Robust Tracking-Based PHY-Authentication in mmWave MIMO Systems

Liza Afeef, Haji M. Furqan, and Hüseyin Arslan, *Fellow, IEEE*

***Abstract*—Physical Layer Authentication (PLA) is a topic of considerable interest in ensuring strong security for upcoming wireless networks. However, existing PLA methods face challenges in maintaining performance in dynamic environments. To overcome this, we propose a novel tracking-based PLA approach, utilizing properties of the beamspace multiple-input multiple-output (MIMO) channel in narrowband millimeter-wave (mmWave) networks. Specifically, In particular, the proposed technique involves extracting a distance signature vector from the positions of the principal components within the beamspace MIMO channel representation. These components are then sorted in descending order based on their indices. To address mobility concerns in dynamic settings, a tracking filter is introduced. This filter allows the authentication system to continuously track and update the stored signature, enhancing overall authentication performance. Additionally, the proposed technique is extended to ultra-wideband signaling. In this extension, the richness of the derived signature is further improved by exploiting the beam squint effect, contributing to a more robust authentication process. Simulation results demonstrate that our approach overcomes the limitations of previous methods, resulting in improved authentication performance measured by detection and false alarm rates.**

***Index Terms*—Physical layer authentication (PLA), MIMO, narrowband, wideband, beamspace channel, beam squint effect, tracking filter.**

I. Introduction

OVER the past few decades, wireless communication technologies have made significant advancements in both reliability and data throughput. These advancements have been made feasible through the utilization of two key innovations: multiple-input multiple-output (MIMO) systems and millimeter wave (mmWave) technology. However, security remains a critical concern in these deployments due to the open and broadcast nature of the wireless medium, which makes it vulnerable to various threats from illegitimate nodes, such as spoofing and Sybil attacks. In a spoofing attack, the attacker attempts to corrupt legitimate communications by injecting some forged identity information, while the Sybil attack is based on creating multiple fake identities that are designed to appear as distinct legitimate participants, giving the attacker the ability to manipulate network activities [1]. In recent years, physical layer authentication (PLA) has emerged as an additional security measure to complement conventional cryptography-based techniques to provide authentication against different security threats. PLA provides a fast, cost-effective, and low-complexity computational security solution, besides its compatibility with forthcoming wireless communication networks such as 6G and beyond. PLA leverages the random nature of the wireless medium and the hardware impairments of the transceiver terminals [2] without the requirement of additional security information, which significantly the available capacity of the channel and improves the system's immunity against various security vulnerabilities.

Received 14 May 2024; revised 28 July 2024; accepted 22 October 2024. Date of publication 30 October 2024; date of current version 2 December 2024. This work was supported in part by the Scientific and Technological Research Council of Türkiye (TUBITAK) under Grant 123E226. The associate editor coordinating the review of this article and approving it for publication was Dr. Jun Zhao. *(Corresponding author: Liza Afeef.)*

Liza Afeef and Hüseyin Arslan are with the Department of Electrical and Electronics Engineering, Istanbul Medipol University, Istanbul 34810, Türkiye (e-mail: liza.shehab@std.medipol.edu.tr; huseyinarslan@medipol.edu.tr).

Haji M. Furqan is with the IPR and License Agreements Department, Vestel, Manisa 45030, Türkiye (e-mail: haji.madni@vestel.com.tr).

Digital Object Identifier 10.1109/TIFS.2024.3488362

A. Prior Works and Limitations

The literature contains a wealth of research targeting PLA, these works harness the intrinsic properties of the physical layer and can be broadly classified into two distinct categories: hardware-based schemes and channel-based schemes. The first approach utilizes device-specific radio frequency (RF) hardware features for authentication, which include phase noise [3], [4], carrier frequency offset (CFO) [5], [6], and power amplifier nonlinearity [7]. However, implementing these techniques involves extra costs because of the need for additional extraction equipment. The second scheme, on the other hand, eliminates the need for supplementary feature extraction equipment, as the necessary physical-layer features can be extracted directly from the received signal or channel information, such as received signal strength (RSS) [8], channel impulse response (CIR) [9], and location-based channel gain [4].

Notwithstanding their potential benefits, current channel-based methods possess certain limitations, such as performance degradation in dynamic and sparse environments. Specifically, the introduction of user mobility poses additional obstacles to PLA, where even a small movement of a mobile device can cause significant changes in channel response, resulting in a notable increase in false alarm rates. To handle this problem, a tracking-based PLA is introduced in [5] and [6], where CFO is investigated to identify legitimate transmitters, and a tracking filter is used to predict the current value given the past tracked CFO variation. Similarly, the authors in [10] proposed a V2X authentication framework based on the characteristics of the physical layer channel, where the tracking process is used to refine both the iterative and threshold models. However, these investigations are limited to addressing multipath time-varying channels and fail to address security concerns when communicating in a challenging, poorly scattered environment, especially when the attacker is strategically positioned along the line of sight (LoS) path.

Taking into account the sparse channel characteristics encountered in sixth-generation (6G) networks, traditional channel-based methods may not be practically feasible. Therefore, alternative characteristics must be employed for PLA. This can be accomplished by integrating mmWave and massive MIMO technologies, which enable the exploration of novel and distinctive attributes for PLA [11]. For instance, in [12], the authors leverage perturbed antenna array geometries for PLA. Similarly, the work in [13] utilizes spatial beam patterns to perform RF fingerprinting by exploiting the antenna array structure's and phase shifters' inherent impairments. Meanwhile, the authors in [9] use MIMO channel coefficients to construct a multi-feature-based authentication method. Furthermore, [14] exploits the location-specific property of wireless channels for PLA in a massive MIMO system while incorporating hardware impairments into the authentication system. On the other hand, [15] exploits the mmWave MIMO channel features, angle of arrivals (angle of arrivals), angle of departures (angle of departures), and channel gain, with the combination of hardware phase noise features to provide a novel PLA scheme. The work in [16] proposes a novel PLA system against spoofing attacks using a hybrid distance signature of both the beamspace channel representation and the mutual coupling effect in the MIMO antenna array.

However, the aforementioned PLA studies are susceptible to channel variations and user mobility. Given that they are primarily tailored for narrowband transmission, they cannot be applied to wideband mmWave MIMO systems, which are crucial for achieving high data rates. Furthermore, these methods can only be implemented in the time division duplexing (TDD) transmission and are not viable in the frequency division duplexing (FDD) mode.

B. Contributions

In this work, a novel tracking-based PLA scheme is proposed that takes advantage of the beamspace parameters for the mmWave MIMO channels, offering versatility in static and dynamic environments and robustness against channel variations in both time and frequency domains. The work builds upon the stability of beamspace parameters, such as angle of arrivals and angle of departures, in dynamic settings, contrasting their reliability with counterparts in time and frequency domains [17]. The proposed PLA framework employs a tracking-based approach, creating a unique authentication signature by extracting principal components from the beamspace representation of the mmWave MIMO channel. This scheme is designed to operate effectively in both static and dynamic environments, covering narrowband and wideband mmWave MIMO systems.

The proposed authentication signature, detailed in this work, is an extension of the distance-based signature introduced in our previous work [16]. The earlier method focused on static environments, assuming fixed positions of legitimate nodes during authentication and connection establishment, and was tailored for narrowband transmission with TDD mode only. In contrast, the current scheme is versatile, accommodating various environments, both static and dynamic, and applies to both narrowband and wideband mmWave MIMO systems. The proposed signature stands out for its independence from path gain, a crucial characteristic that enhances its robustness against channel variations across both time and frequency domains. This means that the proposed signature remains stable and reliable regardless of fluctuations in the strength of individual signal paths within the channel. This is due to the structure of the proposed signature that relies only on the departure and arrival angles of the channel paths. Note that these physical angles in the uplink channel are roughly the same as the angles in the downlink channel in TDD/FDD systems, which is called the angle reciprocity [17]. As a result of this phenomenon, the proposed signature is applicable to provide a reliable authorized connection in both TDD and FDD systems.

The study highlights the robustness of the proposed approach to channel variations in sparse dynamic environments, including temporal and frequency changes. This robustness is achieved through effective tracking of beamspace channel attributes between legitimate transceiver nodes.

The proposed approach contributes significantly to the field of PLA in wireless communication networks through the following key aspects:

- First, a novel approach to PLA is proposed, leveraging beamspace MIMO channel representation in narrowband mmWave MIMO systems. The proposed scheme involves creating a distinctive signature, called *enhanced distance (ED) signature*, which measures the distances between the principal components of beamspace representation from a reference point and sorts them according to index values. Unlike existing techniques, our approach provides a more robust and stable signature capable of effectively handling channel variations while maintaining adaptability to both TDD and FDD transmission modes.
- In addressing mobility scenarios, we present an efficient filtering-based tracking algorithm that significantly enhances the scheme's ability to manage database signature mismatches resulting from channel variations due to mobility. By continuously tracking and updating the stored signature using both the previous and current observed signatures of the legitimate node, we successfully reduce the overhead of the authentication process. This improvement allows for longer authorized connections between nodes, applicable both in static and mobile environments.
- Moreover, we extend the scope of our proposed tracking-based PLA scheme to encompass wideband mmWave MIMO systems. This extension involves the integration of the ED-based signature with the beam squint effect and tracking approach, thereby further enhancing the authentication process.
- Finally, to validate the effectiveness of our tracking-based PLA scheme, we conduct a comprehensive simulation

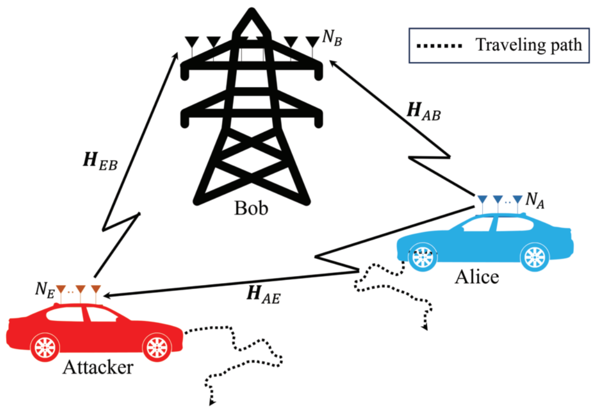


Fig. 1. System model for a mmWave MIMO scenario with an attacker.

analysis. This evaluation encompasses detection and false alarm rates under varying degrees of channel sparsity and dynamicity levels. Through this thorough examination, we provide empirical evidence supporting the robustness and applicability of our proposed approach in diverse scenarios.

C. Organization and Notations

The remaining sections of this paper are organized as follows: Section II presents the model of a dynamic mmWave MIMO system. Subsequently, Section III introduces the proposed tracking-based PLA approach, specifically designed for narrowband transmission. This section provides a detailed explanation of the ED signature extraction process and introduces the tracking model. Section IV discusses the extension of the ED signature to wideband transmission, with emphasis on utilizing the beam squint effect to enhance authentication performance. Additionally, this section outlines the tracking process in wideband signaling. The simulation results and analysis of the proposed tracking-based PLA approach are provided in Section V. Finally, Section VI provides the conclusion of the work.

Notation: Bold uppercase $\mathbf{A}$, bold lowercase $\mathbf{a}$, and unbold letters A, a denote matrices, column vectors, and scalar values, respectively. $(\cdot)^H$, $(\cdot)^T$, and $(\cdot)^{-1}$ denote the Hermitian, transpose, and inverse operators. $\mathbb{C}^{M\times N}$ denotes the space of $M\times N$ complex-valued matrices. $\|\mathbf{a}\|$ is 2-norm of vector $\mathbf{a}$ and $|a|$ is the modulus of scalar a.

II. System Model and Assumptions

A dynamic mmWave MIMO system model is considered with three entities: Alice, Bob, and an attacker, as shown in Fig. 1. Bob is the legitimate base station that needs to authenticate Alice's identity, while the attacker seeks to impersonate Alice. All nodes in the system are assumed to have a multi-antenna array, specifically a one-dimensional uniform linear array (ULA) with N_A, N_B, and N_E antenna elements, respectively.[1] The sparse channel between different nodes is modeled as a time-varying geometric model [18] and expressed by the following equation

$$\mathbf{H}_{XY} = \sum_{l=1}^{L_p^{(XY)}} \beta_l \boldsymbol{a}_R^{(Y)}(\theta_{R,l}, \nu_{R,l}) \boldsymbol{a}_T^{(X)*}(\theta_{T,l}, \nu_{T,l}), \tag{1}$$

where $X \in \{A, E\}$ and $Y \in \{E, B\}$ represent the nodes in the system, and $\mathbf{H}_{\text{AB}}$, $\mathbf{H}_{\text{AE}}$, and $\mathbf{H}_{\text{EB}}$ denote the channels between Alice-Bob, Alice-attacker, and attacker-Bob, respectively. $L_p^{(XY)}$ is the number of channel path between node X and node Y. β_l is a complex channel gain with a complex normal distribution $\mathbb{CN}(0,1)$. The steering vectors of the transmitter and receiver are denoted by $\boldsymbol{a}_T^{(X)} \in \mathbb{C}^{N_X\times 1}$ and $\boldsymbol{a}_R^{(Y)} \in \mathbb{C}^{N_Y\times 1}$. The relative Doppler shift of the transmitter and receiver movement, $\nu_{T,l}$ and $\nu_{R,l}$, are chosen from the set $\nu_l \in [\frac{-\nu_{\max}}{2}, \frac{\nu_{\max}}{2}]$, θ_R is the AoA, and θ_T is the AoD, where both angles follow the uniform distribution $\sim \mathcal{U}(-\pi/2, \pi/2)$. For a ULA structure, the steering vector is given as

$$\boldsymbol{a}(\theta, \nu) = \frac{1}{\sqrt{N}}\Big[1,\ e^{-j2\pi\frac{d_c}{\lambda_c}\ \sin(\theta)\left(1+\frac{\nu}{f_c}\right)}, \cdots,\ e^{-j2\pi(N-1)\frac{d_c}{\lambda_c}\ \sin(\theta)\left(1+\frac{\nu}{f_c}\right)}\Big]^T, \tag{2}$$

where λ_c is the carrier wavelength and d_c is the antenna element spacing, $N \in \{N_A, N_B, N_E\}$, and $\theta \in \{\theta_T, \theta_R\}$.

The sparsity of mmWave channels in the beamspace domain makes the beamspace representation a better choice since, it allows efficient representation and estimation of channel parameters, low overhead processing, and noise robustness. The spatial and beamspace domains are related by a spatial discrete Fourier transform (DFT) represented by the unitary matrix $\mathbf{U}$ [19]. Hence, the beamspace representation of the spatial channel in (1) can be given by

$$\begin{aligned}\mathbf{H}_b^{(XY)} &= \mathbf{U}_Y \mathbf{H}_{XY} \mathbf{U}_X^*,\\ &= \sum_{l=1}^{L_p^{(XY)}} \beta_l \tilde{\mathbf{c}}_{Y,l} \tilde{\mathbf{c}}_{X,l}^*,\end{aligned} \tag{3}$$

where $\mathbf{U}_Y \in \mathbb{C}^{N_Y\times N_Y}$ and $\mathbf{U}_X \in \mathbb{C}^{N_X\times N_X}$ represent the unitary DFT matrices at receiver and transmitter side, respectively. $\tilde{\mathbf{c}}_l$ denotes the l-th path component in the beamspace, and is determined as

$$\begin{aligned}\tilde{\mathbf{c}}_l &= \mathbf{U}\boldsymbol{a}(\theta_l, \nu_l),\\ &= \left[\Upsilon(\bar{\psi}_l - \psi_1), \Upsilon(\bar{\psi}_l - \psi_2), \cdots, \Upsilon(\bar{\psi}_l - \psi_N)\right],\end{aligned} \tag{4}$$

where $\tilde{\mathbf{c}}_l \in \{\tilde{\mathbf{c}}_{X,l}, \tilde{\mathbf{c}}_{Y,l}\}$, $\mathbf{U} \in \{\mathbf{U}_X, \mathbf{U}_Y\}$, $\theta_l \in \{\theta_{T,l}, \theta_{R,l}\}$, $\nu_l \in \{\nu_{T,l}, \nu_{R,l}\}$, and $\Upsilon(\Lambda) = \frac{\sin N\pi\Lambda}{\sin \pi\Lambda}$ is the Dirichlet sinc function. $\bar{\psi}_l = \frac{d_c}{\lambda_c}(1 + \frac{\nu_l}{f_c})\sin\theta_l$, $\bar{\psi}_l \in \{\bar{\psi}_{T,l}, \bar{\psi}_{R,l}\}$, and $\psi_n = \frac{1}{N}(n - \frac{N+1}{2})$ is the spatial direction in the beamspace domain for $n \in \{n_X = 1, 2, \cdots, N_X, n_Y = 1, 2, \cdots, N_Y\}$.

III. Proposed Narrowband Tracking-Based PLA Approach

The PLA process proposed in this work consists of two stages: training and verification. In the training stage, Bob verifies Alice's identity using higher-layer protocols and extracts a unique physical layer signature from the received signal,

[1]Note that the system can be also applied to a two-dimensional antenna arrays such as uniform planar array (UPA) and uniform circular array (UCA).

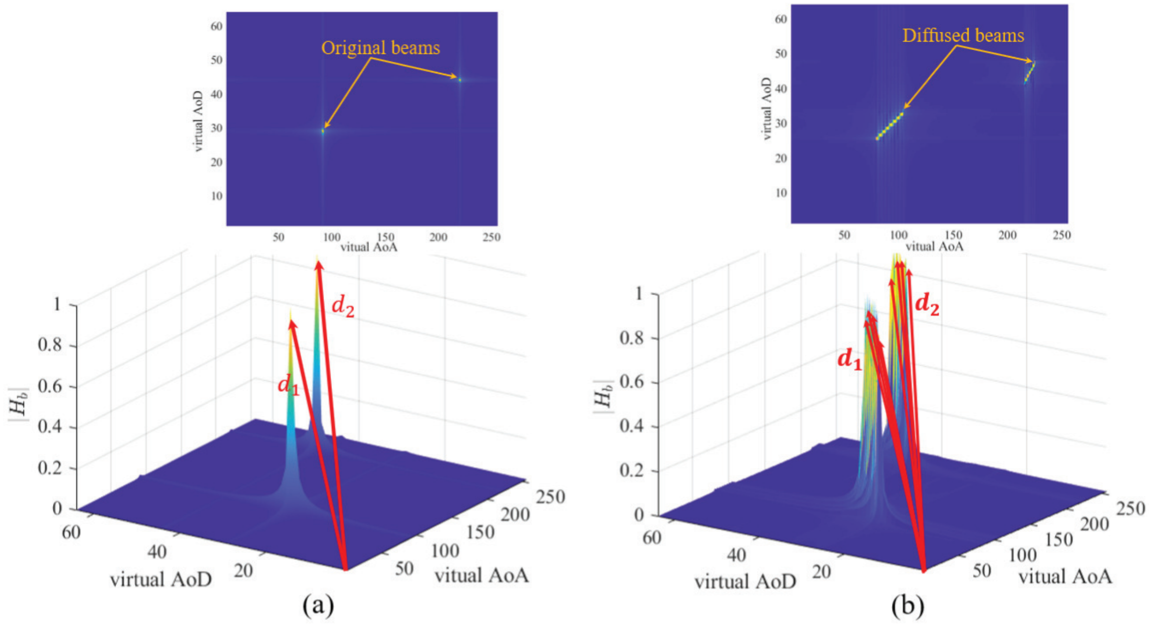


Fig. 2. The beamspace channel representation (a) without considering beam squint effect, and (b) with beam squint effect.

which is then stored in a database [20]. This stage assumes that only Alice and Bob nodes exist. In the verification stage, Bob employs pilots to detect and extract the signature from a received signal, where a hypothesis test is built to compare the stored signature in the database with the extracted one and verify the identity of the transmitter node as legitimate or not. However, due to the high channel variation in dynamic environments where Alice, Bob, or both are moving at a specific speed, database signature mismatching can occur, leading to authentication failures. To address the signature mismatching problem, an additional stage called the tracking stage, is introduced in this work. Through iterative updates over time, the tracking stage minimizes the mismatch between the signature observed in the training stage and the one in the verification stage, thereby improving the authentication system's performance. It should be noted that both the training and verification stages estimate the channels at Bob's end using pilot signals $\mathbf{s}$.

In this section, the procedure for extracting the proposed ED signature is discussed, and then the detection model is described. After that, the tracking process is presented.

A. ED Signature Extraction in Narrowband Transmission

Mmwave channel exhibits a limited scattering nature, resulting in a sparse channel property, while changing more rapidly than the sub-6GHz channels. Hence, a virtual sparse channel representation also called a beamspace representation, is the natural choice for the mmWave MIMO channels. In this beamspace representation, channel parameters including angle of departures and angle of arrivals can be easily estimated and extracted using sparse estimation methods with low overhead processing. It is proved that the angle estimation is robust to noise while presenting an accurate angle reciprocity even at low signal-to-noise ratio (SNR) levels. In this section, we propose a ED signature extraction method based on the channel parameters, angle of departures and angle of arrivals, in the beamspace representation of the MIMO channel.

The process of extracting the ED signature in the narrowband transmission is done during the training stage and can be described as follows:

1) At the first step, the system processes a channel estimation method to estimate the parameters angle of arrivals, angle of departures, and Doppler shift v such as methods in [21].[2]
2) Determine the index of the strongest element in the beamspace representation corresponding to the estimated angle of arrivals and angle of departures. This is done by finding the n value that makes Λ inside the Dirichlet sinc function in (4) equal to zero, i.e., optimum n for path l can be determined as
$$n^*(l) = \arg\min_{1\leq n\leq N} \left| \frac{d_c}{\lambda_c}\left(1+\frac{v_l}{f_c}\right)\sin(\theta_l) - \psi_n \right|. \quad (5)$$
Note that $n \in \{n_X, n_Y\}$, $N \in \{N_X, N_Y\}$, $v_l \in \{v_{T,l}, v_{R,l}\}$, and $\theta_l \in \{\theta_{T,l}, \theta_{R,l}\}$. Since we are in the training stage, there are only Alice and Bob nodes, hence, X here refers to Alice (A) and Y refers to Bob (B). Therefore, $n_X = n_A$, $N_X = N_A$, $n_Y = n_B$, and $N_Y = N_B$.
3) Assuming that $(\psi^*_{n_X}(l), \psi^*_{n_Y}(l))$ is the optimum spatial direction pair at path l for AoA and AoD, respectively, refers to the optimum index selecting in (5), $n_X{}^*(l)$ and $n_Y{}^*(l)$. Assuming the reference point (0,0) as shown in Fig. 2(a), the distance for the pair from the reference point is calculated as
$$d_l = \sqrt{(\psi^*_{n_X}(l))^2 + (\psi^*_{n_Y}(l))^2}. \quad (6)$$

[2]Due to the multi-dimensionality and sparsity of mmWave massive MIMO channels, tensor low-rank decomposition techniques can be fully exploited to obtain higher channel estimation accuracy with less pilot overhead. Therefore, a two-stage parallel factor (PARAFAC) tensor decomposition presented in [21] is employed to estimate the channel parameters in our work.

4) The distances in the ED vector signature $\mathbf{d}_e = [d_1, d_2, d_3, \cdots, d_{L_p}]^T$ are sorted in descend order, i.e.,

$$d_1 > d_2 > d_3 > \cdots > d_{L_p}. \tag{7}$$

5) At the end, the resulting ED signature $\mathbf{d}_e^{\mathrm{st}}(t_0)$ is stored in the database at Bob's side.

B. Detection Model

In the verification process that is based on the proposed ED signature, Bob first estimates the beamspace channel $\hat{\mathbf{H}}_b$ from the received signal $\boldsymbol{y}_b$ to detect its parameters. The received signal in the beamspace domain is given by

$$\boldsymbol{y}_b = \underbrace{\mathbf{U}\mathbf{H}\mathbf{U}^*\mathbf{s}}_{g(\boldsymbol{x}_{t_i})} + \mathbf{U}\mathbf{n}, \tag{8}$$

where $\mathbf{n}$ is a additive white Gaussian noise (AWGN) with zero mean and variance σ^2, $\mathbf{n} \sim \mathcal{CN}(0, \sigma^2)$. The novel ED signature, denoted as $\mathbf{d}_e(t_1)$, is then extracted from the estimated beamspace channel, as explained in Section III-A.

Next, a binary hypothesis test is performed to verify the identity of the transmitted signal:

$$\begin{aligned} K_0 &: \eta_L = \|\mathbf{d}_e(t_1) - \mathbf{d}_e^{\mathrm{st}}(t_0)\| \leq \eta_{th}, \\ K_1 &: \eta_L = \|\mathbf{d}_e(t_1) - \mathbf{d}_e^{\mathrm{st}}(t_0)\| > \eta_{th}, \end{aligned} \tag{9}$$

where $\mathbf{d}_e^{\mathrm{st}}(t_0)$ is the ED signature extracted and stored in the database in the training stage and η_{th} is a threshold used to separate between K_0 and K_1. Hypothesis K_0 corresponds to the case where the legitimate node, Alice, sent the received signal, while K_1 corresponds to the scenario where the legitimate node, Alice, did not send it (an attacker may have done).

By observing the distribution of η_L as analyzed in [16], the value of η_L can be approximated to a normal distribution under a spoofing attack case $\sim \mathcal{CN}(\mu_1, \sigma_1^2)$. Hence, for a given detection rate value γ, the threshold η_{th} can be obtained following $\eta_{th} = Q^{-1}(\gamma)\sigma_1 + \mu_1$, where $Q(\cdot)$ is the tail distribution function of the standard normal distribution. Here, the detection probability γ is defined as the probability of correctly detecting a forged signal when Alice did not transmit, i.e., $\gamma = Pr(\eta_L > \eta_{th}|K_1)$.

Under the assumption that the legitimate node channel and the attacker channel are independent, based on the first-order Gauss-Markov model [22], the channel correlation of the legitimate node can be represented

$$\mathbf{H}_{AB}^{t_i} = \sum_{l=1}^{L_p} \beta_l(t_i) \boldsymbol{a}_R^{(B)}(\theta_{R,l}(t_i), \nu_{R,l}) \boldsymbol{a}_T^{(A)*}(\theta_{T,l}(t_i), \nu_{T,l}), \tag{10}$$

where the channel parameters, $\theta_{R,l}$, $\theta_{T,l}$, and β_l, at successive time slots t_{i-1} and t_i can be mathematically expressed by

$$\begin{aligned} \beta_l(t_i) &= \rho\beta_l(t_{i-1}) + \varepsilon_1(t_{i-1}), \\ \theta_{T,l}(t_i) &= \theta_{T,l}(t_{i-1}) + \varepsilon_2(t_{i-1}), \\ \theta_{R,l}(t_i) &= \theta_{R,l}(t_{i-1}) + \varepsilon_3(t_{i-1}), \end{aligned} \tag{11}$$

with ρ is channel correlation coefficient between channel gain samples, $\varepsilon_1(t_{i-1}) \sim \mathbb{CN}(0, 1-\rho^2)$, $\varepsilon_2(t_{i-1})$ and $\varepsilon_3(t_{i-1}) \sim \mathcal{U}(-\varrho, \varrho)$ [23].

C. Tracking Process for The ED Signature in Narrowband Transmission

In mmWave transmission, the channel information obtained may last for a short period, due to short channel coherence time at these bands. Then, the channel has to be estimated again in the later transmission. Hence, a frequent estimation and authentication process is needed. This increases the complexity overhead in the system, especially in an environment where the transmission nodes or the scatters are in a movement, i.e., a dynamic environment. Therefore, a tracking approach can be applied to reduce the estimation overhead.

A tracking stage is integrated into the PLA process to enhance the authentication performance in dynamic environments such as high-speed railways. This mechanism tracks and updates the physical layer database signature in response to channel variations, resulting in a longer authorized connection period. This is possible because the beamspace channel parameters corresponding to Alice's node and signature change slowly, while an unauthorized node likely causes abrupt changes.

In our system model, the authentication process begins with initial channel acquisition to estimate the channel and authorize transmission nodes using upper-layer authentication techniques. Once channel estimation is completed and physical-layer channel features are extracted, the system enters a tracking mode. Various channel tracking techniques are employed to monitor temporal channel variations using a limited amount of radio resources. This tracking procedure is repeated in each transmission cycle and can be sustained for a defined period, denoted as T_o [24], aligning with processes outlined in the 5G NR standard [25]. The tracking mode concludes either when the transmission cycle exceeds T_o or when the connection between the nodes is lost due to sudden blockage or shadowing.

In the tracking stage, the first step is to define the state evolution and measurement models as shown below

$$\begin{aligned} \boldsymbol{x}_{t_i} &= f(\boldsymbol{x}_{t_{i-1}}) + \boldsymbol{w}_{t_i}, \\ z_{t_i} &= g(\boldsymbol{x}_{t_i}) + \boldsymbol{v}_{t_i}. \end{aligned} \tag{12}$$

Here, f denotes the state transition function, g represents the measurement model given in (8), $\boldsymbol{w}$ and $\boldsymbol{v}$ denote the process and observation noises, respectively. The noise vectors follow a Gaussian distribution with $\boldsymbol{w} \backsim \mathcal{N}(0, Q)$ and $\boldsymbol{v} \backsim \mathcal{N}(0, R)$. It is important to note that the state vector $\boldsymbol{x}$ captures the tracking parameters related to the physical layer characteristics of the developed signature, i.e., $\boldsymbol{x} = [\boldsymbol{\theta}_T, \boldsymbol{\theta}_R]^T$.

The model of the state transition function f for the tracked parameters $\boldsymbol{x}$ follows the first-order Gauss-Markov model, i.e., $\boldsymbol{\theta}_{t_i} = \boldsymbol{\theta}_{t_{i-1}} + \boldsymbol{\zeta}_{t_i}$ where $\zeta \backsim \mathcal{N}(0, \Sigma^2)$ [22], $\boldsymbol{\theta} \in \{\boldsymbol{\theta}_T, \boldsymbol{\theta}_R\}$ and $\Sigma \in \{\Sigma_T, \Sigma_R\}$. Note that the vectors $\boldsymbol{\theta}_T$ and $\boldsymbol{\theta}_R$ represent the angle values at all channel paths.

For a time-varying channel, channel gain β changes rapidly, while the angles θ_T and θ_R vary slowly. The angular variation can be measured according to the variation in Σ. Even with high Σ variation, since the correlation between the current angle and the previous one is high, the variation of the angle can be easily tracked over time.

To deal with the nonlinearity of the system, an extended Kalman filter (EKF) [26] is employed in this work due to its excellent performance and low computational complexity. The EKF effectively addresses error accumulation in track filtering by combining predictions based on a dynamic model with corrections from noisy measurements, thereby adapting to nonlinearity and noise in the system. It uses feedback to estimate the process state and divides the main iteration model into two stages: time propagation and observation update [22].

In time propagation, the filter updates the current state vector and error covariance according to the previous time information, i.e.,

$$\begin{aligned} \boldsymbol{x}_{t_i}^- &= f(\boldsymbol{x}_{t_{i-1}}), \\ \boldsymbol{P}_{t_i}^- &= \boldsymbol{A}_{t_{i-1}} \boldsymbol{P}_{t_{i-1}} \boldsymbol{A}_{t_{i-1}}^T + \boldsymbol{Q}, \end{aligned} \tag{13}$$

where $\boldsymbol{x}_{t_i}^-$ represents the priori estimate of the state vector at time t_i, $\boldsymbol{P}_{t_i}^-$ represents the covariance matrix of priori estimate, and $\boldsymbol{A}_{t_{i-1}} = \frac{df}{d\boldsymbol{x}}|_{\boldsymbol{x}_{t_{i-1}}^-}$ is the Jacobian matrix of $f(\boldsymbol{x})$ at $\boldsymbol{x}_{t_{i-1}}^-$.

In the observation update, the filter gain is combined with the prior estimate and observation values to form the posterior estimates, i.e.,

$$\begin{aligned} \boldsymbol{K}_{t_i} &= \boldsymbol{P}_{t_i}^- \boldsymbol{H}_{t_i}^T \frac{1}{\boldsymbol{H}_{t_i} \boldsymbol{P}_{t_i}^- \boldsymbol{H}_{t_i}^T + R} \\ \boldsymbol{x}_{t_i} &= \boldsymbol{x}_{t_i}^- + \boldsymbol{K}_{t_i} \left(\boldsymbol{y}_b - g(\boldsymbol{x}_{t_i}^-) \right) \\ \boldsymbol{P}_{t_i} &= \left(\boldsymbol{I} - \boldsymbol{K}_{t_i} \boldsymbol{H}_{t_i} \right) \boldsymbol{P}_{t_i}^- \end{aligned} \tag{14}$$

where $\boldsymbol{K}_{t_i}$ is the filter gain and $\boldsymbol{H}_{t_i} = \frac{dg}{d\boldsymbol{x}}|_{\boldsymbol{x}_{t_i}^-}$ is the Jacobian matrix of $g(\boldsymbol{x})$ at $\boldsymbol{x}_{t_i}^-$.

Note that the initial stage of the filter is taken from the physical layer characteristics extracted from the estimated channel at time t_0. As long as the transmitter node is authorized (i.e., the case K_0 occurs showing that the authentication is successful), within tracking duration T_o, Bob tracks the legitimate node's physical layer characteristics and updates its database. The process returns to the first step if authenticating the transmitted node fails (i.e., the case K_1 occurs pointing out that the authentication has failed) or the system exceeds the tracking period.

Figure 3 summarizes the proposed tracking-based PLA mechanism.

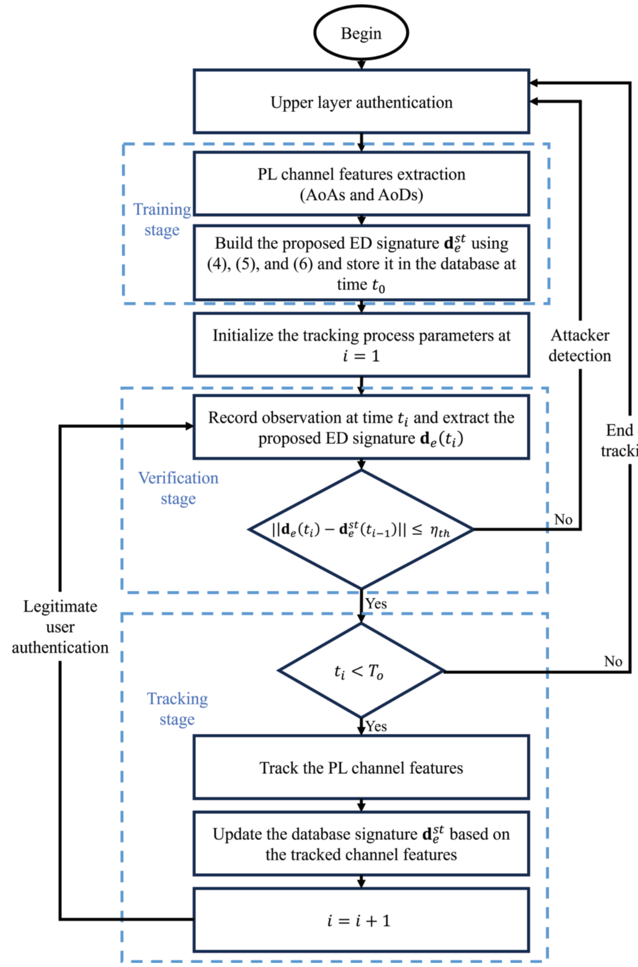


Fig. 3. The proposed tracking-based PLA flowchart.

IV. Proposed Wideband Tracking-Based PLA Approach

In practical wideband mmWave MIMO systems, frequency selectivity leads to wideband characteristics, resulting in the occurrence of the *beam squint effect* [27]. This effect causes the channel steering vector to become frequency-dependent, resulting in a modified expression for (2) as follows

$$\boldsymbol{a}(\theta, f) = \frac{1}{\sqrt{N}} \Big[1, e^{-j2\pi \frac{d_c}{\lambda_c} \left(1+\frac{v+f}{f_c}\right) sin(\theta)}, \cdots, e^{-j2\pi (N-1) \frac{d_c}{\lambda_c} \left(1+\frac{v+f}{f_c}\right) sin(\theta)} \Big]^T. \tag{15}$$

This leads to have different beam pointing direction for a different frequency at both transmission and reception, where the angle at a specific frequency is expressed as [28]

$$\theta(f) = \sin^{-1} \left(\frac{f}{f_c} \sin \hat{\theta} \right). \tag{16}$$

With a beam squint effect, the phase adjustment of the analog beamforming varies as a function of frequency as in (16) which limits the system performance. Therefore, numerous approaches have been proposed in the literature to deal with this problem. For example, some approaches utilize true-time-delay (TTD) lines [29], [30] to mitigate the beam squint effect in terahertz massive MIMO systems. On the other side, analog and hybrid beamforming designs [31], [32], [33], [34], [35] are also proposed to compensate for this effect. Although all these works tend to eliminate the beam squint effect, the squinting effect can be exploited to facilitate some level of security in communication networks. In this work, we propose the use of the beam squint effect in enhancing the proposed PLA scheme in wideband transmission.

Figure 2 provides an example of beamspace channel representation for a two-path MIMO channel. As shown in Fig. 2(a), a single path beam points to a particular grid point. However, due to the beam squint effect, the same path beam diffuses to multiple grid points, as demonstrated in Fig. 2(b). This phenomenon introduces limitations to the communication performance in wideband massive MIMO systems and poses challenges to traditional narrowband techniques. However, in this work, the beam squint effect is utilized to improve the authentication performance by increasing the richness of the enhanced distance signature. The details of this approach will be explained in the following sections.

In the following subsections, the process to detect and extract the ED in the wideband transmission is explained. Then, the modification of the tracking model for the wideband transmission is discussed.

A. Beam Squint-Based ED Signature in Wideband Transmission

The beam diffusion phenomenon in wideband MIMO systems allows for extracting multiple distance values, as shown in Fig. 2. In orthogonal frequency division multiplexing (OFDM) system with N_{FFT} subcarriers, ideally, $2N_{\text{FFT}}$ different distances can be extracted within a single path, as the beam is diffused in both the transmitter and receiver nodes, covering multiple grid points. However, due to the limited resolution of grid points in beamspace representation, resulting from a limited number of antenna elements at both ends, the number of the extracted distances is lower than in the ideal case. To address this, M distance signatures are extracted from a single beam (within one path), where $M \ll N_{\text{FFT}}$, is chosen based on the squinting amount in each beam, to obtain distinct distance values.

The process of extracting the enhanced distance signature in the wideband transmission is done during the training stage and can be described as follows:

1) First, the system processes a channel estimation method to estimate the parameters angle of arrivals, angle of departures, and Doppler shift v such as methods in [36] and [37] under wideband massive MIMO system design.[3]
2) Assume a multicarrier system as in OFDM with N_{FFT} subcarriers, the directions (angle of arrivals and angle of departures) of the beam within one path are calculated for all subcarriers using (16). The step is repeated for all paths to get $2N_{\text{FFT}}$ angles for each path (N_{FFT} values for angle of departures and N_{FFT} values for angle of arrivals).
3) Determine the index of the strongest element in the beamspace representation corresponding to the estimated channel parameters. This is done by finding the n value that makes Λ inside the Dirichlet sinc function in (4) equal to zero, i.e., optimum n for path l at specific subcarrier can be determined as
$$n^* = \arg \min_{1 \le n \le N} \left| \frac{d_c}{\lambda_c} \left(1 + \frac{f+v}{f_c}\right) \sin(\theta(f)) - \psi_n \right|, \quad (17)$$
for $n \in \{n_X, n_Y\}$ and $\theta \in \{\theta_R, \theta_T\}$. The optimum supports (n_X^*, n_Y^*) give the optimum virtual pair $(\psi_{n_X}^*, \psi_{n_Y}^*)$ for AoA and AoD.
4) Since the beamspace representation has a resolution limitation issue based on the antenna array size at both transmitter and receiver nodes, some of the optimum virtual pairs may equal each other. Hence, we drop the repeated pairs and remain with the unique ones which are assumed to be M pairs.[4]
5) Assume that $(\psi_{m_x}^*, \psi_{m_y}^*)$, with m_x and $m_y \in m$ and $m = 1, 2, \cdots, M$, is the optimum spatial direction pair in a single path for AoA and AoD, respectively. Given a reference point of (0,0), the distance of each pair from the reference point is calculated as
$$d_m = \sqrt{(\psi_{m_x}^*)^2 + (\psi_{m_y}^*)^2}, \quad (18)$$
for $m = 1, 2, \cdots, M$.
6) Steps 3 to 5 are repeated on each channel path to get all acceptable pairs to build the distance signature. Then, the distances are sorted in descending order, that is,
$$d_1 > d_2 > d_3 > \cdots > d_{M'}, \quad (19)$$
where $M' = \sum_{l=1}^{L_p} M_l$ with M_l is the number of pairs M that are extracted from the path l.
7) At the end, the resulting enhanced distance signature $\mathbf{d}_{\text{st}}(t_0)$ in the wideband system is stored in the database on Bob's side.

Detection Process: In the verification stage, the discussion in Section III-B is followed here where the channel is estimated from the received signal, then the characteristics of the physical layer are detected and extracted. After that, a hypothesis test is applied to the extracted features using (9) to detect the legitimate node and authenticate it.

B. Tracking Process for The ED Signature in Wideband Transmission

The proposed approach for tracking the beam squint-based enhanced distance signature is extended from the narrowband case discussed in Section III-C where the state vector $\boldsymbol{x}$ must include the angles of all paths and the angles of different frequencies used for constructing the signature for a given path.

As a result, the size of the $\boldsymbol{\theta}$ vector needs to be expanded to include the angles from different frequencies on each channel path for both $\boldsymbol{\theta}_T$ and $\boldsymbol{\theta}_R$. This expansion increases the complexity and time overhead of the tracking approach. To mitigate this complexity, we exploit the correlation between the angles of a single path, which are determined based on a fixed formula (i.e., a function of frequency and angle at the carrier frequency f_c, as given in (16)). Therefore, only the angles corresponding to f_{ref} within are tracked, and the other angles are calculated as $\theta(f_m) = \sin^{-1}(f_m/f_{\text{ref}} \sin\theta_{\text{ref}})$, where θ_{ref} is the reference angle used in the tracking process with its corresponding frequency f_{ref}.

In detail, the state vector $\boldsymbol{x}$ is divided into two parts: $\boldsymbol{x}^A$ and $\boldsymbol{x}^B$. Vector $\boldsymbol{x}^A = [\boldsymbol{\theta}_T^A, \boldsymbol{\theta}_R^A]^T$ is $2L_P \times 1$ a state vector that captures the tracking parameters related to the physical layer characteristics of the developed signature in the reference subcarrier f_{ref}. Vector $\boldsymbol{x}^B = [\boldsymbol{\theta}_T^B, \boldsymbol{\theta}_R^B]^T$ is $2(M' - L_P) \times 1$ state vector that captures the parameters related to the physical

[3]In the work here, we utilize the off-grid sparse Bayesian learning-based channel estimation algorithm, as presented in [36], to estimate the wideband mmWave MIMO channel with the beam squint effect. The algorithm works on the continuous angle-delay parameter domain to avoid grid mismatch problems and estimate the channel parameters with good accuracy.

[4]Note that, for the virtual pair corresponding to the angles AoA and AoD at carrier frequency f_c, if there are similar virtual pairs to this pair, the other pairs are dropped and the pair corresponds to f_c remains for the next step.

layer characteristics of the developed signature, which can be extracted and calculated from the reference angles in the state vector $\boldsymbol{x}^A$ using (16). This approach reduces the tracking complexity to be similar to that of narrowband systems.

The process of tracking the enhanced distance signature in the wideband transmission is done as follows:

1) For time propagation stage, the tracking filter updates the current state vector $\boldsymbol{x}^A$ and its covariance matrix as in (13), i.e.,

$$\begin{aligned}\boldsymbol{x}_{t_i}^{A-} &= f(\boldsymbol{x}_{t_{i-1}}^{A}),\\ \boldsymbol{P}_{t_i}^{A-} &= \boldsymbol{A}'_{t_{i-1}}\boldsymbol{P}_{t_{i-1}}^{A}\boldsymbol{A}'^{T}_{t_{i-1}} + \boldsymbol{Q},\end{aligned} \tag{20}$$

where $\boldsymbol{A}'_{t_{i-1}} = \frac{df}{dx}|_{\boldsymbol{x}_{t_{i-1}}^{A-}}$ is the Jacobian matrix of $f(\boldsymbol{x})$ at $\boldsymbol{x}_{t_{i-1}}^{A-}$. On the other hand, the current state vector $\boldsymbol{x}^B$ is updated as

$$\boldsymbol{x}_{t_i}^{B-} = Q(\boldsymbol{x}_{t_i}^{A-}), \tag{21}$$

where Q is the transition function for the parameters $\boldsymbol{\theta}_T^B$ and $\boldsymbol{\theta}_R^B$ given as $\theta(f_m) = \sin^{-1}(f_m/f_{\text{ref}}\sin\theta_{\text{ref}})$ where $\theta(f_m) \in \{\boldsymbol{\theta}_T^B, \boldsymbol{\theta}_R^B\}$ and $\theta_{\text{Ref}} \in \{\boldsymbol{\theta}_T^A, \boldsymbol{\theta}_R^A\}$.

2) For the observation updating stage, the tracking filter gain is given as

$$\boldsymbol{K}_{t_i}^{A} = \boldsymbol{P}_{t_i}^{A-}(\boldsymbol{H}_{t_i}^{A})^T \frac{1}{\boldsymbol{H}_{t_i}^{A}\boldsymbol{P}_{t_i}^{A-}(\boldsymbol{H}_{t_i}^{A})^T + R}, \tag{22}$$

where $\boldsymbol{H}_{t_i}^{A} = \frac{dg}{dx}|_{\boldsymbol{x}_{t_i}^{A-}}$ is the gradient of the measurement function $g(\boldsymbol{x})$ at $\boldsymbol{x}_{t_i}^{A-}$ and $\boldsymbol{x}_{t_i}^{B-}$. Furthermore, the posterior estimates are given as

$$\begin{aligned}\boldsymbol{x}_{t_i}^{A} &= \boldsymbol{x}_{t_i}^{A-} + \boldsymbol{K}_{t_i}^{A}\left(\boldsymbol{y}_b - g(\boldsymbol{x}_{t_i}^{A-}, \boldsymbol{x}_{t_i}^{B-})\right)\\ \boldsymbol{P}_{t_i}^{A} &= \left(\boldsymbol{I} - \boldsymbol{K}_{t_i}^{A}\boldsymbol{H}_{t_i}^{A}\right)\boldsymbol{P}_{t_i}^{A-}\\ \boldsymbol{x}_{t_i}^{B} &= Q(\boldsymbol{x}_{t_i}^{A})\end{aligned} \tag{23}$$

After tracking the developed signature reserved in the database, the database is updated and the verification process is started again to authenticate the legitimate user.

V. Simulation Results

In this section, we evaluate the performance of the proposed tracking-based PLA scheme through simulation analysis in terms of the probability of detection γ and probability of false alarm α. We assume that the attacker has the same capability as Alice, with $N_E = N_A = 128$ antenna elements, while Bob has $N_B = 256$ antenna elements, and uses $M = 3$ for the wideband systems. The EKF parameters utilized in this study are adopted from [22] where Σ_T and Σ_R are assumed to be 0.25^o in a static environment, and 0.5^o and 0.75^o in a dynamic environment. The initial filter state is $\boldsymbol{x}_{t_o} = \hat{\boldsymbol{x}}_o$, where $\hat{\boldsymbol{x}}_o$ is the estimated values of angle of departures and angle of arrivals, and its covariance is $\boldsymbol{P}_{t_o} = \text{diag}([\Sigma_T, \Sigma_R])$.

Unless stated otherwise, the numerical values of the used system parameters are given in Table I. Note that $L_p = 4$ corresponds to a high sparse channel environment while $L_p = 20$ corresponds to a low sparse one. When the system is static, the parameters are set to $v_{\max} = 0$, $\rho = 0.99$, and $\varrho = 0.01$. In a low-dynamic environment, the parameters are adjusted to $v_{\max} = 0.01f_c$, $\rho = 0.8$, and $\varrho = 0.1$, while in a high-dynamic environment, $v_{\max} = 0.1f_c$, $\rho = 0.7$ and $\varrho = 0.5$.

TABLE I
Simulation Parameters

Parameters		Value
Operating frequency f_c		60 GHz
Antenna elements N_E and N_A		128
Antenna elements N_B		256
SNR		20 dB
Number of subcarrier frequencies N_{FFT}		1024
Number of channel paths L_p		1, 4, 8, 20, 30
$\Sigma_T = \Sigma_R$		0.25^o, 0.5^o, 0.75^o
$v_{\max}$		0 , $0.01f_c$, $0.1f_c$
Tracking period T_o		6
Channel updates	ρ	0.99, 0.8, 0.7
	ϱ	0.01, 0.1, 0.5
Narrowband	System bandwidth W	100 MHz
Wideband	System bandwidth W	5 GHz
	$M = M_1 = M_2 = . = M_{L_p}$	3

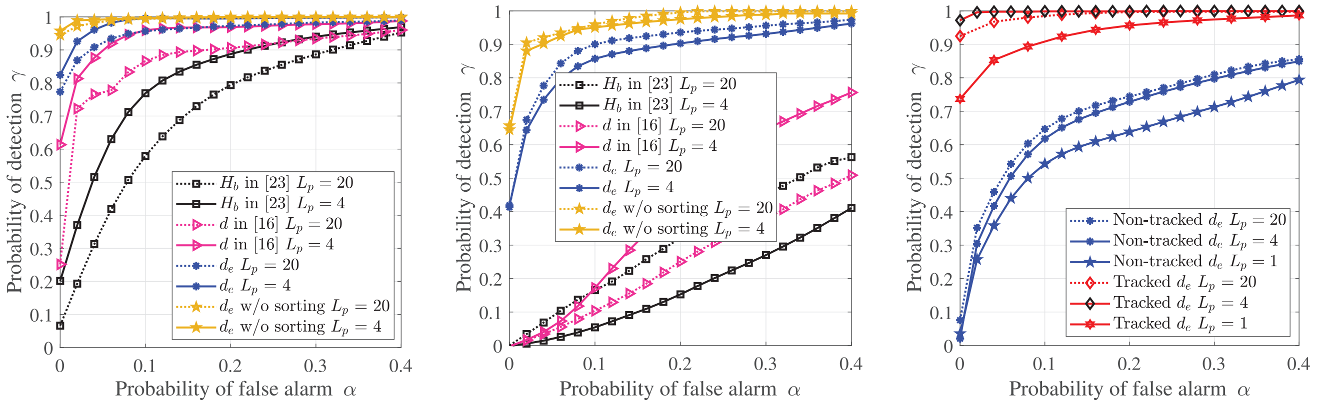
The results of the ED signature-based PLA scheme $\mathbf{d}_e$ are benchmarked against the distance signature proposed in [16] referred to $\mathbf{d}$ and the sparse beamspace channel signature presented in [23] referred to $\mathbf{H}_b$. To provide a more comprehensive evaluation of our proposed approach, we evaluate the performance of the proposed ED signature with and without the sorting step in (6) and (18). The performance of the proposed ED signature with the sorting step refers to "$\mathbf{d}_e$" and without the sorting step refers to "$\mathbf{d}_e$ w/o sorting" in the figures below.

A. Narrowband Transmission

In this section, we evaluate the authentication performance in narrowband transmission where the gain remains the same for each frequency in the range, given that the system bandwidth does not exceed 100 MHz. Narrowband communication is the perfect option for any application that needs reliable, low-power, and long-range communications.

In Fig. 4, we present the analysis of the probability of detection (γ) versus the probability of false alarm (α) across different sparsity levels in narrowband transmission. In Fig. 4(a), we observe that the proposed ED signature $\mathbf{d}_e$ consistently outperforms signatures $\mathbf{d}$ and $\mathbf{H}_b$ across varying levels of channel sparsity in static environments. This superior performance underscores the effectiveness of our proposed approach, particularly in scenarios with sparse channels.

Moving to Fig. 4(b), we delve into the performance of the ED signature in dynamic environments. Here, our approach demonstrates significant improvement over benchmark signatures. This enhancement is primarily attributed to the robustness of the ED signature in adapting to arbitrary channel variations, facilitated by the refinement of the sorting mechanism within our algorithm. Comparing the performance of our proposed ED signature with and without the sorting step in Figs. 4(a) and (b), it is observed that while the sorting mechanism enhances the consistency between Alice and Bob, it introduces a trade-off by slightly reducing the signature's randomness. This reduction in randomness can, in some scenarios, impact the robustness of the signature, particularly in environments with high interference or noise levels thus slightly degrading the PLA system performance.



(a) (b) (c)

Fig. 4. Probability of detection vs probability of false alarm analysis for (a) static, (b) low-dynamic, and (c) high-dynamic environment in narrowband transmission.

Figure 4(c) presents the performance of our tracking-based PLA approach in high-dynamic environments. It is noticed that the tracked ED signature exhibits enhanced performance and resilience across different sparsity levels. Notably, as the number of paths increases, the degradation in performance is mitigated due to the application of the tracking approach. Specifically, the tracking mechanism plays a pivotal role in continuously updating the stored signature for the intended user based on channel variation statistics. This proactive adjustment reduces the mismatch between the intended user's stored signature and their current signature. Consequently, the need for frequent authentication processes for that user is diminished, contributing to a more efficient and seamless authentication experience. Remarkably, from Fig. 4(c), our approach remains applicable even in single-path systems, $L_p = 1$, unlike previous methods such as those based on signatures $\mathbf{d}$ and $\mathbf{H}_b$, which fail to operate effectively in such scenarios.

B. Wideband Transmission

The authentication performance in the wideband transmission is evaluated in this section, where the system bandwidth goes beyond the channel coherence bandwidth and reaches the GHz bands. It is preferable in applications with high data rates such as IoT devices, criminal surveillance applications, and public safety services. Here, we assume that the system bandwidth is $W = 5$ GHz. Therefore, multicarrier signaling is used, such as OFDM with 1024 subcarriers ($N_{\text{FFT}} = 1024$). For simplicity, it is assumed that the number of extracted distances from all paths is similar (i.e., $M = M_1 = M_2 = \cdots = M_{L_p}$) and equal to 3 ($M = 3$) where we utilize the first, last, and middle subcarriers (f_1, $f_{N_{\text{FFT}/2}}$ and $f_{N_{\text{FFT}}}$) in the system band to extract the distance signature within one path.

Figure 5 represents the probability of detection γ versus probability of false alarm α analysis at different sparsity levels in wideband transmission under the beam squint effect. Fig. 5(a) shows the ED signature performance in a static environment, while Fig. 5(b) represents the performance in a low-dynamic environment. For a fair comparison, both the distance signature in [16] and the beamspace channel signature in [23] are modified to be applicable to wideband transmission. For the distance signature, the channel gain-based sorting mechanism is applied to the extracted distance vector at each utilized subcarrier frequency (first, middle, and last subcarriers). Then, the sorted distance vectors are arranged in one vector called $\hat{\mathbf{d}}$. Similarly, the beamspace channel at the utilized subcarriers (first, middle, and last subcarriers) is extracted and stored in one matrix signature called $\hat{\mathbf{H}}_b$. It is noticeable from both figures, Fig. 5(a) and (b), that the proposed ED signature-based wideband transmission outperforms the existing ones $\hat{\mathbf{d}}$ and $\hat{\mathbf{H}}_b$ in both static and dynamic environments. This superiority arises from the fact that the proposed ED signature is constructed based only on virtual angle indices in the beamspace representation corresponding to estimated angles and the distance between the indices and the original point. It is proven that the virtual angle estimation is robust to noise and exhibits high reciprocity even in low SNR regimes. Consequently, sudden channel variations do not significantly affect the estimated virtual angles, ensuring that the proposed ED signature remains stable. In contrast, $\hat{\mathbf{d}}$ and $\hat{\mathbf{H}}_b$ signatures depend on the path gain at each virtual angle, which reduces their stability and makes them more susceptible to noise and channel variations. In wideband transmission with a frequency-selective fading channel, these variations become more pronounced, further diminishing the performance of these signatures. Additionally, it is observed from the figure that the proposed approach makes the authentication performance less dependent on the sparsity level of the channel.

Figure 5(c) showcases the performance of our tracking-based PLA approach in a highly dynamic environment. Mirroring the trends observed in narrowband transmission, the tracked ED signature-based wideband transmission exhibits a substantial improvement in authentication performance compared to non-tracked signatures across different sparsity levels. Moreover, our proposed tracking-based PLA approach demonstrates adaptability even in single-path channels, further extending its applicability. In summary, the tracking-based

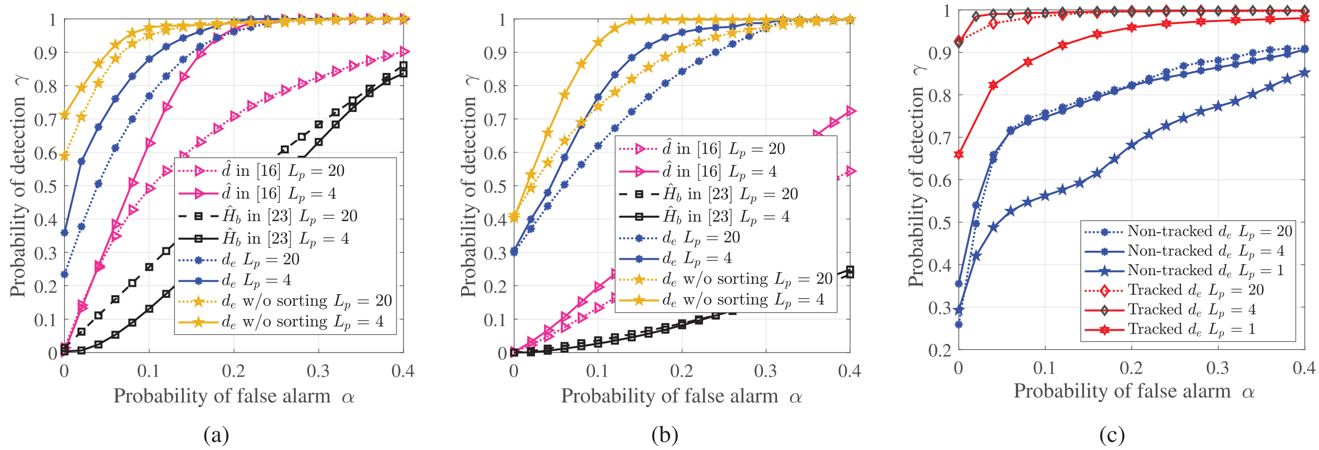


Fig. 5. Probability of detection vs probability of false alarm analysis for (a) static, (b) low-dynamic, and (c) high-dynamic environment in wideband transmission.

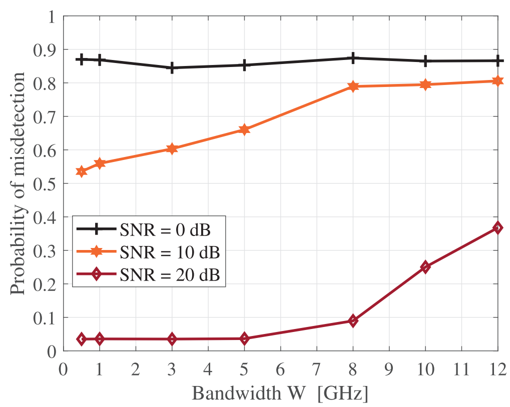


Fig. 6. Probability of misdetection vs system bandwidth.

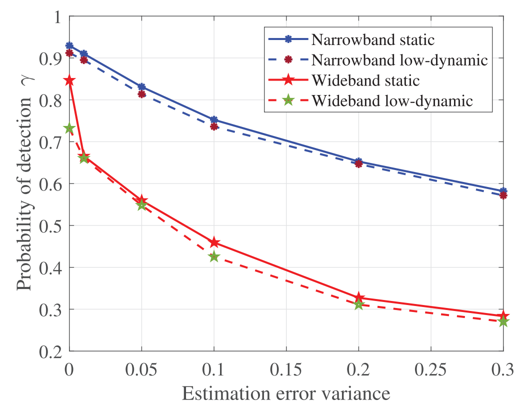


Fig. 7. Probability of detection vs channel estimation error analysis.

approach presents a promising solution for ensuring secure and reliable authentication in wideband mmWave MIMO systems, offering robust performance from the lowest to the highest sparsity levels.

In order to evaluate the performance of our proposed approach within wideband transmission, Fig. 6 illustrates the analysis of the probability of misdetection versus system bandwidth over different SNR levels. The misdetection probability is given as $P_{\text{md}} = 1 - \gamma = 1 - Pr(\eta_L > \eta_{th}|K_1)$. Here, we assume that the system has only 4 paths ($L_p = 4$) and the false alarm rate is 0.1 ($\alpha = 0.1$) operating in a low-dynamic scenario. In our proposed beam squint-based ED signature extraction, we assume M_l is different for different paths and is calculated based on the different d values that are extracted using (17) and (18) from each path. The figure reveals that with an increase in bandwidth, the misdetection probability of our proposed signature increases, holding true for both low and high SNR levels. This phenomenon is due to the escalating squinting effect with larger bandwidths, causing the squinted angles to exhibit greater variations, especially in dynamic environments. Consequently, the tracking process becomes necessary to address these variations effectively.

To evaluate the robustness of our proposed approach against imperfect channel estimation parameters, Fig. 7 shows the analysis of the probability of detection γ versus channel estimation error in both narrowband and wideband transmissions at a false alarm rate of 0.1. We observe that the detection rate of our proposed signature decreases by approximately 33% in narrowband systems and around 64% in wideband systems for both static and low-dynamic scenarios. Despite high error variance, our proposed signature demonstrates robustness to imperfect channel parameter detection in narrowband transmissions. However, the impact of imperfect estimation is more significant on the proposed PLA approach in wideband transmissions. This difference in robustness between narrowband and wideband systems can be attributed to the inherent characteristics of wideband channels. Wideband systems experience more pronounced frequency selectivity and beam squint effects, which exacerbate the sensitivity to estimation errors. These factors lead to greater variation in the channel response across different frequencies, making accurate channel estimation more challenging.

Figure 8 displays the behavior of our enhanced distance signature $\mathbf{d}_e$ during the tracking period in low- and high-dynamic environments. The variation of the normalized enhanced

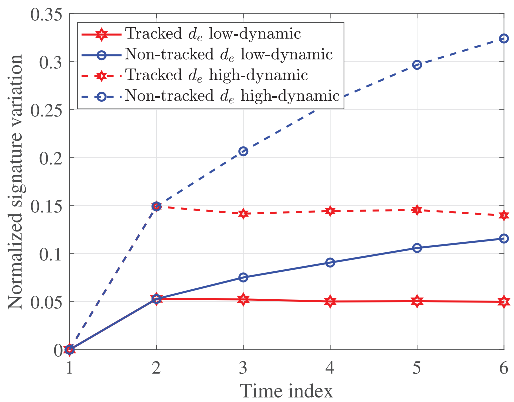


Fig. 8. The normalized signature variation vs time analysis.

signature over time is given as

$$\delta(t_i) = \left|\left|\frac{\mathbf{d}_e(t_i) - \mathbf{d}_e(t_{i-1})}{\mathbf{d}_e(t_{i-1})}\right|\right|. \tag{24}$$

The figure illustrates a noteworthy trend: the enhanced signature variation converges towards a fixed value over time with the adoption of the tracking process in the authentication scheme. Conversely, in higher dynamic systems without tracking, signature variation experiences a significant increase. This divergence in behavior can be attributed to the fundamental design of the proposed signature, which leverages low-variation physical layer features to build a unique signature to legitimate nodes. By implementing the tracking process, we exert control over this variation, effectively stabilizing the signature over time. This stabilization not only extends the duration of authorized connections but also ensures sustained authentication performance. Essentially, the tracking mechanism acts as a stabilizing force, mitigating the impact of dynamic channel conditions and preserving the integrity of the authentication process.

VI. Conclusion

This paper presents a novel tracking-based PLA scheme for narrowband and wideband mmWave MIMO networks in mobility scenarios. The proposed scheme introduces an enhanced distance signature that can be tracked and updated, providing longer authentication periods in both TDD and FDD transmissions within static and dynamic environments. Simulation results demonstrate the superior authentication performance of the proposed scheme compared to existing approaches in narrowband and wideband scenarios. This proposed system provides an efficient authentication solution for future mobile networks that are prevalent in next-generation wireless networks. Future work involves the integration of hardware-based features with the proposed signature to further enhance authentication performance in highly dynamic scenarios.

Acknowledgment

The authors thank the Scientific and Technological Research Council of Türkiye (TUBITAK) for their supports.

References

[1] M. S. J. Solaija, H. Salman, and H. Arslane, "Towards a unified framework for physical layer security in 5G and beyond networks," *IEEE Open J. Veh. Technol.*, vol. 3, pp. 321–343, 2022.

[2] N. Xie, Z. Li, and H. Tan, "A survey of physical-layer authentication in wireless communications," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 282–310, 1st Quart., 2021.

[3] P. Zhang, Y. Shen, X. Jiang, and B. Wu, "Physical layer authentication jointly utilizing channel and phase noise in MIMO systems," *IEEE Trans. Commun.*, vol. 68, no. 4, pp. 2446–2458, Apr. 2020.

[4] P. Zhang, J. Liu, Y. Shen, and X. Jiang, "Exploiting channel gain and phase noise for PHY-layer authentication in massive MIMO systems," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 4265–4279, 2020.

[5] 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.

[6] Y. Liu, P. Zhang, J. Liu, Y. Shen, and X. Jiang, "Physical layer authentication in MIMO systems: A carrier frequency offset approach," *Wireless Netw.*, vol. 28, no. 5, pp. 1909–1921, Jul. 2022.

[7] A. C. Polak, S. Dolatshahi, and D. L. Goeckel, "Identifying wireless users via transmitter imperfections," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 7, pp. 1469–1479, Aug. 2011.

[8] Q. Wang, "A novel physical layer assisted authentication scheme for mobile wireless sensor networks," *Sensors*, vol. 17, no. 2, p. 289, Feb. 2017.

[9] N. Xie, J. Chen, and L. Huang, "Physical-layer authentication using multiple channel-based features," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 2356–2366, 2021.

[10] J. Wang, Y. Shao, Y. Wang, Y. Ge, and R. Yu, "Physical layer authentication based on nonlinear Kalman filter for V2X communication," *IEEE Access*, vol. 8, pp. 163746–163757, 2020.

[11] N. Wang, W. Li, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical layer authentication for 5G communications: Opportunities and road ahead," *IEEE Netw.*, vol. 34, no. 6, pp. 198–204, Nov. 2020.

[12] M. Karabacak, B. Peköz, G. Mumcu, and H. Arslan, "Arraymetrics: Authentication through chaotic antenna array geometries," *IEEE Commun. Lett.*, vol. 25, no. 6, pp. 1801–1804, Jun. 2021.

[13] S. Balakrishnan, S. Gupta, A. Bhuyan, P. Wang, D. Koutsonikolas, and Z. Sun, "Physical layer identification based on spatial–temporal beam features for millimeter-wave wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 1831–1845, 2020.

[14] P. Zhang, T. Taleb, X. Jiang, and B. Wu, "Physical layer authentication for massive MIMO systems with hardware impairments," *IEEE Trans. Wireless Commun.*, vol. 19, no. 3, pp. 1563–1576, Mar. 2020.

[15] Y. Liu, P. Zhang, J. Liu, Y. Shen, and X. Jiang, "Exploiting fine-grained channel/hardware features for PHY-layer authentication in mmWave MIMO systems," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 4059–4074, 2023.

[16] L. Afeef, H. M. Furqan, and H. Arslan, "Physical layer authentication scheme in beamspace MIMO systems," *IEEE Commun. Lett.*, vol. 26, no. 7, pp. 1484–1488, Jul. 2022.

[17] H. Xie, F. Gao, S. Zhang, and S. Jin, "A unified transmission strategy for TDD/FDD massive MIMO systems with spatial basis expansion model," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3170–3184, Apr. 2017.

[18] R. W. Heath Jr., N. González-Prelcic, S. Rangan, W. Roh, and A. M. Sayeed, "An overview of signal processing techniques for millimeter wave MIMO systems," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 3, pp. 436–453, Apr. 2016.

[19] A. M. Sayeed and N. Behdad, "Continuous aperture phased MIMO: A new architecture for optimum line-of-sight links," in *Proc. IEEE Int. Symp. Antennas Propag. (APSURSI)*, Spokane, WA, USA, Jul. 2011, pp. 293–296.

[20] J. Tang, M. Dabaghchian, K. Zeng, and H. Wen, "Impact of mobility on physical layer security over wireless fading channels," *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 7849–7864, Dec. 2018.

[21] J. Du, M. Han, Y. Chen, L. Jin, and F. Gao, "Tensor-based joint channel estimation and symbol detection for time-varying mmWave massive MIMO systems," *IEEE Trans. Signal Process.*, vol. 69, pp. 6251–6266, 2021.

[22] V. Va, H. Vikalo, and R. W. Heath Jr., "Beam tracking for mobile millimeter wave communication systems," in *Proc. IEEE Global Conf. Signal Inf. Process. (GlobalSIP)*, Washington, DC, USA, Dec. 2016, pp. 743–747.

[23] J. Tang, A. Xu, Y. Jiang, Y. Zhang, H. Wen, and T. Zhang, "mmWave MIMO physical layer authentication by using channel sparsity," in *Proc. IEEE Int. Conf. Artif. Intell. Inf. Syst. (ICAIIS)*, Dalian, China, Mar. 2020, pp. 221–224.

[24] S. H. Lim, S. Kim, B. Shim, and J. W. Choi, "Deep learning-based beam tracking for millimeter-wave communications under mobility," *IEEE Trans. Commun.*, vol. 69, no. 11, pp. 7458–7469, Nov. 2021.

[25] *NR; Physical Channels and Modulation (Release 15)*, document TS 38.211 V15.2.0, 3rd Gener. Partnership Project (3GPP), 2018.

[26] T. Kailath, A. H. Sayed, and B. Hassibi, *Linear Estimation*. London, U.K.: Pearson, 2000.

[27] B. Wang, F. Gao, S. Jin, H. Lin, and G. Y. Li, "Spatial- and frequency-wideband effects in millimeter-wave massive MIMO systems," *IEEE Trans. Signal Process.*, vol. 66, no. 13, pp. 3393–3406, Jul. 2018.

[28] M. Cai et al., "Effect of wideband beam squint on codebook design in phased-array wireless systems," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Washington, DC, USA, Dec. 2016, pp. 1–6.

[29] K. Dovelos, M. Matthaiou, H. Q. Ngo, and B. Bellalta, "Channel estimation and hybrid combining for wideband terahertz massive MIMO systems," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 6, pp. 1604–1620, Jun. 2021.

[30] F. Gao, B. Wang, C. Xing, J. An, and G. Y. Li, "Wideband beamforming for hybrid massive MIMO terahertz communications," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 6, pp. 1725–1740, Jun. 2021.

[31] Z. Sattar, J. V. C. Evangelista, G. Kaddoum, and N. Batani, "Antenna array gain and capacity improvements of ultra-wideband millimeter wave systems using a novel analog architecture design," *IEEE Wireless Commun. Lett.*, vol. 9, no. 3, pp. 289–293, Mar. 2020.

[32] R. Zhang, W. Hao, G. Sun, and S. Yang, "Hybrid precoding design for wideband THz massive MIMO-OFDM systems with beam squint," *IEEE Syst. J.*, vol. 15, no. 3, pp. 3925–3928, Sep. 2021.

[33] L. Afeef, A. B. Kihero, and H. Arslan, "Novel transceiver design in wideband massive MIMO for beam squint minimization," 2022, *arXiv:2207.04679*.

[34] Y. Chen, D. Chen, T. Jiang, and L. Hanzo, "Channel-covariance and angle-of-departure aided hybrid precoding for wideband multiuser millimeter wave MIMO systems," *IEEE Trans. Commun.*, vol. 67, no. 12, pp. 8315–8328, Dec. 2019.

[35] Y. Chen, Y. Xiong, D. Chen, T. Jiang, S. X. Ng, and L. Hanzo, "Hybrid precoding for wideband millimeter wave MIMO systems in the face of beam squint," *IEEE Trans. Wireless Commun.*, vol. 20, no. 3, pp. 1847–1860, Nov. 2020.

[36] M. Wang, F. Gao, N. Shlezinger, M. F. Flanagan, and Y. C. Eldar, "A block sparsity based estimator for mmWave massive MIMO channels with beam squint," *IEEE Trans. Signal Process.*, vol. 68, pp. 49–64, 2019.

[37] M. Jian, F. Gao, Z. Tian, S. Jin, and S. Ma, "Angle-domain aided UL/DL channel estimation for wideband mmWave massive MIMO systems with beam squint," *IEEE Trans. Wireless Commun.*, vol. 18, no. 7, pp. 3515–3527, Jul. 2019.