiple attributes-based authentication schemes
Nonlinearity of authentication systems
New techniques required for timely detection of time-varying attributes and adaptation of authentication process

Fig. 1. Comparison of conventional and physical authentication techniques.

(IQI) [11], and so on, which can also be used to generate more unique combinations for authentication. These diverse physical layer attributes and their combinations provide new mechanisms in a multi-dimensional domain for the enhancement of physical layer authentication. Given its obvious advantages including low computational requirement, low network overhead and modest energy consumption, physical layer authentication has been widely studied [12]–[25]. A detailed comparison of conventional and physical authentication techniques is given in Fig. 1.

B. Challenges for Physical Layer Authentication

Despite its many advantages, physical layer authentication also faces several major challenges imposed by the hitherto less well-explored security mechanisms and owing to the analog nature of the link attributes used, as seen in Fig. 1.

Imperfect estimates and *variations* of the physical layer attributes are inevitable in practical wireless networks. These constitute challenges for the physical layer authentication, but beneficially, they provide unique distinguishing features. Having said that, their adequate estimation often imposes challenges on physical layer authentication, mainly due to time-varying channels, dynamic interference conditions, mobility of devices, non-symmetrical observations at the transmitter and receiver, as well as owing to the measurement errors, just to name a few.

To elaborate a little further on the challenges, performance of the single-attribute-based physical layer authentication schemes [12]–[22] remains limited by the imperfect estimates of the specific attribute used. Moreover, the limited range of the specific attribute distribution may not be sufficiently wide-spread for differentiating the devices all the time. These estimations lead to low-reliability and low-robustness of physical layer authentication in conjunction with only a single attribute, especially in a hostile time-varying wireless communication environment.

Hence, multiple physical layer attributes may be taken into account for improving the authentication performance [23], [24], since it is more difficult for an adversary to succeed in predicting or imitating all the attributes based on the received signal. On the other hand, when the environment is time-variant, the performance of physical layer authentication could be severely affected by the unpredicable variations of attributes due to the potential decorrelation of the physical layer attributes observed at different time instants. Although the variations of attributes provide additional scope for improving the security mechanisms by increasing the uncertainty for the adversaries, at the same time also for the legitimate users operating without discovering and tracking the variations of physical layer attributes.

In a nutshell, the main challenge is that a multiple varying attributes-based authentication scheme is capable of achieving high security in the presence of adversaries, but this increases the grade of challenge imposed on the legitimate users as well. More importantly, variations of the physical layer attributes are typically unknown at the design stage and they are hard to predict, thus it is very difficult to pre-design a static physical layer authentication scheme. Hence the conception of an adaptive physical layer authentication scheme is extremely helpful for improving the performance of physical layer authentication, which can promptly adapt to the time-varying environment. However, designing near-instantaneously adaptive physical layer authentication based on multiple attributes in rapidly time-varying environments is challenging due to the following reasons:

- **C1**. Both the computational resources and the time available for estimating the statistical properties of the physical layer attributes are limited;
- **C2**. New authentication schemes based on multiple attributes result in a large search-space, which may lead to both excessive complexity and to non-convex search as well as optimization problems;
- **C3**. In practical wireless communication, the typical authentication schemes rely on nonlinear techniques, as exemplified by the binary hypothesis tests of [12]–[14] and by the generalized likelihood ratio test of [26];
- **C4**. Timely detection of time-varying physical layer attributes and the adaptation of the physical layer authentication process require sophisticated near-instantaneously adaptive processing techniques.

In order to overcome these difficulties, the kernel-based machine learning technique of [27]–[30] is applied for modeling the authentication problem in this paper, which is a non-parametric learning method. Although the family of parametric learning methods has become mature in the literature [31]–[37], as exemplified by the linear regression methods of [31] and the polynomial regression methods of [32], [33], they usually rely on the assumption of knowing the distribution of samples (i.e. the estimates of physical layer attributes) together with the specific form of the training function (e.g. linear function or polynomial function). When the assumptions related to the samples' distribution are correct, the parametric methods are usually more accurate than the non-parametric methods. However, once the assumptions concerning the samples' distribution models become inaccurate, they have a greater chance of failing. This dramatically limits the employment of parametric learning methods in practical dynamic wireless environments when they face challenge **C1**, since computing accurate distributions for multiple physical layer attributes in a complex time-varying environment becomes time-consuming.

The authors of [36] proposed a logistic regression technique based authentication scheme assisted by multiple landmarks at different locations that use multiple antennas to estimate the RSSI of the transmitter for enhanced authentication performance. All the radio nodes are assumed to be static in [36] and the training data for logistic regression are the signals received from different transmitters and gleaned from the corresponding media access control address in similar scenarios. In contrast to the scheme of [36], we study physical layer authentication relying on multiple time-varying attributes without the assistance of any extra device. More importantly, we focus our attention on modelling the uninterrupted authentication between a transmitter and its receiver as an intelligent process without requiring any known system model and without a pre-designed authentication scheme based on our real-time learning technique operating in a time-varying environment.

In contrast to parametric learning methods, the non-parametric methods are not specified *a priori*, but are determined from the data available. Hence, the non-parametric methods are more suitable for tracking dynamically time-varying environments without requiring any assumptions concerning the attributes' statistical distributions. Some examples are constituted by the classic k-nearest neighbors [38] and the decision tree based solutions [39]. However, these two non-parametric methods have a limited ability to deal with challenges **C2-C4**. To be specific, it is not easy to determine the most appropriate k-distance in the k-nearest neighbors method. In the decision tree method, the perturbation of collected data (e.g. by noise) will result in quite a different decision tree, thus leading to inaccurate authentication results.

The authors of [40] proposed a physical layer authentication scheme based on the extreme learning machine concept for improving the spoofing detection accuracy. However, its efficiency critically depends more on the training data set available. Besides, this scheme assumes that all the multiple physical layer attributes obey the same statistical distribution functions, such as the Gaussian distributions, thus their success remains limited in the complex high-dynamic environment considered in this paper. Furthermore, a few other machine learning techniques are introduced for authentication in [41], such as Q-learning and neural network-based techniques, as well as some well-studied fusion methods, as exemplified by the Kalman filter of [21], fuzzy logic of [42], and Bayesian inference techniques of [40]. However, these methods may be limited in dealing with the challenges **C1-C4**. To be specific, the authors of [41] studied the test threshold of authentication based on the Q-learning technique instead of the variations of physical layer attributes in the time-varying environment encountered. The neural network based method of [41] may improve the model accuracy by increasing the number of layers and neurons used, but at the cost of a higher complexity, which hence may not be suitable for near-instantaneous authentication. Moreover, the Kalman filter aided method of [21] is also model-based, relying on the assumption of having Gaussian distributed process noise, the fuzzy logic method of [42] requires tuning of the membership function, and the Bayesian inference method of [40] also requires a statistical model of the observed data, which hence have limited abilities to deal with challenge **C1**.

To overcome these challenges, a promising alternative approach of modeling the authentication process is to track multiple physical layer attributes based on the kernel machine learning. As a benefit, the kernel machine of [27]–[30] is capable of reducing the dimensionality of the authentication problem based on multiple attributes. It models the authentication problem as a linear system without requiring the knowledge of the attributes' statistical properties. More importantly, the variations of attributes as well as of the environment may be tracked (learnt) by the kernel machine learning. All these compelling benefits motivate us to propose a novel authentication scheme based on the kernel machine learning technique as an intelligent process in the face of time-varying wireless communication scenarios to achieve reliable authentication through discovering the complex dynamic environment encountered and through tracking the variations of multiple physical layer attributes.

C. Contributions

In this paper, we develop an adaptive authentication scheme based on an intelligent machine learning-aided process for discovering the associated time-varying environment, and thus for improving the physical layer authentication performance. Firstly, a multiple physical layer attribute fusion model based on the classic kernel machine is designed for modeling the authentication problem without requiring the knowledge of those attributes' statistical properties, which corresponds to **C1** of Section I-B. As for **C2** and **C3**, we cast the authentication problem from a high-dimensional search space to a single-dimensional space by using the classic Gaussian kernel, hence the resultant physical layer authentication can be considered as a linear system. Then an adaptive algorithm is proposed for tracking the variations of the physical layer attributes to achieve a reliable authentication performance, which is a solution for **C4** of Section I-B.

Specifically, the contributions of this paper are summarized as follows:

1) We design a kernel machine-based model for determining the authentication attributes without requiring the knowledge of their statistical properties, and cast the authentication system from a high-dimensional space to a single-dimensional space. Then the resultant physical layer authentication process can be considered as a linear system, which is easier to train based on the estimates of the physical layer attributes and on the authentication results observed. As a result of this transformation, the complexity of our multiple physical layer attribute fusion model can be dramatically reduced, despite considering a high number of physical layer attributes;

2) The learning (training) objective of the physical layer authentication based on kernel machine may be formulated as a convex problem. We then propose an intelligent authentication process based on kernel least-mean-square for tracking the variations of the physical layer attributes to achieve a reliable authentication performance. By deriving the learning rules for both the system parameters and for the authentication system, the proposed intelligent authentication process becomes capable of adapting to time-varying environments. Therefore, a timely detection of the physical layer attributes and the adjustment of the authentication process can be achieved;

3) Our numerical performance and simulations results demonstrate that a larger number of physical layer attributes leads to a more pronounced authentication performance improvement without unduly degrading the convergence and training performance. We also demonstrate the superiority of our authentication process over its non-adaptive benchmarker.

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 design a multiple physical layer attribute fusion model based on the kernel machine. An adaptive authentication algorithm is proposed in Section IV. Both the convergence analysis and our authentication performance analysis are presented in Section IV. The simulation results are discussed in Section V. Finally, Section VI concludes the paper.

II. SYSTEM MODEL

As shown in Fig. 2, we consider a wireless network, where Alice and Bob communicate with each other in the presence of an eavesdropper, explicitly, Eve, who intends to intercept and impersonate Alice, and then to send spoofing signals to obtain illegal advantages. Bob's main objective is to uniquely and unambiguously identify the transmitter by physical layer authentication. The basic physical layer authentication aims for supporting this pair of legitimate devices by a reciprocal wireless link, while the device-dependent features can be used as a unique security signature.

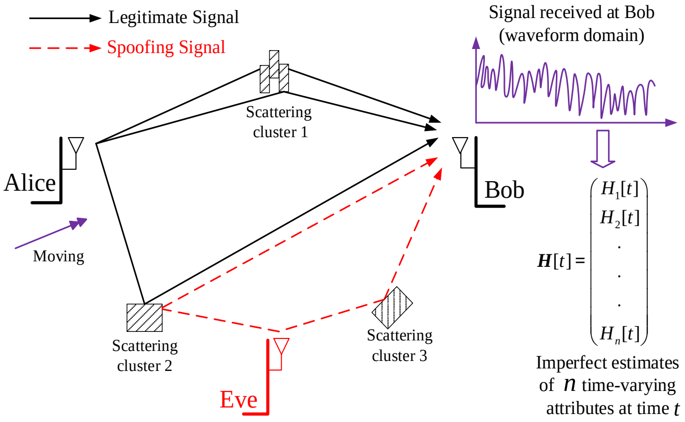
Legitimate Signal
Spoofing Signal
Signal received at Bob (waveform domain)
Scattering cluster 1
Alice
Bob
Moving
$H[t] = \begin{pmatrix} H_1[t] \\ H_2[t] \\ \cdot \\ \cdot \\ \cdot \\ H_n[t] \end{pmatrix}$
Scattering cluster 2
Scattering cluster 3
Eve
Imperfect estimates of n time-varying attributes at time t

Fig. 2. Adversarial system in a wireless network. The transmissions between two legitimate devices (i.e. Alice and Bob) suffer from the spoofing attacks from an attacker, i.e. Eve. Bob should identify the transmitter by using multiple time-varying and imperfectly estimated physical layer attributes.

Again, a combination of multiple attributes can be used for improving the authentication performance, since it is more difficult for Eve to simultaneously infer multiple attributes of a large search-space from a received signal. Naturally, the various combinations of physical layer attributes provide a high grade of uncertainty for the adversaries and simultaneously improve multi-dimensional protection for the legitimate users. Let us denote the number of physical layer attributes used for authentication by N and the estimates of multiple physical layer attributes by $\boldsymbol{H} = (H_1, H_2, ..., H_N)^{\mathrm{T}}$, where T represents the transposition of a vector. Again, these physical layer attributes may include the channel state information (CSI), carrier frequency offset (CFO), received signal strength indicator (RSSI), round-trip time (RTT), in-phase-quadrature-phase imbalance (IQI), and so on. These unique channel and device features offer security guarantee by physical layer authentication.

Let us continue by stipulating a few important assumptions for the authentication scenario considered in this paper, as follows:

Assumption 1. The physical signals transmitted between a pair of legitimate devices rapidly become decorrelated in space, time and frequency. This implies that it is hard for the attacker to observe and predict the channel state between legitimate devices, if the attacker is at a third location, which is further than a wavelength away from Alice and Bob;

Assumption 2. Both the wireless channels and the interference are time-varying, the devices are moving, and hence the wireless environment is dynamically changing. These all lead to unpredictable variations of the physical layer attributes;

Assumption 3. The estimates of the physical layer attributes are imperfect, because the legitimate devices roaming in different locations also suffer from different interferences, a dynamic propagation environment, different estimation errors, and so on.

These assumptions characterize a practical scenario, but naturally, it is more difficult for us to deal with these imperfectly estimated time-varying physical layer attributes.

The physical layer authentication comprises two phases, as described below.

Phase I: Alice broadcasts one or more messages to Bob at time t. From the received signal, Bob infers an imperfect estimate of the multiple attributes

$$\boldsymbol{H}_A^I[t] = (H_{A1}^I[t], H_{A2}^I[t], ..., H_{AN}^I[t])^{\mathrm{T}}, \tag{1}$$

which are associated with Alice. At the same time, Eve overhears the transmission.

Phase II: either Alice or Eve transmits a message to Bob at time $t+\tau$. Then Bob obtains another imperfect estimate

$$\boldsymbol{H}^{II}[t+\tau] = (H_1^{II}[t+\tau], H_2^{II}[t+\tau], ..., H_N^{II}[t+\tau])^{\mathrm{T}}, \tag{2}$$

where τ represents the time interval between the two phases.

Bob should compare the estimate $\boldsymbol{H}^{II}[t+\tau]$ to the previous estimate $\boldsymbol{H}_A^I[t]$. If these two estimates are likely to be originated from the same channel realization and the same imperfect hardware, then the message at time $t+\tau$ is deemed to be coming from Alice.

Remark 1. As we mentioned in the assumptions, the physical layer attributes are time-variant and imperfectly estimated. The objective of this paper is to propose an intelligent authentication process relying on these physical layer attributes. The process proposed aims for achieving reliable and robust authentication through discovering and learning the complex operating environment, in the face of limited computational resources (see **C1**); our new authentication schemes based on multiple attributes result in a higher-dimensional search space (**C2**); the authentication schemes usually rely on nonlinear processing (**C3**); the prompt detection of the time-varying physical layer attributes and the ensuing adjustment of the physical layer authentication require new sophisticated adaptive processing techniques (**C4**).

Let us now conceive an intelligent adaptive function $\mathcal{F}(\cdot)$, which is used for fusing N independent physical layer attributes. Then the authentication process can be formulated relying on a threshold $\nu > 0$ as

$$\begin{cases} \Phi_0: & |\mathcal{F}(\boldsymbol{H}_A^I - \boldsymbol{H}^{II})| \leq \nu; \\ \Phi_1: & |\mathcal{F}(\boldsymbol{H}_A^I - \boldsymbol{H}^{II})| > \nu, \end{cases} \tag{3}$$

where Φ_0 indicates that the signal is from Alice, while Φ_1 indicates that it is from Eve. Due to the variations and imperfect estimates of the physical layer attributes between Alice and Bob, we may encounter both false alarms and misdetections. Therefore, the parameters in $\mathcal{F}(\cdot)$ should be promptly updated to achieve low false alarm rate and misdetection rate in a time-varying environment.

III. KERNEL MACHINE-BASED MULTIPLE PHYSICAL LAYER ATTRIBUTE FUSION

In order to improve the performance of the authentication schemes in time-varying environments using multiple physical layer attributes, which are *imperfectly estimated* and *time-varying*, we propose a kernel machine-based model for fusing multiple physical layer attributes without requiring the knowledge of their statical properties in the spirit of **C1** of Section I-B. Then, the dimension of the search-space is reduced from N to 1 with the aid of our kernel machine-based physical layer attribute fusion model and our authentication problem can be modeled by a linear system as detailed in this section (corresponding to **C2** and **C3** of Section I-B). Therefore, the complexity of our multiple physical layer attribute fusion model can be dramatically reduced, as well as the trade-off between the authentication false alarm and misdetection can be improved by utilizing multiple attributes.

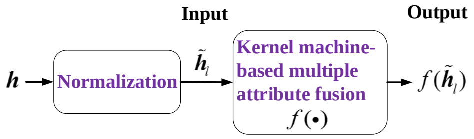
Input
Output
$\boldsymbol{h}$
Normalization
$\tilde{\boldsymbol{h}}_l$
Kernel machine-based multiple attribute fusion
$f(\bullet)$
$f(\tilde{\boldsymbol{h}}_l)$

Fig. 3. Kernel machine-based multiple physical layer attribute fusion.

In the kernel machine-based multiple attribute fusion, Bob will obtain an estimate $\boldsymbol{H}^{II}[t+\tau]$ of (2) at time $t+\tau$. Then, Bob will compare the estimate $\boldsymbol{H}^{II}[t+\tau]$ to the previous estimate at time t, namely for $\boldsymbol{H}_A^I[t]$ of (1). The difference between these two estimates is denoted as $\boldsymbol{h} = (h_1, h_2, ..., h_N)^{\mathrm{T}}$, where each $h_n \in [a_n, b_n]$ is formulated as

$$h_n = H_{An}^I[t] - H_n^{II}[t+\tau], \; n = 1, 2, ..., N, \tag{4}$$

with N being the number of physical layer attributes used.

Since the different attributes exhibit quite different ranges and have different units, the normalization (see Fig. 3) is required for scaling the attributes having different ranges to the same range for the ease of analysis and for the design of the kernel machine-based fusion. In the following, we normalize the attributes having ranges $[a_n, b_n], n = 1, 2, ..., N$, to $[-1, 1]$ by invoking

$$\widetilde{h}_n = \frac{2}{b_n - a_n}(h_n - \frac{a_n + b_n}{2}), \; n = 1, 2, ..., N. \tag{5}$$

It can be observed from (4) and (5) that these two equations are only used for normalizing the estimates of the attributes to the range of $[-1, 1]$, so that the rather diverse multiple physical layer attributes can be processed in the same range. In practical systems, we only have to know the approximate variation ranges of the attributes, which is reasonable because we can always have *a priori* knowledge about the communication systems and environments before designing the authentication system. For example, the CFO variation range was measured to be $[-78.125, 78.125)$ kHz according to [21], while the RSSI range depends on the pathloss [36].

Let us assume that a set of observations $(\widetilde{\boldsymbol{h}}_l, \widehat{y}_l)_{l=1}^L \in [-1, 1]^N \times \{0, 1\}$ is given, which is used for training the authentication process, where $\widetilde{\boldsymbol{h}}_l = (\widetilde{h}_{1l}, \widetilde{h}_{2l}, ..., \widetilde{h}_{Nl})^{\mathrm{T}}$ is the

lth estimate after the normalization, with each element $\widetilde{h}_{nl}$ defined in (5), and

$$\widehat{y}_l = \begin{cases} 1 & \Phi_0 \\ 0 & \Phi_1 \end{cases}. \quad (6)$$

As shown in Fig. 3, the normalized estimates $\widetilde{\boldsymbol{h}}_l, l = 1, 2, ..., L$, are considered as the inputs of the kernel machine, and $f(\widetilde{\boldsymbol{h}}_l)$ represent the outputs of the kernel machine with the corresponding inputs given by $\widetilde{\boldsymbol{h}}_l \in [-1, 1]^N, l = 1, 2, ..., L$. Note that for the legitimate users, the training data of a legitimate communication session is relatively straightforward to obtain.

Our task is then to infer the underlying mapping function $\widehat{y}_l = f(\widetilde{\boldsymbol{h}}_l)$ from the training data set (the samples) received $(\widetilde{\boldsymbol{h}}_l, \widehat{y}_l)_{l=1}^{L} \in [-1, 1]^N \times \{0, 1\}$. In other words, the task in this section is to represent the authentication system $\widehat{y}_l = f(\widetilde{\boldsymbol{h}}_l)$, and to model the relationship between the estimates of multiple attributes and the corresponding authentication results. After this, we can verify whether a transmitter is that of Alice or of Eve once a new normalized estimate $\overline{\boldsymbol{h}} = (\overline{h}_1, \overline{h}_2, ..., \overline{h}_N)^{\mathrm{T}}$ has been obtained. For example, in a continuous authentication session as defined in [22], once the transmitter accesses the system again or sends the messages to Bob continuously, Bob can infer the estimates of this transmitter's physical attributes, and then determine its normalized estimate through (5). This normalized estimate may be different from the previous normalized estimates $\widetilde{\boldsymbol{h}}_l, l = 1, 2, ..., L$, because of the time-varying environment or channels, which will be treated as the new normalized estimate of the attributes used. The authentication is then carried out by using the new normalized estimate to improve the security.

The kernel machine projects the N-dimensional input vector $\overline{\boldsymbol{h}} \in [-1, 1]^N$ into a potentially infinite-dimensional feature space $\mathcal{H}$ through a mapping $\varphi : [-1, 1]^N \rightarrow \mathcal{H}$. Note that the transformation from the input space into the feature space is nonlinear, and the dimensionality of the feature space is high enough. Since the linear model defined in feature space $\mathcal{H}$ satisfies the *universal approximation property* of [43], the authentication system can be expressed as

$$f(\overline{\boldsymbol{h}}) = \boldsymbol{w}^{\mathrm{T}} \varphi(\overline{\boldsymbol{h}}), \quad (7)$$

where $\boldsymbol{w}$ is the weight vector in the feature space $\mathcal{H}$.

According to the *Representer Theorem* of [45], [46], the authentication system expression of (7) can be rewritten as

$$f(\overline{\boldsymbol{h}}) = \sum_{l=1}^{L} \alpha_l \kappa(\widetilde{\boldsymbol{h}}_l, \overline{\boldsymbol{h}}), \quad (8)$$

where $\kappa(\widetilde{\boldsymbol{h}}_l, \overline{\boldsymbol{h}})$ is a Mercer kernel [27]. The classic Gaussian kernel function of [27]–[30] is adopted in this paper, which has an excellent modelling capability and is numerically stable. The Gaussian kernel function used in our authentication scheme is given by

$$\kappa(\widetilde{\boldsymbol{h}}_l, \overline{\boldsymbol{h}}) = \exp(\frac{-\|\widetilde{\boldsymbol{h}}_l - \overline{\boldsymbol{h}}\|^2}{2\sigma^2}), \quad (9)$$

where σ is the kernel width and should be chosen by the users. The popular methods of selecting a suitable kernel width include the cross-validation, nearest neighbor, penalizing function and plug-in based methods of [47]. The Gaussian kernel function of (9) characterizes a similarity between the observed inputs $\widetilde{\boldsymbol{h}}_l$ and the new normalized estimate $\overline{\boldsymbol{h}}$.

An important relationship between (7) and (8) is

$$\kappa(\widetilde{\boldsymbol{h}}_l, \overline{\boldsymbol{h}}) = \varphi(\widetilde{\boldsymbol{h}}_l)^{\mathrm{T}} \varphi(\overline{\boldsymbol{h}}). \quad (10)$$

Remark 2. We can observe both from the kernel function of (9) and from the authentication system expression of (8) that the physical layer attributes are fused without any specific knowledge of their statistical properties, which corresponds to **C1** of Section I-B. As for **C2**, the search-space is transformed from being N-dimensional to single-dimensional by our multiple physical layer attribute fusion model.

Remark 3. In practical wireless networks, the authentication systems are usually nonlinear (see **C3** of Section I-B). By contrast, according to the proposed kernel machine-based physical layer attribute fusion model of (8), the authentication system is formulated as a linear system, since the expression of (8) relies on the linear weights $\alpha_l, \ l = 1, 2, ..., L$.

As discussed above, the estimates of the multiple physical layer attributes $\boldsymbol{H}$ are time-variant, which may lead to a low authentication performance without agile adaptation. Therefore, in the next section, we focus our attention on proposing adaptive learning procedures for promptly adjusting the authentication system of (8) and for updating the parameters, i.e. $\alpha_l, \ l = 1, 2, ..., L$, through discovering and learning the complex time-varying environment encountered, which is the solution of **C4** in Section I-B.

IV. Adaptive Authentication as an Intelligent Process

In this section, a learning procedure is proposed for adaptive authentication based on the kernel least-mean-square for promptly updating the parameters. This authentication process is based on learning from the observed samples $(\widetilde{\boldsymbol{h}}_l, \widehat{y}_l)_{l=1}^{L} \in [-1, 1]^N \times \{0, 1\}$. Explicitly, the proposed learning procedure can be viewed as an intelligent process of learning the time-varying environment for updating the system parameters $\alpha_l, \ l = 1, 2, ..., L$, to achieve a reliable and robust authentication.

A. Adaptive Authentication Algorithm

Given the samples $(\widetilde{\boldsymbol{h}}_l, \widehat{y}_l)_{l=1}^{L} \in [-1, 1]^N \times \{0, 1\}$ observed, we transform the N-dimensional input vector $\widetilde{\boldsymbol{h}}_l \in [-1, 1]^N$ into a kernel Hilbert space $\mathcal{H}$ through a mapping $\varphi : [-1, 1]^N \rightarrow \mathcal{H}$ according to (7). Therefore, we obtain a pair of sample sequences $\{\varphi(\widetilde{\boldsymbol{h}}_1), \varphi(\widetilde{\boldsymbol{h}}_2), ...\}$ and $\{\widehat{y}_1, \widehat{y}_2, ...\}$. The weight vector $\boldsymbol{w}$ in (7) at iteration l should be updated for minimizing the cost function as follows

$$\min_{\boldsymbol{w}} \sum_{i=1}^{l} [\widehat{y}_i - \boldsymbol{w}^{\mathrm{T}} \varphi(\widetilde{\boldsymbol{h}}_i)]^2. \quad (11)$$

Remark 4. We can observe from (11) that the learning (training) objective of the adaptive authentication process is formulated as a convex optimization problem.

Then the learning rules conceived for updating the weight vector $\boldsymbol{\alpha}$ and the authentication system of (8) are given by the following proposition:

Proposition 1: The learning rule conceived for updating the weight vector $\boldsymbol{\alpha}[l]$ in our multiple physical layer attribute fusion model at iteration l can be expressed as

$$\boldsymbol{\alpha}[l] = \mu \times (e[1], e[2], ..., e[l])^{\mathrm{T}}, \tag{12}$$

where μ represents a step-size parameter. Furthermore, $e[l]$ is the prediction error computed as the difference between the desired observation of the transmitter and its prediction relying on the authentication system parameters $\boldsymbol{\alpha}[l-1]$, which is expressed as

$$e[l] = \widehat{y}_l - f(\widetilde{\boldsymbol{h}}_l)[l-1], \tag{13}$$

where we have

$$f(\widetilde{\boldsymbol{h}}_l)[l-1] = \sum_{i=1}^{l-1} \alpha_i[l-1]\kappa(\widetilde{\boldsymbol{h}}_i, \widetilde{\boldsymbol{h}}_l). \tag{14}$$

Furthermore, the learning rule conceived for adjusting the authentication system at iteration l is given by

$$f(\overline{\boldsymbol{h}})[l] = f(\overline{\boldsymbol{h}})[l-1] + \mu e[l]\kappa(\widetilde{\boldsymbol{h}}_l, \overline{\boldsymbol{h}}). \tag{15}$$

Proof: See Appendix A.

According to Proposition 1, our intelligent authentication process based on the kernel least-mean-square is summarized at a glance in Algorithm 1.

Algorithm 1 Intelligent authentication process

```
1. Initialization:
    $f[0] = 0$: initial value of authentication system
    $e[0] = 0$: initial value of prediction error
    $\alpha[0] = 0$: initial value of system parameter $\boldsymbol{\alpha}$
    $\mu$: step-size parameter of learning
    $\sigma$: kernel width
    $\widetilde{\boldsymbol{h}}_1$: initial input, i.e. the normalized estimate of physical
        layer attributes
    $\mathcal{C} = \{\widetilde{\boldsymbol{h}}_1\}$: initial set of input
    $\widehat{y}_1$: initial observation of the transmitter with the
        corresponding normalized estimate $\widetilde{\boldsymbol{h}}_1$
2. Iteration:
    2.1 while samples $(\widetilde{\boldsymbol{h}}_l, \widehat{y}_l)_{l=1}^{L} \in [-1,1]^N \times \{0,1\}$
        available do
    2.2     obtain the output of authentication system $f[l-1]$
            at iteration $l-1$ via (8);
    2.3     calculate the prediction error $e[l]$ via (13);
    2.4     update weight vector $\boldsymbol{\alpha}[l]$ through (12);
    2.5     adjust the authentication system $f[l]$ via (15);
    2.6     update the input set as $\mathcal{C} = \mathcal{C} + \{\widetilde{\boldsymbol{h}}_l\}$;
    2.7     $l = l + 1$;
    2.8 end
```

Remark 5. In conclusion, the search space is transformed from being N-dimensional to single-dimensional (see Remark 2), the authentication is modelled as a linear system (see Remark 3), and the learning (training) objective of the authentication is formulated as a convex problem (see Remark 4). Therefore, the complexity of our physical layer authentication scheme relying on multiple attributes is dramatically reduced. We can also observe from Algorithm 1 that the execution-time is on the order of $O(L)$, which makes Algorithm 1 an attractive solution. In next subsection, we will discuss the selection of the step-size parameter μ, which affects the convergence of our authentication process.

B. Convergence Analysis of the Proposed Authentication Process

The step-size parameter directly affects the convergence of our authentication process, since increasing the step-size of learning will reduce the convergence time but may in fact lead to divergence. Therefore, the step-size parameter μ should be carefully decided.

Theorem 1: The proposed intelligent authentication process (see Algorithm 1) converges to a steady-state value, if the step-size parameter of learning μ satisfies

$$0 < \mu < \frac{L}{\sum_{l=1}^{L} \kappa(\widetilde{\boldsymbol{h}}_l, \widetilde{\boldsymbol{h}}_l)} = 1. \tag{16}$$

Proof. See Appendix B.

Remark 6. Theorem 1 gives the upper bound of the step-size parameter μ in Algorithm 1, so that the proposed intelligent authentication process converges to a steady state.

C. Authentication Performance Analysis

Mathematically, the false alarm rate and the misdetection rate of our intelligent authentication process can be formulated according to (3), respectively, as

$$P_{FA} = P(|\mathcal{F}(\boldsymbol{H}_A^I - \boldsymbol{H}^{II})| > \nu \mid \Phi_0) \tag{17}$$

and

$$P_{MD} = P(|\mathcal{F}(\boldsymbol{H}_A^I - \boldsymbol{H}^{II})| \leq \nu \mid \Phi_1), \tag{18}$$

where $\mathcal{F}$ represents our multiple physical layer attribute fusion model.

According to the proposed authentication system of (8), the false alarm rate and misdetection rate at instant L can be rewritten, respectively, as

$$P_{FA} = P(|\sum_{l=1}^{L-1} \alpha_l \kappa(\widetilde{\boldsymbol{h}}_l, \widetilde{\boldsymbol{h}}_L)| < \nu \mid \Phi_0) \tag{19}$$

and

$$P_{MD} = P(|1 - \sum_{l=1}^{L-1} \alpha_l \kappa(\widetilde{\boldsymbol{h}}_l, \widetilde{\boldsymbol{h}}_L)| \leq \nu \mid \Phi_1), \tag{20}$$

where $\nu \in [0, 1)$.

In the face of the imperfect estimates of time-varying physical layer attributes, we divide them into two parts: the time-varying part $\overline{\boldsymbol{H}}$ that is the real value of physical layer attributes used, and part $\triangle\boldsymbol{H}$ that is the bias of estimated attributes. Then the estimates $\boldsymbol{H}_A^I[l-\tau_l]$ and $\boldsymbol{H}^{II}[l]$ can be written, respectively, as

$$\boldsymbol{H}_A^I[l-\tau_l] = \overline{\boldsymbol{H}}_A^I[l-\tau_l] + \triangle\boldsymbol{H}_A^I[l-\tau_l] \tag{21}$$

and

$$\boldsymbol{H}^{II}[l] = \overline{\boldsymbol{H}}^{II}[l] + \triangle \boldsymbol{H}^{II}[l], \tag{22}$$

where τ_l is the time interval between Phase I and Phase II of the physical layer authentication at iteration $l, l = 1, 2, ..., L$. Furthermore, $\boldsymbol{\upsilon}(\tau_l) = (\upsilon_{1l}, \upsilon_{2l}, ..., \upsilon_{Nl})^{\mathrm{T}}$ represents the variations of part $\overline{\boldsymbol{H}}_A^I$ during the time interval τ_l, which can be expressed as

$$\boldsymbol{\upsilon}(\tau_l) = \overline{\boldsymbol{H}}_A^{II}[l] - \overline{\boldsymbol{H}}_A^{I}[l - \tau_l]. \tag{23}$$

Given the distributions of part $\triangle \boldsymbol{H}$ of the multiple physical layer attributes, we can calculate the false alarm rate and misdetection rate of our scheme as the following theorems. Note that our intelligent authentication process does not need the knowledge of their statistical properties in the training process.

Theorem 2: The false alarm rate expression of our intelligent authentication process at iteration L is given by

$$\begin{aligned} P_{FA} = &F_{Y_1} * F_{Y_2} * \cdots * F_{Y_{L-1}}(\nu) \\ &- F_{Y_1} * F_{Y_2} * \cdots * F_{Y_{L-1}}(-\nu), \end{aligned} \tag{24}$$

where $Y_l = \alpha_l \exp(-\sum_{n=1}^{N} (\widetilde{h}_{nl} - \widetilde{h}_{nL}^{\Phi_0})^2 / 2\sigma^2)$, $l = 1, 2, ..., L-1$, $\widetilde{h}_{nL}^{\Phi_0}$ is shown in (39), F represents the cumulative distribution function, and $*$ represents the convolution.

Proof: See Appendix C.

Theorem 3: The misdetection rate expression of our intelligent authentication process at iteration L is expressed as

$$\begin{aligned} P_{MD} = &F_{Z_1} * F_{Z_2} * \cdots * F_{Z_{L-1}}(\nu + 1) \\ &- F_{Z_1} * F_{Z_2} * \cdots * F_{Z_{L-1}}(1 - \nu), \end{aligned} \tag{25}$$

where $Z_l = \alpha_l \exp(-\sum_{n=1}^{N} (\widetilde{h}_{nl} - \widetilde{h}_{nL}^{\Phi_1})^2 / 2\sigma^2)$, $l = 1, 2, ..., L-1$, and $\widetilde{h}_{nL}^{\Phi_1}$ is shown in (41).

Proof: See Appendix D.

Remark 7. We can observe from Theorem 2 and Theorem 3 that the false alarm rate and misdetection rate of our intelligent authentication process depend on both the number of physical layer attributes N and on the variations of the attributes $\boldsymbol{\upsilon}$. Our intelligent authentication process tracks the variations of the attributes and promptly adjusts the authentication system, so that a compelling false alarm rate vs. misdetection rate trade-off is achieved.

V. Numerical Performance and Simulation Results

In order to evaluate the performance of our intelligent authentication process, we provide both numerical and simulation results in this section. Firstly, we implement our authentication process using some specific physical layer attributes, and characterize the convergence of Algorithm 1. Then its false alarm rate vs. the misdetection rate trade-off is studied. Finally, we demonstrate the superiority of our authentication process over its non-adaptive benchmarker.

First of all, three physical layer attributes, namely the carrier frequency offset (CFO), channel impulse response (CIR), and received signal strength indicator (RSSI) are considered in our simulations to confirm the viability of our intelligent authentication process. Specifically, a communication system having a measurement center frequency of 2.5 GHz, measurement bandwidth of 10 MHz, coherence bandwidth of 0.99, normalized time correlation of 0.99 and sampling time of 50 ms is considered. The transmitted signal is passed through a randomly generated 12-tap multipath fading channel having an exponential power delay profile. We assume that the relative velocity between Alice and Bob is around 20 km/h, and the initial distance between Alice and Bob is 5 m. Then the CFO of an individual transmitter can be approximated as a zero-mean Gaussian variable [21], [48], and the standard deviation of the CFO variation is $\triangle_{\mathrm{CFO}} \approx 2.35 \times 10^{-7}$. The CFO estimation range is $[-78.125, 78.125)$ kHz [21]. Furthermore, according to [26], an autoregressive model of order 1 (AR-1) is used for characterizing the temporal amplitude fluctuation $\mathrm{Amp}_k[t]$ of the kth-tap in our multipath fading channel. Therefore, the variation of CIR can be given as $\upsilon_{\mathrm{CIR}} = \sum_{k=1}^{12} \mathrm{Amp}_k[t] \exp(-j4.99\pi k)$, and the per-tone signal-to-noise ratio (SNR) is in the channel measurements range of $[-12.8, 14.2)$ dB with a median value of 6.4 dB, if the transmit power is 10 mW [26]. Finally, according to [44], the RSSI can be given as $PL[\mathrm{dB}] = 75 + 36.1 \log(\mathrm{d}/10)$, where PL is the path loss, and d represents the direct transmission distance between the transmitter and Bob. The direct transmission distance between the transmitter and Bob is assumed to be in the range of $[0, 100]$ m.

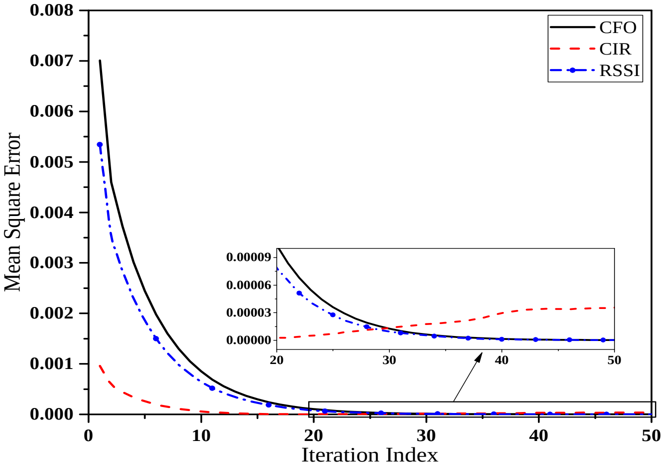

Fig. 4. Training performance of our intelligent authentication process (Algorithm 1) relying on the CFO, CIR and RSSI triplet.

Given 300 samples of the CFO, CIR and RSSI of Alice, i.e. $(\widetilde{\boldsymbol{h}}_l, \widehat{y}_l)_{l=1}^{300} \in [-1, 1]^3 \times \{0, 1\}$, where $\widehat{y}_l = 1$, Fig. 4 shows the training performance of our intelligent authentication process (Algorithm 1) relying on the CFO, CIR and RSSI triplet. The step-size parameter of Algorithm 1 is set to $\mu = 0.1$. We can observe from Fig. 4 that the mean square errors $E[\|e[l]\|^2]$ of all the strategies are significantly reduced, as the iteration index increases from 0 to 50. Furthermore, the mean square error $E[\|e[l]\|^2]$ of each strategy reaches its steady-state value after 30 iterations. We can also observe from Fig. 4 that the CIR estimation performs better than both the CFO and RSSI estimation in the training performance at the beginning, but its training performance becomes the worst after 30 iterations.

The reason for this trend is that the deviation of CIR estimation is lower than that of the CFO and RSSI, while its variation of (23) is the highest.

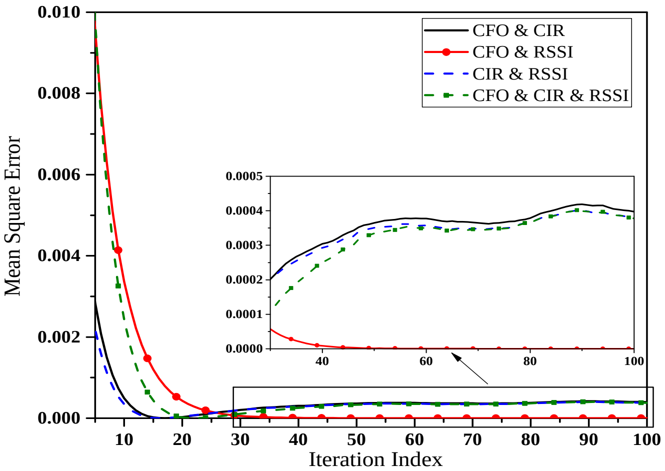

Fig. 5. Training performance of our intelligent authentication process (Algorithm 1) relying on 2 attributes (i.e. CFO & CIR, CFO & RSSI, CIR & RSSI) and 3 attributes (i.e. CFO & CIR & RSSI).

Fig. 5 characterizes the training performance of our intelligent authentication process (see Algorithm 1) relying on multiple attributes. We consider four cases, namely the CFO & CIR, the CFO & RSSI, the CIR & RSSI, and finally the CFO & CIR & RSSI scenarios. We can observe from Fig. 5 that our intelligent authentication process relying on the CFO & RSSI pair has the worst training performance before 30 iterations, while that relying on the CIR & RSSI pair has the lowest mean square error. The reason for this trend is that the mean square error of our intelligent authentication process relying on the CIR is lower than that of the CFO and RSSI before 30 iterations seen in Fig. 4, which adversely affects the training performance in this communication scenario. Additionally, the mean square error of our intelligent authentication process relying on the CFO & RSSI pair is the lowest after 30 iterations, because both the CFO and RSSI are more reliable than the CIR in the authentication process. Furthermore, it is also shown in Fig. 5 that the training performance of our intelligent authentication process relying on the CFO & CIR & RSSI triplet is worse than that of the CFO & RSSI pair after 30 iterations, while it is better than that of the CFO & CIR pair and CIR & RSSI pair. This is because the training performance of our intelligent authentication process depends on both the specific attributes and on the number of physical layer attributes.

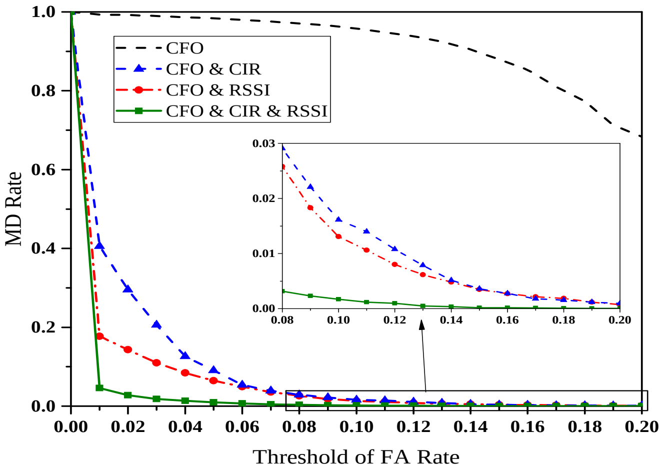

Fig. 6. Authentication performance of our intelligent authentication process relying on the CFO, CFO & CIR, CFO & RSSI, and CFO & CIR & RSSI scenarios. In this case, Eve can intercept and imitate the CFO of Alice.

Fig. 6 considers the case that Eve can intercept and imitate the CFO of Alice, which characterizes the authentication performance of our intelligent authentication process relying on the CFO, CFO & CIR, CFO & RSSI, and finally the CFO & CIR & RSSI scenarios. In other words, Eve intercepts and impersonates the CFO of Alice to obtain unintended advantages from Bob in this case. We can observe from Fig. 6 that our intelligent authentication process relying on the CFO & CIR & RSSI has the best authentication performance, while that only relying on the CFO performs worst. The reason for this trend is that Bob can better identify the transmitter by using CIR and RSSI, although Eve imitates the CFO of Alice in the CFO & CIR & RSSI scenario. On the other hand, Bob suffers from a high misdetection rate in the CFO scenario, since the CFO of Alice is impersonated by Eve. It is also shown in Fig. 6 that there is a small difference between the authentication performance of our intelligent authentication process relying on the CFO & CIR pair and that of the CFO & RSSI pair; and the authentication performances of these two attributes scenarios are better than that of a single-attribute scenario (i.e. CFO). This is because Bob can identify the adversary by using CIR or RSSI in the CFO & CIR or the CFO & RSSI scenarios. Therefore, the increasing number of physical layer attributes is expected to lead to a higher authentication performance in our intelligent authentication process.

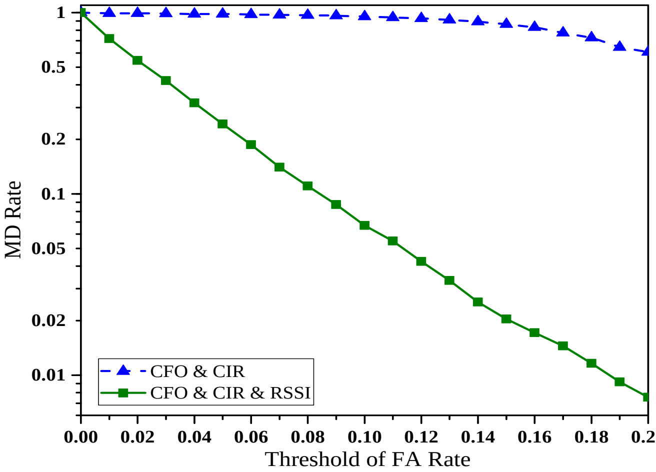

Fig. 7. Authentication performance of our intelligent authentication process relying on the CFO & CIR and CFO & CIR & RSSI scenarios. In this case, Eve can intercept and imitate both the CFO and CIR of Alice.

Fig. 7 considers the scenario when Eve can intercept and impersonate both the CFO and CIR of Alice. It is observed from Fig. 7 that the authentication performance of our intelligent authentication process relying on the CFO & CIR & RSSI triplet is better than that of the CFO & CIR pair. The reason for this trend is that Bob can identify the adversary using the RSSI in the CFO & CIR & RSSI scenario, although Eve imitates both the CFO and CIR of Alice. Both Fig. 6 and Fig. 7 confirm that increasing the number of physical layer attributes leads to a better authentication performance, since it is more difficult for an adversary to succeed in predicting or imitating all the attributes based on the received signal.

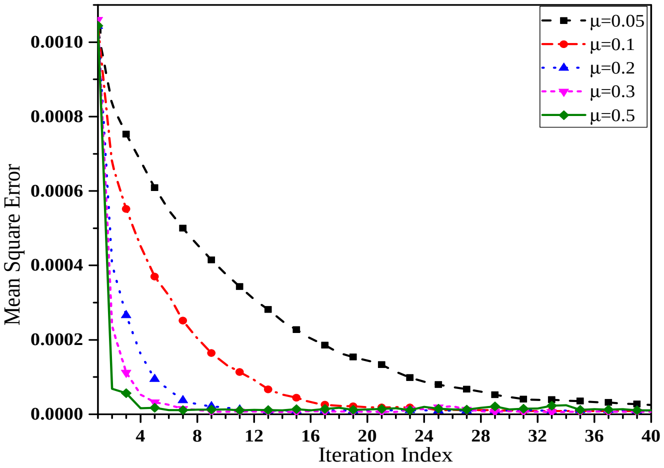

Fig. 8. Training performance comparison results of our intelligent authentication process with different step-sizes, i.e. $\mu = 0.05$, $\mu = 0.1$, $\mu = 0.2$, $\mu = 0.3$, and $\mu = 0.5$.

In Fig. 8, we characterize the training performance of our intelligent authentication process (see Algorithm 1) parameterized by the step-sizes of $\mu = 0.05$, $\mu = 0.1$, $\mu = 0.2$, $\mu = 0.3$, and $\mu = 0.5$. It can be observed from Fig. 8 that our intelligent authentication process reaches its steady-state value in all cases. We can also see from Fig. 8 that our intelligent authentication process having a higher step-size μ converges quicker. In other words, increasing the step-size of learning in a specific range accelerates the convergence. This augments the convergence analysis of Section IV-B.

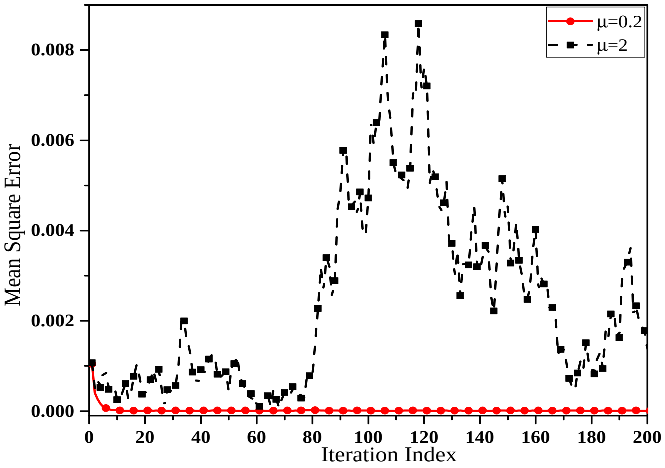

Fig. 9. Convergence and divergence of our intelligent authentication process.

Fig. 9 characterizes the mean square error vs. the iteration index for the step-size parameters of $\mu = 0.2$ and $\mu = 2$. As discussed before, our authentication process associated with $\mu = 0.2$ converges to a steady-state value, while $\mu = 2$ diverges. This is because $\mu = 2$ is out of the range specified in Theorem 1.

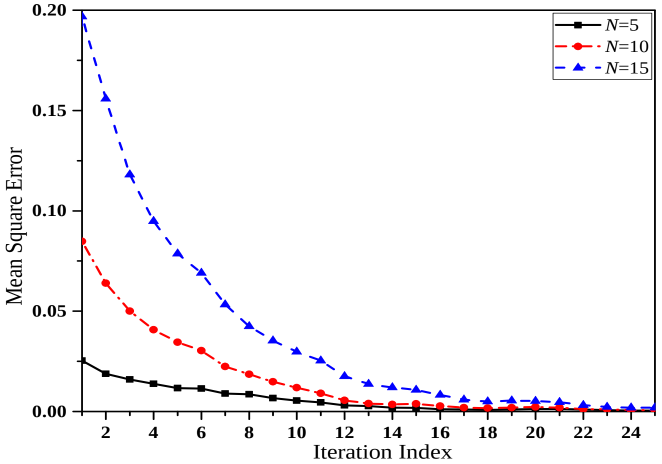

Fig. 10. Training performance comparison results of our intelligent authentication process with different numbers of physical layer attributes, i.e. $N = 5$, $N = 10$ and $N = 15$.

Fig. 10 quantifies the influence of the number of physical layer attributes N on the training performance, which shows the mean square error $E[\|e[l]\|^2]$ vs. the iteration index for different numbers of physical layer attributes, namely for $N = 5$, $N = 10$ and $N = 15$. The step-size parameter is set to $\mu = 0.1$. It can be observed that the mean square error $E[\|e[l]\|^2]$ tends to a steady-state value, as the iteration index increases. Moreover, we can also observe from Fig. 10 that a larger number of attributes only leads to a slightly slower convergence. Therefore, the explosion of computational complexity upon increasing the number of physical layer attributes can be readily avoided by our intelligent authentication process. This validates our analysis provided in Section III, and supported by Remark 2, 3, 4.

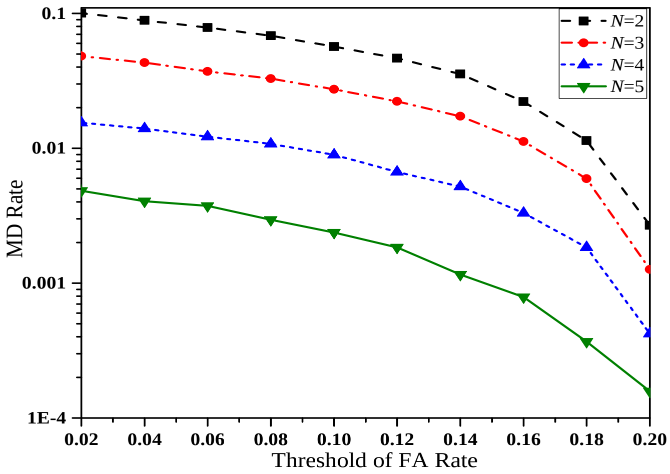

Fig. 11. Authentication performance comparison results of our intelligent authentication process with different numbers of physical layer attributes, i.e. $N = 2$, $N = 3$, $N = 4$ and $N = 5$.

Fig. 11 characterizes the influence of the number of physical layer attributes N on the authentication performance, which quantifies the MD rate vs. the threshold of FA rate for different numbers of physical layer attributes, namely for $N = 2$, $N = 3$, $N = 4$ and $N = 5$. It can be observed that the MD rates are reduced in all cases as the threshold δ of FA rate increases from 0 to 0.2, because there is an inevitable FA-and-MD trade-off. One can also observe from Fig. 11 that a larger number of attributes leads to a more obvious security performance improvement, without substantially degrading the convergence performance (see Fig. 10) of our intelligent authentication process. This trend demonstrates the validity of our authentication performance analysis in Section IV-C. In a nutshell, by using more physical layer attributes, our intelligent authentication process achieves a better authentication performance, indicating the presence of a FA-and-MD trade-off, because we can readily fuse multiple physical layer attributes and control the authentication system to track the variations of multiple attributes. On the same note, the attackers find it more difficult to predict and imitate a larger number of attributes from a received signal.

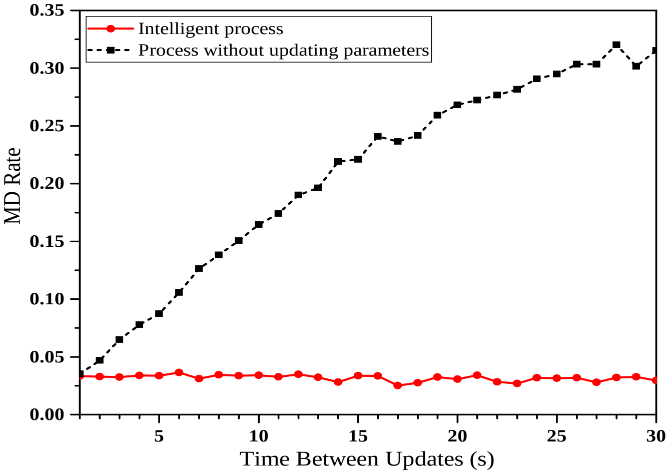

Fig. 12. Comparison results between our intelligent process and the process without updating system parameters relying on CFO & CIR & RSSI.

In Fig. 12, let us now impose the variations on the CFO, CIR and RSSI for comparing our intelligent process and the process operating without updating the system parameters. The threshold of the false alarm rate is 0.02. Then we can observe from Fig. 12 that upon increasing the time between updates, the MD rate of our intelligent process remains robust, tending to around 0.035, while that of the process operating without updating the system parameters increases dramatically from about 0.035 to almost 0.35. This demonstrates that without an adaptive scheme, the authentication performance will be dramatically reduced in time-varying environments. Therefore, our intelligent process performs better than the authentication scheme operating without updating the system parameters.

VI. Conclusions

In this paper, we proposed an intelligent physical layer authentication technique. A kernel machine-based model was proposed for combining the multiple physical layer attributes and for modelling the authentication as a linear system. Through the kernel machine-based multiple attribute fusion model, the number of dimensions of the search-space was reduced from N to 1, and the learning objective was formulated as a convex problem. Therefore, its complexity was substantially reduced. Then, by conceiving an adaptive authentication process relying on the kernel machine-based multiple attribute fusion model, the process advocated readily accommodated a time-varying environment by discovering and learning this complex dynamic environment. Both the convergence performance and the authentication performance of our intelligent authentication process were theoretically analyzed and numerically validated. The simulation results showed that the authentication performance can be dramatically improved by increasing the number of physical layer attributes exploited by our intelligent authentication process without degrading its convergence performance. It was also demonstrated that it has a much better authentication performance in a time-varying environment than its non-adaptive counterpart.

Appendix A
The Proof of Proposition 1

Let

$$J(\boldsymbol{w}) = \sum_{i=1}^{l} [\widehat{y}_i - \boldsymbol{w}^{\mathrm{T}} \varphi(\widetilde{\boldsymbol{h}}_i)]^2. \tag{26}$$

By invoking a step-size parameter μ, the learning rule for the parameter $\boldsymbol{w}$ can be derived by using the gradient. The partial derivative of the function $J(\boldsymbol{w})$ with respect to $\boldsymbol{w} = (w_1, w_2, ..., w_l)^{\mathrm{T}}$ is given by

$$\frac{\partial J(\boldsymbol{w})}{\partial \boldsymbol{w}} = -2 \sum_{i=1}^{l} \varphi(\widetilde{\boldsymbol{h}}_i)[\widehat{y}_i - \boldsymbol{w}^{\mathrm{T}} \varphi(\widetilde{\boldsymbol{h}}_i)], \tag{27}$$

and the instantaneous gradient at iteration l is

$$\frac{\partial J(\boldsymbol{w})}{\partial \boldsymbol{w}}[l] = -\varphi(\widetilde{\boldsymbol{h}}_l)[\widehat{y}_l - \boldsymbol{w}[l-1]^{\mathrm{T}} \varphi(\widetilde{\boldsymbol{h}}_l)]. \tag{28}$$

According to the steepest descent algorithm, we have

$$\boldsymbol{w}[l] = \boldsymbol{w}[l-1] + \mu \varphi(\widetilde{\boldsymbol{h}}_l)[\widehat{y}_l - \boldsymbol{w}[l-1]^{\mathrm{T}} \varphi(\widetilde{\boldsymbol{h}}_l)]. \tag{29}$$

Since $e[l]$ of (13) can also be expressed as

$$e[l] = \widehat{y}_l - \boldsymbol{w}[l-1]^{\mathrm{T}} \varphi(\widetilde{\boldsymbol{h}}_l), \tag{30}$$

the repeated application of (29) through iterations becomes

$$\begin{aligned} \boldsymbol{w}[l] &= \boldsymbol{w}[l-1] + \mu \varphi(\widetilde{\boldsymbol{h}}_l) e[l] \\ &= \boldsymbol{w}[l-2] + \mu \varphi(\widetilde{\boldsymbol{h}}_{l-1}) e[l-1] + \mu \varphi(\widetilde{\boldsymbol{h}}_l) e[l] \\ &= \cdots = \sum_{i=1}^{l} \mu \varphi(\widetilde{\boldsymbol{h}}_i) e[i]; \;\; (\boldsymbol{w}[0] = 0). \end{aligned} \tag{31}$$

According to (7), (8) and (9), we can derive the authentication system as

$$f(\overline{\boldsymbol{h}}) = \sum_{l=1}^{L} \alpha_l \kappa(\widetilde{\boldsymbol{h}}_l, \overline{\boldsymbol{h}}) = \sum_{l=1}^{L} \alpha_l \varphi(\widetilde{\boldsymbol{h}}_l)^{\mathrm{T}} \varphi(\overline{\boldsymbol{h}}) \\ = \boldsymbol{w}[L]^{\mathrm{T}} \varphi(\overline{\boldsymbol{h}}) = \sum_{l=1}^{L} \mu e[l] \varphi(\widetilde{\boldsymbol{h}}_l)^{\mathrm{T}} \varphi(\overline{\boldsymbol{h}}), \tag{32}$$

then we have

$$\alpha_l[l] = \mu e[l]. \tag{33}$$

Therefore, the parameter vector $\boldsymbol{\alpha}$ at iteration l, i.e. $\boldsymbol{\alpha}[l] = (\alpha_1[l], \alpha_2[l], ..., \alpha_l[l])^{\mathrm{T}}$, can be updated through (12).

Then the authentication system at iteration l can be formulated as

$$f(\overline{\boldsymbol{h}})[l] = \sum_{i=1}^{l} \alpha_i \kappa(\widetilde{\boldsymbol{h}}_i, \overline{\boldsymbol{h}}) = \mu \sum_{i=1}^{l} e[i] \kappa(\widetilde{\boldsymbol{h}}_i, \overline{\boldsymbol{h}}) \\ = \mu \sum_{i=1}^{l-1} e[i] \kappa(\widetilde{\boldsymbol{h}}_i, \overline{\boldsymbol{h}}) + \mu e[l] \kappa(\widetilde{\boldsymbol{h}}_l, \overline{\boldsymbol{h}}) \\ = f(\overline{\boldsymbol{h}})[l-1] + \mu e[l] \kappa(\widetilde{\boldsymbol{h}}_l, \overline{\boldsymbol{h}}). \tag{34}$$

Therefore, learning rule for adjusting the authentication system of (8) is expressed as (15). □

Appendix B
The proof of Theorem 1

A practical convergence criterion is the convergence in the mean square error sense, which is formulated as

$$E[\|e[l]\|^2] \rightarrow \text{constant}, \text{as } l \rightarrow \infty, \tag{35}$$

where $E[\cdot]$ represents the expectation of $\cdot$. It was shown in [43], [45] that the least-mean-square criterion based learning is convergent in the mean square, if μ satisfies

$$0 < \mu < \frac{1}{\beta_{max}}, \tag{36}$$

where β_{max} is the largest eigenvalue of the correlation matrix $\boldsymbol{\Theta}[L]$ given by

$$\boldsymbol{\Theta}[L] = [\varphi(\widetilde{\boldsymbol{h}}_1), \varphi(\widetilde{\boldsymbol{h}}_2), ..., \varphi(\widetilde{\boldsymbol{h}}_L)]_{N \times L}. \tag{37}$$

Since $\beta_{max} < \mathrm{tr}(\boldsymbol{\Theta}[L])/L$, where $\mathrm{tr}(\boldsymbol{\Theta}[L])$ is the trace of the matrix $\boldsymbol{\Theta}[L]$, we have

$$0 < \mu < \frac{L}{\mathrm{tr}(\boldsymbol{\Theta}[L])} = \frac{L}{\sum_{l=1}^{L} \kappa(\widetilde{\boldsymbol{h}}_l, \widetilde{\boldsymbol{h}}_l)} = 1. \tag{38}$$

Therefore, the proposed intelligent authentication process (see Algorithm 1) converges to a steady-state value if the step-size parameter of learning μ satisfies (16). □

Appendix C
The proof of Theorem 2

According to (5), (21), (22), and (23), we can calculate $\widetilde{\boldsymbol{h}}_L = (\widetilde{h}_{1L}, \widetilde{h}_{2L}, ..., \widetilde{h}_{NL})^{\mathrm{T}}$ in case of Φ_0 as

$$\widetilde{h}_{nL}^{\Phi_0} = \frac{2}{b_n - a_n} (\upsilon_n(\tau_L) + \triangle H_{An}^{I}[L - \tau_L] - \triangle H_{An}^{II}[L] \\ - \frac{a_n + b_n}{2}), \ n = 1, 2, ..., N, \tag{39}$$

where τ_L is the time interval between Phase I and Phase II of our physical layer authentication at iteration L. Given the distributions of $\triangle H_{An}^{I}$ and $\triangle H_{An}^{II}$ of each physical layer attribute, the probability of density function of $\widetilde{h}_{nL}^{\Phi_0}$ can be obtained. Let $Y_l = \alpha_l \exp(\frac{-\sum_{n=1}^{N} (\widetilde{h}_{nl} - \widetilde{h}_{nL}^{\Phi_0})^2}{2\sigma^2})$, we can calculate the false alarm rate at iteration L as

$$P_{FA} = P(|\sum_{l=1}^{L-1} \alpha_l \exp(\frac{-\sum_{n=1}^{N} (\widetilde{h}_{nl} - \widetilde{h}_{nL}^{\Phi_0})^2}{2\sigma^2})| < \nu) \\ = P(\sum_{l=1}^{L-1} Y_l < \nu) - P(\sum_{l=1}^{L-1} Y_l \leq -\nu) \\ = F_{\sum_{l=1}^{L-1} Y_l}(\nu) - F_{\sum_{l=1}^{L-1} Y_l}(-\nu). \tag{40}$$

Therefore, the false alarm rate expression of our intelligent authentication process at iteration L is shown in (24). □

Appendix D
The proof of Theorem 3

According to (5), (21), and (22), $\widetilde{\boldsymbol{h}}_L = (\widetilde{h}_{1L}, \widetilde{h}_{2L}, ..., \widetilde{h}_{NL})^{\mathrm{T}}$ in case Φ_1 is formulated as

$$\widetilde{h}_{nL}^{\Phi_1} = \frac{2}{b_n - a_n} (\overline{H}_{An}^{I}[L - \tau_L] - \overline{H}_{En}^{II}[L] + \triangle H_{An}^{I}[L - \tau_L] \\ - \triangle H_{En}^{II}[L] - \frac{a_n + b_n}{2}), \ n = 1, 2, ..., N. \tag{41}$$

Given the distributions of $\triangle H_{An}^{I}$ and $\triangle H_{En}^{II}$ of each physical layer attribute, the probability of density function of $\widetilde{h}_{nL}^{\Phi_1}$ can be obtained. Upon letting $Z_l = \alpha_l \exp(\frac{-\sum_{n=1}^{N} (\widetilde{h}_{nl} - \widetilde{h}_{nL}^{\Phi_1})^2}{2\sigma^2})$, the misdetection rate at iteration L yields

$$P_{MD} = P(|1 - \sum_{l=1}^{L-1} \alpha_l \exp(\frac{-\sum_{n=1}^{N} (\widetilde{h}_{nl} - \widetilde{h}_{nL}^{\Phi_1})^2}{2\sigma^2})| \leq \nu) \\ = P(\sum_{l=1}^{L-1} Z_l \leq \nu + 1) - P(\sum_{l=1}^{L-1} Z_l < 1 - \nu) \\ = F_{\sum_{l=1}^{L-1} Z_l}(\nu + 1) - F_{\sum_{l=1}^{L-1} Z_l}(1 - \nu). \tag{42}$$

Therefore, the misdetection rate expression of our intelligent authentication process at iteration L is given by (25). □

References

[1] 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.

[2] 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.

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

[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] M. Rezaee, P. J. Schreie, M. Guillaud, and B. Clerckx, "A unified scheme to achieve the degrees-of-freedom region of the MIMO interference channel with delayed channel state information," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1068-1082, 2016.

[8] H. Lohrasbipeydeh, T. A. Gulliver, and H. Amindavar, "Unknown transmit power RSSD based source localization with sensor position uncertainty," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1784-1797, 2015.

[9] P. Cheng, Z. Chen, F. Hoog, and C. K. Sung, "Sparse blind carrier-frequency offset estimation for OFDMA uplink," *IEEE Trans. Commun.*, vol. 64, no. 12, pp. 5254-5265, 2016.

[10] O. H. Salim, A. A. Nasir, H. Mehrpouyan, and W. Xiang, "Multi-relay communications in the presence of phase noise and carrier frequency offsets," *IEEE Trans. Commun.*, vol. 65, no. 1, pp. 79-94, 2017.

[11] A. A. D'Amico, L. Marchetti, M. Morelli, and M. Moretti, "Frequency estimation in OFDM direct-conversion receivers using a repeated preamble," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1246-1258, 2016.

[12] P. Baracca, N. Laurenti, and S. Tomasin, "Physical layer authentication over MIMO fading wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 11, no. 7, pp. 2564-2573, 2012.

[13] 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.

[14] W. Wang, Z. Sun, S. Piao, B. Zhu, and K. Ren, "Wireless physical-layer identification: modeling and validation," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, pp. 2091-2109, 2016.

[15] A. Ferrante, N. Laurenti, C. Masiero, M. Pavon, and S. Tomasin, "On the error region for channel estimation-based physical layer authentication over Rayleigh fading," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 941-952, 2015.

[16] W. Wang, Y. Chen, and Q. Zhang, "Privacy-preserving location authentication in Wi-Fi networks using fine-grained physical layer signatures," *IEEE Trans. Wireless Commun.*, vol. 15, no. 2, pp. 1218-1225, 2016.

[17] V. Kumar, J. Park, and K. Bian, "PHY-layer authentication using duobinary signaling for spectrum enforcement," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 5, pp. 1027-1038, 2016.

[18] F. Zhu, B. Xiao, J. Liu, and L. Chen, "Efficient physical-layer unknown tag identification in large-scale RFID systems," *IEEE Trans. Commun.*, vol. 65, no. 1, pp. 283-295, 2016.

[19] G. Caparra, M. Centenaro, N. Laurenti, S. Tomasin, and L. Vangelista, "Energy-based anchor node selection for IoT physical layer authentication," *in Proc. IEEE International Conference on Communications (ICC)*, pp. 1-6, 2016.

[20] X. Wu, Z. Yang, C. Ling, and X. Xia, "Artificial-noise-aided physical layer phase challenge-response authentication for practical OFDM transmission," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6611-6625, 2016.

[21] 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.

[22] 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.

[23] 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.

[24] J. Liu and X. Wang, "Physical layer authentication enhancement using two-dimensional channel quantization," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 4171-4182, 2016.

[25] H. Fang, L. Xu, Y. Zou, X. Wang, and K.-K. R. Choo, "Three-stage Stackelberg game for defending against full-duplex active eavesdropping attacks in cooperative communication," *IEEE Trans. Veh. Technol.,* DOI: 10.1109/TVT.2018.2868900, 2018.

[26] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based spoofing detection in frequency-selective Rayleigh channels," *IEEE Trans. Wireless Commun.*, vol. 8, no. 12, pp. 5948-5956, 2009.

[27] W. Liu, J. C. Principe, and S. Haykin, "Kernel adaptive filtering: a comprehensive introduction," John Wiley and Sons, pp. 16-98, 2010.

[28] K. Li and J. C. Principe, "Tranfer learning in adaptive filters: the nearest instance centroid-estimation kernel least-mean-square algorithm," *IEEE Trans. Signal Process.*, vol. 65, no. 24, pp. 6520-6535, 2017.

[29] R. Boloix-Tortosa, J. J. Murillo-Fuentes, I. Santos, and F. Perez-Cruz, "Widely linear complex-valued kernel methods for regression," *IEEE Trans. Signal Process.*, vol. 65, no. 19, pp. 5240-5248, 2017.

[30] B. Chen, L. Xing, B. Xu, H. Zhao, N. Zheng, and J. C. Principe, "Kernel risk-sensitive loss: definition, properties, and application to robust adaptive filtering," *IEEE Trans. Signal Process.*, vol. 65, no. 11, pp. 2888-2901, 2017.

[31] J. Liu, P. C. Cosman, and B. D. Rao, "Robust linear regression via l_0 regularization," *IEEE Trans. Signal Process.*, vol. 66, no. 3, pp. 698-713, 2018.

[32] G. D. Finlayson, M. Mackiewicz, and A. Hurlbert, "Color correction using root-polynomial regression," *IEEE Trans. Image Process.*, vol. 24, no. 5, pp. 1460-1470, 2015.

[33] X. Tan, C. Sun, and T. D. Pham, "Edge-aware filtering with local polynomial approximation and rectangle-based weighting," *IEEE Trans. Cybern.,* vol. 46, no. 12, pp. 2693-2705, 2016.

[34] L. Yang, L. Zhao, G. Bi, and L. Zhang, "SAR ground moving target imaging algorithm based on parametric and dynamic sparse Bayesian learning," *IEEE Trans. Geosci. Remote Sens.,* vol. 54, no. 4, pp. 2254-2267, 2016.

[35] Y. Li, W. Dong, X. Xie, G. Shi, J. Wu, and X. Li, "Image super-resolution with parametric sparse model learning," *IEEE Trans. Image Process.,* DOI: 10.1109/TIP.2018.2837865, 2018.

[36] L. Xiao, X. Wan, and Z. Han, "PHY-layer authentication with multiple landmarks with reduced overhead," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1676-1687, 2017.

[37] X. Shen and Y. Gu, "Nonconvex sparse logistic regression with weakly convex regularization," *IEEE Trans. Signal Process.*, vol. 66, no. 12, pp. 3199-3211, 2018.

[38] S. Wang, Z. Bao, J. S. Culpepper, T. Sellis, and G. Cong, "Reverse k nearest neighbor search over trajectories," *IEEE Trans. Knowledge and Data Eng.*, vol. 30, no. 4, pp. 757-771, 2018.

[39] Y.-C. Cheng and Pi-Chung Wang, "Packet classification using dynamically generated decision trees," *IEEE Trans. Comput.*, vol. 64, no. 2, pp. 582-586, 2015.

[40] N. Wang, T. Jiang, S. Lv, and L. Xiao, "Physical-layer authentication based on extreme learning machine," *IEEE Commun. Letters*, vol. 21, no. 7, pp. 1557-1560, 2017.

[41] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?" *IEEE Signal Processing Mag.*, vol. 35, no. 5, pp. 41-49, 2018.

[42] H. Fang, X. Wang, and L. Xu, "Fuzzy based multi-dimensional adaptive physical layer authentication: a compact and robust approach," *IEEE Trans. Inf. Forensics Security*, under review, 2018.

[43] S. Haykin, "Adaptive filter theory, 4th edition," Upper Saddle River, NJ: Prentice Hall, 2002.

[44] 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.

[45] W. Wang, Y. Liang, E. P. Xing, and L. Shen, "Nonparametric decentralized detection and sparse sensor selection via weighted kernel," *IEEE Trans. Signal Process.*, vol. 64, no. 2, pp. 306-321, 2016.

[46] B. Scholkopf and A. Smola, "Learning with kernels," Cambridge, MA, USA: MIT Press, 2002.

[47] W. Hrdle, "Applied nonparametric regression," Cambridge, UK: Cambridge University Press, 1992.

[48] Y. Shi and M. A. Jensen, "Improved radiometric identification of wireless devices using MIMO transmission," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 4, pp. 1346-1354, 2011.

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-I 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, where he was responsible for the system design of DSL and Gigabit Ethernet chipsets. His current research interests include 5G technologies, Internet-of-Things, communications security, machine learning and locationing technologies. Dr. Wang has over 300 peer-reviewed journal and conference papers, in addition to 29 granted and pending patents and several standard contributions.

Dr. Wang is a Fellow of Canadian Academy of Engineering, 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 and 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. Dr. Wang 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.

Lajos Hanzo (http://www-mobile.ecs.soton.ac.uk) 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 112 PhD students, co-authored 18 John Wiley/IEEE Press books on mobile radio communications totalling in excess of 10 000 pages, published 1792 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 a 60-strong 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