Utilizing Multi-Dimensional MmWave MIMO Channel Features for Location Verification

Pinchang Zhang 1, Yangyang Liu 2 and Ji He 2,*

1 School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China
2 School of Computer Science, Xidian University, Xi’an 710071, China
* Correspondence: jihe@xidian.edu.cn

Abstract: In this paper, we address the problem of authenticating transmitters in millimeter-wave (mmWave) multiple-input multiple-output (MIMO) communication systems, and propose a location verification scheme based on multi-dimensional mmWave MIMO channel features. In particular, we first examine the mmWave MIMO channel features in terms of azimuth angle of arrival (AAoA), elevation angle of arrival (E AoA), and path gain, and then extract these fine-grained channel features through the maximum-likelihood (ML) estimation method. Based on the extracted feature parameters, authentication validation is cast in the framework of hypothesis testing theory. We also derive the analytical expressions for the typical false alarm and detection rates by using the likelihood ratio test and thus the statistical performance is analytically established. Finally, extensive numerical results are provided to demonstrate the performance of the proposed authentication scheme.

Keywords: location verification; physical layer authentication; millimeter-wave (mmWave) communications; multiple-input multiple-output (MIMO); channel features

1. Introduction

Millimeter-wave (mmWave) multiple-input multiple-output (MIMO) systems serve as a critical technique for 5G (fifth-generation communication) and beyond wireless communication networks. The mmWave MIMO technique can lead to a significant increase in data rates, wide bandwidth, and higher spectrum efficiency. By integrating huge antenna arrays, 5G and beyond communication systems operating from 30 to 300 GHz can support huge connections among a bulk of smart devices, contributing to various applications such as the Industrial Internet of Things (IIoT) and the Internet of Vehicles (IoV).

However, mmWave MIMO communication systems may become subject to malicious attacks because of the above important applications they can support. Moreover, the mmWave wireless communication medium is open in space and thus attackers can easily access the communication network and obtain the transferred information between legitimate users and base stations. One of the main threats in mmWave MIMO systems is identity-based spoofing attack, where an attacker eavesdrops the legitimate communication links and further impersonates a legitimate transmitter to inject harmful signals into the communication network. To tackle the spoofing attacks in mmWave systems, identity authentication presents a promising solution to secure mmWave MIMO communication systems.

We note that the existing authentication schemes can be roughly divided into higher layer and physical layer authentication schemes. The higher layer authentication schemes are mainly dependent on secret keys and encryption/decryption algorithms to validate transmitter identities [1–3]. Meanwhile, the physical layer authentication schemes verify transmitter identities through physical layer features [4]. It is noted that the higher layer authentication may not completely adapt to the emerging mmWave MIMO systems which include distributed, dynamic and highly heterogeneous devices. Such mmWave MIMO systems may not support the cryptographic key distribution and management, high consumption of communication and computation resources in higher layer authentication.
schemes. As a complement and an enhancement of the higher layer authentication, physical layer authentication possesses several characteristics such as high security, low complexity and high compatibility [5]. Thus, in this paper we focus on physical layer authentication in mmWave MIMO systems.

Existing physical layer authentication schemes mainly include channel-based authentication and hardware-impairment-based authentication. The hardware-impairment-based method authenticates the legitimacy of a transmitter identity by extracting specific non-ideal hardware parameters from received signals. In contrast, channel-based authentication utilizes the fact that wireless channels decorrelate rapidly as the source (e.g., a transmitter or user using transmitter is transmitting signals to an intended destination/receiver) changes location in an environment with rich scatterers and reflectors. In fact, channel-based authentication verifies the location of the current transmitter rather than transmitter physics identity, and hence is referred to as location verification. There exists some research works on physical layer authentication for mmWave systems [6–15]. In [6], the authors propose a physical layer authentication scheme by using sparse mmWave channel. A power allocation technique for the precoder and the authentication tag is first developed for fingerprint-based authentication in a multi-user mmWave UAV network [7]. Multipath time delay caused by planar specular reflectors is acquired to illustrate the authenticity of user position 5G mmWave communication with planar reflectors [8]. The intrinsic physical attributes for 5G communications are analyzed for physical layer authentication in detail and the future possible directions for the exploitation of physical attributes is demonstrated in [9]. The authors in [10] further study the physical characteristics of 5G IoT in various application scenarios and describe the possible security threats resulting from the 5G IoT physical layer. Based on virtual angles of arrival in mmWave systems and machine learning methods, the authors in [11] propose a physical layer authentication scheme to detection spoofing attacks. Two effective pilot contamination attack detection approaches are proposed for power non-orthogonal multiple access in massive MIMO 5G communications, based on the sparseness and statistics of mmWave virtual channels [12]. Following this line, the authors in [13] present a new physical layer countermeasure using channel virtual representation to defend against pilot contamination attack. In [14], unique beam pattern features are utilized to achieve physical layer spoofing attack detection and the detection problem is cast as a machine learning classification through the sector level sweep (SLS) process. The authors in [15] develop a physical layer authentication scheme by using signal-to-noise ratio (SNR) trace features to detect spoofing attacks in mmWave systems.

Frequency-selective Rayleigh channel time variations are used to detect spoofing attacks in wireless networks, considering the channel estimation errors [16]. To improve the spoofing detection accuracy, a logistic regression-based authentication approach is developed without the requirements of the known channel model [17]. The authors jointly use multipath delay and channel gain characteristics of the channel impulse response to achieve performance improvement of physical layer authentication [18]. The above existing approaches demonstrate the uniqueness and usability of physical layer features for spoofing attack detection and authentication. It is noted that the above existing approaches are developed for spoofing detection by conventional channel state information. These approaches cannot be extended directly to mmWave MIMO communication systems because it is difficult for them to sufficiently excavate fine-grained physical layer characteristics from mmWave MIMO channels. Hardware-impairment-based authentication generally needs to employ high-precision hardware equipment for hardware feature extraction and bears high computational complexity [14,15]. Moreover, machine-learning-based authentication framework requires an expensive training stage with a large amount of training data, which might be unrealistic in practice. In addition, the analytic establishment of statistical performances still remains an open problem in machine-learning-based authentication frameworks. To this end, we explore the exploitation of multi-dimensional mmWave MIMO channel features to design a new location verification scheme for mmWave MIMO communication systems. These channel features include azimuth angle of arrival (AAoA),
elevation angle of arrival (EAoA) and path gain, which are jointly used to validate the legitimacy of transmitters and to improve the authentication performance. The main difference between the schemes proposed in this paper and those in previous works [16–18] is that the previous approaches mainly focus on channel statistics in the time domain while this paper extracts channel features in the time domain as well as the angle domain. In addition, the scheme proposed in this paper attempts to explore the exploitation of multi-dimensional mmWave MIMO channel features to achieve location verification.

The main contributions of this paper are summarized as follows:

- By exploiting multi-dimensional mmWave MIMO channel features in both the time domain and angle domain, we develop a new location verification scheme to achieve validation of a transmitter location for mmWave MIMO communication systems.
- To determine estimation error variances of channel features in terms of AAoA, EAoA, and path gain, we estimate the mmWave MIMO channels based on maximum-likelihood estimation theory. To analytically evaluate the performance of our proposed location verification scheme, we derive the typical two performance metrics and the statistical performance is analytically established.
- Extensive numerical results are provided to demonstrate that the proposed scheme achieves desired performance. Numerical results are used to further show how the system parameters can affect the statistical performance.

The remainder of this paper is organized as follows. Section 2 introduces the concerned system model and problem formulation. Sections 3 and 4 present the proposed location verification scheme and performance analysis, respectively. Section 5 shows the numerical results and performance evaluation. Finally, Section 6 concludes this paper.

Notation: $(\cdot)^H$, $(\cdot)^T$, $(\cdot)^{*}$, $(\cdot)^{-1}$, $(\cdot)^\dagger$ denote the conjugate-transpose, transpose, conjugate, inverse and pseudo-inverse of a matrix, respectively. The $(m, n)$-th element of a matrix $H$ is $H_{m,n}$. $	ext{diag}(a_1, ..., a_N)$ is a diagonal matrix with $a_1, ..., a_N$ on the main diagonal. $	ext{vec}(H)$ is the vectorization of matrix $H$. $	ext{tr}(\cdot)$ and $\hat{\cdot}$ represent the matrix trace function and definitions, respectively. $\mathbb{E}\{\cdot\}$ represents the expectation operator. $\|\cdot\|_2$ is the Euclidean norm operator. A Gaussian random variable $x$ with mean $\mu$ and variance $\sigma^2$ can be represented by $x \sim \mathcal{N}(\mu, \sigma^2)$. If let $\langle X \rangle$ be the subspace spanned by the columns of matrix $X$, then $P_X$ denotes the orthogonal projection matrix onto $\langle X \rangle$, that is, $P_X = X(X^H X)^{-1}X^H$.

2. Problem Formulation and System Model

2.1. Problem Formulation

Similar to previous works [16–18], we also use a three-entity model including a legitimate transmitter (Alice), a malicious attacker (Eve) and a legitimate base station (Bob), where Alice and Eve are both equipped with a single antenna and Bob is equipped with $N_t$ antennas, as shown in Figure 1. Eve intends to spoof Bob by using the identity of Alice and thus may launch some more advanced attacks, such as a man-in-the-middle attack and session hijacking attack while Alice communicates with Bob.

![Figure 1. System model.](image-url)
Suppose Alice transmits one data frame to Bob at time $t - 1$ and this data frame was validated by cryptography-based higher layer authentication approaches. In this process, Bob measures and stores physical layer features information, e.g., mmWave MIMO channel features, with the help of signal estimation techniques. Subsequently, at time $t$, an unknown transmitter (either Alice or Eve) sends another data frame to Bob and Bob needs to validate the data frame origin (i.e., the current transmitter identity) to avoid impersonation attack.

Eve has data frame structure information by probing the transmitted signals between Alice and Bob and some publicly known information (e.g., training sequences and pilot signals). The estimation techniques and authentication schemes that Bob utilizes cannot be known by the attacker, Eve. Further, we exploit the carrier sense multiple access/collision detection protocol.

### 2.2. Channel Model

Bob has a $N_r$-antenna uniform planar array (UPA) where the numbers of antennas in the horizon and vertical directions are $M$ and $N$, respectively, where $N_r = MN$. The number of radio frequency chains of Bob is $M_{RF}[19]$. Let $d$ be the distance between any arbitrary two adjacent antennas, and $G_{RF}$ be the analog beamformer equipped at Bob. Considering the limited scattering characteristics of the mmWave communication environments, we here adopt the extended Saleh-Valenzuela (SV) model to characterize the mmWave MIMO channels [20,21]. Denote $\phi_l$ as the azimuth angle of arrival (AAoA) of the $l$-th propagation multipath of the transmitter and $\theta_l$ as the elevation angle of arrival (E AoA) of that, for $l = 1, 2, \cdots, L$, respectively. We assume $\phi_l \sim \mathcal{N}(0, \sigma_{\phi_l, XB}^2)$ and $\theta_l \sim \mathcal{N}(0, \sigma_{\theta_l, XB}^2)$. The steering matrix $A(\phi_l, \theta_l)$ is expressed by

$$A(\phi_l, \theta_l) = \frac{1}{\sqrt{MN}} \begin{bmatrix}
1 & \cdots & e^{j2\pi d/\lambda(N-1)} \sin \phi_l \cos \theta_l \\
\vdots & \ddots & \vdots \\
e^{j2\pi d/\lambda(M-1)} \cos \phi_l & \cdots & e^{j2\pi d/\lambda((M-1) \cos \phi_l + (N-1) \sin \phi_l \cos \theta_l)}
\end{bmatrix},$$

(1)

where $\lambda$ is the wavelength of the carrier signal [22]. For simplicity, let $v_{1,l} = \frac{2\pi d}{\lambda} \cos \phi_l$ and $v_{2,l} = \frac{2\pi d}{\lambda} \sin \phi_l \cos \theta_l$. The steering matrix $A(\phi_l, \theta_l)$ can be further written as

$$A(\phi_l, \theta_l) = A(v_{1,l}, v_{2,l}) = a(v_{1,l})^T(v_{2,l}),$$

(2)

where $a(v_{1,l}) = \frac{1}{\sqrt{M}} [1, \cdots, e^{j((M-1)v_{1,l})}]^T$ and $a(v_{2,l}) = \frac{1}{\sqrt{N}} [1, \cdots, e^{j((N-1)v_{2,l})}]^T$.

Similar to [23], the mmWave channel with $L$ being the number of propagation paths is modeled as

$$H = \frac{1}{\sqrt{L}} \sum_{l=1}^{L} a_l A(\phi_l, \theta_l) = \frac{1}{\sqrt{L}} \sum_{l=1}^{L} a_l a(v_{1,l})^T(v_{2,l}) = \frac{1}{\sqrt{L}} A_{v_l} H_a A_{v_l}^T,$$

(3)

where $A_{v_l} = [a(v_{1,1}), a(v_{2,1}), \cdots, a(v_{1,L})], \ A_{v_2} = [a(v_{2,1}), a(v_{2,2}), \cdots, a(v_{2,L})], \ H_a = \text{diag}(\alpha_1, \alpha_2, \cdots, \alpha_L)$ and $a_l \sim \mathcal{CN}(0, \sigma_{a_l, XB}^2)$ is the path gain of the $l$-th propagation path [22,24,25].

The $(m, n)$-th element $(m = 0, 1, \cdots, M - 1$ and $n = 0, 1, \cdots, N - 1)$ for matrix $H$ is

$$H_{m,n} = \frac{1}{\sqrt{LMN}} \sum_{l=1}^{L} a_l e^{j(mv_{1,l} + nv_{2,l})}.$$

(4)

Path gain is assumed to keep unchanged during one frame [26]. Based on [27], we use first-order Gauss–Markov process to model the time-varying path gain as

$$a_l(t) = \rho_a a_l(t - 1) + \sqrt{1 - \rho_a^2} u_a(t),$$

(5)
where $\rho_{\alpha}$ is the path gain correlation coefficient [28] and $u_{\alpha_l}(t)$ is zero-mean Gaussian noise, i.e., $u_{\alpha_l}(t) \sim CN(0, \sigma_{\alpha_l}^2)$. Similarly, we use first-order Gauss–Markov process to model the time-varying azimuth angle of arrival as

$$\phi_l(t) = \rho_{\phi}\phi_l(t-1) + \sqrt{1-\rho_{\phi}^2}u_{\phi_l}(t),$$

(6)

where $\rho_{\phi}$ is the AAoA correlation coefficient [28] and $u_{\phi_l}(t)$ is zero-mean Gaussian noise, i.e., $u_{\phi_l}(t) \sim N(0, \sigma_{\phi_l}^2)$. We also use first-order Gauss–Markov process to model the time-varying elevation angle of arrival as

$$\theta_l(t) = \rho_{\theta}\theta_l(t-1) + \sqrt{1-\rho_{\theta}^2}u_{\theta_l}(t),$$

(7)

where $\rho_{\theta}$ is the EAoA correlation coefficient [28] and $u_{\theta_l}(t)$ is zero-mean Gaussian noise, i.e., $u_{\theta_l}(t) \sim N(0, \sigma_{\theta_l}^2)$. Channel-based verification utilizes the fact that wireless channels decorrelate rapidly as the source (e.g., a transmitter or user using transmitter is transmitting signals to an intended destination/receiver) changes location in an environment with rich scatterers and reflectors. This indicates that wireless channel features are spatially decorrelated between different geographic locations. When the distance between a legitimate source and an adversary is greater than half of the wavelength, it is extremely difficult for the adversary to obtain the accurate wireless channel features. Although the channel-based method essentially authenticates the practical geographic location related to the inherent properties of channel features, it is an effective authentication to achieve legitimacy validation of the source identity. Therefore, this paper aims to design a new location verification scheme for validating data frame origin to resist against the impersonation attack.

2.3. Communication Model

The baseband signal received by Bob at time $t$ is written as

$$r(t) = G^H_{RB}\text{vec}(H_{XB}(t))s(t) + n(t),$$

(8)

where

- $s(t)$ is the transmitted signal at time $t$. The signal power is $p = \mathbb{E}\{|s(t)|^2\}$.
- $H_{XB}(t)$ denotes the channel matrix between transmitter $X$ (either Alice or Eve) and receiver Bob.
- $n(t)$ is a zero-mean complex additive white Gaussian noise (AWGN), i.e., $n(t) \sim CN(0, \sigma_n^2 I)$.

3. Proposed Location Verification Scheme

3.1. Estimation of MmWave Channels

To exploit the fine-grained mmWave channel features, we estimate the channel parameters separately. We first estimate AAoA and EAoA, and then estimate the mmWave path gain. We can write the estimations of $\hat{\phi}_{l, XB}(t)$, $\hat{\theta}_{l, XB}(t)$ and $\hat{\alpha}_{l, XB}(t)$, respectively, as

$$\hat{\phi}_{l, XB}(t) = \phi_{l, XB}(t) + \Delta\phi_l(t),$$

(9)

$$\hat{\theta}_{l, XB}(t) = \theta_{l, XB}(t) + \Delta\theta_l(t),$$

(10)

$$\hat{\alpha}_{l, XB}(t) = \alpha_{l, XB}(t) + \Delta\alpha_l(t),$$

(11)
where $\Delta \phi \sim \mathcal{N}(0, \sigma_{\Delta \phi}^2)$, $\Delta \theta \sim \mathcal{N}(0, \sigma_{\Delta \theta}^2)$ and $\Delta \alpha \sim \mathcal{CN}(0, \sigma_{\Delta \alpha}^2)$ are the corresponding estimation errors, respectively. Next, we calculate the variances of the estimation errors, i.e., $\sigma_{\Delta \phi}^2$, $\sigma_{\Delta \theta}^2$ and $\sigma_{\Delta \alpha}^2$.

For notational simplicity, here we ignore the time index $t$ and the path index $l$. The signal received by Bob at time $t$ is given by

$$
\mathbf{r} = \mathbf{G}_{RF}^H \mathbf{vec}(\mathbf{H}) s + \mathbf{n} = \mathbf{G}_{RF}^H \mathbf{vec}(\mathbf{A}) s + \mathbf{n},
$$

where $\mathbf{A}$ is the $M \times N$ steering matrix with its $(m,n)$-th element given by

$$
A_{mn} = \frac{1}{\sqrt{MN}} e^{j(\pi n_1 + \pi n_2)}.
$$

The conditional PDF of $\mathbf{r}$ is expressed by

$$
f(\mathbf{r}|v_1, v_2, \alpha) = \frac{1}{(\pi \sigma_n^2)^{MN}} \exp \left\{ -\frac{||\mathbf{r} - \mathbf{G}_{RF}^H \mathbf{vec}(\mathbf{A}) s||^2}{\sigma_n^2} \right\}.
$$

The maximum-likelihood (ML) method in [29] is used to estimate mmWave channel features $v_1$, $v_2$, and $\alpha$. The estimation of these features can be expressed as

$$
[v_1, v_2, \hat{\alpha}] = \arg \max_{v_1, v_2, \alpha} f(\mathbf{r}|v_1, v_2, \alpha).
$$

Based on (14) and (15), we can equivalently write (15) as

$$
[v_1, v_2, \hat{\alpha}] = \arg \min_{v_1, v_2, \alpha} ||\mathbf{r} - \mathbf{G}_{RF}^H \mathbf{vec}(\mathbf{A}) s||^2.
$$

When giving $v_1$ and $v_2$, the estimation of $\alpha$ is calculated as

$$
\hat{\alpha} = \mathbf{vec}(\mathbf{A})^H (\mathbf{G}_{RF}^H)^s^* \mathbf{r}.
$$

Substituting (17) into (16), the estimations of $v_1$ and $v_2$ is written as

$$
[v_1, v_2] = \arg \min_{v_1, v_2} ||\mathbf{r} - \mathbf{G}_{RF}^H \mathbf{vec}(\mathbf{A}) \mathbf{vec}(\mathbf{A})^H (\mathbf{G}_{RF}^H)^s^* \mathbf{r}||^2
$$

$$
= \arg \max_{v_1, v_2} g(v_1, v_2),
$$

where $g(v_1, v_2)$ is the cost function related to $v_1$ and $v_2$, $\sigma_n^2 = s^* s$ is the signal power and $\mathbf{P}_b = \mathbf{vec}(\mathbf{A})^H \mathbf{vec}(\mathbf{A})^H$.

Next, we give Lemma 1 regarding the variance of the estimations for $v_1$ and $v_2$.

**Lemma 1.** The variance of the estimations for $v_1$ and $v_2$ in (18) are given by

$$
\sigma_{\Delta v_k}^2 = \frac{\sigma_n^2}{2\sigma_n^2 |\mathbf{a}|^2 \mathbf{vec}(\mathbf{A})^H \mathbf{V}_k \mathbf{P}_b \mathbf{V}_k \mathbf{vec}(\mathbf{A})}, \quad k = 1, 2,
$$

where $\mathbf{P}_b = \mathbf{I} - \mathbf{P}_b$. $\mathbf{V}_1$ and $\mathbf{V}_2$ are the diagonal matrices given by

$$
\mathbf{V}_1 = \text{diag}(0, \ldots, 0, \ldots, (M - 1), \ldots, (M - 1), \ldots, 0, \ldots, 0).
$$

$$
\mathbf{V}_2 = \text{diag}(0, \ldots, 0, \ldots, (N - 1), \ldots, (N - 1), \ldots, 0, \ldots, 0).
$$
Proof. The received signal without noise can be written as
\[ r_s = G_R^H \cdot \text{vec}(A) \text{as}. \] (22)

When considering the receiver noise, the received signal can be further written as \( r = r_s + n \). By using Taylor series expansion, the first derivative of the cost function \( g(v_1, v_2) \) is given by
\[
\frac{\partial g(v_1, v_2)}{\partial v_k} \bigg|_{v_k = \hat{v}_k} \approx \frac{\partial g(v_1, v_2)}{\partial v_k} \bigg|_{v_k = \hat{v}_k} + \frac{\partial^2 g(v_1, v_2)}{\partial^2 v_k} \bigg|_{v_k = \hat{v}_k} \Delta v_k,
\] (23)
where \( \Delta v_k = \hat{v}_k - v_k \) denotes perturbation on \( v_k \).

Setting (23) equal to zero, \( \Delta v_k \) is given by
\[
\Delta v_k = -\frac{\frac{\partial g(v_1, v_2)}{\partial v_k}}{\frac{\partial^2 g(v_1, v_2)}{\partial^2 v_k}} \bigg|_{v_k = \hat{v}_k} = \frac{g'(v_1, v_2 | v_k)}{g'(v_1, v_2 | v_k)}',
\] (24)
where \( g'(v_1, v_2 | v_k) \) and \( g'(v_1, v_2 | v_k) \) are the first- and second-order derivatives of the cost function \( g(v_1, v_2) \) conditioned on \( v_k \), respectively.

\( g'(v_1, v_2 | v_k) \) is expressed as
\[
g'(v_1, v_2 | v_k) = j r^H G_R^H V_k P_b^† (G_R^H)^† r - j r^H G_R^H V_k P_b^† V_k (G_R^H)^† r. \] (25)

By substituting (22) into (25), \( g(v_1, v_2 | v_k) \) in (25) becomes
\[
g'(v_1, v_2 | v_k) = j r^H G_R^H V_k P_b^† (G_R^H)^† r + j (r_s + n)^H G_R^H V_k P_b^† W_e (G_R^H)^† r
= -23 \{ r_s^H G_R^H V_k P_b^† (G_R^H)^† r + 23 \{ (n^H G_R^H V_k P_b^† (G_R^H)^† n \}. \] (26)

Due to the independence between \( n \) and \( r_s \), we have
\[
E\{g(v_1, v_2 | v_k)\} = -2 \sigma_n^2 \text{Im}\{\text{tr}(G_R^H V_k P_b^† (G_R^H)^†)\} = 0. \] (27)

The second-order conditional derivative \( g(v_1, v_2 | v_k) \) with respect to \( v_k \) is written as
\[
g''(v_1, v_2 | v_k) = -r^H G_R^H V_k P_b^† (G_R^H)^† r + r^H G_R^H V_k P_b^† V_k (G_R^H)^† r
+ r^H G_R^H V_k P_b^† V_k (G_R^H)^† r - n^H G_R^H V_k P_b^† V_k (G_R^H)^† r. \] (28)

Similarly, \( E\{g(v_1, v_2 | v_k)\} \) is calculated as
\[
E\{g(v_1, v_2 | v_k)\} = 2 \sigma_n^2 \text{Im}\{\text{tr}(A H V_k P_b^† V_k (G_R^H)^†)\} + 2 \text{Im}\{\text{tr}(V_k P_b^† V_k (G_R^H)^†)\}
= 2 \sigma_n^2 |\text{vec}(A)|^H V_k P_b^† V_k \text{vec}(A). \] (29)

Based on (28) and (29), \( g(v_1, v_2 | v_k) \) is further written as
\[
g'(v_1, v_2 | v_k) = E\{g(v_1, v_2 | v_k)\} + f_2(n) + f_2(n^2),
\] (30)
where \( f_2(n) \) and \( f_2(n^2) \) represent the linear and quadrature functions of \( n \) in \( g(v_1, v_2 | v_k) \), respectively. \( g'(v_1, v_2 | v_k) \) can be written as
\[
g'(v_1, v_2 | v_k) = f_1(n) + f_1(n^2), \] (31)
where \( f_1(n) \) and \( f_1(n^2) \) are the linear and quadrature functions of \( n \) in \( g(v_1, v_2 | v_k) \), respectively.
Substituting (30) and (31) into (24), $\Delta v_k$ in (24) can be rewritten as

$$\Delta v_k = - \frac{f_1(n) + f_1(n^2)}{E\{g(v_1,v_2|v_k)\} + f_2(n) + f_2(n^2)}$$

$$= - \frac{f_1(n) + f_1(n^2)}{E\{g(v_1,v_2|v_k)\}} \left( 1 - \frac{f_2(n) + f_2(n^2)}{E\{g(v_1,v_2|v_k)\}} \right)^2 - \cdots$$

$$\approx - \frac{f_1(n) + f_1(n^2)}{E\{g(v_1,v_2|v_k)\}} = - \frac{g(v_1,v_2|v_k)}{E\{g(v_1,v_2|v_k)\}}. \quad (32)$$

$c_{\Delta v_k}$ is expressed by

$$c_{\Delta v} = \frac{E\{g(v_1,v_2|v_k)\}}{E\{g(v_1,v_2|v_k)\}^2}, \quad (33)$$

where

$$E\{g(v_1,v_2|v_k)\} \approx 2\sigma_n^2\mathbf{g}_R^H\mathbf{v}_k\mathbf{p}_b^H\mathbf{v}_k(\mathbf{g}_R^H)^\dagger \mathbf{r}_k = 2\sigma_n^2\mathbf{v}_k^2|\mathbf{a}|^2 \text{vec} (\mathbf{A})^H \mathbf{v}_k \mathbf{p}_b^H \mathbf{v}_k \text{vec} (\mathbf{A}). \quad (34)$$

Substituting (27), (29) and (34) into (33) yields (19).

Using the formulations of $v_1$ and $v_2$ in Section 2.2, $\phi$ and $\theta$ are written, respectively, as

$$\phi = \cos^{-1}\left( \frac{\lambda v_1}{2\pi d} \right), \quad (35)$$

$$\theta = \cos^{-1}\left( \frac{\lambda v_2}{2\pi d \sin \phi} \right). \quad (36)$$

Based on (19), (35) and (36), $E\{\Delta \phi\} = E\{\Delta \theta\} = 0$, and $E\{\Delta \phi^2\}$ is expressed as

$$c_{\Delta \phi} = E\{(\hat{\phi} - \phi)(\hat{\phi} - \phi)^H\} = \left( \frac{1}{\pi d} \right)^2 \frac{\sigma_n^2}{2\sigma_n^2|\mathbf{a}|^2 \text{vec} (\mathbf{A})^H \mathbf{v}_1 \mathbf{p}_b^H \mathbf{v}_1 \text{vec} (\mathbf{A})}. \quad (37)$$

$$c_{\Delta \theta} = E\{(\hat{\theta} - \theta)(\hat{\theta} - \theta)^H\} = \left( \frac{\lambda v_2}{2\pi d \sin \phi} \right)^2 \frac{\sigma_n^2}{2\sigma_n^2|\mathbf{a}|^2 \text{vec} (\mathbf{A})^H \mathbf{v}_2 \mathbf{p}_b^H \mathbf{v}_2 \text{vec} (\mathbf{A})}. \quad (38)$$

Based on (17), $\hat{\alpha}$ is rewritten as

$$\hat{\alpha} = \text{vec} (\hat{\mathbf{A}})^H (\mathbf{G}_R^H)^\dagger s^* (\mathbf{G}_R^H)^\dagger \text{vec} (\mathbf{A}) \alpha^* + \mathbf{n}$$

$$= \sigma_n^2 \text{vec} (\hat{\mathbf{A}})^H \text{vec} (\mathbf{A}) \alpha + \text{vec} (\hat{\mathbf{A}})^H (\mathbf{G}_R^H)^\dagger s^* \mathbf{n}, \quad (39)$$

where $\text{vec} (\hat{\mathbf{A}})^H$ is calculated by the estimation of $(\hat{\mathbf{v}}_1, \hat{\mathbf{v}}_2)$. By using Taylor’s expansion, we approximate $\text{vec} (\hat{\mathbf{A}})^H$ as

$$\text{vec} (\hat{\mathbf{A}})^H \approx \text{vec} (\mathbf{A}) + j \text{vec} (\mathbf{A})^H \mathbf{v}_k \Delta v_k, \quad k = 1, 2. \quad (40)$$

Substituting (40) into (39), $\hat{\alpha}$ in (39) can be written as

$$\hat{\alpha} = \sigma_n^2 \left( \text{vec} (\mathbf{A})^H + j \text{vec} (\mathbf{A})^H \mathbf{v}_1 \Delta v_1 \right) \text{vec} (\mathbf{A}) \alpha + \text{vec} (\hat{\mathbf{A}})^H (\mathbf{G}_R^H)^\dagger s^* \mathbf{n}$$

$$= \alpha + j \text{vec} (\mathbf{A})^H \mathbf{v}_1 \text{vec} (\mathbf{A}) \Delta v_1 \alpha + \text{vec} (\hat{\mathbf{A}})^H (\mathbf{G}_R^H)^\dagger s^* \mathbf{n}. \quad (41)$$
Based on (19), the statistical characteristics of the estimation error of the mmWave path gain is calculated as

$$
\mu_{\Delta \alpha} = \mathbb{E}\{\Delta \alpha\} = \mathbb{E}\{\text{vec}(\mathbf{A})^H \mathbf{V}_1 \text{vec}(\mathbf{A}) \Delta v_1 \alpha + \text{vec}(\hat{\mathbf{A}})^H (\mathbf{G}_{RF}^H)^H z^* \mathbf{n}\} = 0,
$$

(42)

$$
c_{\Delta \alpha} = \mathbb{E}\{(\hat{\alpha} - \alpha)(\hat{\alpha} - \alpha)^H\} = \frac{\sigma_s^2 |\text{vec}(\mathbf{A})^H \mathbf{V}_1 \text{vec}(\mathbf{A})|^2}{2\sigma_v^2 \text{vec}(\mathbf{A})^H \mathbf{V}_1 \mathbf{F}_b^1 \mathbf{V}_1 \text{vec}(\mathbf{A})} + \sigma_n^2.
$$

(43)

### 3.2. Location Validation

The location validation is implemented by comparing the similarity between the current channel parameters and the previous ones with preset thresholds, based on a binary hypothesis test. If we denote the difference between the current channel parameters (i.e., $\phi, \alpha, \theta$) at successive time as $\Theta_\zeta$ for $\zeta \in \{\phi, \alpha, \theta\}$, then we have

$$
\Theta_\zeta = \sum_{l=1}^{L} |\hat{\zeta}_{l,AB}(t) - \hat{\zeta}_{l,AB}(t-1)|^2, \zeta \in \{\phi, \alpha, \theta\}.
$$

(44)

Let $\eta_\phi, \eta_\alpha$ and $\eta_\theta$ be preset thresholds for AAoA, EAoA and path gain, respectively. Next, we design a simple binary hypothesis testing for location validation as

$$
\begin{cases}
H_0: \Theta_\zeta \leq \eta_\zeta, & \zeta \in \{\phi, \alpha, \theta\}, \\
H_1: \Theta_\zeta > \eta_\zeta, & \zeta \in \{\phi, \alpha, \theta\},
\end{cases}
$$

(45)

Under $H_0$, the current transmitter is Alice. In contrast, $H_1$ means that the current transmitter is Eve.

The fundamental principle for the proposed scheme in this paper is that location validation decision is implemented by comparing the similarities between current estimated channel features at time $t$ and previous ones at time $t-1$ with the corresponding preset thresholds, based on the framework of hypothesis testing theory. Channel statistics and the temporal values for AAoA, EAoA and path gain at time $t-1$, and correlation coefficients can be modeled as side information that is known at both the transmitter (Alice) and the legitimate receiver (Bob), but not the adversary (Eve). The legitimate transmitter (Alice) and intended legitimate receiver (Bob) cooperate to secure communication transmission by means of the knowledge of this side information; this is beneficial for both partners. It should be stressed that the validation and efficiency of this idea were already studied from an information-theoretical point-of-view in [30], and the work [30] also provided the right guidance to the appropriate code design in practice.

### 4. Performance Analysis

In this section, we focus on the modeling of false alarm rate (denoted by $P_f$) and detection rate (denoted by $P_d$). To facilitate the calculation of the two probabilities, we denote $P_{\Theta_\zeta,H_i}$ the probability of $(\Theta_\zeta > \eta_\zeta)$ under $H_i$ for $i = 1, 2$ and $\zeta \in \{\phi, \alpha, \theta\}$, and we consider $\sigma_{\zeta,AB}^2 = \sigma_{\zeta,AB}^2$, and $\sigma_{\zeta,EB}^2 = \sigma_{\zeta,EB}^2$. Based on authentication decision in (45), we establish the following lemmas regarding the probability $P_{\Theta_\zeta,H_i}$.

**Lemma 2.** Based on (44) and (45), $P_{\Theta_\zeta,H_0}$ is expressed by

$$
P_{\Theta_\zeta,H_0} = \exp\left(-\frac{\eta_\phi}{2\sigma_{\phi,H_0}^2}\right) \sum_{z=0}^{L-1} \frac{1}{z!} \left(\frac{\eta_\phi}{2\sigma_{\phi,H_0}^2}\right)^z,
$$

(46)

where $\sigma_{\phi,H_0}^2 = 2(1-\rho_\phi)\sigma_{\phi,AB}^2 + 2\sigma_{\Delta \phi}^2$ and $\sigma_{\phi,H_1}^2 = \sigma_{\phi,EB}^2 + \sigma_{\phi,AB}^2 + 2\sigma_{\Delta \phi}^2$. 

**Proof.** To calculate the probability distribution of $\Theta_\phi$ in (44), we define $\Lambda \phi$ as

$$
\Lambda \phi \triangleq \hat{\phi}_{\text{EB}}(t) - \hat{\phi}_{\text{LAB}}(t - 1).
$$

Under $H_0$, by substituting (9) into (47), $\Lambda \phi_{H_0}$ is obtained as

$$
\Lambda \phi_{H_0} = \hat{\phi}_{\text{LAB}}(t) - \hat{\phi}_{\text{LAB}}(t - 1)
= (\rho_\phi - 1)\phi_{\text{LAB}}(t - 1) + \sqrt{1 - \rho^2_\phi}\mu_{\phi, \text{EB}}(t) + \Delta \phi(t) - \Delta \phi(t - 1). \tag{48}
$$

One can see that $\Lambda \phi_{H_0}$ is a zero-mean Gaussian distribution with variance $\sigma^2_{\phi, H_0} = 2(1 - \rho_\phi)\sigma^2_{\phi, \text{LAB}} + 2\sigma^2_{\Delta \phi}$. Therefore, $\Theta_\phi$ under $H_0$ is a central chi-square distribution random variable and the PDF of $\Theta_\phi$ under $H_0$ is then written as

$$
f_{\Theta_\phi, H_0}(x) = \frac{x^{\frac{L}{2} - 1}}{2\sigma^2_{\phi, H_0}\Gamma(L/2)} \exp \left( -\frac{x}{2\sigma^2_{\phi, H_0}} \right), \quad x \geq 0,
$$

where $\Gamma(\cdot)$ is a Gamma function. The CDF of $\Theta_\phi$ under $H_0$ is written as

$$
F_{\Theta_\phi, H_0}(x) = 1 - \exp \left( -\frac{x}{2\sigma^2_{\phi, H_0}} \right) \frac{1}{z!} \sum_{z=0}^{\frac{L}{2} - 1} \left( \frac{x}{2\sigma^2_{\phi, H_0}} \right)^z. \tag{50}
$$

Accordingly, $P_{\Theta_\phi, H_0}$ is written as

$$
P_{\Theta_\phi, H_0} = \Pr\{\Theta_\phi > \eta_\phi | H_0\} = \exp \left( -\frac{\eta_\phi}{2\sigma^2_{\phi, H_0}} \right) \frac{1}{z!} \sum_{z=0}^{\frac{L}{2} - 1} \left( \frac{\eta_\phi}{2\sigma^2_{\phi, H_0}} \right)^z. \tag{51}
$$

Similarly, based on (47), we derive $\Lambda \phi_{H_1}$ under hypothesis $H_1$ as

$$
\Lambda \phi_{H_1} = \hat{\phi}_{\text{LAB}}(t) - \hat{\phi}_{\text{LAB}}(t - 1) = \phi_{\text{LAB}}(t) + \Delta \phi(t) - \phi_{\text{LAB}}(t - 1) - \Delta \phi(t - 1). \tag{52}
$$

Because $\phi_{\text{LAB}}(t)$, $\Delta \phi(t)$, $\phi_{\text{LAB}}(t - 1)$ and $\Delta \phi(t - 1)$ are independent zero-mean Gaussian random variables with variances $\sigma^2_{\phi, \text{LAB}}$, $\sigma^2_{\Delta \phi}$, $\sigma^2_{\phi, \text{LAB}}$ and $\sigma^2_{\Delta \phi}$, respectively, and then the PDF of $\Theta_\phi$ under $H_1$ is written as

$$
f_{\Theta_\phi, H_1}(x) = \frac{x^{\frac{L}{2} - 1}}{2\sigma^2_{\phi, H_1}\Gamma(L/2)} \exp \left( -\frac{x}{2\sigma^2_{\phi, H_1}} \right), \quad x \geq 0,
$$

where $\sigma^2_{\phi, H_1} = \sigma^2_{\phi, \text{EB}} + \sigma^2_{\phi, \text{LAB}} + 2\sigma^2_{\Delta \phi}$. Then, the CDF of $\Theta_\phi$ under $H_1$ is written as

$$
F_{\Theta_\phi, H_1}(x) = 1 - \exp \left( -\frac{x}{2\sigma^2_{\phi, H_1}} \right) \frac{1}{z!} \sum_{z=0}^{\frac{L}{2} - 1} \left( \frac{x}{2\sigma^2_{\phi, H_1}} \right)^z. \tag{54}
$$

According to (54), $P_{\Theta_\phi, H_1}$ is written as

$$
P_{\Theta_\phi, H_1} = \Pr\{\Theta_\phi > \eta_\phi | H_1\} = \exp \left( -\frac{\eta_\phi}{2\sigma^2_{\phi, H_1}} \right) \frac{1}{z!} \sum_{z=0}^{\frac{L}{2} - 1} \left( \frac{\eta_\phi}{2\sigma^2_{\phi, H_1}} \right)^z. \tag{55}
$$
Lemma 3. Using (45), $P_{\Theta_{\phi},H_{i}} (i = 1, 2)$ is evaluated as

$$P_{\Theta_{\phi},H_{i}} = \exp\left(-\eta_{\phi} \frac{2}{2\sigma_{\phi, H_{i}}^{2}} \sum_{z=0}^{l-1} \frac{1}{z!} \left( \frac{\eta_{\phi}}{2\sigma_{\phi, H_{i}}^{2}} \right)^{z}\right),$$

where $\sigma_{\phi, H_{0}}^{2} = 2(1 - \rho_{\theta})\sigma_{\phi, AB}^{2} + 2\sigma_{\Delta_{\phi}}^{2}$ and $\sigma_{\phi, H_{1}}^{2} = \sigma_{\phi, EB}^{2} + \sigma_{\phi, AB}^{2} + 2\sigma_{\Delta_{\phi}}^{2}$.

Lemma 4. Using (45), $P_{\Theta_{\theta},H_{i}} (i = 1, 2)$ is evaluated as

$$P_{\Theta_{\theta},H_{i}} = \exp\left(-\eta_{\theta} \frac{2}{2\sigma_{\theta, H_{i}}^{2}} \sum_{z=0}^{l-1} \frac{1}{z!} \left( \frac{\eta_{\theta}}{2\sigma_{\theta, H_{i}}^{2}} \right)^{z}\right),$$

where $\sigma_{\theta, H_{0}}^{2} = 2(1 - \rho_{\alpha})\sigma_{\theta, AB}^{2} + 2\sigma_{\Delta_{\theta}}^{2}$ and $\sigma_{\theta, H_{1}}^{2} = \sigma_{\theta, EB}^{2} + \sigma_{\theta, AB}^{2} + 2\sigma_{\Delta_{\theta}}^{2}$.

Based on the above lemmas, we can establish the following theorem regarding the closed expressions of $P_f$ and $P_d$.

Theorem 1. For the mmWave MIMO communication model shown in Figure 1, $P_f$ and $P_d$ of the proposed authentication scheme are determined, respectively, as

$$P_f = P_{\Theta_{\phi},H_{0}} P_{\Theta_{\phi},H_{0}} P_{\Theta_{\theta},H_{0}},$$

$$P_d = 1 - (1 - P_{\Theta_{\phi},H_{1}})(1 - P_{\Theta_{\theta},H_{1}})(1 - P_{\Theta_{\theta},H_{1}}).$$

Suppose that Bob has no knowledge of the channel parameters from data frame at time $l$ such as $\hat{r}_{l, AB}(l - 1)$ and $\rho_{u}$ for $\zeta \in \{\phi, \alpha, \theta\}, l = 1, ..., L$. In this case $\Theta_{\zeta}$ becomes

$$\Theta_{\zeta} = \sum_{l=1}^{L} |\hat{r}_{l, XB}(l)|^2, \zeta \in \{\phi, \alpha, \theta\}.$$  

(60)

Following similar steps for the derivation of $P_{\Theta_{\phi},H_{i}}$, we can obtain $P_{\Theta_{\phi},H_{i}}^u$ with $u$ being without the knowledge of channel parameters at time $l - 1$, and then we have

$$P_{\Theta_{\phi},H_{i}}^u = \exp\left(-\eta_{\phi} \frac{2}{2\sigma_{\phi, H_{i}}^{2}} \sum_{z=0}^{l-1} \frac{1}{z!} \left( \frac{\eta_{\phi}}{2\sigma_{\phi, H_{i}}^{2}} \right)^{z}\right),$$

(61)

$$P_{\Theta_{\theta},H_{i}}^u = \exp\left(-\eta_{\theta} \frac{2}{2\sigma_{\theta, H_{i}}^{2}} \sum_{z=0}^{l-1} \frac{1}{z!} \left( \frac{\eta_{\theta}}{2\sigma_{\theta, H_{i}}^{2}} \right)^{z}\right),$$

(62)

$$P_{\Theta_{\theta},H_{i}}^u = \exp\left(-\eta_{\theta} \frac{2}{2\sigma_{\theta, H_{i}}^{2}} \sum_{z=0}^{l-1} \frac{1}{z!} \left( \frac{\eta_{\theta}}{2\sigma_{\theta, H_{i}}^{2}} \right)^{z}\right),$$

(63)

where $\sigma_{\phi, H_{0}}^{2} = \sigma_{\phi AB}^{2} + \sigma_{\Delta_{\phi}}^{2}$, $\sigma_{\phi, H_{1}}^{2} = \sigma_{\phi EB}^{2} + \sigma_{\phi AB}^{2} + 2\sigma_{\Delta_{\phi}}^{2}$, $\sigma_{\theta, H_{0}}^{2} = \sigma_{\theta AB}^{2} + \sigma_{\Delta_{\theta}}^{2}$, $\sigma_{\theta, H_{1}}^{2} = \sigma_{\theta EB}^{2} + \sigma_{\Delta_{\theta}}^{2}$. In this case, $P_f^u$ and $P_d^u$ of the proposed authentication scheme are determined, respectively, as

$$P_f^u = P_{\Theta_{\phi},H_{0}}^u P_{\Theta_{\theta},H_{0}}^u P_{\Theta_{\theta},H_{0}}^u,$$

(64)
Suppose that legitimate Alice and adversary Eve transmit signals to Bob with equal probability. We use $P_s$ to denote the secrecy rate improvement afforded by the knowledge of data frame at time $t-1$ for both legitimate transmitter and receiver, relative to the case in which the knowledge is not used. Then, $P_s$ can be calculated as

$P_s = \frac{1}{2} (P_u^f - P_f + P_d - P_d^u). \tag{66}$

5. Numerical Results

5.1. System Parameters and Simulation Settings

Let signal-to-noise ratio (SNR) denote as $\text{SNR} = \frac{P}{\sigma_n^2}$ and $k_\phi = \frac{\sigma_{\phi,EB}}{\sigma_{\phi,LAB}}$ be the ratio of Eve’s and Alice’s AAoA variances. We use $k_\theta = \frac{\sigma_{\theta,EB}}{\sigma_{\theta,LAB}}$ to denote the ratio of Eve’s and Alice’s EAoA variances, and $k_\alpha = \frac{\sigma_{\alpha,EB}}{\sigma_{\alpha,LAB}}$ to denote the ratio of Eve’s and Alice’s path gain variances. We set the number of the receiver antennas as $N_r = M \times N$. In the simulations, the first frame is validated based on a higher layer verification scheme and the second frame is validated by using the proposed location verification scheme.

5.2. Impact of SNR on the Verification Performance

We plot in Figure 2 ROC (receiver operating characteristic, ROC) variations under the settings of $(N_r = 128, L = 20, k_\phi = 2 \text{ dB}, k_\theta = 2 \text{ dB}, k_\alpha = 2 \text{ dB})$ at different SNRs. From Figure 2, we can see that the authentication performance ($P_f$ and $P_d$) under SNR = 5 dB outperforms that of the others and the performance for SNR = −5 dB is poorest. This indicates that the SNRs have severe impacts on the authentication performance. One can improve the authentication performance by setting a higher SNR. However, the SNR level usually has a limit due to the practical conditions. In many practical environments, $P_f < 0.1$ and $P_d > 0.9$ are usually a required constraint pair to satisfy the requirements of a practical authentication system. As shown in Figure 2, the authentication performance ($P_f$ and $P_d$) for SNR = 0 dB and SNR = 5 dB can satisfy the practical requirements and the performance at SNR = 5 dB is best. From Figure 2, we also can see that when $P_f$ is fixed, $P_d$ increases when SNR increases. This means that a higher SNR can lead to a better authentication performance.

![Figure 2. ROC curves under different SNRs with the settings of ($N_r = 128, L = 20, k_\phi = 2 \text{ dB}, k_\theta = 2 \text{ dB}, k_\alpha = 2 \text{ dB}$).](image-url)
5.3. Impact of the Number of Antennas on the Authentication Performance

We show in Figure 3 the ROC results under different receiver antenna numbers with the settings of (SNR = 10 dB, L = 20, k_φ = 2 dB, k_θ = 2 dB, k_α = 2 dB). From Figure 3, we can see that the authentication performance (P_f, P_d) under 64 receiver antennas outperforms that of the others, and the performance under 16 receiver antennas is poorest. This is because multiple antennas can improve feature dimensions and further improve the authentication performance. When P_f is fixed, P_d increases when the number of receiver antennas increases. Moreover, the authentication performance (P_f, P_d) under 64 receiver antennas can satisfy the practical authentication requirements.

5.4. Impact of the Number of Multipaths on the Authentication Performance

We show in Figure 4 the ROC curves under different numbers of multipaths with the settings of (SNR = 10 dB, N_r = 64, k_φ = 2 dB, k_θ = 2 dB, k_α = 2 dB). From Figure 4, we can see that the authentication performance (P_f, P_d) under L = 15 multipaths outperforms that of the others, and the performance under L = 5 multipaths is poorest. This means that more multipaths can contribute to the authentication performance. We can also see that when P_f is fixed, P_d increases when the number of multipaths increases.
5.5. Impact of \( k_a \) on the Authentication Performance

To investigate the impact of the distance between Eve–Bob and Alive–Bob on performance, we need to characterize \( \sigma_{\alpha_l, XB}^2 \) being the variance of the path gain of the \( l \)-th propagation path from the transmitter \( X \) to Bob. According to [31], baseband path gain \( \alpha_{1, XB} \) is written as

\[
\alpha_{l, XB} = \beta_{l, XB} \exp\left(-\frac{2\pi f_c d_{l, XB}}{c}\right),
\]

where \( \beta_{l, XB} \) is the attenuation coefficient of the \( l \)-th propagation path and \( f_c \) is carrier frequency. According to the Central Limit Theorem, the path gain can be modeled as a zero-mean complex circular symmetric Gaussian process and for large-scale fading channels, \( \sigma_{\alpha_l, XB}^2 \) can be modeled by applying ([32], Chapter 2), as

\[
\sigma_{\alpha_l, XB}^2 = K \left( \frac{d_0}{d_{l, XB}} \right)^{\varsigma} \Omega, \quad (67)
\]

where \( K \) is a reference path gain value; \( d_0 \) is a reference distance for antenna far-field; \( \varsigma \) is a path loss exponent ranging between 2 and 5 in free space propagation wireless environments; and \( \Omega \) is a shadowing factor modeled as a log-normal random variable. Because the distance between the transmitter and receiver is much larger than antenna separation, we can use the approximation

\[
d_{l, XB} \approx \cdots \approx d_{L, XB} = d_{XB} \text{ for } X = \{A, E\}.
\]

From (67), we have \( \sigma_{\alpha_l, LX}^2 = \cdots = \sigma_{\alpha_l, XB}^2 = \sigma_{\alpha_l, AB}^2 \). Both Alice and Eve are assumed to be randomly deployed at arbitrary locations in a circular area centered on Bob, and there is no shadow fading in that area. By using (67), \( k_a \) by dB value without shadow fading is given by

\[
k_a = 10\varsigma \log \left( \frac{d_{AB}}{d_{EB}} \right).
\]

We make an assumption (without loss of generality) that Alice is in a fixed location, i.e., \( d_{AB} \) is a constant and we adjust the distance between Eve and Bob \( d_{EB} \) to obtain different \( k_a \).

We show in Figure 5 how \( P_d \) varies with \( k_a \) under different \( P_f \)s and with the settings of (SNR = 10 dB, \( N_r = 128 \), \( L = 25 \), \( k_\phi = 2 \) dB, \( k_\theta = 2 \) dB). From Figure 5, \( P_d \) increases when \( k_a \) increases for a given \( P_f \). This clearly indicates that if Eve is closer to Bob, she might be successfully detected by Bob, and Eve might select an appropriate location in which she has a high probability of successfully impersonating Alice. In addition, the authentication performance under \( P_f = 0.08 \) outperforms that of the others, and the performance under \( P_f = 0.02 \) is poorest. This is because a lower \( P_f \) value means a stricter performance requirement and there would be a trade-off between \( P_d \) and \( P_f \). We can also see from Figure 5 that when \( k_a \) is fixed, \( P_d \) increases when \( P_f \) increases.

![Figure 5. \( P_d \) vs. \( k_a \) with the settings of (SNR = 10 dB, \( N_r = 128 \), \( L = 25 \), \( k_\phi = 2 \) dB, \( k_\theta = 2 \) dB).](image)

5.6. Performance Comparison

Figure 6 displays a performance comparison between the authentication scheme proposed in [16] and our scheme. From Figure 6, we can see that the performance \( (P_f, P_d) \) of our scheme jointly using AAoA, EAoA and path gain outperforms that of the
scheme only using path gain [16]. This is because the scheme in [16] uses coarse-grained channel information while our scheme uses multi-dimensional mmWave MIMO channel features (i.e., AAoA, EAoA and path gain) to effectively utilize the fine-grained channel information. It is also noted that when \( P_f \) increases, the detection rates of both schemes increase. Moreover, the authentication performance \( (P_f, P_d) \) of our scheme can better satisfy the practical authentication requirements. This is beneficial for exploiting both the AAoA and EAoA features, and allows us to gain important insights on the impacts of angle domain features on authentication performance.

**Figure 6.** Performance comparison between the scheme in [16] and our scheme with the settings of \((\text{SNR} = 5 \text{ dB, } N_r = 128, L = 20, k_{\phi} = 2 \text{ dB, } k_{\theta} = 2 \text{ dB, } k_{\alpha} = 2 \text{ dB})\).

### 5.7. Impact of \( \rho_{\alpha} \) on the Authentication Performance

We show in Figure 7 ROC variations under the settings of \((\text{SNR} = 10 \text{ dB, } N_r = 128, L = 20, k_{\phi} = 2 \text{ dB, } k_{\theta} = 2 \text{ dB, } k_{\alpha} = 2 \text{ dB})\) at different correlation coefficients of path gain. From Figure 7, we can see that the authentication performance \( (P_f, P_d) \) under \( \rho_{\alpha} = 0.9 \) outperforms that of the others, and the performance under \( \rho_{\alpha} = 0.7 \) is the poorest. This is because a larger \( \rho_{\alpha} \) means that the communication entities move slower. When \( P_f \) is fixed, \( P_d \) increases when \( \rho_{\alpha} \) increases. Moreover, the authentication performance \( (P_f, P_d) \) under \( \rho_{\alpha} = 0.9 \) can satisfy the practical authentication requirements.

**Figure 7.** ROC curves under different correlation coefficients of path gain with the settings of \((\text{SNR} = 10 \text{ dB, } N_r = 128, L = 20, k_{\phi} = 2 \text{ dB, } k_{\theta} = 2 \text{ dB, } k_{\alpha} = 2 \text{ dB})\).
6. Conclusions

By utilizing multi-dimensional mmWave MIMO channel features, this paper developed a location verification scheme for mmWave MIMO communication systems. Furthermore, we modeled the three-dimensional mmWave channel features (i.e., AAoA, EAoA and path gain) and extracted these feature parameters through maximum-likelihood estimator. We also derived the analytical expressions for the typical performance metrics. Numerical results indicate that the proposed authentication scheme can benefit from using multi-dimensional mmWave channel features. The results in this paper reveal that the proposed scheme is general in nature and can be applied to more communication systems, and we expect the methodology developed in this paper to be valuable for devising new physical layer authentication schemes in other network scenarios.

Author Contributions: Conceptualization, Y.L. and P.Z.; methodology, Y.L.; validation, J.H., Y.L. and P.Z.; investigation, P.Z.; writing—original draft preparation, P.Z.; writing—review and editing, J.H.; funding acquisition, J.H. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the Natural Science Foundation of China (NSFC) Grant (62272241), Japan Society for the Promotion of Science (JSPS) Grant (18H03235), and Nanjing University of Posts and Telecommunications Scientific Research Foundation Grant (NY221122).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Wu, F.; Xu, L.; Kumari, S.; Li, X.; Shen, J.; Choo, K.R.; Wazid, M.; Das, A.K. An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment. J. Netw. Comput. Appl. 2017, 89, 72–85. [CrossRef]

2. Esfahani, A.; Mantas, G.; Matischek, R.; Saghezchi, F.B.; Rodriguez, J.; Bicaku, A.; Maksutı, S.; Tauber, M.G.; Schmittner, C.; Bastos, J. A lightweight authentication mechanism for M2M communications in industrial IoT environment. IEEE Internet Things J. 2019, 6, 288–296. [CrossRef]

3. Stergiou, C.; Psannis, K.E.; Kim, B.; Gupta, B.B. Secure integration of IoT and cloud computing. Future Gener. Comput. Syst. 2018, 78, 964–975. [CrossRef]

4. Wang, X.; Hao, P.; Hanzo, L. Physical-layer authentication for wireless security enhancement: Current challenges and future developments. IEEE Commun. Mag. 2016, 54, 152–158. [CrossRef]

5. Xie, N.; Chen, J.; Huang, L. Physical-layer authentication using multiple channel-based features. IEEE Trans. Inf. Forensics Secur. 2021, 16, 2356–2366. [CrossRef]

6. Tang, J.; Xu, A.; Jiang, Y.; Zhang, Y.; Wen, H.; Zhang, T. MmWave MIMO physical layer authentication by using channel sparsity. In Proceedings of the 2020 IEEE International Conference on Artificial Intelligence and Information Systems (ICAIIS), Dalian, China, 20–22 March 2020; pp. 221–224.

7. Maeng, S.J.; Yapici, Y.; Güvenç, I.; Dai, H.; Bhuyan, A. Power allocation for fingerprint-based PHY-Layer authentication with mmWave UAV networks. In Proceedings of the ICC 2021-IEEE International Conference on Communications, Montreal, QC, Canada, 14–23 June 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–6.

8. Lord, S.F. 5G Millimeter-Wave Physical-Layer Authentication with Planar Reflectors. Ph.D. Thesis, Naval Postgraduate School, Monterey, CA, USA, 2019.

9. Wang, N.; Li, W.; Wang, P.; Alipour-Fanid, A.; Jiao, L.; Zeng, K. Physical layer authentication for 5G communications: Opportunities and road ahead. IEEE Netw. 2020, 34, 198–204. [CrossRef]

10. Wang, N.; Wang, P.; Alipour-Fanid, A.; Jiao, L.; Zeng, K. Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities. IEEE Internet Things J. 2019, 6, 8169–8181. [CrossRef]

11. Wang, N.; Jiao, L.; Wang, P.; Dabaghchian, M.; Zeng, K. Efficient identity spoofing attack detection for IoT in mm-Wave and Massive MIMO 5G communication. In Proceedings of the IEEE Global Communications Conference, Globecom 2018, Abu Dhabi, United Arab Emirates, 9–13 December 2018; IEEE: Piscataway, NJ, USA, 2018; pp. 1–6.

12. Wang, N.; Jiao, L.; Alipour-Fanid, A.; Dabaghchian, M.; Zeng, K. Pilot contamination attack detection for NOMA in 5G mm-Wave massive MIMO networks. IEEE Trans. Inf. Forensics Secur. 2020, 15, 1363–1378. [CrossRef]

13. Wang, N.; Li, W.; Alipour-Fanid, A.; Jiao, L.; Dabaghchian, M.; Zeng, K. Pilot contamination attack detection for 5G mmWave grant-Free IoT networks. IEEE Trans. Inf. Forensics Secur. 2021, 16, 658–670. [CrossRef]
14. Wang, N.; Jiao, L.; Wang, P.; Li, W.; Zeng, K. Exploiting beam features for spoofing attack detection in mmWave 60-GHz IEEE 802.11ad networks. *IEEE Trans. Wirel. Commun.* 2021, 20, 3321–3335. [CrossRef]

15. Wang, N.; Jiao, L.; Wang, P.; Li, W.; Zeng, K. Machine learning-based spoofing attack detection in MmWave 60GHz IEEE 802.11ad Networks. In Proceedings of the 39th IEEE Conference on Computer Communications, INFOCOM 2020, Toronto, ON, Canada, 6–9 July 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 2579–2588.

16. Xiao, L.; Greenstein, L.J.; Mandayam, N.B.; Trappe, W. Channel-based spoofing detection in frequency-selective Rayleigh channels. *IEEE Trans. Wirel. Commun.* 2009, 8, 5948–5956. [CrossRef]

17. Xiao, L.; Wan, X.; Han, Z. PHY-Layer authentication with multiple landmarks with reduced overhead. *IEEE Trans. Wirel. Commun.* 2018, 17, 1676–1687. [CrossRef]

18. Liu, F.J.; Wang, X. Physical layer authentication enhancement using two-dimensional channel quantization. *IEEE Trans. Wirel. Commun.* 2016, 15, 4171–4182. [CrossRef]

19. Alkhateeb, A.; Ayach, O.E.; Leus, G., Jr; Heath R.W. Channel estimation and hybrid precoding for millimeter Wave cellular systems. *IEEE J. Sel. Top. Signal Process.* 2014, 8, 831–846. [CrossRef]

20. Méndez-Rial, R.; Rusu, C.; Alkhateeb, A.; González Prelcic, N.; Heath, R.W., Jr. Channel estimation and hybrid combining for mmWave: Phase shifters or switches? In Proceedings of the 2015 Information Theory and Applications Workshop, ITA 2015, San Diego, CA, USA, 1–6 February 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 90–97.

21. Singh, J.; Ramakrishna, S. On the feasibility of codebook-based beamforming in millimeter wave systems with multiple antenna arrays. *IEEE Trans. Wirel. Commun.* 2015, 14, 2670–2683. [CrossRef]

22. Hemadeh, I.A.; Satyanarayana, K.; El-Hajjar, M.; Hanzo, L. Millimeter-wave communications: Physical channel models, design considerations, antenna constructions, and link-budget. *IEEE Commun. Surv. Tutor.* 2018, 20, 870–913. [CrossRef]

23. Fan, D.; Gao, F.; Liu, Y.; Deng, Y.; Wang, G.; Zhong, Z.; Nallanathan, A. Angle domain channel estimation in hybrid millimeter wave massive MIMO systems. *IEEE Trans. Wirel. Commun.* 2018, 17, 8165–8179. [CrossRef]

24. Buzzi, S.; D’Andrea, C. On clustered statistical MIMO millimeter wave channel simulation. *arXiv* 2016, arXiv:1604.00648.

25. Ayach, O.E.; Rajagopal, S.; Abu-Surra, S.; Pi, Z.; Heath, R.W., Jr. Spatially sparse precoding in millimeter wave MIMO systems. *IEEE Trans. Wirel. Commun.* 2014, 13, 1499–1513. [CrossRef]

26. Shen, W.; Dai, L.; Shim, B.; Wang, Z.; Heath, R.W., Jr. Channel feedback based on AoD-adaptive subspace codebook in FDD massive MIMO systems. *IEEE Trans. Commun.* 2018, 66, 5235–5248. [CrossRef]

27. Xie, N.; Zhang, S. Blind authentication at the physical layer under time-varying fading channels. *IEEE J. Sel. Areas Commun.* 2018, 36, 1465–1479. [CrossRef]

28. Médard, M. The effect upon channel capacity in wireless communications of perfect and imperfect knowledge of the channel. *IEEE Trans. Inf. Theory* 2000, 46, 933–946. [CrossRef]

29. Kay, S.; Hall, P. Fundamentals of statistical signal processing, Volume II: Detection theory. *Technometrics* 1993, 37, 465–466.

30. Zaidi, A.; Vandendorpe, L. Coding schemes for relay-assisted information embedding. *IEEE Trans. Inf. Forensics Secur.* 2009, 4, 70–85. [CrossRef]

31. Tse, D.; Viswanath, P. *Fundamentals of Wireless Communication*; Cambridge University Press: Cambridge, UK, 2005.

32. Goldsmith, A. *Wireless Communications*; Cambridge University Press: Cambridge, UK, 2005.