CovertAuth: Joint Covert Communication and Authentication in MmWave Systems

Yulin Teng, Keshuang Han, Pinchang Zhang, *Member, IEEE*, Xiaohong Jiang, *Senior Member, IEEE*, Yulong Shen, *Member, IEEE*, and Fu Xiao, *Senior Member, IEEE*

***Abstract*—Beam alignment (BA) is a crucial process in millimeter-wave (mmWave) communications, enabling precise directional transmission and efficient link establishment. However, due to characteristics like omnidirectional exposure and the broadcast nature of the BA phase, it is particularly vulnerable to identity impersonation and eavesdropping attacks. To this end, this paper proposes a novel secure framework named CovertAuth, designed to enhance the security of the BA phase against such attacks. In particular, mutual coupling effect of antenna array impairments is explored as the device feature to design a weighted-sum energy detector-based physical layer authentication scheme. Moreover, theoretical models for authentication metrics like detection and false alarm probabilities are also provided to conduct performance analysis. Based on these models, an optimization problem is constructed to determine the optimal weight value that maximizes authentication accuracy. To combat eavesdropping attacks, the closed-form expressions of successful BA probability and covert transmission rate are derived. Then, a covert communication problem aimed at jointly optimizing beam training budget and transmission power is formulated to maximize covert communication throughput, subject to the covertness requirement. An alternating optimization algorithm combined with successive convex approximation is employed to iteratively achieve optimal results. Finally, simulation results demonstrate that CovertAuth outperforms existing works by an average of 11.8% and 9.9% detection accuracy improvement under the same covertness requirement.**

***Index Terms*—Physical layer authentication, covert transmission, antenna array impairment, mmWave beam alignment.**

I. Introduction

BENEFIT from the abundant spectrum resources and massive antenna arrays, millimeter-wave (mmWave) communication can exploit the highly directional beamforming technology to acquire ultra-high data transmission rates and extremely low latency [1]. Beam alignment (BA) is a critical prerequisite for the effective implementation of beamforming in mmWave communication. Accurate BA can significantly improve signal reception quality, compensate for high path loss, and maximize beamforming gain. However, the inherent characteristics of the BA process such as omnidirectional exposure, high-probability line-of-sight channel, and broadcast nature of training sequences also make it particularly vulnerable to identity impersonation and eavesdropping attacks [2]. Specifically, omnidirectional or quasi-omnidirectional scanning is generally used to find the optimal transmission path during the BA phase [3], inadvertently increasing exposure to potential adversaries. By transmitting deceptive alignment signals that mimic legitimate ones, adversaries can mislead the base station into aligning their beams with a malicious source [4]. Furthermore, the broadcast nature of beam training sequences during the BA stage allows adversaries to readily capture and analyze these sequences to infer beam directions and the underlying signal frame structure [5]. Once the beam direction is grasped, adversaries can position themselves strategically to monitor the communication process and even locate the location of the transmitter. Consequently, it is essential to design an effective and reliable defense mechanism for the BA stage to secure the establishment of the mmWave communication link.

Recently, physical layer security (PLS) technique has been considered a cost-effective approach to combat impersonation and eavesdropping attacks with reduced resource demands and higher architecture compatibility [6], [7]. On one hand, PLS for authentication utilizes inherent wireless channel characteristics or device-specific hardware fingerprints to validate user/device legitimacy [8]. On the other hand, PLS exploits the randomness of wireless channels such as fading, noise, and interference to improve communication secrecy [9]. However, in certain critical scenarios like military combat and location tracking service, merely protecting content confidentiality is far insufficient. It is also imperative to conceal the existence of transmission activities to effectively mitigate potential threats. Physical layer covert communication is an emerging PLS technique that allows the transmitter to discreetly convey information to the intended receiver at a specific rate, remaining undetected by adversaries and fundamentally preventing eavesdropping [10]. Therefore, it is expected that physical layer authentication combined with covert communication techniques can provide novel insights for designing secure mechanisms in the BA phase of mmWave systems.

Several recent studies have focused on deploying PLS methods in mmWave systems to address identity-based impersonation [11], [12], [13], [14], or eavesdropping attacks [15], [16], [17], [18]. For the physical layer authentication approaches, Wang *et. al* exploit the signal-to-ratio (SNR) trace in the sector-level sweep process to design an efficient spoofing attack detection scheme for IEEE 802.11ad mmWave networks

Y. Teng, K. Han, and P. Zhang are with the School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu, 210023, China (email:{2023040511, 1023041139, zpc}@njupt.edu.cn). They are also with the State Key Laboratory of Integrated Services Networks (Xidian University).

X. Jiang is with the School of Systems Information Science, Future University Hakodate, Hakodate, 041-8655, Japan (e-mail: jiang@fun.ac.jp).

Y. Shen is with the School of Computer Science and Technology, Xidian University, Xi'an 710071, China (e-mail: ylshen@mail.xidian.edu.cn).

F. Xiao (corresponding author) is with the School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu, 210023, China (e-mail: xiaof@njupt.edu.cn).

[11]. Following this line, the work in [12] investigates the uniqueness of the mmWave beam pattern feature and utilizes a deep autoencoder for illegal device detection with 98.6% accuracy. Later, Lu *et. al* leverage channel phase responses to mitigate performance losses due to imperfect channel correlation, demonstrating superior authentication performance even under low SNR conditions [13]. For the covert communication schemes, the authors of [16] employ a dual-beam mmWave transmitter to concurrently transmit desired signal to the legitimate receiver and a jamming signal to interfere with the adversary's detection capability. In [17], a full-duplex receiver is considered to generate jamming signals with a time-varying power for masking the presence of the legitimate transmitter. Xiao *et. al* explore the use of simultaneously transmitting and reflecting reconfigurable intelligent surfaces to support covert communication in a mmWave system [18]. However, the above methods are primarily designed to address one specific security threat, and their reliability may degrade when facing adversaries possessing multiple attack capabilities.

Given that few studies simultaneously consider impersonation and eavesdropping attacks in mmWave systems, we broaden our scope to include other wireless communication systems like non-orthogonal multiple access systems [19] and location service systems [20]. For instance, Xie *et. al* utilize the channel response to generate the secret keys for message encryption and a hybrid authentication scheme is also designed by using the tag and channel responses to achieve identity validation [19]. On this basis, Li *et. al* consider a cooperative attack scenario and propose an effective privacy-preserving physical layer authentication scheme to simultaneously protect privacy data and identity legitimacy [20]. Nevertheless, the characteristics of the mmWave systems such as sparse propagation environment and rapidly varying channels degrade the feature distinguishability of the adopted channel response fingerprint. Also, these schemes only provide content protection without fundamentally mitigating eavesdropping threats and thus cannot be directly deployed in the mmWave BA stage.

Although significant progress has been made in the design of PLS for mmWave systems by the works in [11], [12], [13], [14], [15], [16], [17], [18], several critical challenges remain unresolved. First, these schemes tend to focus solely on either identity authentication or privacy protection, lacking a unified security mechanism that can simultaneously address both aspects in mmWave systems. Second, they mainly focus on established mmWave communication links, without considering the identity validation and covertness requirement during the BA phase. This oversight enables BA prone to beam stealing or detection, compromising overall system security. Third, we observe the beam pattern is generally impacted by hardware impairments in antenna arrays (e.g., mutual coupling (MC) effects) [21]. It remains unclear whether such fine-grained imperfection could be leveraged to enhance authentication performance in mmWave systems, suggesting an opportunity for further research in incorporating MC effects into the secure authentication scheme design. Finally, current authentication schemes primarily rely on deep learning methods for feature extraction and identity verification. However, the reliance on such data-driven methods lacks a solid theoretical foundation, making it difficult to conduct rigorous performance analysis and to establish predictable guarantees.

To this end, we propose CovertAuth, a novel PLS framework suitable for the mmWave BA stage that simultaneously combats identity-based impersonation and eavesdropping attacks. For impersonation attacks, CovertAuth investigates the feature feasibility of the MC effect and incorporates it into the beam pattern to improve authentication reliability. For eavesdropping attacks, we first derive the closed-form expression of the BA performance metric. An optimization problem is then formulated to design the beam training budget and transmitting power for maximizing the covert communication throughput while satisfying the covertness transmission requirement. The main contributions of this paper are as follows:

- **MC Effect-based Authentication Scheme.** We first analyze the feature feasibility of the MC effect and explore its impact on the beam pattern. Considering the omni-directional scanning in BA phase, we assign different weight values to the received BA signals (involving the beam pattern impacted by the MC feature) and then design a cost-effective weighted-sum energy detector-based physical layer authentication scheme.
- **Design of Covert Communication for the BA Phase.** Based on a predefined beam codebook, we derive closed-form expressions for the BA performance metric and covert transmission capacity. Under the imperfect channel state information (CSI), the covert communication problem is formulated to design the beam training budget and transmission power for maximizing the covert communication throughput, subject to the required covertness constraint. The alternating optimization algorithm with successive convex approximation is adopted to iteratively find the optimal solution.
- **Theoretical Analysis and Optimal Weight Determination.** We also provide theoretical modeling for the authentication performance metrics like detection and false alarm probabilities. To enhance the authentication performance of CovertAuth, a quantitative relationship is established between weight and performance metrics using a sum-weighted approximation technique. With this relationship, we formulate an optimization problem to determine the optimal weight allocation that maximizes authentication accuracy under a false alarm constraint.
- **Performance Validation.** Extensive simulations are conducted to validate the correctness of the theoretical models and evaluate the robustness of CovertAuth against impersonation and eavesdropping attacks. The results indicate that CovertAuth exhibits performance improvement compared to existing works under the same covertness performance requirement.

The remainder of this article is organized as follows. Section II illustrates the problem formulation and system model. The design of CovertAuth is introduced in Section III and Section IV presents the theoretical analysis of CovertAuth. Numerical results are presented in Section V and Section VI reviews the related work. Finally, concluding remarks are provided in Section VII.

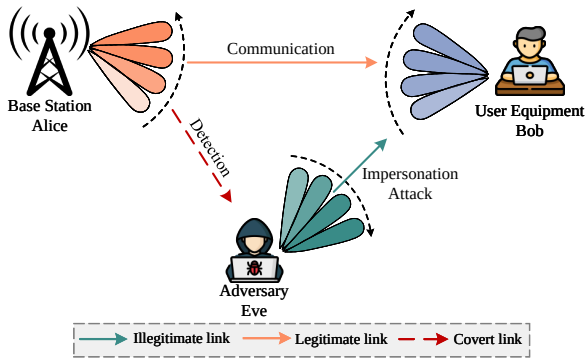


Fig. 1. System model.

II. Problem Formulation and System Model

A. Problem Formulation

As shown in Fig. 1, we consider a mmWave communication link establishment scenario consisting of a typical three-entity security model: one legal base station Alice with N_t antennas, a user equipment Bob with N_r antennas, and a malicious adversary Eve deployed with N_t antennas. Here, the uniform linear array (ULA) is adopted with half-wavelength antenna spacing. To establish the downlink between Alice and Bob, Alice initially transmits reference signals with different transmit antenna patterns to identify the useful spatial directions in the channel environment. Then, Bob sweeps the beam codebook with a variety of receiving beams to search for the optimal beam pair with the maximal received power and then reports the selection of the beam pair to Alice to accomplish the beam training [3], [22]. At the same time, the adversary Eve attempts to launch both passive and active attacks during the BA stage for confidential information recording and unauthorized access. Consequently, this paper aims to develop an effective and robust defensive framework for the BA stage to address the above security threats. Here, we assume that Bob possesses the fingerprint template of the legal transmitters for the identity validation phase.

B. Threat Model

To evaluate the resilience of the proposed defensive framework CovertAuth, a powerful adversary is assumed to perform passive surveillance or active manipulation during the mmWave communication link establishment. For the passive surveillance operation, the adversary attempts to detect the location of the transmitter and wiretap the communication channel for the sensitive information. For active attacks, the adversary intends to cheat the receiver to pass the authentication by impersonating the identity of the legal transmitter. The prototypical offensive tactics that an adversary may exploit in the BA stage are as follows.

- **Eavesdropping Attack.** In such a passive attack, Eve attempts to detect the position of the legal transmitter and stealthily record the transmitting signals. Then, She analyzes the captured signals for confidential information such as optimal beam pair selection and beampattern direction.
- **Identity-based Impersonation Attack.** We assume that Eve has prior knowledge about the adopted authentication scheme and communication protocol. Then, the adversary employs a device with the same model and hardware configuration to communicate with Bob by imitating the identity of Alice (e.g., the media access control address) for unauthorized access.

C. Mutual Coupling Effect Model

Mathematical Model of MC effects. The mutual coupling (MC) effects, as a kind of hardware imperfection in the antenna array, denote the electromagnetic interaction between antenna elements and are significantly influenced by the physical arrangement, antenna polarization, and manufacturing materials. For the considered ULA array, a symmetric Toeplitz matrix is generally exploited to model the MC structure [23]. If we use M to denote the number of non-zero MC coefficients, then the MC matrix of the transmit array $\mathbf{C}_t \in \mathbb{C}^{N_t \times N_t}$ is modeled by

$$\mathbf{C}_t = \text{Toeplitz}\{\mathbf{c}_\text{t}, 0, \cdots, 0\}. \tag{1}$$

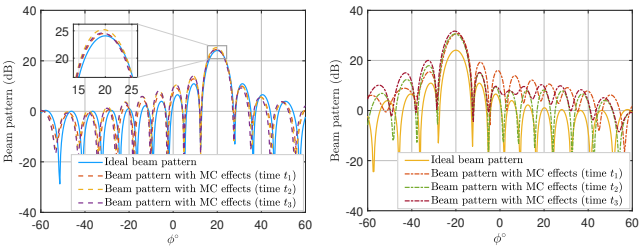
The MC vector $\mathbf{c}_t = [1, c_{t,1}, \cdots, c_{t,M-1}]^T \in \mathbb{C}^M$ and $c_{t,m}$ is the m-th non-zero element with $m = 1, 2, \cdots, M-1$. Following a similar way, we can obtain the MC matrix corresponding to the receiving antenna array $\mathbf{C_r}^{N_r \times N_r}$. Similar to previous work in [24], a complex Gaussian distribution with mean vector $\bar{\mathbf{c}}_t = [\bar{c}_{t,0}, \bar{c}_{t,1}, \cdots, \bar{c}_{t,M-1}]^T$ and covariance matrix $\sigma_c^2\mathbf{I}$ is adopted to generate the MC coefficient vector $\mathbf{c}_t$, that is, $\mathbf{c}_t \sim \mathcal{CN}(\bar{\mathbf{c}}_t, \sigma_c^2\mathbf{I})$. In specific, $\bar{c}_{t,m} = \frac{\varsigma}{d_m}$ and $\sigma_c^2 = \varsigma$, where d_m denotes the normalized antenna spacing distance between the first and the m-th element and ς represents the combined effects of antenna material properties and manufacturing tolerance, respectively.

Feature Feasibility Analysis of MC Effects. We analyze the feasibility of the MC effects in terms of feature uniqueness and stability. On one hand, the feature uniqueness of MC is attributed to the fact that several factors like array geometry, array element tolerance, and manufacturing material properties collectively result in a unique coupling pattern, which is challenging to replicate across different antenna arrays. On the other hand, the feature stability of MC is rooted in the fixed physical structure and high-performance materials (e.g., high temperature and wear resistance) of the antenna array. The former minimizes mechanical deformation, while the latter preserves structural integrity and mitigates the impact of temperature variations on MC effects. The above characteristics present the authentication potential of MC as the hardware fingerprint.

Effects of MC on Transmit Beam Pattern. The transmit beam pattern represents the radiation characteristics of an antenna array, depicting how signal power is distributed across different directions in space. For an ideal beam pattern with no hardware impairment, the response B_ideal is written as

$$B_\text{ideal}(\phi) = \mathbf{w}^H\mathbf{a}_t(\phi), \tag{2}$$

where $\mathbf{w} \in \mathbb{C}^{N_t}$ denotes the weight vector, representing the amplitude and phase adjustments applied to each antenna element. $\mathbf{a}_t(\phi)$ is the transmit array manifold vector, representing



(a) Device 1 at different time. (b) Device 2 at different time.

Fig. 2. Impacts of MC on transmit beam pattern using two devices with different antenna arrays.

the phase response of the transmit array at the angle ϕ. In practice, however, hardware imperfections such as MC effects between antenna elements alter the transmit beam pattern. Then, the actual beam pattern becomes:

$$B_{\mathrm{MC}}(\phi) = \mathbf{w}^H \mathbf{C}_t \mathbf{a}_t(\phi). \tag{3}$$

To further present the feasibility of MC as a unique antenna array fingerprint, we investigate its impact on the array radiation pattern. In this regard, we employ two transmitting devices with different antenna arrays and observe how the MC from two different antenna arrays affects the beam pattern under different time instants. The comparison results of the ideal and actual beam patterns are depicted in Fig. 2 and several interesting observations deserve attention. First, we can see from Fig. 2(a) and Fig. 2(b) that the MC effect makes the actual beam pattern deviate from the ideal one, primarily manifested as increased side-lobe levels and slightly broadened main-lobe width. Second, different devices with different antenna arrays lead to varying degrees of distortion in the beam pattern. This implies that the actual beam patterns with MC effects exhibit discernible device-specific characteristics. Moreover, due to the distinct locations of the two devices, the orientation angles of the main lobes are also markedly different, further enhancing the distinguishability of the beam pattern. Third, one can note from Fig. 2(a) or Fig. 2(b) that a high degree of similarity between the beam patterns generated by the same device at different time instants, indicating the relatively stable nature of MC effects within a certain time frame. The above observations motivate us to exploit the beam pattern feature incorporating MC effects to achieve identity authentication for the BA stage.

D. Signaling Model of Beam Alignment Stage

Due to the sparse scattering environment in the mmWave communication system, a single-path line of sight (LoS) channel between Alice and Bob $\mathbf{H} \in \mathbb{C}^{N_r \times N_t}$ is considered here. If we use α, θ and ϕ to denote the channel gain, angle of arrival (AoA), and angle of departure (AoD) respectively, then $\mathbf{H}$ with MC effects is characterized by

$$\mathbf{H} = \alpha[\mathbf{C_r}\mathbf{a}_r(\theta)][\mathbf{C_t}\mathbf{a}_t(\phi)]^H, \tag{4}$$

where $\mathbf{a}_r(\theta)$ and $\mathbf{a}_t(\phi)$ denote the steering vectors associated with the AoA and AoD, respectively. They can be further written as

$$\mathbf{a}_r(\theta) = [1, e^{j\pi\sin(\theta)}, \ldots, e^{j\pi(N_r-1)\sin(\theta)}]^T, \tag{5}$$

$$\mathbf{a}_t(\phi) = [1, e^{j\pi\sin(\phi)}, \ldots, e^{j\pi(N_t-1)\sin(\phi)}]^T. \tag{6}$$

During the BA stage, an exhaustive search-based beam scanning scheme is adopted by Alice and Bob with the predefined beam codebooks $\mathcal{C}_T = \{\mathbf{w}_{l_T} \in \mathbb{C}^{N_t \times 1}, l_T \in [1, 2, \ldots, L_T]\}$ and $\mathcal{C}_R = \{\mathbf{f}_{l_R} \in \mathbb{C}^{N_r \times 1}, l_R \in [1, 2, \ldots, L_R]\}$. In specific, $\mathbf{w}_{l_T} \in \mathbb{C}^{N_t \times 1}$ and $\mathbf{f}_{l_R} \in \mathbb{C}^{N_r \times 1}$ denote the selected codewords from the codebooks by Alice and Bob, respectively. L_T and L_r are the size of $\mathcal{C}_T$ and $\mathcal{C}_R$, respectively. The L_T unit-norm beams jointly cover the entire AoD region Φ and the L_R unit-norm beams jointly span the entire AoA region Θ. Then, the entire transceiver beam pair codebook $\mathcal{C}$ is composed of the Cartesian product of $\mathcal{C}_T$ and $\mathcal{C}_R$ (i.e., $\mathcal{C} = \{(\mathbf{w}, \mathbf{f}) : \mathbf{w} \in \mathcal{C}_T, \mathbf{f} \in \mathcal{C}_\mathbf{R}\}$) with the size of $L = L_R L_T$. For ease of expression, we represent $(\mathbf{w}_l, \mathbf{f}_l)$ as the l-th beam pair in the codebook $\mathcal{C}$, $l \in [1, L]$.

Based on the above beam scanning scheme, Alice utilizes the selected codeword $\mathbf{w}_l$ to transmit the pilot sequence $\mathbf{x} \in \mathbb{C}^N$ with beam training budget N symbols and Bob employs the receiver beam $\mathbf{f}_l$ to measure the power of the received signal. For the l-th beam pair, the output signal observed at the receiver side $\mathbf{y} \in \mathbb{C}^{N \times 1}$ is formulated by

$$\mathbf{y}_l = \sqrt{P}\mathbf{f}_l^H \mathbf{H}\mathbf{w}_l\mathbf{x} + \mathbf{n}, \tag{7}$$

where P is the transmission power and the pilot sequence carries energy $||\mathbf{x}||_2^2 = N$. Moreover, $\mathbf{n} \in \mathbb{C}^{N \times 1}$ denotes the zero-mean complex Gaussian noise with variance σ_n^2.

After receiving $\mathbf{y}_l$, Bob applies the known $\mathbf{x}$ to conduct a match-filtered output:

$$y_l = \mathbf{x}^H \mathbf{y}_l = \sqrt{P}N\mathbf{f}_l^H \mathbf{H}\mathbf{w}_l + \tilde{n}, \qquad l \in [1, L], \tag{8}$$

where $\tilde{n} = \mathbf{x}^H\mathbf{n} \sim \mathcal{CN}(0, N\sigma_n^2)$. Then, SNR of y_l is defined as SNR = $\frac{NP|\mathbf{f}_l^H\mathbf{H}\mathbf{w}_l|^2}{\sigma_n^2}$. For the received L beam signals, Bob selects the beam pair that maximizes the match-filtered output as the beam establishment candidate:

$$\hat{l} = \underset{l \in [1:L]}{\arg\max} \left| y_l \right|. \tag{9}$$

If we use R to denote the communication throughput between Alice and Bob during the BA stage, given the effects of BA quality on R, we adopt the concept of average effective capacity to characterize R as

$$R = \mathbb{E}\left\{ \sum_{l=1}^{L} \log\left(1 + \frac{NP|\mathbf{f}_l^H\mathbf{H}\mathbf{w}_l|^2}{\sigma_n^2}\right) \right\}. \tag{10}$$

III. Design of the CovertAuth

A. Overview of CovertAuth

To provide secure protection against eavesdropping and identity impersonation attacks during the BA stage, CovertAuth first jointly optimizes the transmission power P and beam training budget N to ensure covert transmission. Furthermore, it capitalizes on the beam feature induced by MC effects for signal origin validation. Consequently, the proposed CovertAuth mainly comprises two phases: covert transmission phase and identity authentication phase.

1) Covert Transmission Phase: In this phase, CovertAuth first uses the probability of successful alignment $P_{\rm a}$ to evaluate the BA quality and derives the analytical expression of the communication throughput by incorporating the impact of $P_{\rm a}$. Then, the covertness constraint on the adversary is characterized by the metric of detection error probability. Finally, CovertAuth carefully designs the transmission power P and beam training sequence length N to maximize the communication throughput between authorized entities subject to the covertness constraint. The detailed process of the covert transmission design is introduced in Section III-B.

2) Identity Authentication Phase: It is noted that the received BA signals $y_l, l \in [1, L]$ contain the beam pattern feature stemming from both the device-specific MC effect and spatial information of the transmitter. Therefore, in this phase, CovertAuth performs a weighted summation of L beam pair signals to design a weighting energy detector-based identity discriminator. This discriminator is then employed within a binary hypothesis testing framework to validate the identity legitimacy of the transmitter. The detailed process of identity authentication is introduced in Section III-C.

B. Covert Transmission Phase

Closed-form Expression of Communication Throughput. To derive the closed-form expression of R in (10), we proceed in two steps: 1) accurately characterize BA performance, and 2) derive an analytical expression for the average throughput model that captures the effects of BA performance. For the first step, we intend to quantify the effective channel gain corresponding to the l-th beam pair $g_l = |\mathbf{f}_l^H \mathbf{H} \mathbf{w}_l|^2$ with a predefined beam codebook and then exploit the probability of successful beam alignment $P_{\rm a}$ to evaluate BA quality. In particular, g_l is further written as

$$\begin{aligned} g_l =& |\mathbf{f}_l^H \mathbf{H} \mathbf{w}_l|^2 \\ =& |\alpha|^2 |\mathbf{f}_l^H \tilde{\mathbf{a}}_r(\theta) \tilde{\mathbf{a}}_t(\phi)^H \mathbf{w}_l|^2 \\ =& |\alpha|^2 F_l(\theta) W_l(\phi), \end{aligned} \tag{11}$$

where $\tilde{\mathbf{a}}_t(\phi) = \mathbf{C_t} \mathbf{a}_t(\phi)$ and $\tilde{\mathbf{a}}_r(\theta) = \mathbf{C_r} \mathbf{a}_r(\theta)$ denote the actual steering vectors at the transceiver ends impacted by the MC effects. In addition, $W_l(\phi) = |\tilde{\mathbf{a}}_t(\phi)^H \mathbf{w}_l|^2$ and $F_l(\theta) = |\mathbf{f}_l^H \tilde{\mathbf{a}}_r(\theta)|^2$ are beamforming gain at the transmitter and receiver side, respectively. Then, we use the beam codebook in [25] to quantify $W_l(\phi)$ and $F_l(\theta)$:

$$W_l(\phi) = \begin{cases} W_T \triangleq \frac{4\pi}{|\Omega_T|/L_T}, & \text{if } \phi \in \Phi_{\mathbf{w}_l}, \\ 0, & \text{otherwise}, \end{cases} \tag{12}$$

$$F_l(\theta) = \begin{cases} F_R \triangleq \frac{4\pi}{|\Omega_R|/L_R}, & \text{if } \theta \in \Theta_{\mathbf{f}_l}, \\ 0, & \text{otherwise}, \end{cases} \tag{13}$$

where Ω_T and Ω_R denote the solid angles covering the entire AoD and AoA region. Moreover, $\Phi_{\mathbf{w}_l}$ and $\Theta_{\mathbf{f}_l}$ are the covered regions related to the beam pair $\mathbf{w}_l$ and $\mathbf{f}_l$, respectively. The beam codebook quantization implies that when ϕ and θ fall within the coverage area $\Phi_{\mathbf{w}_l}$ and $\Theta_{\mathbf{f}_l}$, respectively, the maximum transmitting and receiving beamforming gain can be obtained as W_T and F_R. Otherwise, the beamforming gain is quantified as zero. Accordingly, g_l is quantified as

$$g_l = \begin{cases} |\alpha|^2 F_R W_T, & \text{if } \phi \in \Phi_{\mathbf{w}_l} \text{ and } \theta \in \Theta_{\mathbf{f}_l}, \\ 0, & \text{otherwise}. \end{cases} \tag{14}$$

It is evident that the precision of BA significantly affects the beamforming gain, and thus the metric for measuring BA performance is of particular interest. We propose to adopt the BA successful probability $P_{\rm a}$ as the evaluation metric. Without loss of generality, it is assumed that the optimal beam pair is $l = 1$. To obtain the analytical expression of $P_{\rm a}$, we define $Y_l = \frac{2|y_l|^2}{N\sigma_n^2}$ and explore the statistic information of Y_l. With the quantified channel gain g_l in (14), y_l is a complex Gaussian variable with mean $N\sqrt{Pg_l}$ and variance $N\sigma_n^2$. Then, the normalized statistic Y_l obeys a non-central Chi-square distribution $\chi_2^2(\lambda_l)$ with non-central parameter $\lambda_l = \frac{2NPg_l}{\sigma_n^2}$ and degrees of freedom (DoF) 2. In specific, for $l = 1$, $Y_1 \sim \chi_2^2(\lambda_1)$ with $\lambda_1 = \frac{2|\alpha|^2 NPF_R W_T}{\sigma_n^2}$; otherwise, $Y_l \sim \chi_2^2(0), l \in [2, L]$. The successful beam alignment event occurs when $\hat{l} = 1$, thus $P_{\rm a}$ is mathematically expressed by

$$\begin{aligned} P_{\rm a} &= 1 - \mathbf{Pr}(\hat{l} \neq 1) \\ &= 1 - \mathbf{Pr}(|y_1| < \max\{|y_2|, \cdots, |y_L|\}) \\ &= 1 - \mathbf{Pr}(Y_1 < \max\{Y_2, \cdots, Y_L\}). \end{aligned} \tag{15}$$

Then, we rank $(Y_2, Y_3, \cdots Y_L)$ in an ascending order $(Y_1^{'}, Y_2^{'}, \cdots, Y_{L-1}^{'})$ and $P_{\rm a}$ is rewritten as

$$P_{\rm a} = 1 - \mathbf{Pr}(Y_1 < Y_{L-1}^{'}). \tag{16}$$

To obtain the analytical expression of $P_{\rm a}$, the probability density function (PDF) of the $(L-1)$-th order statistic $Y_{L-1}^{'}$ (denoted as $f_{Y_{L-1}^{'}}(y)$) is necessary. The following Lemma 1 is first introduced to obtain $f_{Y_{L-1}^{'}}(y)$.

Lemma 1. *Let $X_1, X_2, \cdots, X_L$ be a set of independent and identically distributed (i.i.d.) order statistics from a continuous distribution with PDF $f(x)$ and cumulative distribution function $F(x)$. The PDF of the l-th order statistic X_l is given by*

$$f_{X_l}(x) = \frac{L!}{(l-1)!(L-l)!} [F(X)]^{l-1} [1 - F(X)]^{L-l} f(x). \tag{17}$$

Then, the PDF of $Y_{L-1}^{'}$ is evaluated as

$$f_{Y_{L-1}^{'}}(y) = \frac{(L-1)}{2} \left[\left(1 - \exp\left(-\frac{y}{2} \right) \right) \right]^{L-2} \exp\left(-\frac{y}{2} \right). \tag{18}$$

Proof. Since the $(L-1)$-th order statistic $Y_{L-1}^{'}$ is drawn from a central Chi-square distribution with DoF 2, the corresponding PDF and CDF are given as follows:

$$f(y) = \frac{1}{2} \exp\left(-\frac{y}{2} \right), \tag{19}$$

$$F(y) = 1 - \exp\left(-\frac{y}{2} \right). \tag{20}$$

Utilizing the equation in (17), the PDF of $Y_{L-1}^{'}$ is easily obtained in (18). □

With the Lemma 1, we present the following Theorem 1 to give the closed-form expression of $P_{\rm a}$:

Theorem 1. *For the adopted exhaustive search-based beam training scheme, let $P_{\rm a}$ denote the probability of successful beam alignment. Then, the closed-form expression of $P_{\rm a}$ is derived as follows:*

$$P_{\rm a} = 1 - \sum_{l=0}^{L-2}\left[(-1)^l \frac{\binom{L-2}{l}}{(l+1)(l+2)} \exp\left(-\frac{\lambda_1(l+1)}{2(l+2)}\right)\right] \times (L-1), \tag{21}$$

where $\binom{L-2}{l} = \frac{(L-2)!}{l!(L-2-l)!}$ is a combinatorial coefficient.

Proof. The key step in deriving $P_{\rm a}$ is to calculate the misalignment probability $P_{\rm ma} = \mathbf{Pr}(Y_1 < Y_{L-1}^{'})$:

$$\begin{aligned} P_{\rm ma} &= \int_0^\infty \left[1 - Q_1\left(\sqrt{\lambda_1}, \sqrt{y}\right)\right] f_{Y_{L-1}^{'}}(y)\mathrm{d}y \\ &= \frac{L-1}{2} \times \Bigg[\underbrace{\int_0^\infty \left[1-\exp\left(-\frac{y}{2}\right)\right]^{L-2} \exp\left(-\frac{y}{2}\right)\mathrm{d}y}_{J_1} - \\ &\underbrace{\int_0^\infty \left[1-\exp\left(-\frac{y}{2}\right)\right]^{L-2} \exp\left(-\frac{y}{2}\right) Q_1\left(\sqrt{\lambda_1}, \sqrt{y}\right)\mathrm{d}y}_{J_2}\Bigg], \end{aligned} \tag{22}$$

where $Q_1(a,b)$ denotes the Marcum Q-function with parameters a and b. Then, we can use the binomial theorem to obtain $[1-\exp\left(-\frac{y}{2}\right)]^{L-2} = \sum_{l=0}^{L-2}\binom{L-2}{l}[-\exp(-\frac{y}{2})]^l$, and J_1 is further written as

$$J_1 = \sum_{l=0}^{L-2}\binom{L-2}{l}\int_0^\infty \left[-\exp\left(-\frac{y}{2}\right)\right]^l \exp\left(-\frac{y}{2}\right)\mathrm{d}y, \tag{23}$$

and we define $J_{11} = \int_0^\infty [-\exp(-\frac{y}{2})]^l \exp(-\frac{y}{2})\mathrm{d}y$, simplified as

$$\begin{aligned} J_{11} &= \int_0^\infty (-1)^l \exp\left(-\frac{l}{2}y\right)\exp\left(-\frac{y}{2}\right)\mathrm{d}y \\ &= \int_0^\infty (-1)^l \exp\left(-\frac{(l+1)}{2}y\right)\mathrm{d}y. \end{aligned} \tag{24}$$

Finally, we can derive J_1 as

$$\begin{aligned} J_1 &= \sum_{l=0}^{L-2}\binom{L-2}{l}(-1)^l \int_0^\infty \exp\left(-\frac{(l+1)}{2}y\right)\mathrm{d}y \\ &= \sum_{l=0}^{L-2}\binom{L-2}{l}(-1)^l \frac{2}{l+1}. \end{aligned} \tag{25}$$

Similarly, J_2 can be obtained in (26), shown at the top of the next page. Substituting the results of J_1 and J_2 into (22) yields the closed-form expression of $P_{\rm ma}$, and the final result in (21) can be achieved. □

Considering the beam alignment performance, we now derive the analytical expression of the average communication throughput R as follows:

$$\begin{aligned} R &= \mathbb{E}\left\{\sum_{l=1}^{L}\log\left(1+\frac{NP|\mathbf{f}_l^H\mathbf{H}\mathbf{w}_l|^2}{\sigma_n^2}\right)\right\} \\ &= P_{\rm a}\log\left(1+\frac{|\alpha|^2 NPF_R W_T}{\sigma_n^2}\right). \end{aligned} \tag{27}$$

Characterization of Covertness Constraint. In this part, we adopt the detection performance at the Eve side to evaluate the covertness level during the transmission phase [15], [26]. Accordingly, a binary hypothesis testing of the received l-th beam pair signal $y_{e,l}, l \in [1, L]$ is formulated as

$$\begin{cases} \mathcal{D}_0: & y_{e,l} = \tilde{v}_l, \\ \mathcal{D}_1: & y_{e,l} = N\sqrt{P}\mathbf{h}_e\mathbf{w}_l + \tilde{v}_l, \end{cases} \tag{28}$$

where $\tilde{v}_l$ is a zero-mean Complex Gaussian noise with variance $N\sigma_e^2$ at Eve and $\mathbf{h}_e = \alpha_e\tilde{\boldsymbol{a}}_t(\phi)^H \in \mathbb{C}^{1\times N_t}$ denotes the channel between Alice and Eve with complex gain α_e. In particular, $\mathcal{D}_0$ represents the null hypothesis, indicating that Alice keeps silent. Under $\mathcal{D}_0$, $y_{e,l}$ is independently and identically distributed following $y_{e,l} \sim \mathcal{CN}(0, N\sigma_e^2)$. Conversely, $\mathcal{D}_1$ is the alternative hypothesis, indicating that Alice performs a transmission behavior with Bob. In this case, $y_{e,l} \sim \mathcal{CN}(N\sqrt{P}\mathbf{h}_e\mathbf{w}_l, N\sigma_e^2)$. After stacking all L beam pair signals into a column, we can obtain PDFs of $\mathbf{y}_e = [y_{e,1}, y_{e,2}, \cdots, y_{e,L}]^T \in \mathbb{C}^{L\times 1}$ under $\mathcal{D}_0$ and $\mathcal{D}_1$ (denoted by $P_0(\mathbf{y}_e)$ and $P_1(\mathbf{y}_e)$, respectively):

$$P_0(\mathbf{y}_e) = \frac{1}{[\pi(N\sigma_e^2)]^L}\exp\left(-\frac{\sum_{l=1}^{L}|y_{e,l}|^2}{N\sigma_e^2}\right), \tag{29}$$

$$P_1(\mathbf{y}_e) = \frac{1}{[\pi(N\sigma_e^2)]^L}\exp\left(-\frac{\sum_{l=1}^{L}|y_{e,l}-N\sqrt{P}\mathbf{h}_e\mathbf{w}_l|^2}{N\sigma_e^2}\right). \tag{30}$$

It is noted that Eve will make a binary decision to determine whether Alice transmits the signal to Bob and the total detection error probability (DEP) ξ is generally used to constrain the covertness performance. Specifically, ξ is a sum of the false alarm probability β_1 and miss detection probability β_2. We assume a minimum DEP ξ^* is achieved by using an optimal detector [27]. Then, the covertness constraint is formulated by $\xi^* \geq 1-\epsilon$ with the required covertness level ϵ. However, the intractability of ξ^* makes the closed-form expression of covertness constraint difficult to obtain. In line with [28], we employ the Kullback-Leibler divergence $\mathcal{D}(P_0(\mathbf{y}_e)||P_1(\mathbf{y}_e))$ to characterize the lower bound of ξ^* and then the above covertness constraint can be converted by using the Pinsker's inequality as

$$\xi^* \geq 1 - \sqrt{\frac{\mathcal{D}(P_0(\mathbf{y}_e)||P_1(\mathbf{y}_e))}{2}} \geq 1-\epsilon, \tag{31}$$

where $\mathcal{D}(P_0(\mathbf{y}_e)||P_1(\mathbf{y}_e))$ is specifically written as

$$\begin{aligned} \mathcal{D}(P_0(\mathbf{y}_e)||P_1(\mathbf{y}_e)) &= \mathbb{E}_{P_0}\left\{\ln P_0(\mathbf{y}_e) - \ln P_1(\mathbf{y}_e)\right\} \\ &= \frac{\sum_{l=1}^{L} NP|\mathbf{h}_e\mathbf{w}_l|^2}{\sigma_e^2}. \end{aligned} \tag{32}$$

$$J_2 = \sum_{l=0}^{L-2} \binom{L-2}{l} (-1)^l \int_0^{\infty} \exp\left(-\frac{(l+1)}{2} y\right) Q_1\left(\sqrt{\lambda_1}, \sqrt{y}\right) \mathrm{d}y$$
$$= \sum_{l=0}^{L-2} \binom{L-2}{l} (-1)^l \left[\frac{2}{l+1} - \frac{2}{(l+1)(l+2)} \exp\left(-\frac{\lambda_1(l+1)}{2(l+2)}\right)\right]. \quad (26)$$

Finally, the covertness performance constraint imposed on Eve is characterized by

$$\frac{\sum_{l=1}^{L} NP|\mathbf{h}_e \mathbf{w}_l|^2}{\sigma_e^2} \leq 2\epsilon^2. \quad (33)$$

Design of N and P for Covert Communication. To prevent eavesdropping attacks, we aim to maximize the covert throughput between Alice and Bob by carefully designing the beam training budget N and transmitting power P, subject to the covertness constraint. Due to the channel estimation error and non-cooperation between Alice and Eve, the imperfect channel with a bounded error model is also assumed:

$$\mathbf{h}_e = \hat{\mathbf{h}}_e + \Delta\mathbf{h}_e, \quad \forall ||\Delta\mathbf{h}_e||^2 \leq h_e^2, \quad (34)$$

where $\hat{\mathbf{h}}_e$ and $\Delta\mathbf{h}_e$ denote the imperfect channel and channel estimation error, respectively. The norm of estimation error $\Delta\mathbf{h}_e$ is bounded by a known constant h_e^2. Let $P_{\max}$ and $N_{\max}$ denote the maximum power on the transmitter and beam training budget, respectively. Therefore, under the imperfect channel state information scenario, the optimization problem with respect to N and P is formulated as

$$\max_{P,N} \ P_{\mathrm{a}} \log\left(1 + \frac{|\alpha|^2 NP F_R W_T}{\sigma_n^2}\right), \quad (35a)$$
$$\text{s.t. } 0 < P \leq P_{\max}, \quad (35b)$$
$$1 \leq N \leq N_{\max}, \quad (35c)$$
$$(33), (34).$$

It is noted that existing algorithms make it difficult to solve the above optimization problem due to the following reasons: 1) the coupling between N and P involved in constraint (33) and objective function; 2) the uncertainty in channel estimation leads to the infinite inequality constraints in (34); and 3) the discrete variable N results in a mixed integer non-convex optimization problem.

To tackle these problems, we first exploit the inequality transformation to obtain a more tractable manner. By using [29, Eq. 26], we can obtain the following inequality

$$\left|(\hat{\mathbf{h}}_e + \Delta\mathbf{h}_e)\mathbf{w}_l\right| \leq \left|\hat{\mathbf{h}}_e \mathbf{w}_l\right| + |\Delta\mathbf{h}_e \mathbf{w}_l| \leq \left|\hat{\mathbf{h}}_e \mathbf{w}_l\right| + h_e ||\mathbf{w}_l||. \quad (36)$$

Based on this inequality transformation, the constraints in (33) and (34) can be written into a more compact manner:

$$NP \sum_{l=1}^{L} \left||\hat{\mathbf{h}}_e \mathbf{w}_l| + h_e |\mathbf{w}_l|\right|^2 \leq 2\sigma_e^2 \epsilon^2. \quad (37)$$

To address the couple variables in objective function and constraints, the Lagrange dual-decomposition method is employed to decouple the problem (35) into a master dual problem and a subproblem. Let ν denote the nonnegative multiplier and $\boldsymbol{\varsigma} = [N, P]^T$ denote the optimization variable vector, then the Lagrange function is given by

$$\mathcal{L}(\nu; \boldsymbol{\varsigma}) = \log P_{\mathrm{a}} + \log\left(\log\left(1 + \frac{NP|\alpha|^2 F_R W_T}{\sigma_n^2}\right)\right)$$
$$- \nu\left(NP \sum_{l=1}^{L} \left||\hat{\mathbf{h}}_e \mathbf{w}_l| + h_e |\mathbf{w}_l|\right|^2 - 2\sigma_n^2 \epsilon^2\right). \quad (38)$$

Accordingly, the dual function $\mathcal{F}(\nu)$ is formulated by

$$\mathcal{F}(\nu) = \max_{\boldsymbol{\varsigma}} \mathcal{L}(\nu; \boldsymbol{\varsigma}). \quad (39)$$

For the given dual variable ν, the subproblem in terms of $\boldsymbol{\varsigma}$ is given by

$$\max_{\boldsymbol{\varsigma}} \ \log P_{\mathrm{a}} + \log\left(\log\left(1 + \frac{NP|\alpha|^2 F_R W_T}{\sigma_n^2}\right)\right) - \nu NP\Gamma, \quad (40a)$$
$$\text{s.t. } (35b), (35c),$$

where $\Gamma = \sum_{l=1}^{L} \left||\hat{\mathbf{h}}_e \mathbf{w}_l| + h_e |\mathbf{w}_l|\right|^2$. Based on the optimal variable $\boldsymbol{\varsigma}$, the master dual problem with respect to ν is as follows:

$$\min_{\nu} \ \mathcal{F}(\nu), \quad (41a)$$
$$\text{s.t. } (35b), (35c).$$

As to the master dual problem in (41a) and the subproblem in (40a), an alternating optimization algorithm combined with the successive convex approximation (SCA) method is employed to achieve an optimal solution of ν and $\boldsymbol{\varsigma}$. Let the superscript t be the t-th iteration.

1) Update ν for fixed N and P: Since the master dual problem in (41a) is always convex, we propose to adopt the subgradient method to optimize ν^{t+1} given the fixed $\boldsymbol{\varsigma}^t$, that is,

$$\nu^{t+1} = \max\left(0, \nu^t + \eta\left(N^t P^t \Gamma - 2\sigma_e^2 \epsilon^2\right)\right), \quad (42)$$

where η denotes the step size and operator $\max(0, a)$ ensures that the result is non-negative.

2) Update P for fixed N and ν: For the given N and ν, the optimization subproblem with respect to P can be formulated as

$$\max_{P} \ \log P_{\mathrm{a}} + \log\left(\log\left(1 + \frac{NP|\alpha|^2 F_R W_T}{\sigma_n^2}\right)\right)$$
$$- \nu NP\Gamma, \quad (43a)$$
$$\text{s.t. } (35b).$$

It is obvious that the above problem is difficult to solve due to the non-concave part of the objective function. To this end, we first partition the objective function into concave and non-concave parts (denoted by $\mathcal{F}_{\rm c}(P)$ and $\mathcal{F}_{\rm n}(P)$, respectively):

$$\mathcal{F}_{\rm c}(P) = \log\left(\log\left(1+\frac{NP|\alpha|^2F_RW_T}{\sigma_n^2}\right)\right) - \nu NP\Gamma, \quad (44)$$

$$\mathcal{F}_{\rm n}(P) = \log P_{\rm a}. \quad (45)$$

Then, we retain the partial concavity of the original objective function $\mathcal{F}_{\rm c}(P)$ and linearize the non-concave part $\mathcal{F}_{\rm n}(P)$. This allows us to construct a concave surrogate function $\tilde{F}(P)$ that approximates the original function while maintaining the desirable properties for optimization:

$$\tilde{\mathcal{F}}(P) = \mathcal{F}_{\rm c}(P) + \left.\frac{\partial \mathcal{F}_{\rm n}(P)}{\partial P}\right|_{P=P^t}\left(P-P^t\right) - \tau_p\left(P-P^t\right)^2, \quad (46)$$

where τ_p is a positive constant such that the surrogate function $\tilde{F}(P)$ is strongly concave. $\frac{\partial \mathcal{F}_{\rm n}(P)}{\partial P}$ is the partial derivative of $\mathcal{F}_{\rm n}(P)$ with respect to P, written as

$$\frac{\partial \mathcal{F}_{\rm n}(P)}{\partial P} = \frac{L-1}{P_{\rm a}\ln 2}\left[\sum_{l=0}^{L-2}(-1)^l\frac{\binom{L-2}{l}}{(l+1)(l+2)} \times \exp\left(-\frac{\lambda_1(l+1)}{2(l+2)}\right)\left(\frac{(l+1)}{(l+2)}\frac{|\alpha|^2NW_TF_R}{\sigma_n^2}\right)\right]. \quad (47)$$

Finally, the optimal value of P^{t+1} is obtained by solving the following concave optimization problem:

$$\max_{P} \ \tilde{F}(P), \quad \text{s.t. (35b).} \quad (48a)$$

It is obvious that the above problem can be effectively solved by using the CVX toolbox [30].

3) Update N for fixed P and ν: With fixed P and ν, the optimization for N is formulated as

$$\max_{N} \ \log P_{\rm a} + \log\left(\log\left(1+\frac{NP|\alpha|^2F_RW_T}{\sigma_n^2}\right)\right) - \nu NP\Gamma, \quad \text{s.t. (35c).} \quad (49a)$$

Similar to the optimization process for P, we also partition the objective function into concave and non-concave parts (denoted by $\mathcal{F}_{\rm c}(N)$ and $\mathcal{F}_{\rm n}(N)$, respectively):

$$\mathcal{F}_{\rm c}(N) = \log\left(\log\left(1+\frac{NP|\alpha|^2F_RW_T}{\sigma_n^2}\right)\right) - \nu NP\Gamma, \quad (50)$$

$$\mathcal{F}_{\rm n}(N) = \log P_{\rm a}. \quad (51)$$

The concave surrogate function $\tilde{F}(P)$ is written as

$$\tilde{F}(N) = F_c(N) + \left.\frac{\partial \mathcal{F}_{\rm n}(N)}{\partial N}\right|_{N=N^t}\left(N-N^t\right) - \tau_N\left(N-N^t\right)^2, \quad (52)$$

where τ_N is a positive constant ensuring that $\tilde{\mathcal{F}}(N)$ is strongly concave. $\frac{\partial \mathcal{F}_{\rm n}(N)}{\partial N}$ is the derivative part of $\mathcal{F}_{\rm n}(N)$ with respect to N, given by

$$\frac{\partial \mathcal{F}_{\rm n}(N)}{\partial N} = \frac{L-1}{P_{\rm a}\ln 2}\left[\sum_{l=0}^{L-2}(-1)^l\frac{\binom{L-2}{l}}{(l+1)(l+2)} \times \exp\left(-\frac{\lambda_1(l+1)}{2(l+2)}\right)\left(\frac{l+1}{l+2}\frac{|\alpha|^2PW_TF_R}{\sigma_n^2}\right)\right]. \quad (53)$$

Finally, the variable N is optimized by solving the following problem

$$\max_{N} \ \tilde{\mathcal{F}}(N), \quad \text{s.t. (35c).} \quad (54a)$$

Obviously, the above problem can be solved by using existing algorithms or the CVX toolbox. To ensure that the obtained N^{t+1} conforms to the constraint of a discrete integer, we round N^{t+1} to its nearest integer:

$$N^{t+1} = \left\lfloor N^{t+1} + \frac{1}{2}\right\rfloor. \quad (55)$$

Based on the above process, CovertAuth jointly designs the beam training budget N and transmitting power P to protect the transmission intention with maximized communication throughput between Alice and Bob. The whole design scheme is summarized in Algorithm 1.

Algorithm 1 Joint Transmitting Power and Beam Training Budget Design Algorithm.

Input: Γ, σ_e^2, σ_n^2, $t_{\max}$, tolerance $\tilde{\rho}$, ϵ, η, τ_p, τ_N.
Output: $P^\star$ and $N^\star$.
1: **Initialization:** feasible initial point (ν^0 ,P^0, N^0), $t=0$, $\rho^0=0$.
2: **while** $\rho^t > \tilde{\rho}$ and $t \le t_{\max}$ **do**
3: Update ν^{t+1} by (42).
4: Update P^{t+1} by solving (48a).
5: Update N^{t+1} by solving (54a).
6: Round N^{t+1} by (55).
7: Calculate $\rho^{t+1} = \left|\mathcal{L}(\nu^{t+1};\boldsymbol{\varsigma}^{t+1}) - \mathcal{L}(\nu^t;\boldsymbol{\varsigma}^t)\right|$.
8: $t = t+1$.
9: **end while**
10: **return** $P^\star = P^t$ and $N^\star = N^t$.

C. Identity Authentication Phase

Authentication Criterion with $N^\star$ and $P^\star$. For the receiver Bob, it is imperative to authenticate the identity of the signals and then decide whether to establish a communication link with the transmitter. Due to the beam pattern feature involved in the beam pair signals y_l, Bob intends to exploit y_l to accomplish identity verification. The identity validation criterion can be formulated by using a binary hypothesis testing:

$$\begin{cases} \mathcal{H}_0: & y_l = N_0^\star\sqrt{P_0^\star}\mathbf{f}_l^H\alpha_0\tilde{\mathbf{a}}_{r,0}(\theta_0)\tilde{\mathbf{a}}_{t,0}^H(\phi_0)\mathbf{w}_l + \tilde{n}_l, \\ \mathcal{H}_1: & y_l = N_1\sqrt{P_1}\mathbf{f}_l^H\alpha_1\tilde{\mathbf{a}}_{r,1}(\theta_1)\tilde{\mathbf{a}}_{t,1}^H(\phi_1)\mathbf{w}_l + \tilde{n}_l. \end{cases} \quad (56)$$

In specific, under the null hypothesis $\mathcal{H}_0$, $\tilde{\mathbf{a}}_{r,0}(\theta_0) = \mathbf{C}_{\mathbf{r},0}\mathbf{a}_r(\theta_0)$ and $\tilde{\mathbf{a}}_{t,0}(\phi_0) = \mathbf{C}_{\mathbf{t},0}\mathbf{a}_t(\phi_0)$ denote the steering vectors containing both MC feature and spatial information of the authorized transmitter, indicating that the signals are from Alice. In contrast, on $\mathcal{H}_1$, $\tilde{\mathbf{a}}_{r,1}(\theta_1) = \mathbf{C}_{\mathbf{r},0}\mathbf{a}_r(\theta_1)$ and $\tilde{\mathbf{a}}_{t,1}(\phi_1) = \mathbf{C}_{\mathbf{t},1}\mathbf{a}_t(\phi_1)$ denote the steering vectors containing both MC feature and spatial information of the unauthorized transmitter, implying that the current transmitter is Eve. Due to the different wireless channels (i.e., Alice-Bob and Eve-Bob), it is difficult for Eve to possess the same beam training budget N and transmitting power P as those related to Alice. Herein, we consider a challenging scenario (i.e., $N_1 \approx N_0^\star$ and $P_1 \approx P_0^\star$) to evaluate the robustness of the proposed authentication method.

Sum-weighted Authentication Scheme. Note that each beam pair signal y_l carries a certain degree of MC fingerprint and spatial location information of the transmitter. The degree of device fingerprints in y_l is related to its beamforming gain. Therefore, we assign various weights ω_l to the L beam pair signals $y_l, l \in [1, L]$ and then exploit the energy detector to design the final identity discriminator:

$$T = \sum_{l=1}^{L} \omega_l \frac{2|y_l|^2}{N^\star \sigma_n^2} \underset{H_0}{\overset{H_1}{\gtrless}} \tau, \tag{57}$$

where T is the decision test statistic and τ is the threshold. Based on this identity discriminator, Bob can effectively validate the identity legitimacy of the current transmitter. The weighting scheme ensures that y_l with stronger fingerprint characteristics contributes more to the final decision, thereby enhancing the reliability of CovertAuth.

IV. Theoretical Performance Analysis

A. Modeling of Authentication Performance Metrics

Theoretical analysis of the proposed authentication scheme can facilitate the prediction and optimization of the security performance. Accordingly, we derive the analytical expressions of authentication metrics in terms of false alarm (denoted by P_f) and detection probabilities (denoted by P_d). The false alarm event refers to the receiver incorrectly identifying a legitimate device as an unauthorized one. Thus, P_f is mathematically expressed as $P_f \triangleq \mathbf{Pr}(T > \tau|\mathcal{H}_0)$. On the other hand, a detection event is triggered when the receiver successfully identifies ongoing unauthorized attempts, that is $P_d \triangleq \mathbf{Pr}(T > \tau|\mathcal{H}_1)$. To derive the closed-form expressions of P_f and P_d, for a given τ, it is necessary to investigate the right tail probabilities of test statistic T under two hypotheses. However, since T is a weighted sum of L noncentral Chi-square variables, the PDF of T cannot be directly acquired. Thus, we provide the following Lemma 2 to approximate the right tail probability of T under a threshold τ.

Lemma 2. *Let Y_l denote the l-th noncentral chi-squared random variable with noncentrality parameter λ_l and DoF 2. Consider a weighted sum of L noncentral chi-squared random variables $T = \sum_{l=1}^{L} \omega_l Y_l$, then the right-tail probability of T with a threshold τ is approximated by a right-tail probability for a noncentral chi-squared random variable $K \sim \chi^2_{\upsilon_K}(\lambda_K)$ under a new threshold τ_K:*

$$\mathbf{Pr}\left(T > \tau\right) \approx \mathbf{Pr}\left(K > \tau_K\right), \tag{58}$$

where $\tau_K = [(\tau - \mu_T)/\sigma_T]\sqrt{2\upsilon_K + 4\lambda_K} + \upsilon_K + \lambda_K$. $\mu_T = \gamma_1$ and $\sigma_T = \sqrt{2\gamma_2}$ denote the mean and standard deviation of T with $\gamma_k = 2\sum_{l=1}^{L}(\omega_l)^k + k\sum_{l=1}^{L}(\omega_l)^k\lambda_l$. Moreover, λ_K and υ_K are respectively calculated by

$$\lambda_K = s_1 a^3 - a^2, \quad \upsilon_K = a^2 - 2\lambda_K, \tag{59}$$

where $a = 1/(s_1 - \sqrt{(s_1)^2 - s_2})$ with $s_1 = \gamma_3/(\gamma_2)^{3/2}$ and $s_2 = \gamma_4/(\gamma_2)^2$.

Proof. Please refer to [31] for more details. □

Based on the above Lemma 2, the analytical expressions of P_f and P_d are summarized in Theorem 2.

Theorem 2. *For the considered mmWave beam alignment stage, we exploit the beam pattern feature induced by both the MC fingerprint and spatial information related to the device to authenticate the identity legitimacy of the transmitter. Given a fixed threshold τ, P_f and P_d are given by, respectively*

$$P_f \approx \int_{\tau_A}^{\infty} \frac{1}{2}\left(\frac{x}{\lambda_A}\right)^{\frac{(\upsilon_A-2)}{4}} \exp\left(-\frac{1}{2}\left(x + \lambda_A\right)\right) \times I_{\frac{\upsilon_A}{2}-1}\left(\sqrt{x\lambda_A}\right)\mathrm{d}x, \tag{60}$$

$$P_d \approx \int_{\tau_E}^{\infty} \frac{1}{2}\left(\frac{x}{\lambda_E}\right)^{\frac{(\upsilon_E-2)}{4}} \exp\left(-\frac{1}{2}\left(x + \lambda_E\right)\right) \times I_{\frac{\upsilon_E}{2}-1}\left(\sqrt{x\lambda_E}\right)\mathrm{d}x, \tag{61}$$

where $\tau_K = [(\tau - \mu_{T,K})/\sigma_{T,K}]\sqrt{2\upsilon_K + 4\lambda_K} + \upsilon_K + \lambda_K, K = \{A, E\}$. To avoid the repetition, the detailed calculation of parameters $(\mu_{T,K}, \sigma_{T,K}, \upsilon_K, \lambda_K)$ are explained in the following proof. $I_\upsilon(\cdot)$ is the modified Bessel function of the first kind with order $\upsilon = \frac{\upsilon_K}{2} - 1$.

Proof. Under $\mathcal{H}_0$, let $Y_l = \frac{2|y_l|^2}{N^\star\sigma_n^2}$ and we can easily observe that $Y_l|\mathcal{H}_0$ is distributed to a noncentral Chi-square distribution with DoF 2 and noncentral parameter $\lambda_{l,0} = \frac{2N^\star P^\star |\mathbf{f}_l^H \mathbf{H}_0 \mathbf{w}_l|^2}{\sigma_n^2}$, where $\mathbf{H}_0 = \alpha_0 \tilde{\mathbf{a}}_{r,0}(\theta_0)\tilde{\mathbf{a}}_{t,0}^H(\phi_0)$. Thus, the test statistic T is a weighted sum of L noncentral Chi-squared variables Y_l with $\lambda_{l,0}$ and DoF 2. From Lemma 2, P_f can be approximated by the right tail probability of a noncentral Chi-square variable K_A with noncentral parameter λ_A and DoF υ_A:

$$\begin{aligned} P_f &\triangleq \mathbf{Pr}(T > \tau|\mathcal{H}_0) \\ &\approx \mathbf{Pr}(K_A > \tau_A), \end{aligned} \tag{62}$$

where $\tau_A = [(\tau - \mu_{T,A})/\sigma_{T,A}]\sqrt{2\upsilon_A + 4\lambda_A} + \upsilon_A + \lambda_A$. The parameters $\mu_{T,A}$ and $\sigma_{T,A}$ are given by, respectively

$$\mu_{T,A} = \gamma_{A,1}, \tag{63}$$

$$\sigma_{T,A} = \sqrt{2\gamma_{A,2}}, \tag{64}$$

where the k-th cumulant of T is calculated as $\gamma_{A,k} = 2\sum_{l=1}^{L}(\omega_l)^k + k\sum_{l=1}^{L}(\omega_l)^k\lambda_{l,0}$. In addition, the new noncentral parameter λ_A and DoF υ_A are calculated by

$$\lambda_A = s_{A,1}a_A^3 - a_A^2, \quad \upsilon_A = a_A^2 - 2\lambda_A, \tag{65}$$

where $a_A = 1/(s_{A,1} - \sqrt{(s_{A,1})^2 - s_{A,2}})$ with $s_{A,1} = \gamma_{A,3}/(\gamma_{A,2})^{3/2}$ and $s_{A,2} = \gamma_{A,4}/(\gamma_{A,2})^2$. Based on the PDF of non-central Chi-square distribution, we can achieve the final result in (60).

Under alternative hypothesis $\mathcal{H}_1$, $Y_l|\mathcal{H}_1 \sim \chi_2^2(\lambda_{l,1})$ with $\lambda_{l,1} = \frac{2N^\star P^\star |\mathbf{f}_l^H \mathbf{H}_1 \mathbf{w}_l|^2}{\sigma_n^2}$, where $\mathbf{H}_1 = \alpha_1 \tilde{\mathbf{a}}_{r,1}(\theta_1)\tilde{\mathbf{a}}_{t,1}^H(\phi_1)$. Similar to the derivation of P_f, P_d can also be approximated by a right tail probability of noncentral Chi-square variable K_E with parameters λ_E and DoF υ_E. Following a similar manner in (65), we can calculate λ_E as well as υ_E, and the theoretical expression of P_d can be obtained in (61). □

B. Optimization of Weight Values

The strategic allocation of optimal weights $\boldsymbol{\omega} = [\omega_1, \omega_2, \cdots, \omega_L]^T$ to L beam pair signals $y_l, l \in [1, L]$ is crucial for significantly enhancing the authentication performance of CovertAuth. However, how to determine the optimal allocation strategy of $\boldsymbol{\omega}$ poses a challenge that remains unresolved. This is primarily because the interplay between weight values and authentication performance metrics has not been clearly revealed. As a result, we first establish a functional relationship between $\boldsymbol{\omega}$ and P_d. Then, based on such a relationship, an optimization problem is formulated to acquire the optimal $\boldsymbol{\omega}$ that maximizes P_d under a specified P_f constraint. The detailed optimization process is illustrated as follows.

According to the Neyman-Pearson theorem, we generally evaluate the performance of P_d under a maximum allowable false alarm probability $P_f = P_f^\dagger$. Let $Q_{\chi_v^2(\lambda)}(\tau)$ denote the right tail probability of a noncentral Chi-square variable with a threshold τ [32]. Then, the corresponding $\tau_A^\dagger$ and $\tau^\dagger$ are given by, respectively

$$\tau_A^\dagger = Q^{-1}_{\chi^2_{\upsilon_A}(\lambda_A)}\left(P_f^\dagger\right), \tag{66}$$

$$\tau^\dagger = \frac{\tau_A - (\upsilon_A + \lambda_A)}{\sqrt{2\upsilon_A + 4\lambda_A}}\sigma_{T,A} + \mu_{T,A}. \tag{67}$$

For the given threshold $\tau^\dagger$, $P_d^\dagger$ under the constraint $P_f^\dagger$ is expressed by

$$P_d^\dagger = Q_{\chi^2_{\upsilon_E}(\lambda_E)}\left(\tau_E^\dagger\right), \tag{68}$$

where $\tau_E^\dagger = [(\tau^\dagger - \mu_{T,E})/\sigma_{T,E}]\sqrt{2\upsilon_E + 4\lambda_E} + \upsilon_E + \lambda_E$. Note that the parameters of ($\upsilon_K, \lambda_K, \mu_{T,K}$ and $\sigma_{T,K}, K \in \{A, E\}$) are dependent on the $\boldsymbol{\omega}$. In other words, the equation (68) is a function of $\boldsymbol{\omega}$, implying that $\boldsymbol{\omega}$ directly influences $P_d^\dagger$. By exploiting this functional relationship, an optimization problem with the aim of finding the optimal $\boldsymbol{\omega}$ is formulated:

$$\max_{\boldsymbol{\omega}} \quad P_d^\dagger, \tag{69a}$$

$$\text{s.t. } P_f = P_f^\dagger, \tag{69b}$$

$$\sum_{l=1}^{L} \omega_l = 1, \tag{69c}$$

$$0 < \omega_l < 1. \tag{69d}$$

It is observed that the optimization problem in (69a) is non-convex due to the product of the exponential function and polynomial in the objective function. Thus, we employ the sequential quadratic programming (SQP) algorithm to solve it with the initialization $\boldsymbol{\omega} = \frac{1}{L}\mathbf{I}$ and the whole process is summarized in the Algorithm 2.

Algorithm 2 Feature Weight Allocation Algorithm.

Input: $P_f^\dagger$.
1: **Initialization:** $\boldsymbol{\omega} = \frac{1}{L}\mathbf{I}$.
2: Calculate λ_A and υ_A using equation (65).
3: Acquire $\tau_A^\dagger$ via equation (66).
4: Compute $\tau^\dagger$ using equation (67).
5: Calculate λ_E and υ_E following a similar way in (65).
6: Obtain $\tau_E^\dagger = [(\tau^\dagger - \mu_{T,E})/\sigma_{T,B}]\sqrt{2\upsilon_E + 4\lambda_E} + \upsilon_E + \lambda_E$.
7: Solve (69) with SQP method to acquire $\boldsymbol{\omega}^\star$.
Output: $\boldsymbol{\omega}^\star$.

V. Numerical Results

A. Parameter Settings

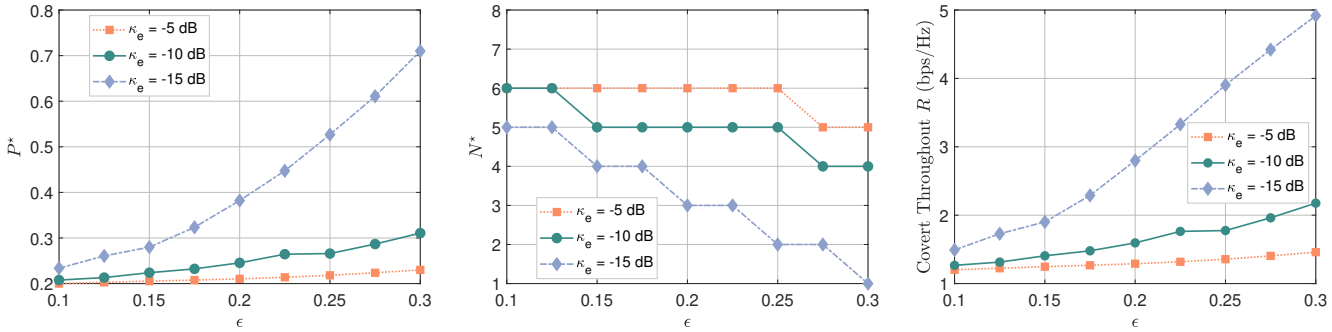
For the concerned mmWave BA stage, we consider that the transmitter sides of Alice and Eve are both equipped with an imperfect ULA array with $N_t = 6$ elements. Moreover, the size of the transmitting beam codebook is set as $L_T = 6$. As to the receiver Bob, the number of antenna elements is $N_r = 8$ with a receiving beam codebook of size $L_R = 8$. Consequently, the total number of candidate beam pairs is $L = 48$. In regard to the location of these communication entities, we assume that Alice and Eve are located around the receiver Bob. In specific, the AoA-AoD pair of Alice-Bob is set to $(\theta_0, \phi_0) = (30°, 60°)$, while the AoA-AoD pair related to Eve-Bob is set as $(\theta_1, \phi_1) = (15°, 18°)$. The corresponding channel gains associated with Alice and Eve are set as $\alpha_0 \sim \mathcal{CN}(0, 1)$ and $\alpha_1 \sim \mathcal{CN}(0, 2)$, respectively. Let $\kappa_n = |\alpha|^2/\sigma_n^2$ and $\kappa_e = |\alpha|_e^2/\sigma_e^2$ denote the pre-beamforming SNR at the Bob and Eve side, respectively. The MC effects of Alice and Eve are evaluated by $\sigma_{c,0}^2 = 0.1$ and $\sigma_{c,1}^2 = 0.4$, respectively. The other simulation parameters are summarized in Table I. The above parameters serve as the default values if not explicitly stated otherwise. We conduct 3000 Monte-Carlo trials on a PC with a 5.4 GHz Intel 14-Core i7 CPU and 32GB RAM to obtain average results.

TABLE I
Simulation Parameters

Parameter	Value
Carrier Frequency	28 GHz
Step size η	0.001
Iteration tolerance $\tilde{\rho}$	0.01
Covertness level ϵ	0.1
Maximum number of iteration $t_{\max}$	50
Bounded estimation error h_e	0.01
Constant τ_p	1
Constant τ_N	1

B. Covert Transmission Performance

In this part, we focus on evaluating the secure communication performance of the proposed CovertAuth scheme. In particular, we utilize the covertness level ϵ to characterize the secure communication demand. From (31), we observe that a



(a) (b) (c)

Fig. 3. The impact of covertness level ϵ on: (a) optimal transmitting power $P^\star$; (b) optimal beam training budget $N^\star$; (c) optimal covert throughput R.

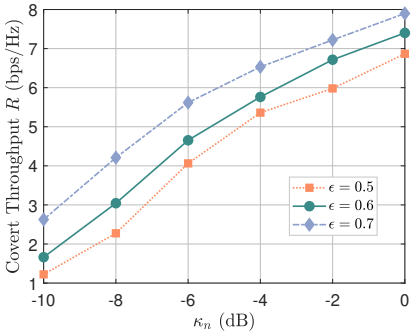


Fig. 4. R versus κ_n with different ϵ.

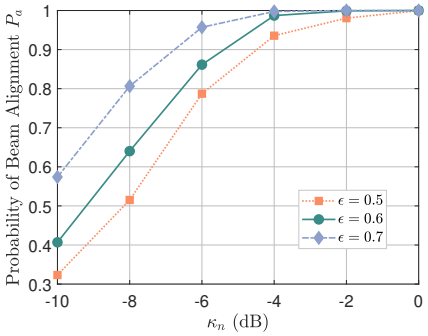


Fig. 5. P_{a} versus κ_n with different ϵ.

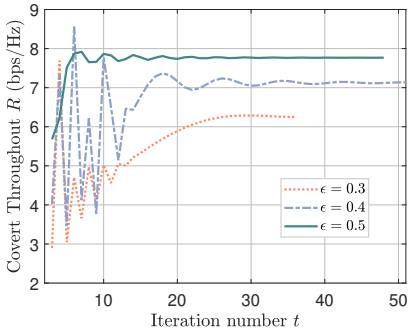


Fig. 6. The convergence of the CovertAuth scheme.

lower ϵ signifies a higher DEP at Eve. This suggests that the CovertAuth scheme is designed with a more stringent covertness requirement, which in turn results in a higher DEP for Eve. The secure communication performance of CovertAuth is evaluated by considering different impact parameters.

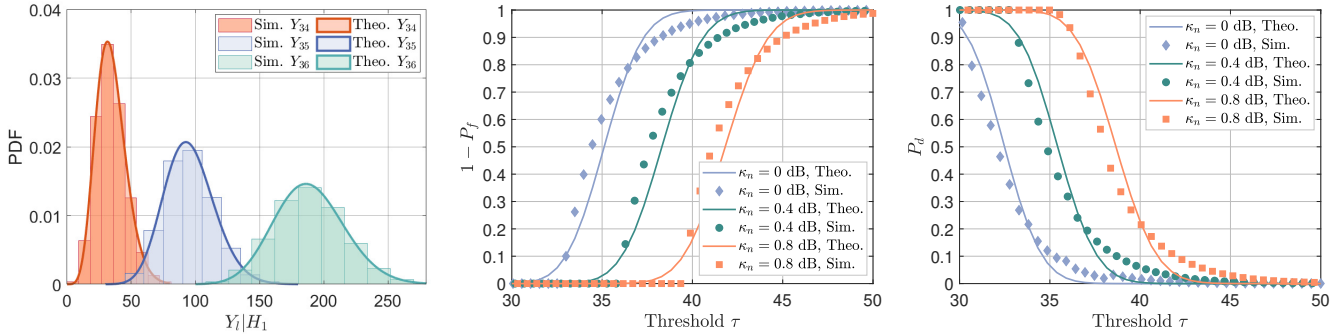
Impact of ϵ on Covert Transmission Performance. In Fig. 3, we illustrate the impact of ϵ on optimized variables in terms of $P^\star$ and $N^\star$ as well as the resulting covert throughput R with the setting $\kappa_n = -15$ dB. As observed from Fig. 3(a), a larger ϵ leads to an increased $P^\star$, implying that more transmitting power can be used in the BA stage as the covertness requirement is relaxed. Moreover, given a constant $\epsilon = 0.2$, the optimized $P^\star$ under $\kappa_e = \{-5, -10, -15\}$ dB are 0.21, 0.25 and 0.38, respectively. The reason is the increased noise uncertainty level at Eve makes it difficult to successfully detect the covert transmission and thus Alice can transmit signals with a larger power P. Another interesting observation in Fig. 3(b) is that a larger $P^\star$ allows for a reduction in beam training budget N. In concert, for $\kappa_e = -15$ dB, as $P^\star$ increases from 0.21 to 0.71, the optimization variable $N^\star$ correspondingly decreases from 5 to 1. This indicates the trade-off between transmitting power and beam training budget needed to achieve the desired covertness constraint. In Fig. 3(c), we can see that the relaxed covertness requirement obviously results in a larger communication throughput between Alice and Bob. For example, with $\kappa_e = -15$ dB, R presents an increased tendency from 1.49 bps/Hz to 4.92 bps/Hz with ϵ in the range of $[0.1, 0.3]$.

Impact of κ_n on Covert Transmission Performance. Given the fixed $\kappa_e = -15$ dB, Fig. 4 and Fig. 5 present the effects of κ_n on covert throughput R and probability of successful beam alignment P_{a} under different covertness constraints $\epsilon \in \{0.5, 0.6, 0.7\}$. In specific, one can note from Fig. 4 that R of all three curves exhibit an increasing tendency as κ_n improves. This is because a lower noise interference in the Alice-Bob link enhances the channel transmission quality, thereby increasing the number of effective information bits that can be transmitted under the same covertness constraint. Also, with a constant $\kappa_n = -2$ dB, R under three covertness constraints are 6 bps/Hz, 6.8 bps/Hz, and 7.2 bps/Hz, respectively. We can conclude that the increased ϵ (i.e., lower covertness requirement) can lead to higher R. As the demand for covertness diminishes, CovertAuth can afford to be more aggressive in data transmission, thus increasing the overall data rate. From Fig. 5, it is demonstrated that P_{a} can achieve over 0.85 when κ_n is larger than -5 dB, ensuring the high transmission reliability of CovertAuth in low SNR conditions.

Convergence Behavior of the CovertAuth Scheme. We investigate the convergence performance of the proposed CovertAuth scheme and plot in Fig. 6 three curves how covert throughput R varies with iteration number t with the settings of ($\kappa_n = -5$ dB, $\kappa_e = -15$ dB, $\epsilon = \{0.3, 0.4, 0.5\}$). It can be seen that the covert throughput R experiences significant fluctuations within the first 10 iterations and then converges to stable constants after a certain amount of iterations (e.g., $t = 25$), indicating the effectiveness of the optimization framework in Algorithm 1. The algorithm convergence can be primarily attributed to the linearized surrogate functions in (46) and (52), which offer improved computational traceability.

C. Identity Authentication Performance

In this part, we evaluate the authentication performance of CovertAuth combating identity-based impersonation attacks.



(a) (b) (c)

Fig. 7. Comparison between theoretical and simulation results of (a) PDF of $Y_l|\mathcal{H}_1$; (b) P_f versus τ; (c) P_d versus τ.

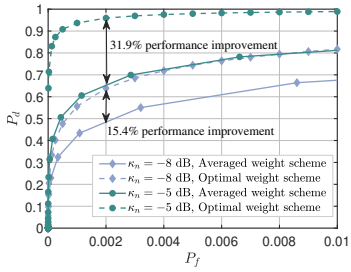


Fig. 8. ROC curves under different weight design schemes.

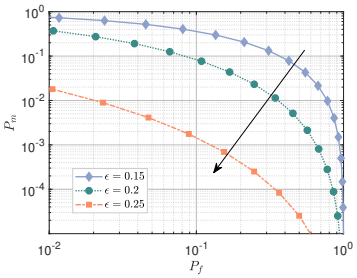


Fig. 9. Impact of ϵ on authentication performance.

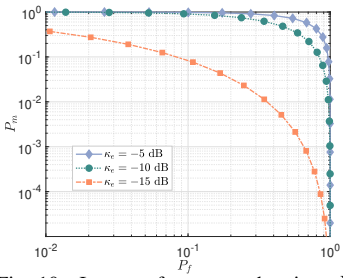


Fig. 10. Impact of κ_e on authentication performance.

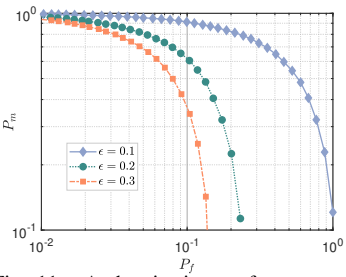
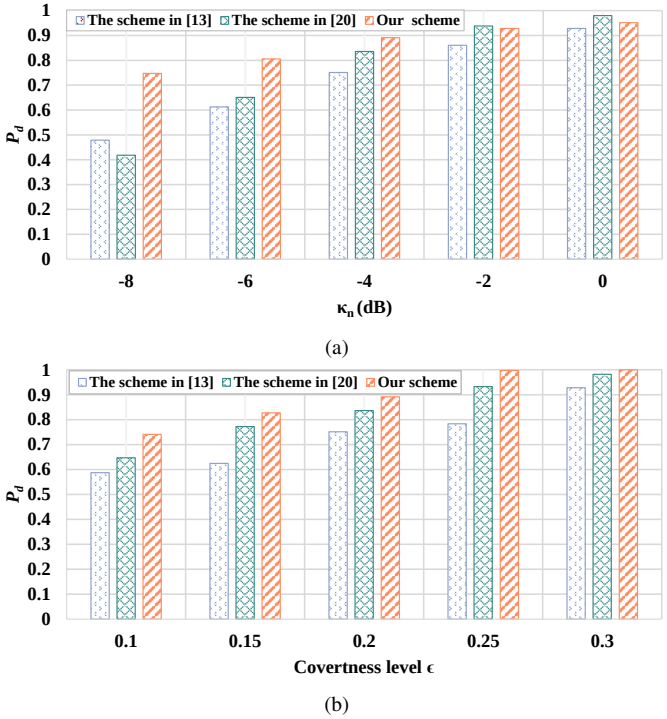


Fig. 11. Authentication performance under worst-case scenario.

Theoretical Model Validation. To validate the correctness of analytical expressions regarding P_f in (60) and P_d in (61), we plot in Fig. 7(a) - Fig. 7(c) the theoretical and simulated results about PDFs of $Y_l|\mathcal{H}_1$, P_d and P_f, respectively. The relevant system parameters are set as ($\kappa_e = -15$ dB, $\epsilon = 0.3$). Fig. 7(a) presents that the theoretical PDF curves of $Y_l|\mathcal{H}_1$ are fitted well with the simulated ones under randomly selected beam signals $\{Y_{34}, Y_{35}, Y_{36}\}$. This implies the correct statistical analysis of $Y_l|\mathcal{H}_1$ and provides support for the subsequent derivation of P_d. It is observed from Fig. 7(b) and Fig. 7(c) that the theoretical curves of P_f and P_d are close to the corresponding simulated ones under all three different SNR conditions, suggesting a high-level agreement between the derived expressions and empirical ones. Also, the gap between theoretical and simulated ones is gradually decreasing as κ_n increases. This indicates that the proposed theoretical model can largely characterize the authentication performance of the proposed scheme. One can also note that under a given τ, a higher κ_n leads to a lower P_f with better P_d. This is because the diminished noise uncertainty at Bob enhances the authentication precision using the energy detector-based identity validation method.

Performance Comparison with Different Weight Allocation Schemes. To exhibit the performance superiority of CovertAuth using the optimal weight allocation strategy obtained in problem (69), we compare it with the one exploiting the averaged weight design scheme and summarize the results in Fig. 8 with the receiver operating characteristic (ROC) curve. It is noted that for a fixed $P_f = 0.002$, the scheme with optimal weight value can achieve 15.4% and 31.9% detection performance improvement over that with average weight value under $\kappa_n = \{-8, -5\}$ dB, respectively. This indicates that the solved optimal weight enables CovertAuth to obtain a larger detection accuracy gain and to possess more reliability in countering impersonation attacks.



(a)

(b)

Fig. 12. Authentication performance comparison with existing works under the impacts of (a) κ_n; (b) Covertness level ϵ.

Impact of ϵ on Authentication Performance. To investigate the trade-off performance between covert transmission and identity authentication, we examine the impact of $\epsilon = \{0.15, 0.2, 0.25\}$ on P_d and P_f in Fig. 9. One can see that a higher ϵ results in a lower miss detection probability $P_m = 1 - P_d$ and a lower P_f. This is due to the reason

that a relaxed covertness requirement leads to an increase in the allocated transmitting power P, making a more accurate beam pattern feature. However, the increase in authentication performance often comes with the sacrifice of performance in combating eavesdropping attacks, thus a balance between covert transmission and identity authentication should be achieved based on the current security requirements of the mmWave system.

Impact of κ_e on Authentication Performance. To explore the performance of CovertAuth under different attack levels, Fig. 10 illustrates the effect of κ_e on P_m and P_f with the settings of ($\kappa_n = -5$ dB, $\epsilon = 0.1$). One can note that the metric of P_m and P_f both present an increasing tendency as κ_e improves. The reason is that as the noise level at Eve decreases, Eve gains an improved capacity to accurately analyze and interpret the transmitted signals, making it easier to mimic legitimate users during the authentication phase. This results in a degraded authentication performance. Consequently, if the priority of identity authentication is high, it may be necessary to appropriately compromise the secrecy of information transmission to improve authentication accuracy.

Robustness Illustration of CovertAuth. To further examine the reliability of CovertAuth, we consider a worst-case scenario, where the attacker Eve is located along the transmission path between Alice and Bob. Under the considered scenario, Eve possesses the same AoA-AoD pair as that in the Alice-Bob link. In addition, we further assume that the channel gains α_0 and α_1 maintain the same value during the BA stage. Then, we investigate the performance of the proposed scheme under different ϵ with ($\kappa_n = -5$ dB and $\kappa_e = -15$ dB). The covert transmission performance is summarized in Table II and the corresponding authentication performance is plotted in Fig. 11. Although a low ϵ may constrain the authentication performance, CovertAuth can demonstrate a remarkable enhancement in authentication accuracy when the covertness constraints are moderately relaxed. In specific, under a given $P_m = 0.1$, P_f under $\epsilon = \{0.2, 0.3\}$ are 0.25 and 0.144, respectively. This suggests that CovertAuth can still achieve a relatively satisfactory performance even under the worst-case scenario.

TABLE II
COVERTNESS PERFORMANCE UNDER THE WORST-CASE SCENARIO

Covertness level ϵ	0.1	0.2	0.3
$P^\star$	0.1602	0.2747	0.4059
$N^\star$	7	4	3
R (bps/Hz)	2.0549	2.3671	3.4466

Performance Comparison with Existing Works. In Fig. 12(a) and Fig. 12(b), we present a comparative analysis with existing works of channel phase response-based scheme in [13] and multiple channel responses-based scheme in [20] under the impacts of κ_n and ϵ, respectively. From Fig. 12(a), one can note that all three methods present an increased P_d due to the decreased noise interference at Bob. Although the proposed CovertAuth is comparable or even slightly inferior to the method in [20] under high SNR conditions (i.e., $\kappa_n > -2$ dB), our scheme exhibits the best detection performance in low SNR regime (e.g., $\kappa_n = [-8, -4]$ dB). This indicates that the proposed scheme not only delivers superior detection capabilities but also exhibits robustness against noise interference. Specifically, given a fixed $\kappa_n = -8$ dB, CovertAuth can provide 26% and 32% performance improvement compared to the methods in [13] and [20], respectively.

Fig. 12(b) illustrates the authentication performance considering the covertness constraint $\epsilon = [0.1, 0.3]$. We can intuitively see that the performance of the three schemes gradually improves with the relaxation of covertness constraints, and CovertAuth exhibits the best performance under all conditions. This is because under a low ϵ, the allocated transmission power $P^\star$ is limited, leading to poor feature extraction precision and degraded authentication performance of existing works. In contrast, CovertAuth exploits the fine-grained beam pattern feature caused by both the antenna hardware fingerprint MC effect and the spatial information of the transmitter to devise an energy detector-based authentication scheme without the need for feature extraction. Such a scheme effectively meets the security requirements in the mmWave BA stage.

VI. RELATED WORK

Some preliminary efforts have been devoted to the secure mechanism design for the mmWave BA stage, which can be categorized into approaches addressing jamming attacks [33], [34], eavesdropping attacks [15], [35], [36], and impersonation attacks [4], [37].

Countermeasures for Jamming Attacks. To mitigate the BA misalignment from jamming attacks, a countermeasure exploiting randomized probing technique has been proposed in [33], where the base station corrupts the probing sequence randomly to enable jamming rejection at the user equipment using subspace-based techniques, such as orthogonal projection and jamming cancellation. Then, the authors in [34] use an autoencoder-based approach for jamming detection and mitigation, enabling recovery of the corrupted received signal strength vector during the BA stage.

Countermeasures for Eavesdropping Attacks. As to the countermeasure for eavesdropping attacks, Zhang *et. al* introduce a covert multi-user beam training strategy to minimize detection probability while enabling simultaneous beam training for multiple users [15]. Moreover, a two-stage power optimization scheme is developed in [35] to maximize the average covert rate for the BA and data transmission phase while achieving the covertness requirement to avoid eavesdropping threat. With the random beam switching aid, Ju *et. al* exploit the virtual angles of effective and activated beams as the random source to generate the secret key for information security between the transceiver pair [36].

Countermeasures for Impersonation Attacks. To counter forged feedback from malicious attackers in the BA stage, the authors in [4] establish a session secret through asymmetric key exchange, and then appends a cryptographic nonce to the beam feedback, thus ensuring devices accept feedback only from authorized devices. Following this line, Li *et. al* propose a novel secure beam sweeping protocol, named SecBeam, which leverages power/sector randomization techniques along with coarse angle-of-arrival information to effectively detect beam-stealing attacks during the BA phase [37].

VII. Conclusion

This paper proposed an innovative PLS framework named CovertAuth to effectively address identity-based impersonation and eavesdropping attacks for the BA stage in mmWave communication systems. CovertAuth exploited the beam pattern feature impacted by the MC effects to achieve identity validation. Moreover, a covert communication optimization framework was developed to jointly design the beam training budget and transmission power for maximizing covert communication throughput while satisfying the covertness requirement during the BA phase. Simulation results indicate: 1) incorporating the MC effect into the beam pattern enhances the authentication reliability of CovertAuth; 2) the derived theoretical models provide a valuable framework for authentication performance characterization and optimization; and 3) a trade-off between authentication and covert communication performance is observed under different security requirements. It is anticipated that CovertAuth can provide insightful guidelines for the design of a secure BA framework in mmWave communication systems.

References

[1] J. Tan, T. H. Luan, W. Guan, Y. Wang, H. Peng, Y. Zhang, D. Zhao, and N. Lu, "Beam Alignment in mmWave V2X Communications: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 26, no. 3, pp. 1676–1709, 2024.

[2] D. Steinmetzer, Y. Yuan, and M. Hollick, "Beam-Stealing: Intercepting the Sector Sweep to Launch Man-in-the-Middle Attacks on Wireless IEEE 802.11ad Networks," in *WiSec 2018*. ACM, 2018, pp. 12–22.

[3] J. Yang, W. Zhu, M. Tao, and S. Sun, "Hierarchical Beam Alignment for Millimeter-Wave Communication Systems: A Deep Learning Approach," *IEEE Trans. Wirel. Commun.*, vol. 23, no. 4, pp. 3541–3556, 2024.

[4] D. Steinmetzer, S. Ahmad, N. A. Anagnostopoulos, M. Hollick, and S. Katzenbeisser, "Authenticating the Sector Sweep to Protect Against Beam-Stealing Attacks in IEEE 802.11ad Networks," in *MobiCom 2018*. ACM, 2018, pp. 3–8.

[5] B. Qiu, W. Cheng, and W. Zhang, "Robust Multi-Beam Secure mmWave Wireless Communication for Hybrid Wiretapping Systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 1393–1406, 2023.

[6] T. Lu, L. Chen, J. Zhang, C. Chen, and T. Q. Duong, "Reconfigurable Intelligent Surface-Assisted Key Generation for Millimeter-Wave Multi-User Systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 19, pp. 5373–5388, 2024.

[7] J. Li, L. Zhang, K. Xue, Y. Fang, and Q. Sun, "Secure Transmission by Leveraging Multiple Intelligent Reflecting Surfaces in MISO Systems," *IEEE Trans. Mob. Comput.*, vol. 22, no. 4, pp. 2387–2401, 2023.

[8] N. Xie, J. Zhang, Q. Zhang, H. Tan, A. X. Liu, and D. Niyato, "Hybrid Physical-Layer Authentication," *IEEE Trans. Mob. Comput.*, vol. 23, no. 2, pp. 1295–1311, 2024.

[9] R. Sun, H. Wu, B. Yang, Y. Shen, W. Yang, X. Jiang, and T. Taleb, "On Covert Rate in Full-Duplex D2D-Enabled Cellular Networks With Spectrum Sharing and Power Control," *IEEE Trans. Mob. Comput.*, vol. 23, no. 10, pp. 9931–9945, 2024.

[10] Y. Jiang, L. Wang, H. Chen, and X. Shen, "Physical Layer Covert Communication in B5G Wireless Networks - its Research, Applications, and Challenges," *Proc. IEEE*, vol. 112, no. 1, pp. 47–82, 2024.

[11] N. Wang, L. Jiao, P. Wang, W. Li, and K. Zeng, "Machine Learning-based Spoofing Attack Detection in MmWave 60GHz IEEE 802.11ad Networks," in *INFOCOM 2020*. IEEE, 2020, pp. 2579–2588.

[12] M. R. Nosouhi, K. Sood, M. Grobler, and R. Doss, "Towards Spoofing Resistant Next Generation IoT Networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 17, pp. 1669–1683, 2022.

[13] X. Lu, J. Lei, Y. Shi, and W. Li, "Physical-Layer Authentication Based on Channel Phase Responses for Multi-Carriers Transmission," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 1734–1748, 2023.

[14] Y. Teng, P. Zhang, X. Chen, X. Jiang, and F. Xiao, "PHY-Layer Authentication Exploiting Channel Sparsity in MmWave MIMO UAV-Ground Systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 19, pp. 4642–4657, 2024.

[15] J. Zhang, M. Li, M. Zhao, X. Ji, and W. Xu, "Multi-User Beam Training and Transmission Design for Covert Millimeter-Wave Communication," *IEEE Trans. Inf. Forensics Secur.*, vol. 17, pp. 1528–1543, 2022.

[16] M. V. Jamali and H. Mahdavifar, "Covert Millimeter-Wave Communication: Design Strategies and Performance Analysis," *IEEE Trans. Wirel. Commun.*, vol. 21, no. 6, pp. 3691–3704, 2022.

[17] C. Wang, Z. Li, and D. W. K. Ng, "Covert Rate Optimization of Millimeter Wave Full-Duplex Communications," *IEEE Trans. Wirel. Commun.*, vol. 21, no. 5, pp. 2844–2861, 2022.

[18] H. Xiao, X. Hu, A. Li, W. Wang, Z. Su, K. Wong, and K. Yang, "STAR-RIS Enhanced Joint Physical Layer Security and Covert Communications for Multi-Antenna mmWave Systems," *IEEE Trans. Wirel. Commun.*, vol. 23, no. 8, pp. 8805–8819, 2024.

[19] N. Xie, Q. Zhang, J. Chen, and H. Tan, "Privacy-Preserving Physical-Layer Authentication for Non-Orthogonal Multiple Access Systems," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 4, pp. 1371–1385, 2022.

[20] Y. Li, J. Zhang, J. Chen, Y. Chen, N. Xie, and H. Li, "Privacy-Preserving Physical-Layer Authentication Under Cooperative Attacks," *IEEE/ACM Trans. Netw.*, vol. 32, no. 2, pp. 1171–1186, 2024.

[21] C. M. Schmid, S. Schuster, R. Feger, and A. Stelzer, "On the Effects of Calibration Errors and Mutual Coupling on the Beam Pattern of an Antenna Array," *IEEE Trans. Antennas Propag.*, vol. 61, no. 8, pp. 4063–4072, 2013.

[22] M. Naguib, Y. Shabara, and C. E. Koksal, "Continuous Beam Alignment for Mobile MIMO," *IEEE Trans. Wirel. Commun.*, vol. 23, no. 6, pp. 6378–6393, 2024.

[23] A. Aubry, A. D. Maio, L. Lan, and M. Rosamilia, "Adaptive Radar Detection and Bearing Estimation in the Presence of Unknown Mutual Coupling," *IEEE Trans. Signal Process.*, vol. 71, pp. 1248–1262, 2023.

[24] P. Chen, Z. Cao, Z. Chen, and X. Wang, "Off-Grid DOA Estimation Using Sparse Bayesian Learning in MIMO Radar With Unknown Mutual Coupling," *IEEE Trans. Signal Process.*, vol. 67, no. 1, pp. 208–220, 2019.

[25] J. Zhang, Y. Huang, Q. Shi, J. Wang, and L. Yang, "Codebook Design for Beam Alignment in Millimeter Wave Communication Systems," *IEEE Trans. Commun.*, vol. 65, no. 11, pp. 4980–4995, 2017.

[26] X. Wang, Z. Fei, P. Liu, J. A. Zhang, Q. Wu, and N. Wu, "Sensing-Aided Covert Communications: Turning Interference Into Allies," *IEEE Trans. Wirel. Commun.*, vol. 23, no. 9, pp. 10 726–10 739, 2024.

[27] C. Wang, X. Chen, J. An, Z. Xiong, C. Xing, N. Zhao, and D. Niyato, "Covert Communication Assisted by UAV-IRS," *IEEE Trans. Commun.*, vol. 71, no. 1, pp. 357–369, 2023.

[28] Y. Zhang, Y. Zhang, J. Wang, S. Xiao, and W. Tang, "Distance-Angle Beamforming for Covert Communications via Frequency Diverse Array: Toward Two-Dimensional Covertness," *IEEE Trans. Wirel. Commun.*, vol. 22, no. 12, pp. 8559–8574, 2023.

[29] M. Zhao, Y. Cai, Q. Shi, B. Champagne, and M. Zhao, "Robust Transceiver Design for MISO Interference Channel With Energy Harvesting," *IEEE Trans. Signal Process.*, vol. 64, no. 17, pp. 4618–4633, 2016.

[30] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge university press, 2004.

[31] H. Liu, Y. Tang, and H. H. Zhang, "A New Chi-Square Approximation to the Distribution of Non-Negative Definite Quadratic Forms in Non-Central Normal variables," *Computational Statistics & Data Analysis*, vol. 53, no. 4, pp. 853–856, 2009.

[32] S. M. Kay, *Fundamentals of Statistical Signal Processing: Estimation Theory*. Prentice-Hall, Inc., 1993.

[33] D. Darsena and F. Verde, "Anti-Jamming Beam Alignment in Millimeter-Wave MIMO Systems," *IEEE Trans. Commun.*, vol. 70, no. 8, pp. 5417–5433, 2022.

[34] S. Dinh-Van, T. M. Hoang, B. B. Cebecioglu, D. S. Fowler, Y. K. Mo, and M. D. Higgins, "A Defensive Strategy Against Beam Training Attack in 5G mmWave Networks for Manufacturing," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 2204–2217, 2023.

[35] Z. Xing, C. Qi, Y. Cheng, Y. Wu, D. Lv, and P. Li, "Covert Millimeter Wave Communications Based on Beam Sweeping," *IEEE Commun. Lett.*, vol. 27, no. 5, pp. 1287–1291, 2023.

[36] Y. Ju, G. Zou, H. Bai, L. Liu, Q. Pei, C. Wu, and S. A. Otaibi, "Random Beam Switching: A Physical Layer Key Generation Approach to Safeguard mmWave Electronic Devices," *IEEE Trans. Consumer Electron.*, vol. 69, no. 3, pp. 594–607, 2023.

[37] J. Li, L. Lazos, and M. Li, "SecBeam: Securing mmWave Beam Alignment Against Beam-Stealing Attacks," in *CNS 2024*. IEEE, 2024, pp. 1–9.