IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 18, 2019, accepted March 17, 2019, date of publication March 21, 2019, date of current version April 5, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2906699

End-to-End Physical Layer Authentication for Dual-Hop Wireless Networks

PINCHANG ZHANG[1,2], JINXIAO ZHU[3], YIN CHEN[4], (Member, IEEE), AND XIAOHONG JIANG[1], (Senior Member, IEEE)

[1]School of Systems Information Science, Future University Hakodate, Hakodate 041-8655, Japan
[2]School of Computer and Information Engineering, Chuzhou University, Chuzhou 239000, China
[3]Faculty of Information Networking for Innovation and Design, Toyo University, Tokyo 115-0053, Japan
[4]Graduate School of Media and Governance, Keio University, Fujisawa 252-8520, Japan

Corresponding author: Yin Chen (yin@ht.sfc.keio.ac.jp)

This work was supported in part by the National Natural Science Foundation of China under Grant 61702068, in part by the Japan Society for the Promotion of Science under Grant JP18H06470, in part by the Anhui NSF Grant under Grant 1808085MF165, in part by the Anhui Province Department of Human Resources and Social Security for the Returned Overseas Chinese Scholars of Chuzhou University Grant under Grant zrjz201700, and in part by the Research Initiation Fund Project of Chuzhou University Grant under Grant 2014qd013.

ABSTRACT End-to-end (E2E) physical layer authentication for multi-hop wireless networks is still not well-explored by now. Like one step forward in this direction, this paper focuses on the E2E physical layer authentication in a dual-hop wireless network with an untrusted relay and proposes a corresponding physical layer authentication scheme. The scheme fully utilizes the location-specific features of both channel amplitude and delay interval of cascaded channels and adopts the artificial jamming technique, so that it is not only resistant to the impersonate attack from an unauthorized transmitter but also resilient to the replay attack from the untrusted relay. Theoretical analysis is further conducted to derive the expressions for the probabilities of false alarm and missed detection, which are two fundamental metrics of authentication performance. Finally, the numerical and simulation results are provided to illustrate both the efficiency of these theoretical results and the E2E authentication performance of dual-hop wireless networks under the proposed scheme.

INDEX TERMS Physical layer authentication, wireless security, cascaded channel, dual-hop wireless networks.

I. INTRODUCTION

Authentication serves as a critical property of secure communication to verify the identity of the entity involved in the communication. With the rapid development of wireless technologies, the flexible and cost-effective authentication is becoming an increasingly urgent demand for future wireless networks. This is because that on one hand, the open and broadcast natures of wireless communications make wireless networks more vulnerable to spoofing attacks, where an unauthorized transmitter may impersonate as legitimate one. On the other hand, with the wide deployment of Internet of things (IoT) [1], [2] and continuous evolvement of wireless technologies toward the fifth generation (5G) networks [3], it is foreseeable that future wireless networks will be consisted of an unprecedented huge number of heterogeneous devices, making the authentication in such networks a challenging issue.

Conventionally, authentication is implemented based on the cryptographic technique [4]–[6], where it is usually assumed that a secret key is shared in advance between the transmitter and receiver. Nevertheless, the authentication relying on this assumption is increasingly being questioned in emerging network scenarios such as IoT, low power wide area networks [7] and 5G wireless systems [8]. This is mainly due to the reasons that distribution and management of secret keys become troublesome and even impossible in such large-scale heterogeneous networks. Also, the distributed nature of these scenarios makes the stored secret keys vulnerable to physical attacks. E.g., an attacker may capture a legal device and break the keys via hardware level attacks.

Recently, physical layer authentication (PLA) technique, which exploits the intrinsic and unique features of physical layer for authentication, has drawn a considerable attention

The associate editor coordinating the review of this manuscript and approving it for publication was Chi-Yuan Chen.

to enhance and complement the conventional cryptography-based authentication solutions. By now, some research efforts have been devoted to the study of PLA methods. These PLA methods can be roughly classified into three categories: fingerprinting authentication, watermarking authentication and channel-based authentication. Fingerprinting authentication is based on the intrinsic characteristics of transceiver hardware for authentication, e.g., the radio frequency-distinct native attribute [9]–[12]. Polak and Goeckel [9] explored the analysis of distortion signals resulting from hardware impairments to identify wireless devices. Wang *et al.* [11] further examined the reliability and differentiability of such methods via theoretical modeling as well as experiment validation. It was proved that phase noise can be used to authenticate transmitters through multiple kernel [12].

Watermarking authentication is based on superimposing watermarking information to modulated signals to conduct authentication [13]–[17]. A watermarking-based authentication scheme, which relies on a cryptography secure low-power authentication tag hidden in the modulated signals for authentication, was investigated in [13]. Based on the work of [13], Verma *et al.* [14] further conducted the tag-based authentication experiments in software defined radio system to demonstrate the authentication performance of such method. An extension of the conventional watermarking methods was proposed in [15] to authenticate wireless devices by jointly utilizing the side-channel information and tag selection.

The main idea of channel-based authentication is that channel state information is location-specific according to the radio propagation theory [18]. It is difficult for an adversary to precisely build the same channel that is being used by a legitimate transmitter-received pair. Xiao *et al.* [19] presented a channel-based authentication scheme exploiting the spatial variability of channel frequency response over time-varying channels in a rich scattering environment. Xiao *et al.* [20] further explored the channel-based authentication by using the temporal channel variations of channel impulse response to authenticate transmitters at different locations in frequency-selective Rayleigh channels. Based on [19] and [20], Liu and Wang [21] proposed a novel authentication scheme over time-varying multipath channels jointly using the location-specific properties of both amplitude and multipath delay of wireless channels to authenticate transmitters. Xiao and Han [22] further proposed a logistic regression-based authentication exploiting channel state information and multiple landmarks to improve the spoofing detection accuracy.

It is notable that above available works mainly focus on one-hop PLA, where transmitters and receivers can communicate with each other directly. In the large-scale distributed wireless networks such as IoT and 5G wireless systems [8], the end to end (E2E) communication is usually conducted with the help of relay(s) [23]–[25]. Due to transmission efficiency, delay and secrecy constraints, the multi-hop E2E PLA is an important research issue in wireless communication scenarios, where relay only needs to amplify and forward the signals transmitted by the transmitter to the legitimate receiver, or to decode the signals and then forward them to the legitimate receiver. To the best of our knowledge, the multi-hop E2E PLA is still not well-explored yet. Notice that the available one-hop PLA schemes can not be directly extended to multi-hop E2E PLA mainly due to the following challenges. First, the cascade channels between the transmitter and receiver become much more dynamic and complicated, making multi-hop E2E PLA more challenging [26]. Second, the relay can be potential adversary to record the received signals and initiate replay attacks, bringing new threat to the E2E PLA.

As one step towards the study of E2E multi-hop PLA, this paper focuses on the channel-based E2E PLA in a dual-hop wireless network with an untrusted relay. This is because the dual-hop wireless networks are simple and serve as a foundation for the study of general multi-hop wireless networks. By carefully exploiting the highly dynamic properties of the dual-hop cascade channels, we develop an efficient E2E PLA scheme to discriminate transmitters at different locations. The main contributions of this paper are summarized as follows.

- We propose a new E2E PLA scheme for dual-hop wireless networks with an untrusted relay. This scheme utilizes the location-specific features of both channel amplitude (CA) and delay interval (DI) of cascaded channels to discriminate transmitters, and adopts the artificial jamming technique to resist against possible replay attack from the untrusted relay.
- Using statistical signal estimation theory and the two-dimensional quantizers, we can qualify the temporal variations of CA and DI of cascaded multipath channel.
- Based on the hypothesis test theory, theoretical analysis is then conducted to derive the expressions for probabilities of false alarm (FA) and missed detection (MD), such that E2E authentication performance under the proposed E2E PLA scheme can be fully depicted.
- Finally, extensive numerical/simulation results are provided to validate theoretical results for the probabilities of FA and MD and to illustrate the authentication performance for the proposed E2E PLA scheme.

The remainder of this paper is organized as follows. Section II depicts the system model involved in this study. Section III presents the proposed E2E PLA scheme and carries out the related security analysis. The modeling of the probabilities for FA and MD is provided in Section IV, and the numerical/simulation results are showed in Section V. Finally, Section VI concludes this paper.

Notation: $(\cdot)^*$ denotes conjugate operator. $|\cdot|$ denotes absolute operate. $\mathcal{N}(\mu, \sigma^2)$ and $\mathcal{CN}(\mu, \sigma^2)$ denote real and complex Gaussian distributions with mean μ and variance σ^2, respectively. $\mathbf{E}\{\cdot\}$ and $\mathbf{Pr}(\cdot)$ represent expectation and probability operators, respectively. $\exp(\cdot)$ denotes exponential function. $Laplace(\mu, b)$ denotes Laplace distribution with location parameter μ and scale parameter b.

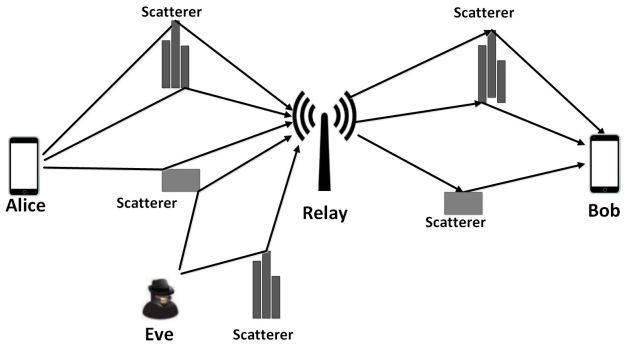

FIGURE 1. System model. The transmitter Alice (*A*) communicates with the receiver Bob (*B*) with the aid of an AF untrusted relay (*R*), and Eve (*E*) serves as the adversary who impersonates *A*. The transmissions for *A* (*E*)-*R* and *R*-*B* experience different multipath effects.

II. SYSTEM MODEL

A. NETWORK MODEL

As depicted in Fig. 1, we consider a dual-hop wireless network scenario consisting of four entities: one legitimate transmitter Alice (A), one untrusted relay (R) adopting the amplify-and-forward (AF) strategy, one intended receiver Bob (B) and one adversary Eve (E). Each entity is equipped with an omnidirectional antenna and operates in half-duplex mode. These entities are spatially located at separated positions in a rich-scattering environment (e.g., in urban area). We assume that the spatial separation between any two entities is more than a distance of half a wavelength, making fading paths independent of each other according to the well-known Jakes uniform scattering model [18]. This is widely adopted in [19]–[21] and [27] and reasonable because if two entities are spaced within a distance of half a wavelength, they will fail to work due to mutual strong interference.

The direct link between A (E) and B suffers from the deep fading so that they can only communicate with the help of R. R can record all the received signals and then initiate replay attacks with the aggressive signals, that is, R serves as a potential adversary. The adversary E monitors the network and attempts to inject aggressive signals into the network in the hope of impersonating A. B not only can receive signals but also can transmit signals (e.g., jamming signals) to R. We assume that adversaries have the knowledge of the modulation method employed in the network, the channel estimation technique employed by B and authentication scheme adopted in the network [19], [28]. Similar to that of previous studies [19], [20], we further assume that E cannot arrive at A's previous location before a new signal arrives at B.

Suppose that B receives two messages (i.e., frames) at times $t-1$ and k (time interval is much less than the channels coherence time). The first one is validated by B from Alice using a standard higher-layer protocol [29]. Based on this authentication, B measures and stores not only the channel connecting A and R with him in terms of CA and DI at time $t-1$. The objective of authentication at B is that utilizing multipath channel estimation for R-B and A-R-B in terms of amplitude and delay based on previous message originated from A, he needs to decide whether the second message received at time t is still from A. We stress that the message to be authenticated is not required to transmit continuously but it is necessary to ensure the continuity of the authentication process by probing the channel at time intervals smaller than the channels coherence time [19]–[21], [30], [31].

We assume that the channels are reciprocal and remains correlated within the total processing time, which mainly includes propagation delay, transmitting time and operation (e.g., AF operation) delay at each entity. This is due to the fact that the total processing time is much less than channel coherent time T_C, For example, for a typical $f = 2.4$ GHz radio frequency carrier, relative motion speed $v = 2$ m/s, T_C can be calculated as $T_C = \frac{9c}{16\pi vf} = 11.2$ ms (c is light speed). The propagation delay might be 30 μ s for a rich scattering environment (will be at least 10 μs) if the distance is 3 km. Transmitting time is 0.5 μs for a frame consisting of 20 symbols when symbol sampling rate is 40 MHz. In general, the operation delay has the same order of transmitting time.

B. CHANNEL MODEL

Since all entities are in a rich scattering and reflecting environment, channel impulse response of each hop in the concerned dual-hop network is modeled as a sum of paths with time-varying CA and propagation delay caused by the changes in the propagation environment (e.g., relative motion between entities and/or movement of scatterers/reflecors). Considering N_{ij} multipath channels between two entities i and j, channel impulse response measured at time t under the delay spread index denoted by d can be expressed by

$$h_{ij}(t,d) = \sum_{n_{ij}=1}^{N_{ij}} h_{n_{ij}}(t)\delta(t - d_{n_{ij}}(t)), \quad n_{ij} = 1, 2, ..., N_{ij}. \tag{1}$$

where $h_{n_{ij}}(t)$ and $d_{n_{ij}}(t)$ $(d_{1_{ij}}(t) < d_{2_{ij}}(t) < \cdots < d_{N_{ij}}(t))$ are the time-varying CA and propagation delay associated with the $n_{ij}{}^{\text{th}}$ multipath component, respectively, and $\delta(\cdot)$ is the Dirac pulse function. subscript ij can be AR, ER or RB. Hence, the CA and propagation delay of the $n_{AR}{}^{\text{th}}$, $n_{RB}{}^{\text{th}}$ and $n_{ER}{}^{\text{th}}$ multipath components for A-R, R-B and E-R are denoted by $h_{n_{AR}}(t)$, $h_{n_{RB}}(t)$ and $h_{n_{ER}}(t)$, and $d_{n_{AR}}(t)$, $d_{n_{RB}}(t)$ and $d_{n_{ER}}(t)$, respectively.

Each multipath component is assumed to be suffer from statistically independent Rayleigh fading and CA and propagation delay of that are assumed to remain constant over a frame (message transmission is organized by frame-by-frame) but to vary independently and continuously from one frame to the next. Such temporal variations in terms of CA and delay are highly correlated [32], [33]. Thus, $h_{n_{ij}}$ follows a zero-mean complex Gaussian distribution. In general, for a specific multipath channel their channel amplitudes might not be identical variance (e.g., in the case of an exponential power delay profile). To simplify the considerations, we assume that channel amplitudes have an identical variance, i.e., $h_{n_{ij}} \sim \mathcal{CN}(0, \sigma^2_{h_{ij}})$ [19]–[21].

To explore the temporal variation of channel amplitude, we need to investigate the auto-correlation function of channel amplitude. According to the Jakes' model [18], channel variation is affected by the Doppler frequency. Similar to that of previous studies [19], [21], [34], identical maximum Doppler frequency is considered in multipath channels. Then, the auto-correlation function of $h_{n_{ij}}(t)$ under arbitrary time lag t_s, can be given by

$$\varphi_{ij}(t_s) = \mathbf{E}\{h_{n_{ij}}(t)h^*_{n_{ij}}(t+t_s)\} = \sigma^2_{h_{ij}} J_0(2\pi f_{ij} t_s), \quad (2)$$

where $J_0(\cdot)$ is the zero$^{\text{th}}$ order Bessel function of the first kind. f_{ij} is maximum normalized Doppler frequency. Based on the above results, we employ the auto-regressive model of order 1 (AR-1) [19], [21], [34] to describe time-varying channel amplitude, and then we have

$$h_{n_{ij}}(t) = \alpha_{ij} h_{n_{ij}}(t-1) + \sqrt{1-\alpha^2_{ij}}\, u_{n_{ij}}(t), \quad (3)$$

where AR coefficient α_{ij} is denoted by $\varphi_{ij}(1)/\sigma^2_{h_{ij}}$; $u_{n_{ij}} \sim \mathcal{CN}(0, \sigma^2_{h_{ij}})$ is independent of $h_{n_{ij}}(t-1)$.

Moreover, the propagation delay of multipath components can be modeled by a Poisson process [35]. Therefore, delay interval (DI) between two delays of adjacent multipath components at time t is an exponentially distributed random variable, which is defined by

$$\tau_{k_{ij}}(t) \triangleq d_{k_{ij}}(t) - d_{k-1_{ij}}(t), \quad k = 1, 2, ..., N_{ij} - 1. \quad (4)$$

One can easily see that $\tau_{k_{ij}}(t)$ is also time-varying. Similar to the simple assumption for $h_{n_{ij}}$, we also assume that $\tau_{k_{ij}}(t)$ is statistically independent and identically distributed random variable [21].

We adopt correlated Gaussian random variables to characterize the correlation between $\tau_{k_{ij}}(t-1)$ and $\tau_{k_{ij}}(t)$. This is reasonable due to the fact that an exponentially distributed random variable can be decomposed as the sum of the squares of two independent Gaussian distributed random variables. Hence, $\tau_{k_{ij}}(t-1)$ and $\tau_{k_{ij}}(t)$ can be decomposed, respectively, as

$$\tau_{k_{ij}}(t-1) = \tau^{(1)}_{k_{ij}}(t-1) + \tau^{(2)}_{k_{ij}}(t-1), \quad (5)$$

$$\tau_{k_{ij}}(t) = \tau^{(1)}_{k_{ij}}(t) + \tau^{(2)}_{k_{ij}}(t), \quad (6)$$

where $\tau^{(1)}_{k_{ij}}, \tau^{(2)}_{k_{ij}}$ are mutually independent Gaussian distributed random variables with zero mean and variance $\sigma^2_{\tau_{ij}}$. Similar to previous work [21], we also use AR-1 to model the temporal processes of $\tau^{(1)}_{k_{ij}}$ and $\tau^{(2)}_{k_{ij}}$, and then we have

$$\tau^{(\ell)}_{k_{ij}}(t) = \beta_{ij}\tau^{(\ell)}_{k_{ij}}(t-1) + \sqrt{(1-\beta^2_{ij})\sigma^2_{\tau_{ij}}}\, u^{(\ell)}_{k_{ij}}(t), \quad \ell = 1, 2, \quad (7)$$

where AR coefficient β_{ij} has the similar definition with α_{ij} given in (3); $u^{(\ell)}_{ij,k}(t) \sim N(0, 1)$ is independent of $\tau^{(\ell)}_{ij,k}(t-1)$.

C. COMMUNICATION MODEL

Frame-by-frame transmission is considered in this paper. A transmission frame consists of deterministic pilot symbols used to channel estimation and stochastic data symbols. When A transmits a signal $s(t)$ to B at time t with the aid of R. The total transmission is accomplished by the following two phases. For Phase I, A transmits the signal $s(t)$ at the average transmitted power P to R and the signal received at R is

$$y_R(t) = \sqrt{P}\sum_{n_{AR}=1}^{N_{AR}} h_{n_{AR}}(t)s(t - d_{n_{AR}}(t)) + w_R(t), \quad (8)$$

where $w_R \sim \mathcal{CN}(0, \sigma^2_w)$ is the additive white Gaussian noise (AWGN).

For Phase II, $y_R(t)$ is then multiplied by an amplification factor ρ and retransmitted to B at power P. The amplification factor commonly used in the literature is

$$\rho = \sqrt{\frac{P}{P\sigma^2_{h_{AR}} + \sigma^2_w}}. \quad (9)$$

Since the transmitting time and operation delay is much less than the operation delay (see Section II-A), so we can neglect the transmitting time and operation delay. Therefore, the AWGN at B is denoted by $w_B \sim \mathcal{CN}(0, \sigma^2_w)$, and then the corresponding received signal at B is given in (10), as shown at the bottom of this page.

From (10), we know that the channel impulse response from the transmitter to the receiver via the relay is a cascade of the multipath channels in two hops, i.e., it is a cascaded multipath channel. According to [32], the double (cascaded) Rayleigh fading model can be used to characterize such cascaded multipath components. The CA of each cascaded multipath component is the product of CAs of two multipath components in two hops over this cascaded path, and the corresponding delay is the sum of delays of two multipath components in two hops over this cascaded path. The CA of the n^{th}_{AB} cascaded multipath components for *A-R-B* is denoted by

$$h_{n_{AB}}(t) = h_{n_{AR}}(t)h_{n_{RB}}(t), \quad (11)$$

where $n_{AB} = 1, 2, ..., N_{AR}N_{RB}$, $n_{AR} = 1, 2, ..., N_{AR}$ and $n_{RB} = 1, 2, ..., N_{RB}$.

Then, the corresponding DI is denoted by

$$\tau_{k_{AB}}(t) = \tau_{k_{AR}}(t) + \tau_{k_{RB}}(t), \quad (12)$$

where $k_{AB} = 1, 2, ..., N_{AR}N_{RB} - 1$, $k_{AR} = 1, 2, ..., N_{AR} - 1$ and $k_{RB} = 1, 2, ..., N_{RB} - 1$. When E transmits signals to B, it has the same the transmission process.

$$y_B(t) = \rho\sqrt{P}\sum_{n_{AR}=1}^{N_{AR}}\sum_{n_{RB}=1}^{N_{RB}} h_{n_{AR}}(t)h_{n_{RB}}(t)s(t - d_{n_{AR}}(t) - d_{n_{RB}}(t)) + \rho\sqrt{P}\sum_{n_{RB}=1}^{N_{RB}} h_{n_{RB}}(t)w_R(t - d_{n_{RB}}(t)) + w_B(t). \quad (10)$$

Using methods in [36]–[40], B can estimate cascaded multipath channel parameters from the received signal in (10) In addition, channel and delay estimation are corrupted by estimation error (additive noise). and such estimation error is much less than the temporal variations of channel and delay [21]. Therefore, both CA and delay of channels can be utilized to differentiate between the legitimate transmitter A and illegitimate transmitter E.

III. E2E PLA SCHEME

The basic principle for the proposed E2E PLA scheme is that the channels are location-specific, which has been widely adopted for authentication transmitters to complement and improve traditional security approaches [19]–[21], [27]. Most importantly, this is demonstrated by the well-known Jakes model [18], that is, the spatial separation of one to two wavelengths results in independent fading channels. It is difficult (if not impossible) for an attacker to generate or accurately model the channel being used by transmitter-receiver pair. In other words, the channels between different geographic locations decorrelate rapidly in space due to path loss and channel fading [18], [19]. As a result, the channel of A-R-B is independent of that of E-R-B. Meanwhile, the channel for the identical transmitter-receiver pair is highly corrected over time. Hence, CA and DI of multipath channels can be jointly exploited to authenticate transmitters.

FIGURE 2. The main procedures of the proposed E2E PLA scheme.

The main procedures of the proposed E2E PLA scheme are illustrated in Fig. 2, where a typical challenge-response procedure is first conducted to initiate the authentication process. The transmissions of authentication and jamming signals is then implemented between entities involved in communication. Finally, B carries out a verification procedure to verify whether the current frame is from A or not.

A. CHALLENGE-RESPONSE PROCEDURE

In the available authentication schemes developed for wireless systems with direct link between an unknown transmitter X (i.e., $X = \{A, E\}$) and the receiver B [19]–[21], [27], the transmitter can directly send authentication signals to the receiver B anytime without pursing the synchronization with the receiver in advance. For the dual-hop wireless system with an untrusted relay R concerned in this paper, however, to deal with the possible replay attack from R based on our proposed E2E PLA scheme, the synchronization between the transmitter and receiver B is required before the authentication process. For this purpose, the transmitter first sends an authentication request frame (i.e., a challenge), which contains only the synchronization signal indicating the time that the authentication signal is to be transmitted, such that the synchronization between the transmitter and B can be achieved in the next transmission process of authentication and jamming signals.

After receiving the authentication request from A, B sends back a response frame which only includes one symbol to confirm the requested time for synchronization.

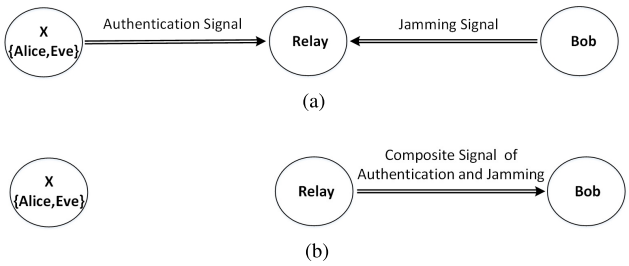

FIGURE 3. (a) First phase transmission. (b) Second phase transmission. Transmissions of authentication and jamming signals.

B. TRANSMISSIONS OF AUTHENTICATION AND JAMMING SIGNALS

As illustrated in Fig. 3, the transmissions of authentication and jamming signals at time $t + 1$ includes two phases. In the first phase transmission (Fig. 3a), transmitter X sends a frame including the signal to be authenticated to R. This signal consists of both pilot and data symbols. Concurrently, receiver B sends a jamming frame with jamming signal to R in a cooperative manner, making the untrusted R to receive a composite signal of authentication and jamming signals. Here, the jamming signals can be generated by utilizing a pseudo-random noise generator such as the one in [41] and is then stored at B. Without loss of generality, we use $v(t)$ and P_B to jamming signal and the average symbol power transmitted by B. When the transmitter is A (i.e., $X = A$), (8) becomes (13), as shown at the bottom of this page. As shown in Fig. 3b, the composite signal given in (13) is then multiplied by an amplification factor given in (9) at R and retransmitted to B in the second phase transmission [33].

C. VERIFICATION PROCEDURE

1) CA/DI ESTIMATION

After receiving the composite signal of jamming and authentication signals, B first removes the jamming signal through the well-developed self-interference cancellation

$$y_R(t) = \sqrt{P_A}\sum_{n_{AR}=1}^{N_{AR}} h_{n_{AR}}(t)s(t - d_{n_{AR}}(t)) + \sqrt{P_B}\sum_{n_{RB}=1}^{N_{RB}} h_{n_{RB}}(t)v(t - d_{n_{RB}}(t)) + w_R(t). \quad (13)$$

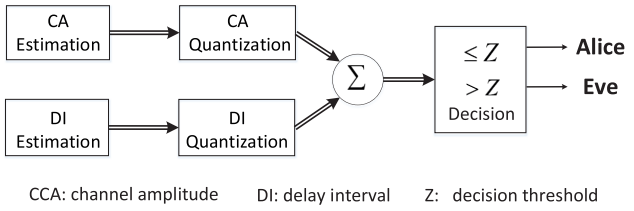

FIGURE 4. Illustration of CA/DI estimation/quantization and decision.

techniques [42], [43], and thus extracts the desired signal (i.e., consisting of pilot and data symbols) from the unknown transmitter X (when $X = A$, the received signal at B has the same expression as (10)). Since the generated jamming signal is known to B, it can be eliminated up to a certain extent through efficient techniques of interference cancellation [42], [43]. To present the optimal authentication performance of the proposed E2E PLA scheme, we follow the ideal assumption here that perfect cancellation of self-interference is achievable [44]. As shown in Fig. 4, the estimation of CA/DI are first performed. Based on the estimation results of CA/DI, quantization is then handled to qualify the temporal variations of CA/DI. Finally, B decides whether the current frame is from A or not under a simple binary hypothesis test.

Notice that CA and DI of cascaded channel can be estimated by using the deterministic pilot symbols, but only a noisy version of cascaded channel is available at B due to the presence of AWGN. The estimation error caused by such AWGN is random and independent of the channel, and can be modeled as AWGN random variable with zero mean.

a: CA ESTIMATION

Let $\hat{h}_{n_{AB}}(t)$ (resp. $\hat{h}_{EB,n_{EB}}(t)$) denote the estimation of $h_{n_{AB}}(t)$ (resp. $h_{EB,n_{EB}}(t)$) at time t, and then each of them can be modeled as a sum of its real value and a complex Gaussian noise (i.e., estimation error) $w_h(t) \sim \mathcal{CN}(0, \sigma_w^2)$. Then, we have

$$\begin{aligned}\hat{h}_{XB,l_{XB}} &\triangleq h_{XB,l_{XB}}(t) + w_h(t) \\ &= h_{XR,l_{XR}}(t)h_{n_{RB}}(t) + w_h(t), \quad X = \{A, E\}. \end{aligned} \tag{14}$$

where σ_w^2 is defined as $\sigma_w^2 = P_w/P$ with P_w representing the average noise power at the receiver, respectively [20].

b: DI ESTIMATION

Actually, the DI of each adjacent paths pair in a cascaded channel can be considered to be the superposition of DIs of each adjacent multipath components pair in two hops over that paths pair. This is because that the delays of multipath channels are spatially uncorrelated, and the processing time at each entity is sufficiently small and thus can be neglected [28].

Let $\hat{\tau}_{k_{AR}}^{(1)}(t)$ and $\hat{\tau}_{k_{AR}}^{(2)}(t)$ represent the estimations of $\tau_{k_{AR}}^{(1)}(t)$ and $\tau_{k_{AR}}^{(2)}(t)$, respectively. Similar to the estimation of CA, each of them can also be considered as a sum of its real value and an AWGN (estimation error) $w_\tau(t)$, they can be written, respectively, as

$$\hat{\tau}_{k_{AR}}^{(\ell)}(t) \triangleq \tau_{k_{AR}}^{(\ell)}(t) + w_\tau^{(\ell)}(t), \quad \ell = 1, 2. \tag{15}$$

where $w_\tau^{(\ell)}(t) \sim \mathcal{N}(0, \sigma_w^2/2)$. One can easily see that $\hat{\tau}_{k_{AR}}^{(\ell)}(t) \sim \mathcal{N}(0, \sigma_{\tau_{AR}}^2 + \sigma_w^2/2)$. Let $\hat{\tau}_{k_{AR}}(t)$ denote the estimation of $\tau_{k_{AR}}(t)$, and then we have

$$\hat{\tau}_{k_{AR}}(t) = (\hat{\tau}_{k_{AR}}^{(1)}(t))^2 + (\hat{\tau}_{k_{AR}}^{(2)}(t))^2. \tag{16}$$

It can be seen from (16) that $\hat{\tau}_{k_{AR}}(t)$ also follows exponential distribution with parameter $\lambda = \frac{1}{2\sigma_{\tau_{AR}}^2 + \sigma_w^2}$. By using the similar derivation, we can see that both $\hat{\tau}_{k_{RB}}(t)$ and $\hat{\tau}_{k_{ER}}(t)$ are also exponentially distributed random variables with parameters $\lambda = \frac{1}{2\sigma_{\tau_{RB}}^2 + \sigma_w^2}$ and $\lambda = \frac{1}{2\sigma_{\tau_{ER}}^2 + \sigma_w^2}$, respectively. The total DI of the k_{XB}^{th} cascaded multipath component can be given by

$$\tau_{k_{XB}}(t) = \hat{\tau}_{k_{XR}}(t) + \hat{\tau}_{k_{RB}}(t). \tag{17}$$

2) CA/DI QUANTIZATION

a: CA QUANTIZATION

To quantify the temporal variation of CA, we use a CA quantizer which compares the square of absolute value of the CA difference between the current and previous CA estimations of the same path at adjacent time with a specified CA threshold. In particular, when the difference is not larger than the specified CA threshold, the output of CA quantizer is 0; otherwise, the output of that is 1. We use Q_h and $O_{h,n}$ to denote CA quantizer and the n^{th} output of CA quantizer, respectively, where $n \in \{1, 2, ..., N\}$ and $N = \min\{N_{XR}N_{RB}, N_{AR}N_{RB}\}$. Then, CA quantization can be formulated as

$$\begin{aligned} O_{h,n} &\triangleq Q_h[|\hat{h}_{n_{AB}}(t) - \hat{h}_{n_{AB}}(t-1)|^2] \\ &= \begin{cases} 0, & |\hat{h}_{n_{AB}}(t) - \hat{h}_{n_{AB}}(t-1)|^2 \le \delta_h, \\ 1, & \text{otherwise.} \end{cases} \end{aligned} \tag{18}$$

where δ_h represents the specified CA threshold.

b: DI QUANTIZATION

To quantify the temporal variation of DI, a DI quantizer is employed by comparing the absolute value of the DI difference between the current and previous DI estimations of the same paths pair at adjacent time with a specified time threshold. Specifically, when the difference is not larger than the specified time threshold, the output of DI quantizer is 0; otherwise, the output of that is 1. Let Q_τ and $O_{\tau,k}$ denote DI quantizer and the k^{th} output of the quantizer, respectively, where $k \in \{1, 2, ..., N-1\}$. Then, DI quantization can be formulated as

$$\begin{aligned} O_{\tau,k} &\triangleq Q_\tau[|\hat{\tau}_{k_{XB}}(t) - \hat{\tau}_{k_{AB}}(t-1)|] \\ &= \begin{cases} 0, & |\hat{\tau}_{k_{XB}}(t) - \hat{\tau}_{k_{AB}}(t-1)| \le \delta_\tau, \\ 1, & \text{otherwise.} \end{cases} \end{aligned} \tag{19}$$

where δ_τ is the specified time threshold.

Let Ω_h and Ω_τ represent the sum of $O_{h,n}$ and $O_{\tau,k}$, respectively, and then we have

$$\Omega_h \triangleq \sum_{n=1}^{N} O_{h,n}, \tag{20}$$

$$\Omega_\tau \triangleq \sum_{k=1}^{N-1} O_{\tau,k}. \tag{21}$$

It is easy to see that we have $\Omega_h \in \{0, 1, ..., N\}$ and $\Omega_\tau \in \{0, 1, ..., N-1\}$.

3) DECISION

Based on the above quantization results, we establish a decision criterion under a binary hypothesis test to differentiate between legitimate frame from A and illegitimate frame from E. For simplicity, we denote by Ω the sum of Ω_h and Ω_τ, and then the binary hypothesis test can be formulated as

$$\begin{aligned} H_0 &: \ \Omega \triangleq \Omega_h + \Omega_\tau \leq Z \\ H_1 &: \ \Omega \triangleq \Omega_h + \Omega_\tau > Z, \end{aligned} \tag{22}$$

where Z represents a non-negative integer decision threshold between 0 and $2N-1$. Under H_0, the newly received frame at B is still from legitimate transmitter A, Under H_1, it is from adversary E. However, there are still two failure events in the authentication process: 1) false alarm (FA), which occurs when a frame transmitted by legitimate transmitter A is mistakenly regarded as unauthentic; 2) missed detection (MD), which occurs when a frame originated from illegitimate transmitter E is wrongly judged as authentic.

D. SECURITY ANALYSIS

The location-specific characteristics of CA and DI make the proposed E2E PLA scheme immune to impersonate attacks from external attackers. Meanwhile, jamming signals can confuse the untrusted R and thus avoid simple replay attack from the possible internal attacker R. Furthermore, due to the lack of pilots and any pre-known reference symbols in authentication request signal, the attackers cannot probe channel in advance. All of these properties ensure the security of this scheme, as analyzed in the followings.

(1) A simple attacker E: When attacker E is located near a legitimate transmitter A, it will fail to impersonate A by inject aggressive signals due to that both CA and DI are location-specific.

(2) A smart attacker E: Due to the presence of artificial jamming, it becomes much more difficult (if not impossible) to estimate multipath channels A-E and E-R via the authentication signal transmitted by A, even the attacker E is close to R. Therefore, the smart attacker E will fail to construct multipath channel A-R and E-R and impersonate A by modifying its signal.

(3) Untrusted relay R: Although the untrusted relay R or other active attacker E are able to replay signals based on what they obtained, the proposed E2E PLA scheme can be immune to such attacks. This is mainly due to the fact that artificial jamming is randomly generated by B and different artificial jamming sequences that are unknown to attackers are generated at different time slots.

Remark 1: In fact, the system model concerned in this paper in terms of network topology is symmetrical. By setting work pattern of entities (e.g., Alice has the ability to estimate, qualify channel and make a decision), E2E mutual authentication between Alice and Bob can be achieved.

IV. MODELING OF PROBABILITIES FOR FA AND MD

In this section, we first derive some basic results regarding the probabilities that the outputs of two quantizers under two hypotheses are 1, respectively, and then use the results to derive the expressions for the probabilities of FA and MD.

A. PROBABILITY OF FA

We now present the following lemmas regarding the probability denoted by P_{ζ,H_0} that Q_ζ outputs 1 under H_0, where $\zeta = \{h, \tau\}$.

Lemma 1: For a given CA threshold δ_h and $h_{n_{RB}}(t-1)$, P_{h,H_0} can be evaluated as

$$P_{h,H_0} = \exp\left(-\frac{\delta_h}{2(1-\alpha)\sigma_{h_{AR}}^2 |h_{n_{RB}}(t-1)|^2 + 2\sigma_w^2}\right). \tag{23}$$

where $\alpha = \alpha_{AR}\alpha_{RB} \leq 1$ is the equivalent auto-correlation coefficient of $h_{n_{AB}}$.

Proof: Under H_0, the newly received signal at B is regarded to be from A, i.e., $X = A$. Based on (3), we first explore the CA evolution of cascaded multipath channels with the time-series model [45]. The time-series model of $h_{n_{AB}}$ can be written as

$$h_{n_{AB}}(t) = \alpha h_{n_{AB}}(t-1) + \sqrt{1-\alpha^2} h_{n_{RB}}(t-1) u_{n_{AR}}(t). \tag{24}$$

Let $\Delta_{h_{A,A}}$ denote the difference between $\hat{h}_{n_{AB}}(t)$ and $\hat{h}_{n_{AB}}(t-1)$, which is given by

$$\begin{aligned} \Delta h_{A,A} &\triangleq \hat{h}_{n_{AB}}(t) - \hat{h}_{n_{AB}}(t-1) \\ &= (\alpha - 1) h_{n_{AR}}(t-1) h_{n_{RB}}(t-1) \\ &\quad + \sqrt{1-\alpha^2} h_{n_{RB}}(t-1) u_{n_{AR}}(t) \\ &\quad + w_h(t) - w_h(t-1). \end{aligned} \tag{25}$$

Since $h_{n_{AR}}(t-1)h_{n_{RB}}(t-1)$ term in (25) follows complex double Gaussian distribution under Rayleigh fading model [46], it is difficult (if not possible) to analytically model $\Delta h_{A,A}$. It is interesting to see that for a given $h_{n_{RB}}(t-1)$, $h_{n_{AR}}(t-1)h_{n_{RB}}(t-1)$ follows complex Gaussian distribution. In the concerned network scenario, B extracts $h_{n_{RB}}(t-1)$ by exploiting the blind channel estimation techniques widely adapted in previous studies [41]. Therefore, for a given $h_{n_{RB}}(t-1)$, $\Delta h_{A,A}$ is also a complex Gaussian distributed random variable with zero mean and variance $\sigma_{\Delta h_{A,A}}^2 = 2(1-\alpha)\sigma_{h_{AR}}^2 |h_{n_{RB}}(t-1)|^2 + 2\sigma_w^2$. We can see that $|\Delta h_{A,A}|^2$ follows

$$\mathbf{Pr}(\Omega = z) = \begin{cases} \sum_{z_1=0}^{z} \binom{N}{z_1}(P_{h,H_0})^{z_1}(1-P_{h,H_0})^{N-z_1}\binom{N-1}{z-z_1}(P_{\tau,H_0})^{z-z_1}(1-P_{\tau,H_0})^{N-1-z+z_1}, & z \in [0, N-1], \quad (30a) \\ \sum_{z_1=z-N}^{N-1} \binom{N}{z-z_1}(P_{h,H_0})^{(z-z_1)}(1-P_{h,H_0})^{N-z+z_1}\binom{N-1}{z_1}(P_{\tau,H_0})^{z_1}(1-P_{\tau,H_0})^{N-1-z_1}, & z \in [N, 2N-1]. \quad (30b) \end{cases}$$

$$P_{fa} = \begin{cases} \sum_{z=Z+1}^{N-1}\sum_{z_1=0}^{z} \binom{N}{z_1}(P_{h,H_0})^{z_1}(1-P_{h,H_0})^{N-z_1}\binom{N-1}{z-z_1}(P_{\tau,H_0})^{z-z_1}(1-P_{\tau,H_0})^{N-1-z+z_1} \\ \quad + \sum_{z=N}^{2N-1}\sum_{z_1=z-N}^{N-1} \binom{N}{z-z_1}(P_{h,H_0})^{z-z_1}(1-P_{h,H_0})^{N-z+z_1}\binom{N-1}{z_1}(P_{\tau,H_0})^{z_1}(1-P_{\tau,H_0})^{N-1-z_1}, & Z \in [0, N-1], \quad (31a) \\ \sum_{z=Z+1}^{2N-1}\sum_{z_1=z-N}^{N-1} \binom{N}{z-z_1}(P_{h,H_0})^{z-z_1}(1-P_{h,H_0})^{N-z+z_1}\binom{N-1}{z_1}(P_{\tau,H_0})^{z_1}(1-P_{\tau,H_0})^{N-1-z_1}, & Z \in [N, 2N-1]. \quad (31b) \end{cases}$$

the exponential distribution and its cumulative distribution function (CDF) can be given by

$$F_{|\Delta h_{A,A}|^2}(x) = 1 - \exp\left(-\frac{x}{2(1-\alpha)\sigma_{h_{AR}}^2|h_{n_{RB}}(t-1)|^2 + 2\sigma_w^2}\right). \quad (26)$$

According to (18), P_{h,H_0} can be determined as

$$\begin{aligned} P_{h,H_0} &\triangleq \mathbf{Pr}(Q_h[|\hat{h}_{n_{AB}}(t) - \hat{h}_{n_{AB}}(t-1)|^2] = 1 \mid H_0) \\ &= 1 - \mathbf{Pr}(|\Delta_{h_{A,A}}|^2 \le \delta_h). \end{aligned} \quad (27)$$

Substituting (26) into (27), we can obtain (23). ■

Lemma 2: For a given time threshold δ_τ, P_{τ,H_0} can be evaluated as

$$P_{\tau,H_0} = \frac{1}{1-\frac{\eta_{AR}^2}{\eta_{RB}^2}}\left(\frac{\eta_{AR}^2}{\eta_{RB}^2}\exp\left(-\frac{\delta_\tau}{\eta_{AR}}\right) - \exp\left(-\frac{\delta_\tau}{\eta_{RB}}\right)\right), \quad (28)$$

where

$$\eta_{AR} = \sqrt{4\sigma_{\tau_{AR}}^4(1-\rho_{AR}^2) + 4\sigma_{\tau_{AR}}^2\sigma_w^2 + \sigma_w^4}, \quad (29a)$$

$$\eta_{RB} = \sqrt{4\sigma_{\tau_{RB}}^4(1-\rho_{RB}^2) + 4\sigma_{\tau_{RB}}^2\sigma_w^2 + \sigma_w^4}. \quad (29b)$$

Proof: See Appendix A for the proof. ■

The following lemma is dedicated to the distribution of Ω, which is of vital importance for the derivation of the probabilities of FA and MD.

Lemma 3: Suppose that z is a non-negative integer between 0 and $2N-1$, then the probability that Ω equals z under H_0 is given by (30)*, shown at the top of this page.*

Proof: The proof of Lemma 3 is straightforward, and a similar one can be found in [21, Appendix]. ■

We use P_{fa} to represent the probability of FA. Then, we can establish the following main results on P_{fa} based on Lemmas 1, 2 and 3.

Theorem 1: P_{fa} of the proposed E2E PLA scheme in a dual-hop wireless network with an untrusted relay can be given in (31)*, shown at the top of this page.*

Proof: Based on (22) and the law of total probability formula, P_{fa} can be given by

$$\begin{aligned} P_{fa} &= \mathbf{Pr}(\Omega > Z|H_0) \\ &= \mathbf{Pr}(\Omega = Z+1, Z+2, \cdots, 2N-1|H_0) \\ &= \sum_{z=Z+1}^{2N-1} \mathbf{Pr}(\Omega = z) \\ &= \sum_{z=Z+1}^{N-1} \mathbf{Pr}(\Omega = z) + \sum_{z=N}^{2N-1} \mathbf{Pr}(\Omega = z). \end{aligned} \quad (32)$$

Therefore, P_{fa} can be derived based on the following two cases: When $Z \in [0, N-1]$, substituting (30a) into (32), P_{fa} can be given in (31a); when $Z \in [N, 2N-1]$, substituting (30b) into (32), we can obtain (31b). ■

Corollary 1: In a dual-hop wireless network with an untrusted relay, P_{fa} of the proposed E2E PLA scheme utilizing the location-specific of CA separately to discriminate transmitters, can be given by

$$\begin{aligned} P_{fa} = \mathbf{Pr}(\Omega > Z|H_0) &= \sum_{z=Z+1}^{N} \mathbf{Pr}(\Omega = z) \\ &= \sum_{z=Z+1}^{N} \binom{N}{z} P_{h,H_0}^z (1-P_{h,H_0})^{N-z}. \end{aligned} \quad (33)$$

B. PROBABILITY OF MD

Under H_1, the current transmitter is regarded as E, i.e., $X = E$. The following lemmas are dedicated to regarding

the probability denoted by P_{ζ,H_1} that Q_ζ outputs 1 under H_1, where $\zeta = \{h, \tau\}$.

Lemma 4: For a given CA threshold δ_h and $h_{n_{RB}}(t-1)$, P_{h,H_1} can be evaluated as

$$P_{h,H_1} = \exp\left(-\frac{\delta_h}{\sigma^2_{\Delta h_{E,A}}}\right), \tag{34}$$

where

$$\sigma^2_{\Delta h_{E,A}} = (\alpha^2_{RB}\sigma^2_{h_{ER}} + \sigma^2_{h_{AR}})|h_{n_{RB}}(t-1)|^2 + (1-\alpha^2_{RB})\sigma^2_{h_{ER}}\sigma^2_{h_{RB}} + 2\sigma^2_w. \tag{35}$$

Proof: See Appendix B for the proof. ■

Lemma 5: For a given time threshold δ_τ, P_{τ,H_1} can be evaluated as

$$P_{\tau,H_1} = \frac{1}{\left(1-\frac{\eta^2_{EA}}{\eta^2_{RB}}\right)}\left(\frac{\eta^2_{EA}}{\eta^2_{RB}}e^{-\frac{\delta_\tau}{\eta_{EA}}} - e^{-\frac{\delta_\tau}{\eta_{RB}}}\right), \tag{36}$$

where

$$\eta_{EA} = \sigma^2_{\tau_{ER}} + \sigma^2_{\tau_{AR}} + \sigma^2_w. \tag{37}$$

Proof: See Appendix C for the proof. ■

We use P_{md} to represent the probability of missed detection. Then, we can establish the following main results on P_{md} based on Lemmas 3,4 and 5.

Theorem 2: P_{md} of the proposed E2E PLA scheme in a dual-hop wireless network with an untrusted relay can be given in (38)*, shown at the bottom of this page.*

Proof: Based on (22), P_{md} is expressed as

$$\begin{aligned} P_{md} &= \mathbf{Pr}(\Omega \le Z|H_1) = \sum_{z=0}^{Z}\mathbf{Pr}(\Omega = z|H_1) \\ &= \sum_{z=0}^{N-1}\mathbf{Pr}(\Omega = z) + \sum_{z=N}^{Z}\mathbf{Pr}(\Omega = z). \end{aligned} \tag{39}$$

Under H_1, P_{md} can be derived based on the following two cases: When $Z \in [0, N-1]$, using P_{h,H_1} and P_{τ,H_1} replace P_{h,H_0} and P_{τ,H_0} in (30a), respectively, and we substitute the new resulting into (39). Then, P_{md} can be given by (38a); when $Z \in [N, 2N-1]$, following a similar manner, P_{md} can be given by (38b). ■

TABLE 1. Main system parameters.

Parameter	Description
$\bar{\gamma}_{AR} = \frac{\sigma^2_{h_{AR}}}{\sigma^2_w}$	The average SNR of the first hop
$\bar{\gamma}_{RB} = \frac{\sigma^2_{h_{RB}}}{\sigma^2_w}$	The average SNR of the second hop
$\kappa_h = \frac{\sigma^2_{h_{ER}}}{\sigma^2_{h_{AR}}}$	The ratio of averaged channel gains for A-R and E-R
α_{AR}, α_{RB}	Channel amplitude correlation coefficients
β_{AR}, β_{RB}	Delay interval correlation coefficients
δ_h, δ_τ, Z	CA threshold, time threshold, decision threshold

Corollary 2: In a dual-hop wireless network with an untrusted relay, P_{md} of the proposed E2E PLA scheme utilizing the location-specific of CA separately to discriminate transmitters, can be given by

$$\begin{aligned} P_{md} &= \mathbf{Pr}(\Omega \le Z|H_1) = \sum_{z=0}^{N}\mathbf{Pr}(\Omega = z) \\ &= \sum_{z=0}^{N}\binom{N}{z}P^z_{h,H_1}(1-P_{h,H_1})^{N-1-z}. \end{aligned} \tag{40}$$

V. SIMULATION AND NUMERICAL RESULTS

A. SYSTEM PARAMETERS AND SIMULATION SETTING

We list in Table 1 the main system parameters that determine the authentication performance in terms of P_{fa} and P_{md}. We use $\bar{\gamma}$ to denote the average signal-to-noise ratio (SNR) per hop and use κ_h to denote the ratio of average CA gains for A-R and E-R. Since $\sigma^2_w = P_w/P$, the variance of noise σ^2_w in the equation of $\bar{\gamma}$ is inversely proportional to the average transmit power P for a given P_w. In our simulation, we set $\sigma^2_{h_{AR}} = \sigma^2_{h_{RB}} = \sigma^2_{\tau_{AR}} = \sigma^2_{\tau_{RB}} = 1$, and then adjust the parameters $\sigma^2_{h_{ER}}$ and $\sigma^2_{\tau_{ER}}$ to achieve a specified κ_h.

To validate the theoretical modeling, a dedicated simulator in MATLAB is developed, which is now available at [47]. The time-varying channels are generated by using the method introduced in [48]. The temporal correlation of the time-varying channels is a function of the normalized Doppler frequency that is affected by the mobility, carrier frequency and symbol duration. Based on the normalized Doppler frequencies illustrated in Table 2, we consider three fading

$$P_{md} = \begin{cases} \sum_{z=0}^{Z}\sum_{z_1=0}^{z}\binom{N}{z_1}(P_{h,H_1})^{z_1}(1-P_{h,H_1})^{N-z_1}\binom{N-1}{z-z_1}(P_{\tau,H_1})^{z-z_1}(1-P_{\tau,H_1})^{N-1-z+z_1}, & Z \in [0, N-1], \quad (38a) \\ \sum_{z=0}^{N-1}\sum_{z_1=0}^{z}\binom{N}{z_1}(P_{h,H_1})^{z_1}(1-P_{h,H_1})^{N-z_1}\binom{N-1}{z-z_1}(P_{\tau,H_1})^{z-z_1}(1-P_{\tau,H_1})^{N-1-z+z_1} \\ \quad + \sum_{z=N}^{Z-1}\sum_{z_1=z-N}^{N-1}\binom{N}{z-z_1}(P_{h,H_1})^{z-z_1}(1-P_{h,H_1})^{N-z+z_1}\binom{N-1}{z_1}(P_{\tau,H_1})^{z_1}(1-P_{\tau,H_1})^{N-1-z_1}, & Z \in [N, 2N-1]. \end{cases} \tag{38b}$$

TABLE 2. Three fading scenarios.

	Channels status	$f_{AR} = f_{RB}$
Case I	Slow-fading	.001
Case II	Fast-fading	.10
Case III	Faster-fading	.15

channels associated with correlation coefficients (i.e., α_{AR}, α_{RB}, $\alpha = \alpha_{AR}\alpha_{RB}$, β_{AR}, β_{RB}). Different normalized Doppler frequency values in Table 2 correspond to different moving velocity of entity under a given carrier frequency and symbol duration [33]. For a fair comparison, the number of multipath components for *A-R* and *E-R* are both fixed to be 3, while that of multipath components for *R-B* is fixed to be 2. For Monte-Carlo experiments, 10^5 independent trails are conducted to obtain the average results.

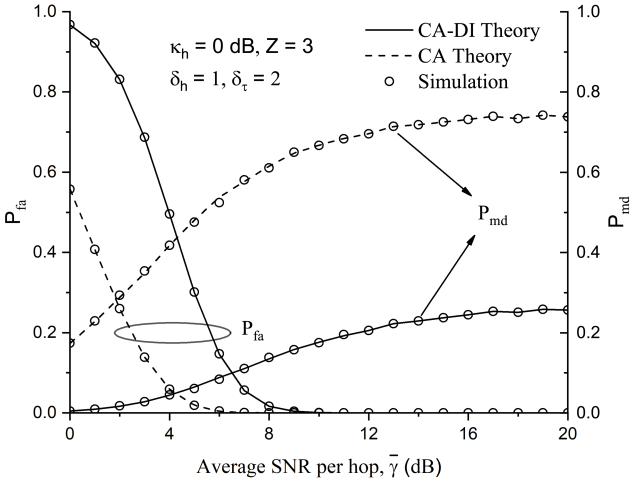

FIGURE 5. The authentication performance (P_{fa}, P_{md}) for the proposed scheme based on CA-DI or CA vs. average SNR per hop ($\bar{\gamma}_{AR} = \bar{\gamma}_{RB} = \bar{\gamma}$) under slow-fading channels.

B. MODEL VALIDATION THE PROBABILITIES OF FA AND MD

To verify the theoretical results, we summarize in Fig. 5 both the simulation and theoretical models of P_{fa} and P_{md} for the proposed E2E PLA scheme based on CA-DI or CA, where the slow-fading channels and settings of ($Z = 3$, $\kappa_h = 0$ dB, $\delta_h = 1$, $\delta_\tau = 2$) are assumed. Fig. 5 shows clearly that the simulation results agree well with the theoretical ones, confirming that our theoretical models can be used to nicely characterize P_{fa} and P_{md}. It can also be seen from Fig. 5 that as the average SNR per hop $\bar{\gamma}$ increases, P_{fa} for the proposed E2E PLA scheme based on CA-DI or CA declines rapidly, whereas the corresponding P_{md} increases slowly. This reveals that a trade-off exists between reliability and security in term of P_{fa} and P_{md}. Moreover, Fig. 5 shows that when $\bar{\gamma}$ is small, the proposed scheme jointly using CA and DI outperforms that only using CA in terms of P_{md}. While for P_{fa}, the result is reverse. This is due to the fact that by jointly utilizing the location-specific properties of cascaded channel in terms of CA and DI, the proposed scheme can effectively detect impersonation attacks at the cost of incurring more false alarm events. In addition, it can be observed from Fig. 5 that when $\bar{\gamma}$ is large (e.g., $\bar{\gamma} \geq 12$dB), P_{fa} for the proposed E2E PLA scheme based on either CA-DI or CA approaches 0, but this scheme jointly using CA and DI still outperforms that only using CA in terms of P_{md}.

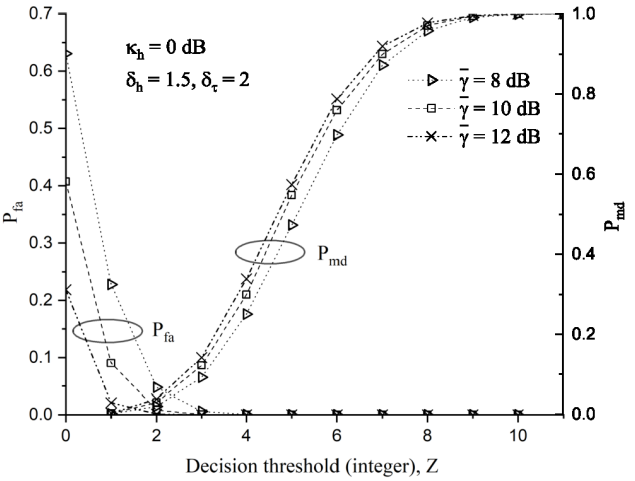

FIGURE 6. Effect of average SNR per hop ($\bar{\gamma}_{AR} = \bar{\gamma}_{RB} = \bar{\gamma}$) on the authentication performance (P_{fa}, P_{md}) vs. decision threshold Z under slow-fading channels.

C. CONTROL OF THE PROBABILITIES OF FA AND MD

To demonstrate that the proposed scheme enables the authentication performance to be flexibly controlled in a large region, we now explore how P_{fa} and P_{md} vary with parameters Z, δ_h and δ_τ. Fig. 6 shows the effect of $\bar{\gamma}$ on the P_{fa} and P_{md} versus Z, where the slow-fading channels and settings of ($\kappa_h = 0$ dB, $\delta_h = 1.5$, $\delta_\tau = 2$) are assumed. As observed from Fig. 6, P_{md} increases rapidly as Z increases, while P_{fa} declines quickly with Z. It is interesting to notice that P_{fa} is extremely sensitive to the variations of Z. For example, when $Z \geq 4$, P_{fa} approaches 0 under $\bar{\gamma} = \{8$ dB, 10 dB, 12 dB$\}$. We can see from Fig. 6 that for a fixed Z, P_{fa} decreases with $\bar{\gamma}$ while P_{md} increases with $\bar{\gamma}$. Noticed that for an authentication system, both P_{fa} and P_{md} are in general required to be below 0.1 [19]–[21], [49]. Therefore, for the specified P_{fa} and P_{md} constraints (e.g., P_{fa}, $P_{md} \leq 0.1$), we can increase the transmit power and find an optimal setting of Z. For example, we can set $Z = 1$ and $\bar{\gamma} \geq 10$ dB to ensure P_{fa}, $P_{md} \leq 0.1$. It is notable, however, that for general wireless networks applications, the total power of system is limited to a certain level due to the energy constraint and the interference requirement among simultaneous transmissions, so it is of great significance to find the optimal setting of parameters δ_h and δ_τ to satisfy the specified P_{fa} and P_{md} constraints under a given Z and power limitation.

Fig. 7 shows how P_{fa} and P_{md} vary with parameters (δ_h, δ_τ) under the slow-fading channels and settings of ($Z = 1$, $\bar{\gamma} = 10$ dB, $\kappa_h = 0$ dB). As shown in Fig. 7a (resp. Fig. 7b)

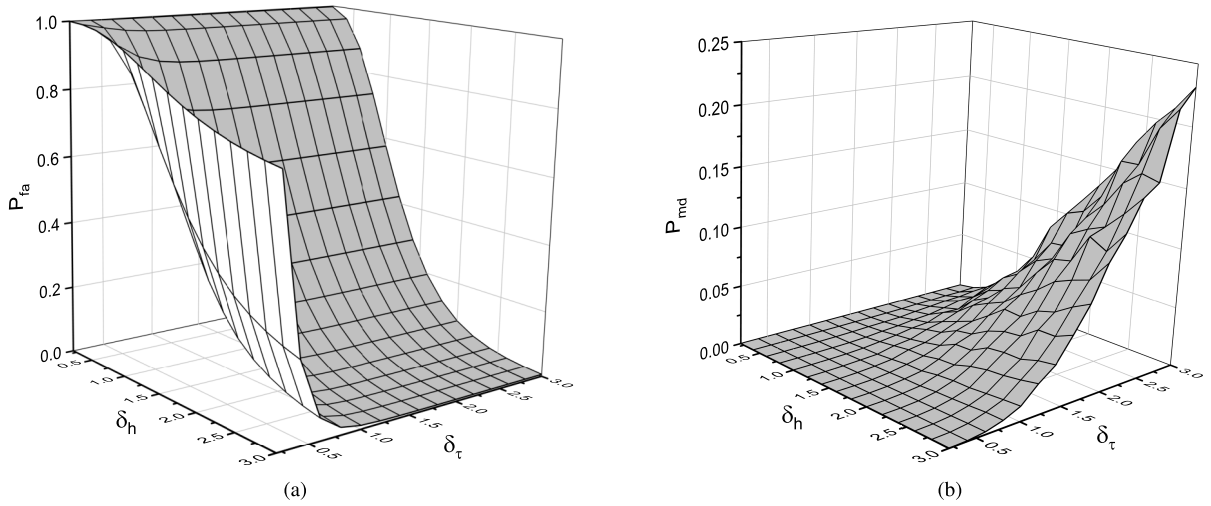

FIGURE 7. P_{fa} and P_{md} vs. (δ_h, δ_τ) when $Z = 1$, $\bar{\gamma} = 10$ dB and $\kappa_h = 0$ dB under slow-fading channels. (a) P_{fa} vs. (δ_h, δ_τ). (b) P_{md} vs. (δ_h, δ_τ).

that for a specified constraint p_{fa} of P_{fa} (resp. a specified constraint p_{md} of P_{md}), we can accordingly set a specified constraint plane intersecting the z-axis orthogonally at the point (2, 2, p_{fa}) (resp. at the point (2, 2, p_{md})), and then can determine a set of (δ_h, δ_τ)-pairs corresponding to the surface below the defined constraint plane. By finding the intersection of these two sets of (δ_h, δ_τ)-pairs, we can obtain the region of (δ_h, δ_τ)-pairs to achieve the P_{fa} and P_{md} constraints in terms of p_{fa} and p_{md}. For example, when $\delta_h, \delta_\tau \in [0.2, 3]$, one can observe from Fig. 7 that the requirement of $P_{fa} \leq 0.1$ can be achieved in the regions of ($\delta_h \in [1, 3]$, $\delta_\tau \in [1.2, 3]$), while the requirement of $P_{md} \leq 0.1$ is achieved in the regions of ($\delta_h \in [0.2, 2.5]$, $\delta_\tau \in [0.2, 2.2]$). Thus, the constraints of ($P_{fa}, P_{md} \leq 0.1$) under the considered network scenario are achieved when $\delta_h \in [1, 2.5]$ and $\delta_\tau \in [1.2, 2.2]$.

Fig. 6 and Fig. 7 indicate that the proposed E2E PLA scheme is flexible and general, since P_{fa} and P_{md} can be flexibly controlled by a proper setting of the decision threshold Z, CA threshold δ_h, and time threshold δ_τ. Also, a trade-off between reliability and security can be controlled by an appropriate setting of δ_h and δ_τ.

D. AUTHENTICATION EFFICIENCY ANALYSIS

To illustrate the authentication efficiency of the proposed E2E PLA scheme, we further explore the authentication performance of the scheme under diverse network scenarios with different positions of E and different channels statuses. Fig. 8 shows the effect of the position of E on the authentication performance (P_{fa}, P_{md}) versus $\bar{\gamma}$ under slow-fading channels, where $Z = 1$, $\delta_h = 1.5$, $\delta_\tau = 2$, and κ_h varies from -5 dB to 5 dB. We can see from Fig. 8 that P_{fa} is not affected by the variations of κ_h. This is because that the position of E is not related to FA events. It is noticed that for a fixed $\bar{\gamma}$, P_{md} increases as κ_h reduces. We also find that when $\bar{\gamma}$ is small, the setting of κ_h has a little impact on P_{md}; when $\bar{\gamma}$ is large,

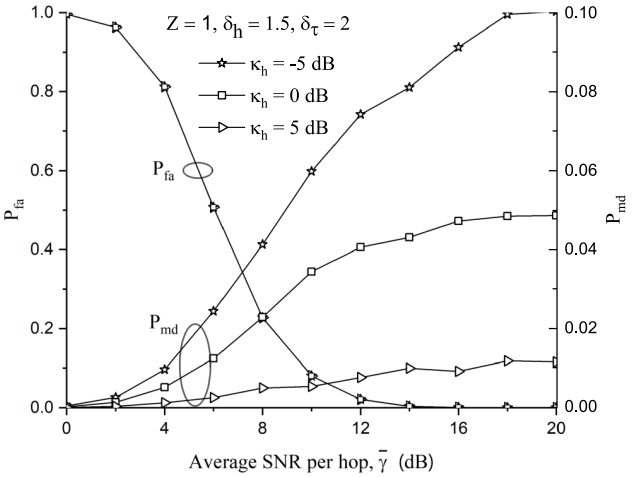

FIGURE 8. Effect of κ_h on the authentication performance (P_{fa}, P_{md}) vs. average SNR per hop ($\bar{\gamma}_{AR} = \bar{\gamma}_{RB} = \bar{\gamma}$) under slow-fading channels.

the setting of κ_h has a significant impact on P_{md}, especially when $\kappa_h = -5$ dB, P_{md} approaches 0.1. It implies that a "smart" intruder E would seek a position where it could have the higher probability to impersonate attacks successfully. Fortunately, the proposed scheme can adjust dynamically the optimal setting of (Z, δ_h, δ_τ) to resist against such attacks. This indicates that for various positions of E, the proposed scheme is efficient to discriminate transmitters through the proper settings of (Z, δ_h, δ_τ).

Finally, Fig. 9 demonstrates that the effect of channel status on the authentication performance (P_{fa}, P_{md}) versus $\bar{\gamma}$, given that $Z = 1$, $\kappa_h = 0$ dB, $\delta_h = 1.5$, $\delta_\tau = 2$. Notice also that in terms of P_{fa}, the proposed scheme under case I (slow-fading channels) outperforms that under the others (case II and case III), and the scheme under case III (faster-fading channels) leads to the highest P_{fa}. This indicates that excessive false alarm events will happen when channels are

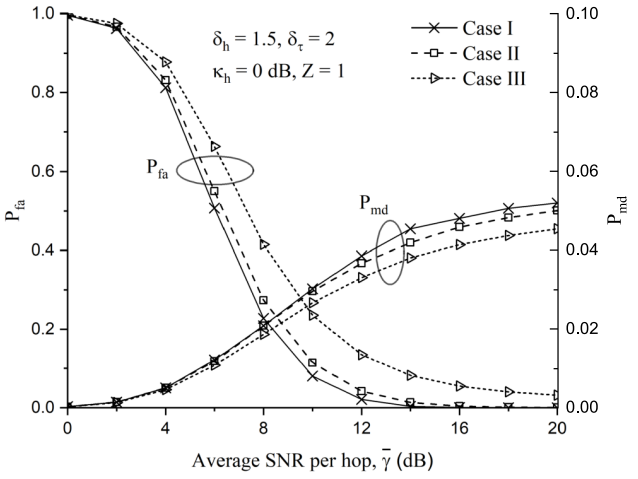

FIGURE 9. Effect of channel status on the authentication performance (P_{fa}, P_{md}) vs. average SNR per hop ($\bar{\gamma}_{AR} = \bar{\gamma}_{RB} = \bar{\gamma}$).

faster-fading (e.g. in a higher mobile scenario). However, in terms of P_{md}, the proposed scheme under faster-fading channels has the lowest P_{md}, which means that the faster-fading channels are beneficial for effectively detecting impersonation attacks. Fig. 9 confirms that under various channels statuses, the proposed scheme is also efficient in identifying transmitters by a proper setting of the decision threshold Z, CA threshold δ_h, time threshold δ_τ and average SNR per hop $\bar{\gamma}$.

VI. CONCLUSION

This paper represents an attempt to explore the E2E PLA issue for dual-hop wireless networks by exploiting the intrinsic properties of cascaded multipath channels. We showed that the proposed E2E PLA scheme is not only efficient in discrimination between the legitimate and illegitimate transmitters, but also resistant to impersonating attacks with the attacker near the legitimate transmitter and resistant to replay attacks with aggressive signals from the untrusted relay. We also proved that the proposed scheme is flexible and general in the sense that this scheme makes it possible for us to flexibly control the probabilities of FA and MD in a large region through the proper settings of parameters. This is an important property for wireless networks to support various applications of different authentication performance requirements. In addition, it is expected that the proposed authentication scheme and related theoretical models will be useful for providing a guideline to devise the coping strategies under various attacks, as well as for understanding the fundamental E2E authentication performance of multi-hop wireless networks.

APPENDIX A
PROOF OF LEMMA 2

Let $\Delta\tau_{AR} = \hat{\tau}_{k_{AR}}(t) - \hat{\tau}_{k_{AR}}(t-1)$ and $\Delta\tau_{RB} = \hat{\tau}_{k_{RB}}(t) - \hat{\tau}_{k_{RB}}(t-1)$, and $\Delta\tau_{A,A} = \hat{\tau}_{k_{AB}}(t) - \hat{\tau}_{k_{AB}}(t-1)$, then $\Delta\tau_{AB}$ can be further written as

$$\begin{aligned}\Delta\tau_{A,A} &\triangleq \hat{\tau}_{k_{AB}}(t) - \hat{\tau}_{k_{AB}}(t-1)\\ &= \hat{\tau}_{k_{AR}}(t) - \hat{\tau}_{k_{AR}}(t-1) + \hat{\tau}_{k_{RB}}(t) - \hat{\tau}_{k_{RB}}(t-1)\\ &= \Delta\tau_{AR} + \Delta\tau_{RB}. \end{aligned} \tag{41}$$

To explore the distribution of random variable $\Delta\tau_{A,A}$, we first examine that of $\Delta\tau_{AR}$. Based on (16), $\Delta\tau_{AR}$ can be written as (42), shown at the top of the next page. Combining (7), (15) and (16), the random variable C_1 defined in (42) can be given by

$$\begin{aligned}C_1 &= (\hat{\tau}^{(1)}_{k_{AR}}(t) - \hat{\tau}^{(1)}_{k_{AR}}(t-1))\\ &= (\beta_{AR}-1)\tau^{(1)}_{k_{AR}}(t-1) + \sqrt{(1-\beta^2_{AR})\sigma^2_{\tau_{AR}}}u^{(1)}_{k_{AR}}(t)\\ &\quad + w^{(1)}_{\tau}(t) - w^{(1)}_{\tau}(t-1). \end{aligned} \tag{43}$$

Since $\tau^{(1)}_{k_{AR}}$, $u^{(1)}_{k_{AR}}$ and $w^{(1)}_{\tau}$ are independent Gaussian distributed random variables with zero mean, C_1 is also a Gaussian distributed random variable with zero mean and variance $\sigma^2_{C_1} = 2\sigma^2_{\tau_{AR}}(1-\beta_{AR}) + \sigma^2_w$. After a similar derivation, C_2, C_3, C_4 are also Gaussian distributed random variables with zero means and variances with $\sigma^2_{C_3} = \sigma^2_{C_1}$, and $\sigma^2_{C_2} = \sigma^2_{C_4} = 2\sigma^2_{\tau_{AR}}(1+\beta_{AR}) + \sigma^2_w$. It is easy to see that C_1, C_2, C_3 and C_4 are independent of each other, and we have

$$\begin{aligned}\Delta\tau_{AR} &= C_1C_2 + C_3C_4\\ &= \underbrace{\sqrt{4\sigma^4_{\tau_{AR}}(1-\beta^2_{AR}) + 4\sigma^2_{\tau_{AR}}\sigma^2_w + \sigma^4_w}}_{\eta_{AR}}\\ &\quad \times \left(\frac{C_1}{\sigma_{C_1}}\frac{C_2}{\sigma_{C_2}} + \frac{C_3}{\sigma_{C_3}}\frac{C_4}{\sigma_{C_4}}\right) \end{aligned} \tag{44}$$

According to [50, eq. (2.2.13)], $\Delta\tau_{AR}$ follows the Laplace distribution, that is,

$$\Delta\tau_{AR} \sim Laplace(0, \eta_{AR}). \tag{45}$$

After a similar derivation, we can know that $\Delta\tau_{RB}$ also follows the Laplace distribution

$$\Delta\tau_{RB} \sim Laplace(0, \eta_{RB}). \tag{46}$$

According to [50, Eq.(2.3.23)], the probability density function (PDF) of the sum of two independent Laplace distributed random variables $\Delta\tau_{AR}$ and $\Delta\tau_{RB}$ can be determined as

$$f_{\Delta\tau_{AB}}(x) = 1 + \frac{1}{1-\frac{\eta^2_{AR}}{\eta^2_{RB}}}\left(\frac{\eta^2_{AR}}{\eta^2_{RB}}e^{-\frac{x}{\eta_{AR}}} - e^{-\frac{x}{\eta_{RB}}}\right). \tag{47}$$

After a simple mathematical derivation, we can obtain the CDF of $|\Delta\tau_{A,A}|$ as

$$F_{|\Delta\tau_{A,A}|}(x) = 1 + \frac{1}{1-(\frac{\eta_{AR}}{\eta_{RB}})^2}\left(\frac{\eta^2_{AR}}{\eta^2_{RB}}e^{-\frac{x}{\eta_{AR}}} - e^{-\frac{x}{\eta_{RB}}}\right). \tag{48}$$

$$\begin{aligned}\Delta\tau_{AR} &= (\hat{\tau}^{(1)}_{k_{AR}}(t))^2 + (\hat{\tau}^{(2)}_{k_{AR}}(t))^2 - (\hat{\tau}^{(1)}_{k_{AR}}(t-1))^2 - (\hat{\tau}^{(2)}_{k_{AR}}(t-1))^2 \\ &= \underbrace{(\hat{\tau}^{(1)}_{k_{AR}}(t) - \hat{\tau}^{(1)}_{k_{AR}}(t-1))}_{C_1}\underbrace{(\hat{\tau}^{(1)}_{k_{AR}}(t) + \hat{\tau}^{(1)}_{k_{AR}}(t-1))}_{C_2} + \underbrace{(\hat{\tau}^{(2)}_{k_{AR}}(t) - \hat{\tau}^{(2)}_{k_{AR}}(t-1))}_{C_3}\underbrace{(\hat{\tau}^{(2)}_{k_{AR}}(t) + \hat{\tau}^{(2)}_{k_{AR}}(t-1))}_{C_4}. \end{aligned} \tag{42}$$

Based on (19), the probability that Q_τ outputs 1 under H_0, can be determined as

$$\begin{aligned}P_{\tau,H_0} &\triangleq \mathbf{Pr}(Q_\tau[|\hat{\tau}_{k_{AB}}(t) - \hat{\tau}_{k_{AB}}(t-1)|] = 1 \mid H_0) \\ &= \mathbf{Pr}(|\Delta\tau_{A,A}| > \delta_\tau) \\ &= 1 - \mathbf{Pr}(|\Delta\tau_{A,A}| \le \delta_\tau). \end{aligned} \tag{49}$$

Substituting (48) into (49), we can obtain (28).

APPENDIX B
PROOF OF LEMMA 4

Let $\Delta_{h_{E,A}}$ represent the difference between $\hat{h}_{n_{EB}}(t)$ and $\hat{h}_{n_{AB}}(t-1)$. Combining (14) and (24), $\Delta_{h_{E,A}}$ is determined as

$$\begin{aligned}\Delta_{h_{E,A}} &\triangleq \hat{h}_{n_{EB}}(t) - \hat{h}_{n_{AB}}(t-1) \\ &= \alpha_{RB} h_{n_{ER}}(t) h_{n_{RB}}(t-1) \\ &\quad + h_{n_{ER}}(t)\sqrt{1-\alpha^2_{RB}}u_{n_{RB}}(t-1) \\ &\quad - h_{n_{AR}}(t-1)h_{n_{RB}}(t-1) \\ &\quad + w_h(t) - w_h(t-1). \end{aligned} \tag{50}$$

For a given $h_{n_{RB}}(t-1)$, $\Delta_{h_{E,A}}$ is a complex Gaussian distributed random variable with zero mean and variance $\sigma^2_{\Delta h_{E,A}} = (\alpha^2_{RB}\sigma^2_{h_{ER}} + \sigma^2_{h_{AR}})|h_{n_{RB}}(t-1)|^2 + (1-\alpha^2_{RB})\sigma^2_{h_{ER}}\sigma^2_{h_{RB}} + 2\sigma^2_w$. Then, the CDF of $|\Delta h_{E,A}|^2$ can be derived as

$$F_{|\Delta h_{E,A}|^2}(x) = 1 - \exp\left(-\frac{x}{\sigma^2_{\Delta h_{E,A}}}\right). \tag{51}$$

Based on (18), P_{h,H_1} can be evaluated as

$$\begin{aligned}P_{h,H_1} &\triangleq \mathbf{Pr}(Q_h[|\hat{h}_{n_{EB}}(t) - \hat{h}_{n_{AB}}(t-1)|^2] = 1 \mid H_1) \\ &= 1 - \mathbf{Pr}(|\Delta h_{E,A}|^2 \le \delta_h). \end{aligned} \tag{52}$$

Substituting (51) into (52), we can get (34).

APPENDIX C
PROOF OF LEMMA 5

Let $\Delta\tau_{E,A} = \hat{\tau}_{k_{EB}}(t) - \hat{\tau}_{k_{AB}}(t-1)$ and $\Delta\tau_{EA} = \hat{\tau}_{k_{ER}}(t) - \hat{\tau}_{k_{AR}}(t-1)$, and then we have $\Delta\tau_{E,A} \triangleq \Delta\tau_{EA} + \Delta\tau_{RB}$. Based on (16), $\Delta\tau_{EA}$ can be further written as

$$\begin{aligned}\Delta\tau_{EA} \triangleq\ & (\hat{\tau}^{(1)}_{k_{ER}}(t))^2 + (\hat{\tau}^{(2)}_{k_{ER}}(t))^2 \\ & - (\hat{\tau}^{(1)}_{k_{AR}}(t-1))^2 - (\hat{\tau}^{(2)}_{k_{AR}}(t-1))^2. \end{aligned} \tag{53}$$

Similar to the derivation of (45), we know that $\Delta\tau_{EA}$ is also a Laplace distributed random variable [50], that is,

$$\Delta\tau_{EA} \sim Laplace(0, \eta_{EA}). \tag{54}$$

Similarly, we can derive the PDF of the sum of two independent Laplace distributed random variables $\Delta\tau_{EA}$ and $\Delta\tau_{RB}$ by applying [50, eq. (2.3.23)]. Thus, we have

$$\begin{aligned}&f_{\Delta\tau_{E,A}}(x) \\ &= 1 + \frac{1}{\left(1 - \frac{\eta^2_{EA}}{\eta^2_{RB}}\right)}\left(\frac{\eta^2_{EA}}{\eta^2_{RB}}e^{-\frac{x}{\eta_{EA}}} - e^{-\frac{x}{\eta_{RB}}}\right). \end{aligned} \tag{55}$$

The CDF of $|\Delta\tau_{E,A}|$ can be given by

$$F_{|\Delta\tau_{E,A}|}(x) = 1 + \frac{1}{\left(1 - \frac{\eta^2_{EA}}{\eta^2_{RB}}\right)}\left(\frac{\eta^2_{EA}}{\eta^2_{RB}}e^{-\frac{x}{\eta_{EA}}} - e^{-\frac{x}{\eta_{RB}}}\right). \tag{56}$$

According to (19), the probability that Q_τ outputs 1 under H_1 can be given by

$$\begin{aligned}P_{\tau,H_1} &\triangleq \mathbf{Pr}(Q_\tau[|\hat{\tau}_{k_{EB}}(t) - \hat{\tau}_{k_{AB}}(t-1)|] = 1 \mid H_1) \\ &= 1 - \mathbf{Pr}(|\Delta\tau_{EB}| \le \delta_\tau). \end{aligned} \tag{57}$$

Finally, substituting (56) into (57) yields (36).

REFERENCES

[1] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.
[2] Y. Shen, T. Zhang, Y. Wang, H. Wang, and X. Jiang, "Microthings: A generic IoT architecture for flexible data aggregation and scalable service cooperation," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 86–93, Sep. 2017.
[3] X. Deng and Y. Yang, "Online adaptive compression in delay sensitive wireless sensor networks," *IEEE Trans. Comput.*, vol. 61, no. 10, pp. 1429–1442, Oct. 2012.
[4] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.
[5] S. V. Kartalopoulos, "A primer on cryptography in communications," *IEEE Commun. Mag.*, vol. 44, no. 4, pp. 146–151, Apr. 2006.
[6] C. Paar, J. Pelzl, and B. Preneel, *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer, 2010.
[7] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: An overview," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 855–873, 2nd Quart., 2017.
[8] J. G. Andrews *et al.*, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, Jun. 2014.
[9] A. C. Polak and D. L. Goeckel, "Identification of wireless devices of users who actively fake their RF fingerprints with artificial data distortion," *IEEE Tran. Wireless Commun.*, vol. 14, no. 11, pp. 5889–5899, Nov. 2015.
[10] W. Hou, X. Wang, J.-Y. 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, May 2014.
[11] 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. 2091–2106, Sep. 2016.
[12] C. Zhao, M. Huang, L. Huang, X. Du, and M. Guizani, "A robust authentication scheme based on physical-layer phase noise fingerprint for emerging wireless networks," *Comput. Netw.*, vol. 128, no. 9, pp. 164–171, Dec. 2017.

[13] P. L. Yu, J. S. Baras, and B. M. Sadler, "Physical-layer authentication," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 1, pp. 38–51, Mar. 2008.
[14] G. Verma, P. Yu, and B. M. Sadler, "Physical layer authentication via fingerprint embedding using software-defined radios," *IEEE Access*, vol. 3, pp. 81–88, 2015.
[15] J. B. Perazzone, P. L. Yu, B. M. Sadler, and R. S. Blum, "Cryptographic side-channel signaling and authentication via fingerprint embedding," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 9, pp. 2216–2225, Sep. 2018.
[16] N. Xie and S. Zhang, "Blind authentication at the physical layer under time-varying fading channels," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 7, pp. 1465–1479, Jul. 2018.
[17] Y. Zheng, S. S. Dhabu, and C.-H. Chang, "Securing IoT monitoring device using PUF and physical layer authentication," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2018, pp. 1–5.
[18] W. C. Jakes and D. C. Cox, *Microwave Mobile Communications*. Hoboken, NJ, USA: Wiley, 1994.
[19] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2571–2579, Jul. 2008.
[20] 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, Dec. 2009.
[21] 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, Jun. 2016.
[22] 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, Mar. 2017.
[23] X. He and A. Yener, "End-to-end secure multi-hop communication with untrusted relays," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 1–11, Jan. 2013.
[24] S. Vatedka, N. Kashyap, and A. Thangaraj, "Secure compute-and-forward in a bidirectional relay," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2531–2556, May 2015.
[25] Q. Liu and G. Gong, "Physical layer secure information exchange protocol for mimo ad hoc networks against passive attacks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2016, pp. 1–6.
[26] P. Zhang and X. Jiang, "Channel-based authentication for dual-hop wireless networks," in *Proc. Int. Conf. Netw. Netw. Appl. (NaNA)*, Oct. 2018, pp. 42–46.
[27] H. Liu, Y. Wang, J. Liu, J. Yang, Y. Chen, and H. V. Poor, "Authenticating users through fine-grained channel information," *IEEE Trans. Mobile Comput.*, vol. 17, no. 2, pp. 251–264, Feb. 2018.
[28] D. Shan, K. Zeng, W. Xiang, P. Richardson, and Y. Dong, "PHY-CRAM: Physical layer challenge-response authentication mechanism for wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1817–1827, Sep. 2013.
[29] U. M. Maurer, "Authentication theory and hypothesis testing," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1350–1356, Jul. 2000.
[30] J. K. Tugnait and H. Kim, "A channel-based hypothesis testing approach to enhance user authentication in wireless networks," in *Proc. 2nd Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Jan. 2010, pp. 1–9.
[31] Y. Zhang, Y. Shen, X. Jiang, and S. Kasahara, "Mode selection and spectrum partition for D2D inband communications: A physical layer security perspective," *IEEE Trans. Commun.*, vol. 67, no. 1, pp. 623–638, Jan. 2019.
[32] M. Uysal, "Diversity analysis of space-time coding in cascaded Rayleigh fading channels," *IEEE Commun. Lett.*, vol. 10, no. 3, pp. 165–167, Mar. 2006.
[33] M. R. Avendi and H. H. Nguyen, "Performance of selection combining for differential amplify-and-forward relaying over time-varying channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 8, pp. 4156–4166, Aug. 2014.
[34] C. Komninakis, C. Fragouli, A. H. Sayed, and R. D. Wesel, "Multi-input multi-output fading channel tracking and equalization using Kalman estimation," *IEEE Trans. Signal Process.*, vol. 50, no. 5, pp. 1065–1076, May 2002.
[35] Y. S. Cho, J. Kim, W. Y. Yang, and C. G. Kang, *MIMO-OFDM wireless communications with MATLAB*. Hoboken, NJ, USA: Wiley, 2010.
[36] T. G. Manickam, R. J. Vaccaro, and D. W. Tufts, "A least-squares algorithm for multipath time-delay estimation," *IEEE Trans. Signal Process.*, vol. 42, no. 11, pp. 3229–3233, Nov. 1994.
[37] M. C. Vanderveen, A.-J. van der Veen, and A. Paulraj, "Estimation of multipath parameters in wireless communications," *IEEE Trans. Signal Process.*, vol. 46, no. 3, pp. 682–690, Mar. 1998.
[38] F. X. Ge, D. Shen, Y. Peng, and V. O. K. Li, "Super-resolution time delay estimation in multipath environments," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 54, no. 9, pp. 1977–1986, Sep. 2007.
[39] C. S. Patel and G. L. Stuber, "Channel estimation for amplify and forward relay based cooperation diversity systems," *IEEE Trans. Wireless Commun.*, vol. 6, no. 6, pp. 2348–2356, Jun. 2007.
[40] F. Gao, T. Cui, and A. Nallanathan, "On channel estimation and optimal training design for amplify and forward relay networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 5, pp. 1907–1916, May 2008.
[41] C. Wang, H.-M. Wang, and X.-G. Xia, "Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 589–605, Feb. 2015.
[42] E. Everett, A. Sahai, and A. Sabharwal, "Passive self-interference suppression for full-duplex infrastructure nodes," *IEEE Trans. Wireless Commun.*, vol. 13, no. 2, pp. 680–694, Jan. 2014.
[43] F. Zhu, F. Gao, T. Zhang, K. Sun, and M. Yao, "Physical-layer security for full duplex communications with self-interference mitigation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 329–340, Jan. 2016.
[44] J.-B. Kim, J. Lim, and J. M. Cioffi, "Capacity scaling and diversity order for secure cooperative relaying with untrustworthy relays," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 3866–3876, Jul. 2015.
[45] M. R. Avendi and H. H. Nguyen, "Performance of differential amplify-and-forward relaying in multinode wireless communications," *IEEE Trans. Veh. Technol.*, vol. 62, no. 8, pp. 3603–3613, Oct. 2013.
[46] N. O'Donoughue and J. M. F. Moura, "On the product of independent complex gaussians," *IEEE Trans. Signal Process.*, vol. 60, no. 3, pp. 1050–1063, Mar. 2012.
[47] *Baesd-MATLAB Simulator for E2E PLA for Dual-Hop Wireless Networks*. [Online]. Available: https://github.com/zpcanson/E2E-PLA-simulation
[48] Y. R. Zheng and C. Xiao, "Simulation models with correct statistical properties for Rayleigh fading channels," *IEEE Trans. Commun.*, vol. 51, no. 6, pp. 920–928, Jun. 2003.
[49] 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, Jul. 2012.
[50] S. Kotz, T. Kozubowski, and K. Podgorski, *The Laplace Distribution and Generalizations: A Revisit with Applications to Communications, Economics, Engineering, and Finance*. Springer, 2012.

PINCHANG ZHANG received the B.S. degree in electronic information engineering from Wuyi University, China, in 2009, and the M.S. degree in electronic and communication engineering from the Kunming University of Science and Technology, China, in 2012. He is currently pursuing the Ph.D. degree with Future University Hakodate, Hakodate, Japan. From 2012 to 2017, he was with Chuzhou University, China. His research interests include wireless security, physical layer authentication, and location spoofing detection.

JINXIAO ZHU received the B.S. and M.E. degrees in software engineering from Xidian University, China, in 2008 and 2011, respectively, and the Ph.D. degree in systems information science from Future University Hakodate, Japan, in 2014, where she was a Postdoctoral Researcher, from 2014 to 2015. From 2015 to 2017, she was a Researcher with the National Institute of Information and Communications Technology (NICT), Japan. Since 2018, she has been an Assistant Professor with the Faculty of Information Networking for Innovation and Design, Toyo University, Japan. Her research interests include information-theoretic security for wireless communications and performance evaluation of wireless networks.

YIN CHEN received the B.S. and M.S. degrees in computer science from Xidian University, China, in 2008 and 2011, respectively, and the Ph.D. degree in systems information science from Future University Hakodate, Japan, in 2014, where he was a Postdoctoral Researcher, in 2014. He is currently a Research Assistant Professor with the Graduate School of Media and Governance, Keio University. He is a member of IEEE, ACM, and IPSJ. His research interest includes the wide area of wireless communication and networks and their applications in the Internet of Things and smart cities.

XIAOHONG JIANG (M'03–SM'08) received the B.S., M.S., and Ph.D. degrees from Xidian University, China, in 1989, 1992, and 1999, respectively. Before joining Future University, he was an Associate Professor with Tohoku University, from 2005 to 2010. He is currently a Full Professor with Future University Hakodate, Japan. He has published over 300 technical papers at premium international journals and conferences, which include over 70 papers published in top IEEE journals and top IEEE conferences, such as the IEEE/ACM TRANSACTIONS ON NETWORKING, the IEEE JOURNAL OF SELECTED AREAS ON COMMUNICATIONS, the IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, and the IEEE INFOCOM. His research interests include computer communications networks, mainly wireless networks and optical networks, network security, and routers/switches design. He is a member of IEICE. He was a recipient of the Best Paper Award from the IEEE HPCC 2014, the IEEE WCNC 2012, the IEEE WCNC 2008, the IEEE ICC 2005-Optical Networking Symposium, and the IEEE/IEICE HPSR 2002.