Low-Complexity Beamforming for NF Secure ISAC

Diluka Galappaththige, *Member, IEEE*, and Chintha Tellambura, *Fellow, IEEE,*

***Abstract*—This letter investigates secure beamforming for a near-field (NF) integrated sensing and communication system, where an extremely large-scale antenna array (ELAA) base station (BS) serves multiple users and sensing targets under eavesdropping threats. Conventional algorithms are computationally prohibitive in large-scale scenarios. To address this, we propose a low-complexity beamforming algorithm that exploits NF beam-focusing in both angular and distance domains. The design maximizes the secrecy sum rate while satisfying the user's SINR, target beampattern, and BS power constraints. By converting the power constraint into a complex sphere manifold, the algorithm combines manifold optimization with the augmented Lagrangian method to efficiently handle the remaining constraints. This drastically reduces the search space; for example, with 257 BS antennas, it achieves an 18-fold speedup over the convex-concave procedure algorithm (CCPA).**

***Index Terms*—Integrated sensing and communication, Secure communication, Extremely large-scale antenna arrays, Near-field.**

I. Introduction

NEAR-FIELD (NF)-Integrated Sensing and Communications (ISAC) can successfully accommodate growing data traffic and high-resolution sensing for diverse applications, exploiting extremely large-scale antenna arrays (ELAA) and high frequencies ($10\,\mathrm{GHz}$ to $10\,\mathrm{THz}$) [1], [2]. These include remote healthcare, weather monitoring, asset tracking, gesture recognition, autonomous vehicles, and more [1], [2].

Information leakage to eavesdroppers poses a heightened threat at the ISAC physical layer, making reliability essential for practical applications [3], [4]. While secure beamforming has been studied in far-field (FF) ISAC and NF communication-only scenarios, few works address NF ISAC. Reference [3] maximizes the minimum sensing beampattern gain across multiple targets while satisfying user signal-to-interference-plus-noise ratio (SINR) requirements and limiting the eavesdropper's SINR, solved via semidefinite programming (SDP) with sequential rank-one relaxation. In [4], an NF non-orthogonal multiple access ISAC system with a single target is considered, where a convex-concave procedure algorithm (CCPA) combining semidefinite relaxation (SDR) and successive convex approximation (SCA) maximizes the sum secrecy rate subject to a sensing Cramér-Rao bound.

When applied to ELAA systems, these traditional algorithms are often inefficient due to matrix lifting, high-dimensional search spaces, and long run times. For instance, simulating a 200-antenna BS ISAC system using CCPA can take nearly two weeks for a single curve [5]. Moreover, SDP expands the search space from MKN to M^2KN, where M, K, and N denote the numbers of BS antennas, users, and targets, respectively. Thus, these approaches are unsuitable for large-scale NF systems, leading to exponential complexity. This motivates the need for fundamentally different algorithms.

To address these limitations, we go beyond our earlier work [6] by incorporating an eavesdropper model and secrecy-rate maximization into the NF ISAC framework. Unlike [6], which focused solely on communication–sensing trade-off, we introduce secrecy metrics, eavesdropper SINR constraints, and corresponding Lagrangian gradients. Moreover, instead of applying standard manifold optimization (MO) for unconstrained problems, we develop an augmented Lagrangian manifold optimization (ALM-MO) algorithm that directly handles non-convex secrecy and sensing constraints without convex relaxations such as SDR or SCA. This integration significantly lowers complexity while ensuring scalability to ELAAs. Furthermore, the algorithm explicitly exploits NF beam focusing in both angular and distance domains, enabling efficient secure communication and multi-target detection. To the best of our knowledge, this is the first tailored, low-complexity algorithm for secure NF ISAC with ELAAs, complementing and advancing the emerging literature in NF secure ISAC [3], [4] and going substantially beyond conventional MO approaches.

The proposed beamforming algorithm maximizes the users' sum secrecy rate given an eavesdropper, subject to each user's minimum SINR requirement, the sensing beampattern gain for each target, and the BS transmit power constraint. This algorithm leverages the power constraint to define a complex sphere manifold and utilizes the ALM to handle the other constraints. It iteratively updates the optimization variables, Lagrange multipliers, and penalty parameters to ensure that all constraints are satisfied. Compared with standard optimization techniques, it achieves substantially lower computational complexity and execution time. For example, with 257 BS antennas, it runs 18 times faster than CCPA and operates over a $(M+1)(K+N)$ reduced search space, yielding a drastic complexity reduction.

Notation: $\mathbf{I}_M$ is the $M \times M$ identity matrix. $\Re(\cdot)$ denotes the real part. $\mathcal{CN}(\boldsymbol{\mu}, \mathbf{R})$ is a complex Gaussian vector with mean $\boldsymbol{\mu}$ and co-variance $\mathbf{R}$. $\mathbf{1}_{\{x\}}$ is 1 if $x > 0$ and 0 otherwise. $\mathrm{unt}(\mathbf{a}) = [a_1/|a_1|, \ldots, a_n/|a_n|]$. $\mathbf{A} \circ \mathbf{B}$ is the Hadamard product. $\mathrm{clip}_{[a,b]}(x) = \max\{a, \min(b, x)\}$ and $[x]^+ = \max(0, x)$. $\mathbb{R}^n$ and $\mathbb{C}^n$ are n-dimensional Euclidean and complex spaces. The *complex sphere manifold* is $\mathcal{M} = \left\{\mathbf{x} \in \mathbb{C}^n : \|\mathbf{x}\|_2 = 1\right\}$.

II. Preliminaries

This section describes the system model, channel model, and transmission signals.

1) System and Channel Models: Fig. 1 shows an NF secure ISAC system with an $M = 2\tilde{M} + 1$-antenna BS, K single-antenna users, N potential targets, and an eavesdropper (Eve).

D. Galappaththige and C. Tellambura are with the Department of Electrical and Computer Engineering, University of Alberta, Edmonton, AB, T6G 1H9, Canada (e-mail: {diluka.lg, ct4}@ualberta.ca).

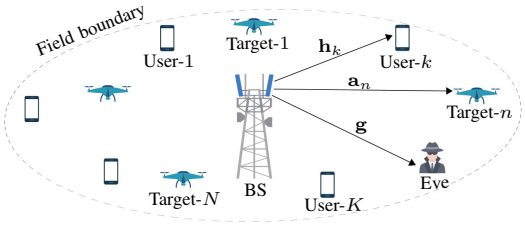

Fig. 1. An NF secure ISAC system.

The Eve is assumed to be a legitimate device (e.g., a registered user in the network) that may later behave maliciously [3], [4]. The BS simultaneously transmits probing signals to the targets and data to the users while ensuring data security against Eve. Without loss of generality, the BS employs a uniform linear array (ULA) with spacing $d = \lambda_c/2$ and its origin at the array center, where λ_c is the wavelength at carrier frequency f_c [7]. The ULA aperture is $D = (M-1)d$, yielding a Rayleigh distance of $2D^2/\lambda_c$ [2]. Both users and targets are located in the BS's NF region [7]–[10].

We use the NF spherical wave channel model [5], [10]. The BS-user, BS-target, and BS-Eve channels are denoted by $\mathbf{h}_k \in \mathbb{C}^{M\times 1}$, $\mathbf{a}_n \in \mathbb{C}^{M\times 1}$, and $\mathbf{g} \in \mathbb{C}^{M\times 1}$, respectively. In general, the NF channel between the BS and the b-th node is expressed as $\mathbf{f}_b = \beta_b \mathbf{c}_b$, where $\mathbf{f}_b \in \mathbf{h}_k, \mathbf{a}_n, \mathbf{g}$. Here, $\mathbf{c}_b \in \mathbb{C}^{M\times 1}$ is the NF array response vector with $[\mathbf{c}_b]_m = e^{-j\frac{2\pi}{\lambda_c} r_{mb}(r_b,\theta_b)}$, and $r_{mb}(r_b,\theta_b)$ is the distance from the m-th antenna to the b-th node [5, Eqn. (1)]. The parameters r_b and θ_b represent the node's distance and angle relative to the ULA center, while $\beta_b = \sqrt{\lambda/(4\pi)} r_b^{-1}$ models the free-space path-loss between the 0-th antenna and the b-th node.

Remark 1. *As an initial study, we assume perfect CSI for all channels, including Eve's, by considering Eve as a registered device whose CSI was obtained during prior training or pilot signaling. In practice, CSI is inevitably imperfect due to estimation errors, uncertainty, and mobility. Robust extensions, such as (i) norm-bounded uncertainty models for worst-case secrecy guarantees and (ii) statistical CSI models for distributional robustness, can be incorporated into the proposed framework to address imperfect CSI and mobility.*

2) Transmission Model: The BS transmitted signal $\mathbf{x}(n) \in \mathbb{C}^{M\times 1}$ is designed for joint communication and sensing, i.e., $\mathbf{x} = \sum_{k=1}^{K} \mathbf{w}_k q_k + \sum_{n=1}^{N} \mathbf{s}_n$, where $q_k \in \mathbb{C}$ is the unit-power data symbol for the k-th user, i.e., $\mathbb{E}\{|q_k|^2\} = 1$, $\mathbf{w}_k \in \mathbb{C}^{M\times 1}$ is the BS beamforming vector for the k-th user, and $\mathbf{s}_n \in \mathbb{C}^{M\times 1}$ is the sensing signal for detecting the n-th target. It is assumed that q_k and $\mathbf{s}_n$ are independent, and BS beamforming is achieved via the joint design of $\mathbf{w}_k$ and $\mathbf{s}_n$ [11]. The received signal at the k-th user is given as

$$y_k = \mathbf{h}_k^{\mathrm{H}} \mathbf{w}_i q_k + \sum\nolimits_{i\neq k}^{K} \mathbf{h}_k^{\mathrm{H}} \mathbf{w}_i q_i + \sum\nolimits_{j=1}^{N} \mathbf{h}_k^{\mathrm{H}} \mathbf{s}_j + z_k, \quad (1)$$

where $z_k \sim \mathcal{CN}(0,\sigma^2)$ is the k-th user additive white Gaussian noise (AWGN). On the other hand, Eve also receives the BS transmitted signal and tries to decode the information of any user. The received signal at Eve is given as

$$y_e = \sum\nolimits_{i=1}^{K} \mathbf{g}^{\mathrm{H}} \mathbf{w}_i q_i + \sum\nolimits_{j=1}^{N} \mathbf{g}^{\mathrm{H}} \mathbf{s}_j + z_e, \quad (2)$$

where $z_e \sim \mathcal{CN}(0,\sigma^2)$ is the AWGN vector at the Eve.

Remark 2. *Note that N independent sensing beams are used to detect N distinct targets. Unlike FF ISAC systems, NF beams focus on both angle and distance, producing highly localized energy (beam-focusing effect). Hence, a single communication beam primarily illuminates the vicinity of the served user, leaving other spatial regions poorly covered. To achieve reliable multi-target detection and maintain situational awareness, explicit sensing probing signals are therefore required in addition to communication beams [2], [6]. While this introduces a natural trade-off with secrecy rate and throughput, such probing is indispensable in NF ISAC with ELAAs, where the communication waveform alone cannot guarantee adequate sensing coverage. This is further validated by our simulations (Fig. 3 and Fig. 4).*

Next, we introduce several notations. The beamforming vectors are collected in $\mathbf{V} = [\mathbf{w}_1,\ldots,\mathbf{w}_K,\mathbf{s}_1,\ldots,\mathbf{s}_N] \in \mathbb{C}^{M\times(K+N)}$. Let $\mathbf{E} = \mathbf{I}_{K+N} \in \mathbb{R}^{(K+N)\times(K+N)}$ be the index matrix. The individual vectors are expressed as $\mathbf{w}_k = \mathbf{V}\mathbf{E}_k$ and $\mathbf{s}_n = \mathbf{V}\mathbf{E}_{K+n}$, where $\mathbf{E}_i$ is the i-th column of $\mathbf{E}$.

III. System Performance

Secure communication and sensing are measured via the secrecy rate and the BS transmit beampatterns for the targets.

1) Secrecy Rate: The users decode their intended data from the BS signal. From (1), the SINR at the k-th user is given by

$$\gamma_k = \frac{|\mathbf{h}_k^{\mathrm{H}} \mathbf{w}_k|^2}{\sum_{i\neq k}^{K} |\mathbf{h}_k^{\mathrm{H}} \mathbf{w}_i|^2 + \sum_{j=1}^{N} |\mathbf{h}_k^{\mathrm{H}} \mathbf{s}_j|^2 + \sigma^2}. \quad (3)$$

Eve also tries to decode the intended data for the k-th user. Using (2), the SINR at Eve for decoding the k-th user's data can be expressed as

$$\gamma_{e,k} = \frac{|\mathbf{g}^{\mathrm{H}} \mathbf{w}_k|^2}{\sum_{i\neq k}^{K} |\mathbf{g}^{\mathrm{H}} \mathbf{w}_i|^2 + \sum_{j=1}^{N} |\mathbf{g}^{\mathrm{H}} \mathbf{s}_j|^2 + \sigma^2}. \quad (4)$$

Thus, the k-th user secrecy rate can be approximated by $\mathcal{R}_k^{\mathrm{Sec}} \approx [\log_2(1+\gamma_k) - \log_2(1+\gamma_{e,k})]^+$.

2) Sensing Beampattern: The BS computes the transmit beampattern gain for each target, a key criterion for sensing signal optimization [9], [12], [13]. It characterizes the transmitted power distribution over the sensing angle range $\theta \in [-\pi/2, \pi/2]$. Proper shaping of this distribution enhances detection, range/Doppler/angle estimation, tracking, recognition, and overall sensing accuracy. For the n-th target direction, the beampattern is given as

$$p(r_n,\theta_n) = \mathbb{E}\left\{|\mathbf{a}_n^{\mathrm{H}} \mathbf{x}|^2\right\} = \sum\nolimits_{i=1}^{K+N} \mathbf{a}_n^{\mathrm{H}} \mathbf{V}\mathbf{E}_i\mathbf{E}_i^{\mathrm{H}}\mathbf{V}^{\mathrm{H}}\mathbf{a}_n. \quad (5)$$

This measure can be adapted to sensing needs: for unknown target directions, a uniform $p(r_n,\theta_n)$ is preferred, whereas in tracking tasks with approximately known directions, the beampattern should concentrate power in likely target regions to enhance localization accuracy [13].

IV. Problem Formulation

We optimize the NF secure ISAC system (Fig. 1) to maximize the secrecy sum rate under constraints on user SINR, target beampattern gains, and BS transmit power. This ensures user data security against eavesdropping. The optimization problem is formulated as

$$\mathcal{P}1: \max_{\mathbf{V}} \quad \sum\nolimits_{k=1}^{K} \mathcal{R}_k^{\mathrm{Sec}}, \tag{6a}$$

$$\text{s.t.} \quad \gamma_k \geq \gamma_k^{\mathrm{th}}, \quad \forall k, \tag{6b}$$

$$p(r_n, \theta_n) \geq p_n^{\mathrm{th}}, \quad \forall n, \tag{6c}$$

$$\mathrm{Tr}(\mathbf{V}\mathbf{V}^{\mathrm{H}}) \leq p_{\max}. \tag{6d}$$

Here, (6b) ensures the minimum communication SINR γ_k^{th}, (6c) enforces the minimum sensing beampattern gain p_n^{th} for target detection, and (6d) limits the BS transmit power to $p_{\max}$.

V. Proposed Solution

Since $\mathcal{P}1$ is non-convex due to its objective and variable-product constraints, we use one of the constraints to define a manifold. The search is then restricted to this manifold, and a single cost function incorporates the remaining constraints.

First, (6d) can be normalized by setting $\mathrm{Tr}(\mathbf{V}\mathbf{V}^{\mathrm{H}}) \leq 1$. We then introduce $\tilde{\mathbf{V}} = [\tilde{\mathbf{v}}_1, \ldots, \tilde{\mathbf{v}}_{K+N}]$, where $\tilde{\mathbf{v}}_i = [\mathbf{v}_i^{\mathrm{T}}, z_i]^{\mathrm{T}}$ and $\mathbf{z} = [z_1, \ldots, z_{K+N}]$ is an auxiliary vector. This ensures $\mathrm{Tr}(\tilde{\mathbf{V}}\tilde{\mathbf{V}}^{\mathrm{H}}) = \mathrm{Tr}(\mathbf{V}\mathbf{V}^{\mathrm{H}}) + \|\mathbf{z}\|_2^2 = 1$, which simplifies power normalization while preserving feasibility [6]. This yields the complex sphere manifold $\mathcal{M}$ of size $(M+1) \times (K+N)$. This reformulates $\mathcal{P}1$ as an optimization problem on $\mathcal{M}$:

$$\mathcal{P}2: \min_{\tilde{\mathbf{V}} \in \mathcal{M}} \quad f(\tilde{\mathbf{V}}) = -\sum\nolimits_{k=1}^{K} \left(f_k(\tilde{\mathbf{V}}) - f_{e,k}(\tilde{\mathbf{V}}) \right), \tag{7a}$$

$$\text{s.t} \quad u_k(\tilde{\mathbf{V}}) = \gamma_k^{\mathrm{th}} - \frac{|\hat{\mathbf{h}}_k^{\mathrm{H}} \tilde{\mathbf{V}} \mathbf{E}_k|^2}{\sum_{i=1}^{K+N} |\hat{\mathbf{h}}_k^{\mathrm{H}} \tilde{\mathbf{V}} \mathbf{E}_i|^2 + \sigma^2} \leq 0, \ \forall k, \tag{7b}$$

$$g_n(\tilde{\mathbf{V}}) = p_n^{\mathrm{th}} - \sum\nolimits_{i=1}^{K+N} \hat{\mathbf{a}}_n^{\mathrm{H}} \tilde{\mathbf{V}} \mathbf{E}_i \mathbf{E}_i^{\mathrm{H}} \tilde{\mathbf{V}}^{\mathrm{H}} \hat{\mathbf{a}}_n \leq 0, \ \forall n, \tag{7c}$$

where $\hat{\mathbf{h}}_k = \sqrt{p_{\max}}[\mathbf{h}_k, 0]$ and $\hat{\mathbf{a}}_n = \sqrt{p_{\max}}[\mathbf{g}_n, 0]$ are adjusted to match the problem's dimensionality. Moreover, we define $f_k(\tilde{\mathbf{V}}) = \frac{|\hat{\mathbf{h}}_k^{\mathrm{H}} \tilde{\mathbf{V}} \mathbf{E}_k|^2}{\sum_{i=1}^{K+N} |\hat{\mathbf{h}}_k^{\mathrm{H}} \tilde{\mathbf{V}} \mathbf{E}_i|^2 + \sigma^2}$ and $f_{e,k}(\tilde{\mathbf{V}}) = \frac{|\hat{\mathbf{g}}^{\mathrm{H}} \tilde{\mathbf{V}} \mathbf{E}_k|^2}{\sum_{i=1}^{K+N} |\hat{\mathbf{g}}^{\mathrm{H}} \tilde{\mathbf{V}} \mathbf{E}_i|^2 + \sigma^2}$, where $\hat{\mathbf{g}} = \sqrt{p_{\max}}[\mathbf{g}, 0]$. In (7), $f(\tilde{\mathbf{V}})$, $f_{e,k}(\tilde{\mathbf{V}})$, $u_k(\tilde{\mathbf{V}})$, and $g_n(\tilde{\mathbf{V}})$ are continuous differentiable functions from $\mathcal{M}$ to $\mathbb{R}$ [14]. However, the constraints (7b) and (7c) are beyond manifold constraints. To address this challenge, we incorporate (7b) and (7c) into the objective as a penalty term utilizing ALM [14]. The resulting Lagrangian cost function is given as [14]

$$\mathcal{L}_\rho(\tilde{\mathbf{V}}, \boldsymbol{\lambda}, \boldsymbol{\alpha}) = f(\tilde{\mathbf{V}}) + \rho/2 \sum\nolimits_{k=1}^{K} ([\lambda_k/\rho + u_k(\tilde{\mathbf{V}})]^+)^2 + \rho/2 \sum\nolimits_{n=1}^{N} ([\alpha_n/\rho + g_n(\tilde{\mathbf{V}})]^+)^2, \tag{8}$$

where $\rho > 0$ is a penalty parameter and $\boldsymbol{\lambda} \geq \mathbb{R}^K$ and $\boldsymbol{\alpha} \geq \mathbb{R}^N$ are the vectors of Lagrange parameters. The ALM optimizes $\tilde{\mathbf{V}}$ for given $\boldsymbol{\lambda}$ and $\boldsymbol{\alpha}$ using the MO technique, and updates $\boldsymbol{\lambda}$ and $\boldsymbol{\alpha}$ with a gradient-type rule [15]. The decision variable $\tilde{\mathbf{V}}$ is restricted to a manifold $\mathcal{M}$ when applying ALM to Riemannian manifolds. This results in $\mathcal{L}_\rho(\tilde{\mathbf{V}}, \boldsymbol{\lambda}, \boldsymbol{\alpha})$ differentiable over $\tilde{\mathbf{V}}$, allowing the ALM framework to be applied directly [14]. Thus, the resultant problem can be given as $\mathcal{P}3: \min_{\tilde{\mathbf{V}} \in \mathcal{M}, \boldsymbol{\lambda}, \boldsymbol{\alpha}} \ \mathcal{L}_\rho(\tilde{\mathbf{V}}, \boldsymbol{\lambda}, \boldsymbol{\alpha})$. The ALM-based MO search, i.e., Algorithm 1, optimizes $\mathcal{L}_\rho(\tilde{\mathbf{V}}, \boldsymbol{\lambda}, \boldsymbol{\alpha})$ on manifold $\mathcal{M}$ through four main steps [14], [16]:

Algorithm 1 : Secure Beamforming Algorithm

1: **Require**: $\mathcal{M}$, $f(\tilde{\mathbf{V}})$, $u_k(\tilde{\mathbf{V}})$, $g_n(\tilde{\mathbf{V}})$.
2: **Initialization**: $\tilde{\mathbf{V}}_0 \in \mathcal{M}$, multipliers $\{\boldsymbol{\lambda}^0, \boldsymbol{\alpha}^0\}$, tolerances $\{\epsilon_{\min}, \epsilon_0 > 0, \delta_1 > 0, \delta_2 > 0\}$, penalty ρ_0, reduction factors $\{\theta_\epsilon \in (0,1), \theta_\rho > 1\}$, bounds $\{\lambda^{\min}, \lambda^{\max}, \alpha^{\min}, \alpha^{\max}\}$, ratio τ, minimum distance $d_{\min}$, $t = 0$.
3: **while** $\mathrm{dist}(f(\tilde{\mathbf{V}}_t), f(\tilde{\mathbf{V}}_{t+1})) \geq \delta_2$ **do**
4: Update $\boldsymbol{\eta}_t = -\mathrm{grad}_{\tilde{\mathbf{V}}_t} \mathcal{L}_\rho(\tilde{\mathbf{V}}, \boldsymbol{\lambda}, \boldsymbol{\alpha})$.
5: **while** $\|\mathrm{grad}_{\tilde{\mathbf{V}}_t} \mathcal{L}_\rho\|_2 > \delta_1$ **do**
6: Compute ν_t, update $\tilde{\mathbf{V}}_{t+1}$ via $R_{\tilde{\mathbf{V}}_t}(\nu_t \boldsymbol{\eta}_t)$, update $\mathcal{T}_{\tilde{\mathbf{V}}_t \to \tilde{\mathbf{V}}_{t+1}}(\boldsymbol{\eta}_t)$, compute β_t, update $\boldsymbol{\eta}_{t+1}$, $t \leftarrow t+1$.
7: **end while**
8: Update $\boldsymbol{\lambda}^{t+1}, \boldsymbol{\alpha}^{t+1}$.
9: $\sigma_i^{t+1} = \max\left\{ \frac{h_i(\tilde{\mathbf{V}}_{t+1})}{\mu_i^{t+1}}, -\frac{\mu_i^{t+1}}{\rho_t} \right\}$, $i \in \{k, n\}$, $h_i \in \{u_k, g_n\}$, and $\mu_i \in \{\lambda_k, \alpha_n\}$.
10: Adjust $\epsilon_{t+1} = \max\{\epsilon_{\min}, \theta_\epsilon \epsilon_t\}$.
11: $\rho_{t+1} = \begin{cases} \rho_t, & t=0 \text{ or } \max_{k,n}\{|\sigma_k^{t+1}|, |\sigma_n^{t+1}|\} \leq \tau \max_{k,n}\{|\sigma_k^t|, |\sigma_n^t|\}, \\ \theta_\rho \rho_t, & \text{otherwise.} \end{cases}$
12: $t \leftarrow t+1$, $\tilde{\mathbf{V}}_t \leftarrow \tilde{\mathbf{V}}_{t+1}$.
13: **end while**
14: **Output**: $\mathbf{V}^* = \tilde{\mathbf{V}}^*(1:M, K+N)$.

(i) **Riemannian gradient**: The Euclidean gradient $\nabla_{\tilde{\mathbf{V}}_t} \mathcal{L}_\rho(\tilde{\mathbf{V}}, \boldsymbol{\lambda}, \boldsymbol{\alpha})$ is projected onto the tangent of $\mathcal{M}$ [16, Eqn. (17)]. The required Euclidean gradient of (8) is given by (9), where $\nabla f_b(\tilde{\mathbf{V}})$ is given in (10) with $\hat{\mathbf{c}} = \hat{\mathbf{h}}_k$ for $b = k$ and $\hat{\mathbf{c}} = \hat{\mathbf{g}}$ for $b = \{e, k\}$. Moreover, $\nabla \gamma_k$ is given by $\nabla \gamma_k = \frac{2\hat{\mathbf{h}}_k^{\mathrm{H}} \tilde{\mathbf{V}} \mathbf{E}_k \hat{\mathbf{h}}_k \mathbf{E}_k^{\mathrm{H}}}{\sum_{i=1}^{K+N} |\hat{\mathbf{h}}_k^{\mathrm{H}} \tilde{\mathbf{V}} \mathbf{E}_i|^2 + \sigma^2} - \sum_{j=1}^{K+N} \frac{2|\hat{\mathbf{h}}_k^{\mathrm{H}} \tilde{\mathbf{V}} \mathbf{E}_k|^2 \hat{\mathbf{h}}_k^{\mathrm{H}} \tilde{\mathbf{V}} \mathbf{E}_j \hat{\mathbf{h}}_k \mathbf{E}_j^{\mathrm{H}}}{\left(\sum_{i \neq k}^{K+N} |\hat{\mathbf{h}}_k^{\mathrm{H}} \tilde{\mathbf{V}} \mathbf{E}_i|^2 + \sigma^2\right)^2}$.

(ii) **Search direction and mapping**: The descent direction is updated by a conjugate gradient rule, $\boldsymbol{\eta}_{t+1} = -\mathrm{grad}_{\tilde{\mathbf{V}}_{t+1}} \mathcal{L}_\rho(\tilde{\mathbf{V}}, \boldsymbol{\lambda}, \boldsymbol{\alpha}) + \beta_t \mathcal{T}_{\tilde{\mathbf{V}}_t \to \tilde{\mathbf{V}}_{t+1}}(\boldsymbol{\eta}_t)$, where β_t uses the Hestenes–Stiefel formula and $\mathcal{T}(\cdot)$ denotes vector transport to align tangent spaces [16, Eqn. (20)].

(iii) **Retraction**: The new iterate is mapped back to $\mathcal{M}$ via $R_{\tilde{\mathbf{V}}_t}(\nu_t \boldsymbol{\eta}_t) = \mathrm{unt}(\nu_t \boldsymbol{\eta}_t)$, where ν_t is the step size [14], [16].

(iv) **Updating the Lagrange multipliers**: This is done as $\lambda_k^{t+1} = \mathrm{clip}_{[\lambda^{\min}, \lambda^{\max}]} \left(\lambda_k^t + \rho_t u_k(\tilde{\mathbf{V}}_{t+1}) \right)$ and $\alpha_n^{t+1} = \mathrm{clip}_{[\alpha^{\min}, \alpha^{\max}]} \left(\alpha_k^t + \rho_t g_n(\tilde{\mathbf{V}}_{t+1}) \right)$, where ρ_t is the penalty parameter and clipping ensures boundedness and stability.

The proposed NF ISAC secure beamforming algorithm is outlined in Algorithm 1. At iteration t, it generates a candidate solution that satisfies $\mathcal{L}_\rho(\tilde{\mathbf{V}}_{t+1}, \boldsymbol{\lambda}_{t+1}, \boldsymbol{\alpha}_{t+1}) \leq \mathcal{L}_\rho(\tilde{\mathbf{V}}_t, \boldsymbol{\lambda}_t, \boldsymbol{\alpha}_t) + \epsilon_t$, where $\{\epsilon_t\}$ is an infinite sequence that converges to zero, ensuring monotonic decrease of the objective and convergence to a stationary point. The total complexity per iteration is $\mathcal{O}(T(M(K+N) + M(K+N)^2))$, with T iterations required for convergence [14], [16]. The manifold-specific operations, i.e., projection of the Euclidean gradient onto the tangent space and retraction back onto the manifold, consist of standard linear algebra steps that scale as $\mathcal{O}(M(K+N))$. Thus, the manifold operations themselves

$$\nabla_{\tilde{\mathbf{V}}_t}\mathcal{L}_\rho(\tilde{\mathbf{V}},\boldsymbol{\lambda},\boldsymbol{\alpha}) = -\sum_{k=1}^{K}\left(\nabla f_k(\tilde{\mathbf{V}}) - \nabla f_{e,k}(\tilde{\mathbf{V}})\right) - 2\rho\sum_{k=1}^{K}\mathbf{1}_{\left\{\lambda_k+\frac{u_k(\tilde{\mathbf{V}})}{\rho}\right\}}\left(\frac{\lambda_k}{\rho}+u_k(\tilde{\mathbf{V}})\right)\nabla\gamma_k$$
$$-2\rho\sum_{n=1}^{N}\mathbf{1}_{\left\{\alpha_n+\frac{g_n(\tilde{\mathbf{V}})}{\rho}\right\}}\left(\frac{\alpha_n}{\rho}+g_n(\tilde{\mathbf{V}})\right)\left(\sum_{i=1}^{K+N}\hat{\mathbf{a}}_n^{\mathrm{H}}\tilde{\mathbf{V}}\mathbf{E}_i\hat{\mathbf{a}}_n\mathbf{E}_i^{\mathrm{H}}\right) \tag{9}$$

$$\nabla f_b(\tilde{\mathbf{V}}) = \frac{1}{\ln(2)}\left(\frac{2\hat{\mathbf{c}}^{\mathrm{H}}\tilde{\mathbf{V}}\mathbf{E}_k\hat{\mathbf{c}}\mathbf{E}_k^{\mathrm{H}}}{\sum_{i=1}^{K+N}|\hat{\mathbf{c}}^{\mathrm{H}}\tilde{\mathbf{V}}\mathbf{E}_i|^2+\sigma^2} - \sum_{j=1}^{K+N}\frac{2|\hat{\mathbf{c}}^{\mathrm{H}}\tilde{\mathbf{V}}\mathbf{E}_k|^2\hat{\mathbf{c}}^{\mathrm{H}}\tilde{\mathbf{V}}\mathbf{E}_j\hat{\mathbf{c}}\mathbf{E}_j^{\mathrm{H}}}{\left(\sum_{i=1}^{K+N}|\hat{\mathbf{c}}^{\mathrm{H}}\tilde{\mathbf{V}}\mathbf{E}_i|^2+\sigma^2\right)\left(\sum_{i\neq k}^{K+N}|\hat{\mathbf{c}}^{\mathrm{H}}\tilde{\mathbf{V}}\mathbf{E}_i|^2+\sigma^2\right)}\right) \tag{10}$$

TABLE I
SIMULATION AND ALGORITHM PARAMETERS.

Parameter	Value	Parameter	Value
f_c	54 GHz	$d_{\min}$	10^{-10}
K	$\{2, 4\}$	$\epsilon_{\min}$	10^{-6}
N	3	θ_ρ	0.25
$p_{\max}$	30 dBm	$\{\delta_1, \delta_2\}$	10^{-6}
γ_k^{th}	10 dB	ϵ_0	10^{-3}
p_n^{th}	10 dB	$\{\tau, \theta_\epsilon\}$	0.5
σ^2	-90 dBm	$\{\lambda^{\min}, \lambda^{\max}\}$	$\{0, 100\}$
ρ_0	1	$\{\alpha^{\min}, \alpha^{\max}\}$	$\{0, 100\}$

do not dominate the runtime. This overall complexity is substantially lower than conventional approaches such as CCPA or SDR/SCA-based methods, which involve lifted matrices of size $\mathcal{O}(M^2KN)$ and cubic or higher-order complexity. For more details on computational aspects of MO, we refer the readers to [14], [16].

VI. Simulation Results

We evaluate the performance of the proposed NF secure ISAC beamforming algorithm (i.e., Algorithm 1). The BS is placed at $\{0, 0\}$. Unless stated otherwise, the system configuration consists of $K = 2$ and $N = 3$. The users are positioned at distances of 30 m and 40 m from the BS, with respective angles of $-35°$ and $50°$. The sensing targets are placed at 15 m, 15 m, and 25 m, with angular directions of $-15°$, $30°$, and $30°$, respectively. The simulation results are obtained over 10^3 independent Monte Carlo trials. Additional simulation parameters are provided in Table I.

CCPA benchmark: We compare the proposed algorithm with a benchmark based on CCPA [5], which solves $\mathcal{P}1$ via an iterative SDR-SCA approach. Specifically, the beamforming and sensing matrices are defined as $\mathbf{W}_k = \mathbf{w}_k\mathbf{w}_k^{\mathrm{H}}$ and $\mathbf{S}_n = \mathbf{s}_n\mathbf{s}_n^{\mathrm{H}}$, where $\mathbf{W}_k$ and $\mathbf{S}_n$ are semidefinite with $\mathrm{Rank}(\mathbf{W}_k) = 1$. To ensure tractability, $\mathcal{P}1$ is reformulated as a semidefinite program (SDP) by relaxing the rank-one constraints [5]. The relaxed SDP is solved via CVX, and Gaussian randomization is applied to approximate the rank-one solution.

FF benchmark: Assuming $D \ll r_b$ and approximating with $\sqrt{1+x} \approx 1 + x/2$ for $x = \frac{1}{r_b}(m^2d^2 - 2r_bmd\cos(\theta_b))$, the array response simplifies to $[\mathbf{c}_b]_m = e^{j\frac{2\pi}{\lambda}md\cos(\theta_b)}$ [2]. This approximation serves as a benchmark to quantify the performance degradation resulting from inaccurate channel modeling in NF secure ISAC systems.

Fig. 2 illustrates the average execution time (left) and convergence behavior (right) of the proposed algorithm compared to the CCPA method, based on MATLAB simulations run on an Intel® Core™ i7 processor (2.50 GHz). As shown in the left plot, execution time increases with M, but the proposed algorithm consistently outperforms CCPA, significantly reducing runtime for all values of M. For instance, at $M = 257$, the proposed method is approximately 18 times faster than CCPA.

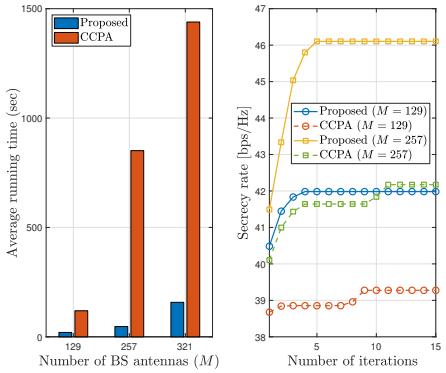

Fig. 2. Execution time (left) and convergence rate (right).

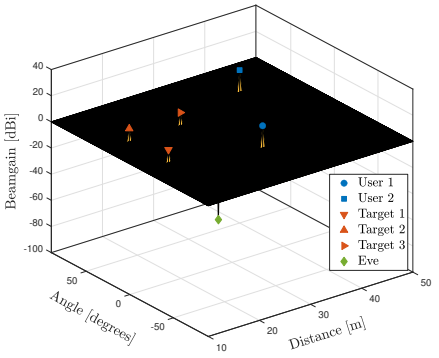

Fig. 3. Secrecy rate of Algorithm 1 with NF channels for $M = 129$.

The right plot in Fig. 2 shows that the proposed algorithm converges significantly faster than CCPA. Specifically, it achieves a stable secrecy rate within five iterations, regardless of the antenna array size, while CCPA requires nine or more iterations to converge. This highlights the lower computational burden and superior efficiency of the proposed algorithm.

Fig. 3 and Fig. 4 illustrate the beam-focusing capabilities of Algorithm 1 under NF and FF channel conditions, respectively, with $M = 129$. The algorithm adaptively forms spatial beams by optimizing transmit signals, leveraging NF/FF propagation characteristics to enable joint sensing and communication.

In Fig. 3, the beampattern (NF case) exhibits distinct peaks accurately aligned with the actual user and target positions in both angle and distance. This demonstrates a key advantage of NF ISAC: spherical wavefronts enable spatial resolution in both domains, allowing the system to distinguish users or

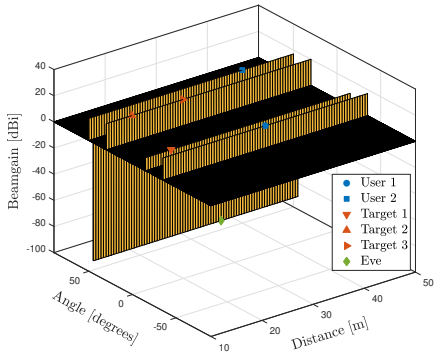

Fig. 4. Beam-focusing of the radar functionality of Algorithm 1 with FF channels for $M = 129$.

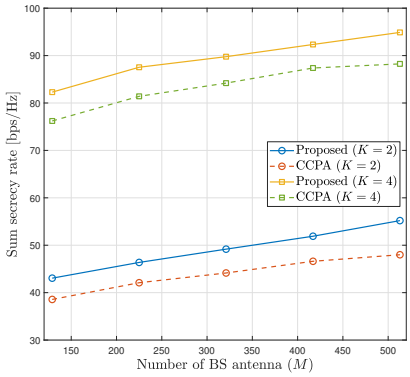

Fig. 5. Sum secrecy rate versus the number of BS antennas.

targets even when they share the same angle but differ in range. Such fine-grained resolution enhances radar detection, communication quality, and physical-layer security by reducing leakage toward unintended directions (e.g., Eve). In contrast, Fig. 4 (FF case) shows beampatterns that distribute energy uniformly along angular directions, regardless of distance. Owing to the planar wavefront assumption, FF models ignore range-dependent phase variations and thus cannot separate objects located at different distances along the same angle. This limits sensing resolution and increases the potential for interference or information leakage in multi-user scenarios.

Fig. 5 compares the secrecy rate performance of both algorithms for different M. A higher number of BS antennas correlates with an increased sum rate for all algorithms. Thus, they can effectively leverage the spatial multiplexing benefits of a greater antenna count. Notably, Algorithm 1 outperforms CCPA in terms of secrecy rate across a wide range of antenna numbers. For example, with $M = 257$ and $K = 2$, it delivers an $11.4\,\%$ gain. The SCA approximation and the rank-one SDR relaxation used in the CCPA may be the cause.

Running time and secrecy rate gains stem from three main factors: (i) CCPA explores over $\mathbb{R}^{MNK}$, whereas Algorithm 1 operates on $\mathcal{M}$ with only $(M+1)(K+N)$ dimensions, drastically reducing complexity; (ii) The proposed method reformulates non-convex $\mathcal{P}1$ directly as a MO problem, without intermediate approximations; (iii) It aggregates all beamforming vectors into a single variable, which is more efficient for large-scale systems. Conversely, CCPA relies on SCA and SDR, which involve computationally expensive matrix operations, particularly as M increases.

VII. Conclusion

An NF ISAC secure beamforming algorithm is developed for supporting multiple users and targets in the presence of an eavesdropper. The algorithm leverages the beam-focusing capability of NF propagation in both angular and distance domains and maximizes the secrecy sum-rate subject to constraints on user SINR, target beampattern gains, and BS transmit power. While the dimensionality of the problem increases rapidly with the number of antennas, the proposed algorithm restricts the search to a complex sphere manifold, reducing the search space to $(M+1)(K+N)$ dimensions, compared to the conventional CCPA approach with M^2KN dimensions. This reduction leads to substantial computational efficiency, making the algorithm suitable for large-scale NF secure ISAC deployments. Future work may address accommodating user and target mobility with dynamic channel conditions, integrating range and velocity estimation, and exploring robust solutions for channel estimation and beam training.

References

[1] A. Hakimi, D. Galappaththige, and C. Tellambura, "A roadmap for NF-ISAC in 6G: A comprehensive overview and tutorial," *Entropy*, vol. 26, no. 9, Sept. 2024.

[2] Z. Wang, X. Mu, and Y. Liu, "Near-field integrated sensing and communications," *IEEE Commun. Lett.*, vol. 27, no. 8, pp. 2048–2052, Aug. 2023.

[3] Z. Chen, F. Wang, G. Han, X. Wang, and V. K. N. Lau, "Robust beamforming design for secure near-field ISAC systems," *IEEE Wireless Commun. Lett.*, pp. 1–1, 2025.

[4] L. Zhang, Y. Wang, H. Chen, and Y. Cao, "Physical-layer security of the NOMA-assisted ISAC systems under near-field scenario," *IEEE Internet of Things Journal*, vol. 12, no. 12, pp. 18 546–18 553, Jun. 2025.

[5] D. Galappaththige, S. Zargari, C. Tellambura, and G. Y. Li, "Near-field ISAC: Beamforming for multi-target detection," *IEEE Wireless Commun. Lett.*, pp. 1–1, Jul. 2024.

[6] ——, "Low-complexity multi-target detection in ELAA ISAC," *IEEE Commun. Lett.*, vol. 29, no. 3, pp. 620–624, 2025.

[7] Y. Zhang, H. Zhang, S. Xiao, W. Tang, and Y. C. Eldar, "Near-field wideband secure communications: An analog beamfocusing approach," *IEEE Trans. Signal Process.*, vol. 72, pp. 2173–2187, Apr. 2024.

[8] H. Liu *et al.*, "Stacked intelligent metasurfaces for wireless communications: Applications and challenges," *arXiv*, 2025.

[9] J. Chen *et al.*, "Physical layer security for near-field communications via directional modulation," *IEEE Trans. Veh. Technol.*, vol. 73, no. 8, pp. 12 242–12 246, Aug. 2024.

[10] X. Jia *et al.*, "Stacked intelligent metasurface enabled near-field multiuser beamfocusing in the wave domain," in *Proc. IEEE 99th Veh. Technol. Conf.*, Jun. 2024, pp. 1–5.

[11] Z. He *et al.*, "Full-duplex communication for ISAC: Joint beamforming and power optimization," *IEEE J. Sel. Areas Commun.*, vol. 41, no. 9, pp. 2920–2936, Sept. 2023.

[12] Z. He, W. Xu, H. Shen, Y. Huang, and H. Xiao, "Energy efficient beamforming optimization for integrated sensing and communication," *IEEE Wireless Commun. Lett.*, vol. 11, no. 7, pp. 1374–1378, Jul. 2022.

[13] P. Stoica, J. Li, and Y. Xie, "On probing signal design for MIMO radar," *IEEE Trans. Signal Process.*, vol. 55, no. 8, pp. 4151–4161, Jul. 2007.

[14] C. Liu and N. Boumal, "Simple algorithms for optimization on Riemannian manifolds with constraints," *Appl. Math. Optim.*, vol. 82, pp. 949–981, Mar. 2020.

[15] E. G. Birgin and J. M. Martínez, *Practical Augmented Lagrangian Methods for Constrained Optimization*. Philadelphia, PA: Soc. Ind. Appl. Math., 2014.

[16] S. Zargari, D. Galappaththige, C. Tellambura, and H. Vincent Poor, "A Riemannian manifold approach to constrained resource allocation in ISAC," *IEEE Trans. Commun.*, pp. 1–1, May 2024.