


Integrated Sensing and Secure Communication with XL-MIMO

Ping Sun ¹ , Haibo Dai ² and Baoyun Wang ^{1,*}¹ School of Communication and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210023, China; 2018010214@njupt.edu.cn² School of Internet of Things, Nanjing University of Posts and Telecommunications, Nanjing 210046, China; hbdai@njupt.edu.cn

* Correspondence: bywang@njupt.edu.cn

Abstract: This paper studies extremely large-scale multiple-input multiple-output (XL-MIMO)-empowered integrated sensing and secure communication systems, where both the radar targets and the communication user are located within the near-field region of the transmitter. The radar targets, being untrusted entities, have the potential to intercept the confidential messages intended for the communication user. In this context, we investigate the near-field beam-focusing design, aiming to maximize the achievable secrecy rate for the communication user while satisfying the transmit beam pattern gain requirements for the radar targets. We address the corresponding globally optimal non-convex optimization problem by employing a semidefinite relaxation-based two-stage procedure. Additionally, we provide a sub-optimal solution to reduce complexity. Numerical results demonstrate that beam focusing enables the attainment of a positive secrecy rate, even when the radar targets and communication user align along the same angle direction.

Keywords: near field; integrated sensing and communication; beam focusing; vehicular ad hoc networks (VANETs)



Citation: Sun, P.; Dai, H.; Wang, B. Integrated Sensing and Secure Communication with XL-MIMO. *Sensors* **2024**, *24*, 295. <https://doi.org/10.3390/s24010295>

Academic Editors: Renato Machado, Pingyi Fan and Qiong Wu

Received: 22 October 2023

Revised: 26 December 2023

Accepted: 28 December 2023

Published: 3 January 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Integrated sensing and communication (ISAC) has emerged as a significant advancement in upcoming wireless systems [1,2]. These systems enable the dual use of hardware platforms and limited spectrum/power resources for both communication and sensing tasks [3]. One of the most promising areas of ISAC application is in *vehicular ad hoc networks* (VANETs), which are at the forefront of the evolution of connected and autonomous vehicles [4]. In VANETs, vehicles communicate with each other and possibly with infrastructure components, such as traffic signals or roadside units. These communications can be used for sharing traffic conditions, alerting nearby vehicles of emergency braking, or even for cooperative driving in the future [5]. With the increasing complexity and density of modern traffic systems, vehicles also need advanced sensing capabilities for safety and navigation purposes. By integrating ISAC into VANETs, vehicles can dynamically optimize resources, streamline hardware, and enhance safety through real-time communication of sensed data, ensuring efficient and adaptive network performance [6,7].

Currently, ISAC systems allow the reuse of information-bearing signals for radar sensing [2]. While this dual operation improves spectrum efficiency and reduces the cost of systems, it introduces potential risks of information leakage. This becomes particularly concerning when sensing targets, being untrusted entities, might intercept these confidential signals [8]. To address this issue, physical layer security techniques have been integrated into ISAC systems to ensure communication security [9–11]. In [9], the authors examine an ISAC scenario consisting of one communication user and one untrusted target, potentially an eavesdropper, and they design the transmit covariance matrices to maximize the achievable secrecy rate. In [10], the authors jointly optimize the transmit information and sensing

beamforming, aiming to minimize the beampattern matching error for sensing while ensuring the minimum secrecy rate requirement. Meanwhile, in [11], optimization-based beamforming designs are presented, focusing on the security of information transmissions within ISAC systems.

It should be noted that all the aforementioned papers on secrecy ISAC address the far-field scenario, where both radar targets and communication users reside within the far-field region of the transmitter. Motivated by the great success of multiple-input multiple-output (MIMO) technology in 4G and 5G [12,13], in future 6G networks, extremely large-scale (XL)-MIMO is envisioned to be utilized. XL-MIMO, deploying hundreds, or even thousands, of antenna elements at base stations or reflecting elements at reconfigurable intelligent surfaces, can significantly improve performance, such as spectral efficiency [14]. The envisioned deployment of XL-MIMO in future 6G networks will likely lead to wireless operations in the radiating near-field (Fresnel) region, in contrast to conventional wireless systems, which typically operate in the far-field region [15]. Thus, there will be a shift in 6G: radar targets and communication users may predominantly operate within the near-field region of the transmitter [16]. While far-field propagation assumes a planar wavefront, the near-field region is characterized by a spherical wavefront. This unique near-field waveform propagation characteristic paves the way for the beam focusing technique, as detailed in [17,18], offering a notable boost in secrecy communication performance by mitigating information leakage. Nevertheless, this promising avenue has garnered limited attention in the current secrecy ISAC literature.

Motivated by the preceding discussion, in this paper, we explore the near-field beam-focusing design for secrecy ISAC systems. Here, one transmitter equipped with an extremely large-scale antenna array senses multiple radar targets and communicates with a single communication user concurrently. Both the radar targets and the communication users are situated within the near-field region of the transmitter. These radar targets, being untrusted, might eavesdrop on the confidential messages intended for the communication user. In this context, we investigate the near-field beam-focusing design to characterize the trade-off between radar sensing and secure communication. The main contributions of this paper are summarized below:

- To the best of the authors' knowledge, this work represents the first study of the near-field secrecy ISAC scenario, with a focus on revealing the benefits of near-field operation for secure communication. To achieve this, we formulate a near-field secrecy beam-focusing problem to maximize the secrecy rate for the communication user while meeting the transmit beampattern gain requirement for each radar target. The considered problem is new and has not been previously studied in either the conventional far-field or near-field contexts.
- While the formulated problem is non-convex, we achieve a global optimum solution by employing a two-stage procedure based on semidefinite relaxation (SDR). Additionally, we propose a novel low-complexity sub-optimal beam-focusing design tailored for this new problem.
- Finally, we provide numerical results to validate the effectiveness of our proposed secrecy beam-focusing designs. Notably, our proposed beam-focusing designs enable a positive secrecy rate even when the radar targets and communication user align along the same angle direction, which is unattainable with far-field beam steering. Additionally, we illustrate the performance trade-off between radar sensing and secrecy communication in near-field ISAC systems.

The remainder of this paper is organized as follows: Section 2 introduces the system model and problem formulation for near-field secrecy ISAC systems. Section 3 presents the development of an optimal solution and a sub-optimal, lower-complexity alternative. In Section 4, we provide extensive simulation results to validate our designs and illustrate the trade-offs involved. Finally, Section 5 concludes the paper with a summary of our findings and potential future research directions.

Let boldface lower-case and upper-case letters denote vectors and matrices, respectively. Use $\|\cdot\|$ for the ℓ_2 norm, $(\cdot)^T$ for the transpose, $(\cdot)^H$ for the Hermitian transpose, $\text{Null}(\cdot)$ for the null space of a matrix, and \mathbb{C} to represent complex numbers.

2. System Model and Problem Formulation

Consider a near-field secrecy ISAC system, as illustrated in Figure 1. Here, one transmitter equipped with an extremely large-scale uniform linear array (ULA) of N antenna elements serves a single-antenna communication user and simultaneously senses L potential targets. Both the radar targets and the communication user are situated within the near-field region of the transmitter. These radar targets, being untrusted, might eavesdrop on the confidential messages intended for the communication user. With an inter-element spacing of d , the total antenna array aperture is $D = (N - 1)d$. The boundary separating the near-field and far-field regions, known as either the Fraunhofer or Rayleigh distance, is defined as $d_F = \frac{2D^2}{\lambda}$ [19]. As the antenna count N increases, d_F can extend over several hundred meters, encompassing numerous communication users and sensing targets. Given these considerations, research on near-field ISAC systems becomes increasingly crucial.

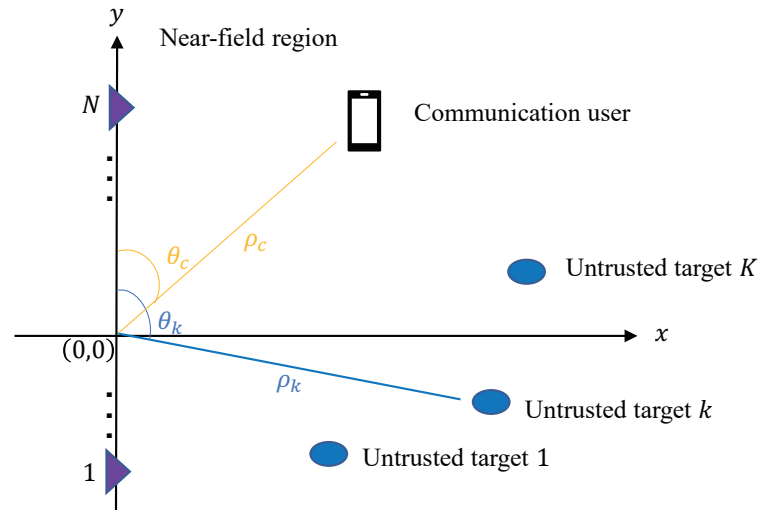


Figure 1. Illustration of near-field secrecy ISAC systems, consisting of one extremely large-scale antenna array that senses potential radar targets and serves communication users simultaneously.

2.1. Near-Field Channel Model

The ULA of the transmitter is positioned along the y -axis. The Cartesian coordinate of the n th antenna element is represented as $p_n = \left(0, \left(n - \frac{N+1}{2}\right)d\right)$, with $n = 1, 2, \dots, N$. The communication user is located at $p_c = (\rho \sin \theta, \rho \cos \theta)$, with ρ and θ denoting the distance and angle between the communication user and the array center, respectively. Let $d_n \triangleq \sqrt{(\rho \sin \theta)^2 + \left(\rho \cos \theta - \left(n - \frac{N+1}{2}\right)d\right)^2}$ denote the distance between the n th antenna element of the transmitter and the communication user. Denote c and f_c as the light speed and the carrier, respectively. Then, the near-field channel between the transmitter and the communication user is given by

$$\mathbf{h}(\rho, \theta) = g e^{-j2\pi f_c \frac{\rho}{c}} \mathbf{a}(\rho, \theta), \quad (1)$$

where $g \triangleq \sqrt{\left(\frac{c}{4\pi f_c d_1}\right)^2}$, and $\mathbf{a}(\rho, \theta)$ denotes the steering vector, given by

$$\mathbf{a}(\rho, \theta) = \left[e^{-j2\pi f_c \frac{(d_1 - \rho)}{c}}, \dots, e^{-j2\pi f_c \frac{(d_N - \rho)}{c}} \right]^T.$$

Let ρ_l and θ_l denote the distance and angle between the l th untrusted radar target and the array center, respectively. The corresponding near-field channel between the transmitter and the l th untrusted radar target is given by

$$\mathbf{h}(\rho_l, \theta_l) = g_l e^{-j2\pi f_c \frac{\rho_l}{c}} \mathbf{a}(\rho_l, \theta_l), \quad 1 \leq l \leq L, \quad (2)$$

where $g_l \triangleq \sqrt{\left(\frac{c}{4\pi f_c d_1^l}\right)^2}$, and the steering vector $\mathbf{a}(\rho_l, \theta_l)$, given by

$$\mathbf{a}(\rho_l, \theta_l) = \left[e^{-j2\pi f_c \frac{(d_1^l - \rho_l)}{c}}, \dots, e^{-j2\pi f_c \frac{(d_N^l - \rho_l)}{c}} \right]^T.$$

2.2. Signal Model

The transmitter uses beam focusing to transmit a combined signal for both communication and radar-sensing tasks. Represented by $\mathbf{x} \in \mathbb{C}^{N \times 1}$, the baseband signal at the transmitter is given by

$$\mathbf{x} = \mathbf{w}s + \mathbf{t}_0, \quad (3)$$

where $\mathbf{w} \in \mathbb{C}^{N \times 1}$ is the beam-focusing vector for the communication user, with s being the information-bearing signal. On the other hand, \mathbf{t}_0 is the dedicated radar signal with zero mean, and its covariance matrix is denoted as $\mathbf{R} = \mathbb{E}[\mathbf{t}_0 \mathbf{t}_0^H] \succeq \mathbf{0}$.

According to (1) and (3), the received signal at the communication user can be written as $y_c = \mathbf{h}^H(\rho, \theta)(\mathbf{w}s + \mathbf{t}_0) + n_c$, where n_c denotes the additive noise at the communication user, with zero mean and variance of δ_c^2 . Thus, the signal-to-interference-plus-noise ratio (SINR) at the communication user is expressed as

$$\Gamma_c(\mathbf{w}, \mathbf{R}) = \frac{|\mathbf{h}(\rho, \theta)^H \mathbf{w}|^2}{\mathbf{h}^H(\rho, \theta) \mathbf{R} \mathbf{h}(\rho, \theta) + \sigma_c^2}. \quad (4)$$

In the near-field ISAC scenarios, both communication and radar signals can contribute to radar-sensing tasks. Consequently, the transmit beampattern gain at the l th radar target is defined as [20]

$$\begin{aligned} \mathcal{B}_l(\mathbf{w}, \mathbf{R}) &= \mathbb{E} \left[\left| \mathbf{a}^H(\rho_l, \theta_l)(\mathbf{w}s + \mathbf{t}_0) \right|^2 \right] \\ &= \mathbf{a}^H(\rho_l, \theta_l) (\mathbf{w} \mathbf{w}^H + \mathbf{R}) \mathbf{a}(\rho_l, \theta_l). \end{aligned} \quad (5)$$

The radar targets are untrusted nodes, which potentially intercept the confidential messages intended for the communication user. The SINR at the l th target is given by

$$\Gamma_l(\mathbf{w}, \mathbf{R}) = \frac{|\mathbf{h}(\rho_l, \theta_l)^H \mathbf{w}|^2}{\mathbf{h}^H(\rho_l, \theta_l) \mathbf{R} \mathbf{h}(\rho_l, \theta_l) + \sigma_l^2}, \quad 1 \leq l \leq L. \quad (6)$$

Based on (4) and (6), the achievable secrecy rate of the communication user can be expressed as

$$r(\mathbf{w}, \mathbf{R}) = \left[\log_2(1 + \Gamma_c(\mathbf{w}, \mathbf{R})) - \max_{1 \leq l \leq L} \log_2(1 + \Gamma_l(\mathbf{w}, \mathbf{R})) \right]^+, \quad (7)$$

where $[x]^+ \triangleq \max(0, x)$.

2.3. Problem Formulation

We are interested in characterizing the performance trade-off between radar sensing and secrecy communication. Specifically, we aim to maximize the secrecy rate of the

communication user while satisfying the transmit beampattern gains for radar targets, by jointly optimizing the beam-focusing vector \mathbf{w} and the radar covariance matrix \mathbf{R} . Mathematically, the problem of interest is formulated as

$$\begin{aligned} \max_{\mathbf{w}, \mathbf{R}} \quad & r(\mathbf{w}, \mathbf{R}) \\ \text{s.t.} \quad & \mathcal{B}_l(\mathbf{w}, \mathbf{R}) \geq b_l, \quad 1 \leq l \leq L, \\ & \|\mathbf{w}\|^2 + \text{Tr}(\mathbf{R}) \leq P_t, \quad \mathbf{R} \succeq 0, \end{aligned} \quad (8)$$

where b_l denotes the transmit beampattern gain threshold for the l th radar target, and P_t is the transmit power at the transmitter.

3. Proposed Solution

In this section, we first propose a two-stage optimization approach to solve the non-convex problem (8) globally optimally in Section 3.1. Then, in Section 3.2, we develop a low-complexity sub-optimal solution.

3.1. Optimal Solution

In this subsection, we present an SDR-based two-stage procedure to achieve the optimal solution for (8). This is accomplished by decomposing (8) into two sub-problems. First, by introducing a variable γ , we reformulate (8) as

$$\begin{aligned} \max_{\mathbf{w}, \mathbf{R}} \quad & \frac{|\mathbf{h}(\rho, \theta)^H \mathbf{w}|^2}{\mathbf{h}^H(\rho, \theta) \mathbf{R} \mathbf{h}(\rho, \theta) + \sigma_c^2} \\ \text{s.t.} \quad & \frac{|\mathbf{h}(\rho_l, \theta_l)^H \mathbf{w}|^2}{\mathbf{h}^H(\rho_l, \theta_l) \mathbf{R} \mathbf{h}(\rho_l, \theta_l) + \sigma_l^2} \leq \gamma, \quad 1 \leq l \leq L, \\ & \mathbf{a}^H(\rho_l, \theta_l) (\mathbf{w} \mathbf{w}^H + \mathbf{R}) \mathbf{a}(\rho_l, \theta_l) \geq b_l, \quad 1 \leq l \leq L, \\ & \|\mathbf{w}\|^2 + \text{Tr}(\mathbf{R}) \leq P_t, \quad \mathbf{R} \succeq 0. \end{aligned} \quad (9)$$

Similar to [21], it can be proven that there always exists a γ for which problem (9) shares the same optimal solution as problem (8). To be specific, let $f(\gamma)$ denote the optimal value of (9) for a given $\gamma > 0$. Consequently, the optimal value of (8) is equivalent to the following problem:

$$\max_{\gamma > 0} \log_2 \left(\frac{1 + f(\gamma)}{1 + \gamma} \right) \quad (10)$$

Based on the above discussion, we conclude that problem (8) can be solved through a two-step process. Firstly, we solve (9) to obtain the optimal value $f(\gamma)$ for any given γ . Secondly, we solve (10) to find the optimal γ^* by conducting a one-dimensional search over the parameter space. Consequently, we next focus on solving (9).

Problem (9) is still non-convex. Next, we apply the SDR technique to solve (9) globally optimally. To this end, by defining $\mathbf{W} = \mathbf{w} \mathbf{w}^H$ and ignoring the non-convex rank-one constraint on \mathbf{W} , we recast (9) as

$$\begin{aligned} \max_{\mathbf{W}, \mathbf{R}} \quad & \frac{\text{Tr}[\mathbf{H}(\rho, \theta) \mathbf{W}]}{\text{Tr}[\mathbf{H}(\rho, \theta) \mathbf{R}] + \sigma_c^2} \\ \text{s.t.} \quad & \frac{\text{Tr}[\mathbf{H}(\rho_l, \theta_l) \mathbf{W}]}{\text{Tr}[\mathbf{H}(\rho_l, \theta_l) \mathbf{R}] + \sigma_l^2} \leq \gamma, \quad 1 \leq l \leq L, \\ & \text{Tr}[\mathbf{A}(\rho_l, \theta_l) (\mathbf{W} + \mathbf{R})] \geq b_l, \quad 1 \leq l \leq L, \\ & \text{Tr}(\mathbf{W}) + \text{Tr}(\mathbf{R}) \leq P_t, \\ & \mathbf{W} \succeq 0, \quad \mathbf{R} \succeq 0, \end{aligned} \quad (11)$$

where $\mathbf{H}(\rho, \theta) \triangleq \mathbf{h}(\rho, \theta)\mathbf{h}(\rho, \theta)^H$, $\mathbf{H}(\rho_l, \theta_l) \triangleq \mathbf{h}(\rho_l, \theta_l)\mathbf{h}(\rho_l, \theta_l)^H$, and $\mathbf{A}(\rho_l, \theta_l) \triangleq \mathbf{a}(\rho_l, \theta_l)\mathbf{a}(\rho_l, \theta_l)^H$.

Problem (11) is non-convex due to the non-concave nature of its objective function. Nevertheless, we can effectively address this by employing the Charnes–Cooper transformation [22], which allows us to equivalently reformulate (11) as

$$\begin{aligned} \max_{\bar{\mathbf{W}}, \bar{\mathbf{R}}, \tau} \quad & \text{Tr}[\mathbf{H}(\rho, \theta)\bar{\mathbf{W}}] \\ \text{s.t.} \quad & \text{Tr}[\mathbf{H}(\rho, \theta)\bar{\mathbf{R}}] + \tau\sigma_c^2 = 1, \\ & \text{Tr}[\mathbf{H}(\rho_l, \theta_l)(\bar{\mathbf{W}} - \gamma\bar{\mathbf{R}})] \leq \tau\sigma_l^2\gamma, 1 \leq l \leq L, \\ & \text{Tr}[\mathbf{A}(\rho_l, \theta_l)(\bar{\mathbf{W}} + \bar{\mathbf{R}})] \geq \tau b_l, 1 \leq l \leq L, \\ & \text{Tr}(\bar{\mathbf{W}}) + \text{Tr}(\bar{\mathbf{R}}) \leq \tau P_t, \\ & \bar{\mathbf{W}} \succeq 0, \bar{\mathbf{R}} \succeq 0, \tau > 0. \end{aligned} \quad (12)$$

Problem (12) is convex, and thus, it can be solved directly using existing solvers such as CVX [23].

Let $\{\bar{\mathbf{W}}^*, \bar{\mathbf{R}}^*, \tau^*\}$ represent the optimal solution to (12). It can be readily demonstrated that $\mathbf{W}^* = \frac{\bar{\mathbf{W}}^*}{\tau^*}$ and $\mathbf{R}^* = \frac{\bar{\mathbf{R}}^*}{\tau^*}$ are the optimal solution to (11). If $\text{Rank}(\mathbf{W}^*) = 1$, the relaxation of the rank-one constraint in (11) does not impact its optimality. We now present a theorem affirming that we can always construct an optimal solution to (12) with a rank-one matrix $\bar{\mathbf{W}}$.

Theorem 1. Suppose that $\{\bar{\mathbf{W}}^*, \bar{\mathbf{R}}^*, \tau^*\}$ represents the optimal solution to problem (12) with $\text{Rank}(\bar{\mathbf{W}}^*) > 1$. Then, we can construct an alternative feasible solution to (12), denoted as $\{\tilde{\mathbf{W}}^*, \tilde{\mathbf{R}}^*, \tilde{\tau}^*\}$. This alternative solution not only attains an equivalent objective value as $\{\bar{\mathbf{W}}^*, \bar{\mathbf{R}}^*, \tau^*\}$, but also satisfies $\text{Rank}(\tilde{\mathbf{W}}^*) = 1$.

Proof of Theorem 1. The Lagrangian of problem (12) is given by

$$\mathcal{L} = \text{Tr}((\mathbf{A} + \mathbf{Z})\bar{\mathbf{W}}) + \text{Tr}(\mathbf{B}\bar{\mathbf{R}}) + \rho\tau + \mu, \quad (13)$$

where $\mathbf{Z} \succeq 0$ is a matrix Lagrange multiplier associated with the constraint $\bar{\mathbf{W}} \succeq 0$; \mathbf{A} , \mathbf{B} , and ρ are, respectively, defined as

$$\mathbf{A} = \mathbf{H}(\rho, \theta) - \sum_{l=1}^L \beta_l \mathbf{H}(\rho_l, \theta_l) + \sum_{l=1}^L \eta_l \mathbf{A}(\rho_l, \theta_l) - \nu \mathbf{I}, \quad (14)$$

$$\mathbf{B} = -\mu \mathbf{H}(\rho, \theta) + \sum_{l=1}^L \beta_l \gamma \mathbf{H}(\rho_l, \theta_l) + \sum_{l=1}^L \eta_l \mathbf{A}(\rho_l, \theta_l) - \nu \mathbf{I}, \quad (15)$$

$$\rho = -\mu + \sum_{l=1}^L \beta_l \sigma_l^2 - \sum_{l=1}^L \eta_l b_l + \nu P_t, \quad (16)$$

where $\mu \geq 0$, $\{\beta_l \geq 0\}$, $\{\eta_l \geq 0\}$, and $\nu \geq 0$ represent the Lagrange multipliers corresponding to the first through fourth constraints in (12), respectively.

Given (13), the relevant Karush–Kuhn–Tucker (KKT) conditions for the proof are formulated as

$$\frac{\partial \mathcal{L}}{\partial \bar{\mathbf{W}}} = \mathbf{A}^* + \mathbf{Z}^* = \mathbf{0}, \quad (17a)$$

$$\mathbf{Z}^* \bar{\mathbf{W}}^* = \mathbf{0}, \quad (17b)$$

$$\mu^*, \beta_l^*, \eta_l^*, \nu^* \geq 0, \quad (17c)$$

where \mathbf{Z}^* , μ^* , β_l^* , η_l^* , and ν^* denote the optimal Lagrange multipliers for the dual problem of (12), and the resulting \mathbf{A} and \mathbf{B} are \mathbf{A}^* and \mathbf{B}^* . Here, (17b) is obtained from the complementary slackness condition.

According to $\mathbf{Z}^* \succeq 0$, (17a) and (17b), we have

$$\mathbf{A}^* \preceq \mathbf{0} \quad (18a)$$

$$\mathbf{A}^* \bar{\mathbf{W}}^* = \mathbf{0}. \quad (18b)$$

Define $\mathbf{C}^* = -\sum_{l=1}^L \beta_l^* \mathbf{H}(\rho_l, \theta_l) + \sum_{l=1}^L \eta_l^* \mathbf{A}(\rho_l, \theta_l) - \nu^* \mathbf{I}$. Then, we have

$$\mathbf{A}^* = \mathbf{C}^* + \mathbf{H}(\rho, \theta). \quad (19)$$

Based on (18b), the columns of $\bar{\mathbf{W}}^*$ must lie in the null space of \mathbf{A}^* when $\bar{\mathbf{W}}^* \neq \mathbf{0}$. Define $M \triangleq \text{Rank}(\mathbf{C}^*)$. If $M = N$, we can conclude that $\text{Rank}(\mathbf{A}^*) \geq \text{Rank}(\mathbf{C}^*) - \text{Rank}(\mathbf{H}) = N - 1$. In this case, we have $\text{Rank}(\bar{\mathbf{W}}^*) = 1$ when $\bar{\mathbf{W}}^* \neq \mathbf{0}$.

We next discuss the case of $M < N$. In this case, let $\mathbf{X} \in \mathbb{C}^{N \times (N-M)}$ denote the orthonormal basis of the null space of \mathbf{C}^* , i.e., $\mathbf{C}^* \mathbf{X} = \mathbf{0}$. Let \mathbf{x}_m , $1 \leq m \leq (N - M)$, denote the m th column of \mathbf{X} . For each \mathbf{x}_m , it follows

$$\mathbf{x}_m^H \mathbf{A}^* \mathbf{x}_m = \mathbf{x}_m^H \mathbf{C}^* \mathbf{x}_m + \mathbf{x}_m^H \mathbf{H} \mathbf{x}_m = \mathbf{x}_m^H \mathbf{H} \mathbf{x}_m \preceq \mathbf{0}. \quad (20)$$

From (20), we conclude that $\mathbf{x}_m^H \mathbf{H} \mathbf{x}_m = 0$. Thus, we have

$$N - M + 1 \geq \text{Rank}(\text{Null}(\mathbf{A}^*)) \geq N - M. \quad (21)$$

If $\text{Rank}(\text{Null}(\mathbf{A}^*)) = N - M$, we have $\text{Null}(\mathbf{A}^*) = \mathbf{X}$. This means $\bar{\mathbf{W}}^*$ can be expressed as $\bar{\mathbf{W}}^* = \sum_{m=1}^M a_m \mathbf{x}_m \mathbf{x}_m^H$. However, since $\mathbf{x}_m^H \mathbf{H} \mathbf{x}_m = 0$, in this case, the achievable secrecy rate is equal to zero. Thus, we obtain $\text{Rank}(\text{Null}(\mathbf{A}^*)) = N - M + 1$. As a result, the optimal $\bar{\mathbf{W}}^*$ can be expressed as

$$\bar{\mathbf{W}}^* = \sum_{m=1}^M a_m \mathbf{x}_m \mathbf{x}_m^H + d \mathbf{u} \mathbf{u}^H, \quad (22)$$

where $a_m \geq 0, \forall m$ and $d > 0$. \mathbf{u} is an extra dimension of orthonormal basis, which lies in the null space of \mathbf{A}^* and is orthogonal to the span of \mathbf{X} , i.e., $\mathbf{A}^* \mathbf{u} = \mathbf{0}$ and $\mathbf{X} \mathbf{u} = \mathbf{0}$.

Based on (22), for the case of $\text{Rank}(\bar{\mathbf{W}}^*) > 1$, we can construct another feasible solution to problem (12), given by

$$\tilde{\mathbf{W}}^* = \bar{\mathbf{W}}^* - \sum_{m=1}^M a_m \mathbf{x}_m \mathbf{x}_m^H = d \mathbf{u} \mathbf{u}^H, \quad (23)$$

$$\tilde{\mathbf{R}}^* = \bar{\mathbf{R}}^* + \sum_{m=1}^M a_m \mathbf{x}_m \mathbf{x}_m^H, \quad (24)$$

$$\tilde{\tau}^* = \tau^*. \quad (25)$$

It can be easily verified that $\{\tilde{\mathbf{W}}^*, \tilde{\mathbf{R}}^*, \tilde{\tau}^*\}$ is a feasible solution to problem (12), which can not only achieve the same objective value as $\{\bar{\mathbf{W}}^*, \bar{\mathbf{R}}^*, \tau^*\}$, but also satisfies $\text{Rank}(\tilde{\mathbf{W}}^*) = 1$. The proof of the optimality of $\{\tilde{\mathbf{W}}^*, \tilde{\mathbf{R}}^*, \tilde{\tau}^*\}$ in problem (12) is thus completed. \square

Theorem 1 indicates that the optimal solution \mathbf{w}^* to (9) can be accurately extracted by the eigenvalue decomposition of \mathbf{W}^* , with $\mathbf{W}^* = \frac{\tilde{\mathbf{W}}^*}{\tilde{\tau}^*}$. Consequently, $\{\mathbf{w}^*, \tilde{\mathbf{R}}^*\}$ are the globally optimal solution to problem (9).

3.2. ZF-Based Sub-Optimal Solution

In this subsection, we propose a sub-optimal solution based on zero-forcing (ZF) for problem (8), which exhibits a significantly lower computational complexity compared to the optimal solution. This sub-optimal approach involves aligning the information beam \mathbf{w} with the null space of the radar target's channel to prevent any information leakage to potential eavesdroppers, as expressed by $\mathbf{h}(\rho_l, \theta_l)^H \mathbf{w} = 0, 1 \leq l \leq L$. Simultaneously, the radar signal is constrained to lie within the null space of the communication user, specified as $\mathbf{h}^H(\rho, \theta) \mathbf{R} \mathbf{h}(\rho, \theta) = 0$, ensuring that it does not interfere with the communication user.

Define $\mathbf{H} \triangleq [\mathbf{h}(\rho_1, \theta_1), \dots, \mathbf{h}(\rho_L, \theta_L)]^H$. Denote its singular value decomposition as $\mathbf{H} = \mathbf{U} \mathbf{\Sigma} \mathbf{V}^H = \mathbf{U} \mathbf{\Sigma} [\mathbf{V}_1, \mathbf{V}_2]^H$, where $\mathbf{U} \in \mathbb{C}^{L \times L}$ and $\mathbf{V} \in \mathbb{C}^{N \times N}$ are unitary matrices, $\mathbf{\Sigma}$ is a $L \times N$ diagonal matrix, $\mathbf{V}_1 \in \mathbb{C}^{N \times L}$ and $\mathbf{V}_2 \in \mathbb{C}^{N \times (N-L)}$ are the first L and the last $N - L$ right singular vectors of \mathbf{H} . In order to guarantee $\mathbf{h}(\rho_l, \theta_l)^H \mathbf{w} = 0, 1 \leq l \leq L$, the ZF-based \mathbf{w} has the following form:

$$\mathbf{w} = \sqrt{p_c} \mathbf{V}_2 \tilde{\mathbf{w}}, \quad (26)$$

where p_c denotes the transmit power of the information beam, and $\tilde{\mathbf{w}} \in \mathbb{C}^{(N-L) \times 1}$ is an arbitrary complex vector of unit norm. To maximize the secrecy rate, $\tilde{\mathbf{w}}$ should match the equivalent channel $\mathbf{h}(\rho, \theta)^H \mathbf{V}_2$, and thus $\tilde{\mathbf{w}} = \frac{\mathbf{V}_2^H \mathbf{h}(\rho, \theta)}{\|\mathbf{V}_2^H \mathbf{h}(\rho, \theta)\|}$.

According to (26), the achievable secrecy rate becomes

$$r_{\text{ZF}} = \log_2 \left(1 + \frac{p_c \|\mathbf{h}(\rho, \theta)^H \mathbf{V}_2\|^2}{\sigma_c^2} \right). \quad (27)$$

To maximize the secrecy rate in (27), we need to minimize the power consumption required to ensure the radar-sensing task. Consequently, we can obtain the optimal radar-sensing covariance matrix \mathbf{R} by solving the following problem:

$$\begin{aligned} \min_{\mathbf{R}} \quad & \text{Tr}(\mathbf{R}) \\ \text{s.t.} \quad & \mathbf{a}^H(\rho_l, \theta_l) \mathbf{R} \mathbf{a}(\rho_l, \theta_l) \geq b_l, \quad 1 \leq l \leq L, \\ & \mathbf{h}^H(\rho, \theta) \mathbf{R} \mathbf{h}(\rho, \theta) = 0. \end{aligned} \quad (28)$$

Problem (28) is convex and can be efficiently solved using CVX [23]. Let \mathbf{R}^* represent the optimal solution to (28). Consequently, the transmit power p_c in (26) or (27) can be expressed as $p_c = P_t - \text{Tr}(\mathbf{R}^*)$.

4. Simulation Results and Discussion

In this section, we showcase numerical results to validate our secure beam-focusing design in the context of near-field ISAC systems. Our system setup involves a transmitter with a ULA of $N = 64$ antennas, operating at 2.4 GHz. The Rayleigh distance for this setup is $d_F = 248$ m. We position the communication user at (32, 0) meters on the x -axis. All receivers are assumed to have an identical noise power of $\sigma_c^2 = \sigma_1^2 = \dots = \sigma_L^2 = -95$ dBm.

We first show the capabilities of beam focusing for ensuring secure communication. For our demonstration, we consider that a single radar target, which can potentially act as an eavesdropper, is positioned at (16, 0) meters. This location coincides with the angular direction of the communication user. Figure 2a,b show the normalized signal power of the communication signal and radar signal at each point of the near-field xy -plane, respectively, given the transmit power $P_t = 1$ dB and the transmit beam pattern gain threshold $b_l = 40, \forall l$. Both the communication signal beam \mathbf{w} and radar signal covariance matrix \mathbf{R} are obtained by solving problem (8) based on the given user locations and the predefined threshold values. From Figure 2a, we observe that most of the energy from the communication beam \mathbf{w} is concentrated around the communication user. This results in minimal information leakage to the radar target. In contrast, Figure 2b shows that the energy from the radar covariance matrix \mathbf{R} predominantly focuses on the radar target, ensuring

limited interference to the communication user. Analyzing both Figure 2a,b, we conclude that our proposed secure beam focusing is adept at facilitating secure communication even when the radar targets and communication user occupy the same angular position—a feat not feasible with traditional far-field beam steering.

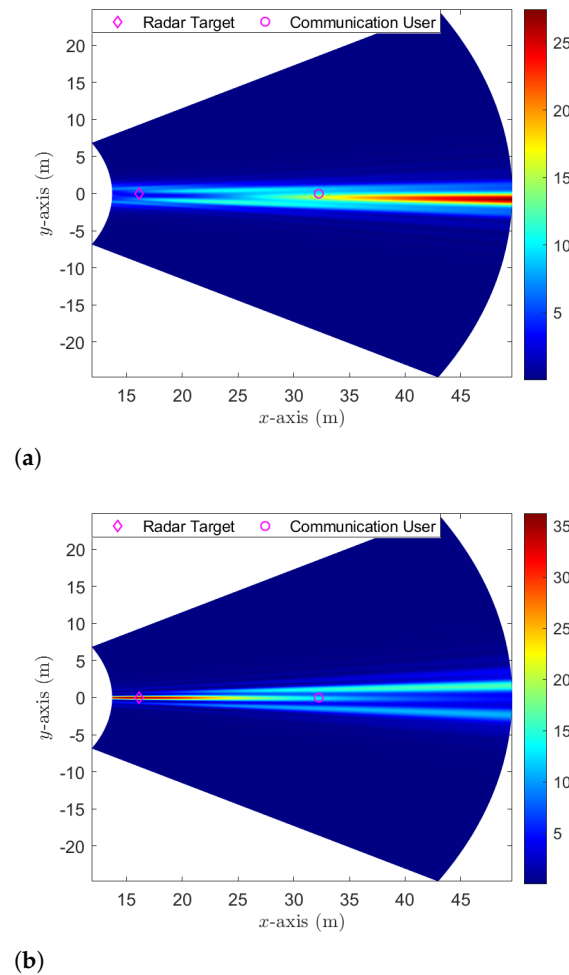


Figure 2. The normalized signal power of communication and radar signals. (a) Communication signal; (b) radar signal.

Figure 3 depicts the trade-off between the achievable secrecy rate and the transmit beampattern gain, as evaluated using both the optimal and sub-optimal solutions. The simulation settings are consistent with those used in Figure 2. It is observed that, as the target beampattern gain requirement rises, the achievable secrecy rate declines sharply. This decline occurs because with a fixed and limited total transmit power, dedicating more power to radar sensing reduces the power available for secure communication. This observation indicates that careful design of the secure beam-focusing scheme is crucial for balancing these two performances. Additionally, the optimal solution consistently surpasses the sub-optimal solution regarding the trade-off between secrecy rate and target beampattern gain. This superior performance stems from the more comprehensive and precise optimization techniques used in deriving the optimal solution, albeit at the cost of increased computational complexity. As anticipated, increasing the transmit budget enhances either the secrecy rate or the target beampattern gain.

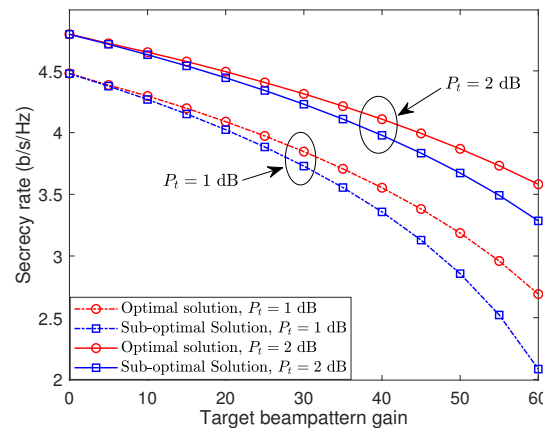


Figure 3. Trade-off between the secrecy rate and the transmit beampattern gain.

Figure 4 effectively illustrates the relationship between the achievable secrecy rate and transmit power, evaluated using both the optimal and sub-optimal near-field solutions, along with the far-field beam steering solution. The far-field beam steering solution is derived by substituting the precise near-field channel model with a standard far-field channel model, thereby neglecting the effects of the near-field. The simulation settings are consistent with those used in Figure 2. Figure 4 shows that the secrecy rates achievable by both the optimal and sub-optimal near-field solutions increase as the transmit power increases. In contrast, the achievable rate of the far-field beam steering remains consistently at zero. This is due to the untrusted radar target, potentially an eavesdropper, sharing an identical angular direction with the communication user, coupled with a relatively smaller distance from the transmitter. Consequently, this potential eavesdropper experiences superior channel conditions compared to the legitimate communication user. Under these circumstances, far-field beam steering fails to differentiate between the untrusted radar target and legitimate communication users, resulting in a zero secrecy rate. Conversely, near-field solutions yield positive secrecy rates, thanks to the beam-focusing capability in the near-field, which proficiently distinguishes users in both angular and distance dimensions.

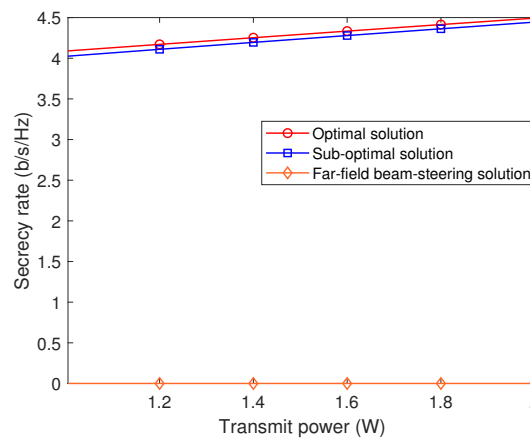


Figure 4. Secrecy rate versus the transmit power.

Finally, we study a general scenario with varying numbers of radar targets randomly positioned on the near-field xy -plane. Figure 5 shows a plot of the achievable secrecy rate against the number of radar targets L , with a consistent radar target threshold $b_l = 20, \forall l$. We successively add radar targets to the near-field xy -plane. As seen in Figure 5, the achievable secrecy rate for both optimal and sub-optimal solutions consistently decreases as the number of radar targets grows. This is because, as the quantity of radar targets rises, so does the likelihood of intercepted communications, consequently leading to a reduced

achievable secrecy rate. Additionally, a higher transmit power can improve the secrecy rate for a given radar target count.

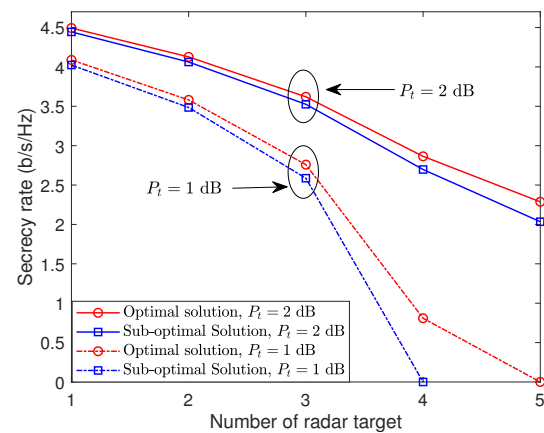


Figure 5. Secrecy rate versus the number of radar targets.

5. Conclusions

This paper addresses beam-focusing design in near-field ISAC systems using XL-MIMO, focusing on maximizing the secrecy rate while meeting radar target requirements. It introduces both globally optimal and practical low-complexity sub-optimal solutions, catering to different computational capacities. Our numerical results demonstrate the efficacy of these solutions, notably achieving positive secrecy rates in challenging scenarios where the radar targets and communication user are positioned at identical angles. This study thus marks a significant advancement in secure communication within near-field ISAC environments, showcasing the potential of XL-MIMO in overcoming traditional security challenges.

One interesting extension of this paper is to use the Cramér–Rao bound (CRB) to evaluate the estimation accuracy. In such a case, the beam-focusing vectors and the radar covariance matrix should be jointly optimized to minimize the CRB. Furthermore, the beam-focusing design can also be extended to the robust beam-focusing case, where perfect channel state information is not necessary. Additionally, while our proposed algorithms have been effectively validated through simulations, we recognize the need for their verification through practical measurements in future research. This step is crucial for a comprehensive assessment of their real-world applicability and performance.

Author Contributions: Conceptualization, P.S. and H.D.; methodology, P.S.; software, P.S.; validation, P.S., H.D. and B.W.; formal analysis, P.S.; investigation, P.S.; resources, P.S.; data curation, P.S.; writing—original draft preparation, P.S.; writing—review and editing, H.D. and B.W.; visualization, P.S.; supervision, H.D. and B.W.; project administration, B.W.; funding acquisition, B.W. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Open Foundation of National Railway Intelligence Transportation System Engineering Technology Research Center under grant No. RITS2021KF02 and the National Natural Science Foundation of China under grant No. 61971238.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data is contained within the article.

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

References

1. Liu, X.; Huang, T.; Shlezinger, N.; Liu, Y.; Zhou, J.; Eldar, Y.C. Joint transmit beamforming for multiuser MIMO communications and MIMO radar. *IEEE Trans. Signal Process.* **2020**, *68*, 3929–3944. [\[CrossRef\]](#)
2. Liu, F.; Cui, Y.; Masouros, C.; Xu, J.; Han, T.X.; Eldar, Y.C.; Buzzi, S. Integrated sensing and communications: Toward dual-functional wireless networks for 6G and beyond. *IEEE J. Sel. Areas Commun.* **2022**, *40*, 1728–1767. [\[CrossRef\]](#)
3. Liu, A.; Huang, Z.; Li, M.; Wan, Y.; Li, W.; Han, T.; Liu, C.; Du, R.; Tan, D.; Lu, J., and others. A survey on fundamental limits of integrated sensing and communication. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 994–1034. [\[CrossRef\]](#)
4. Sheikh, M.S.; Liang, J.; Wang, W. A survey of security services, attacks, and applications for vehicular ad hoc networks (VANETs). *Sensors* **2019**, *19*, 3589. [\[CrossRef\]](#)
5. Hartenstein, H.; Laberteaux, L.P. A tutorial survey on vehicular ad hoc networks. *IEEE Commun. Mag.* **2008**, *46*, 164–171. [\[CrossRef\]](#)
6. Wu, Q.; Wang, S.; Ge, H.; Fan, P.; Fan, Q.; Letaief, K.B. Delay-sensitive task offloading in vehicular fog computing-assisted platoons. *arXiv* **2023**, arXiv:2309.10234.
7. Wu, Q.; Zhao, Y.; Fan, Q.; Fan, P.; Wang, J.; Zhang, C. Mobility-aware cooperative caching in vehicular edge computing based on asynchronous federated and deep reinforcement learning. *IEEE J. Sel. Top. Signal Process.* **2022**, *17*, 66–81. [\[CrossRef\]](#)
8. Wei, Z.; Liu, F.; Masouros, C.; Su, N.; Petropulu, A.P. Toward multi-functional 6G wireless networks: Integrating sensing, communication, and security. *IEEE Commun. Mag.* **2022**, *60*, 65–71. [\[CrossRef\]](#)
9. Deligiannis, A.; Daniyan, A.; Lambotaran, S.; Chambers, J.A. Secrecy rate optimizations for MIMO communication radar. *IEEE Trans. Aerosp. Electron. Syst.* **2018**, *54*, 2481–2492. [\[CrossRef\]](#)
10. Ren, Z.; Qiu, L.; Xu, J. Optimal transmit beamforming for secrecy integrated sensing and communication. In Proceedings of the ICC 2022-IEEE International Conference on Communications, Seoul, Republic of Korea, 16–20 May 2022; pp. 5555–5560.
11. Su, N.; Liu, F.; Masouros, C. Secure Radar-Communication Systems With Malicious Targets: Integrating Radar, Communications and Jamming Functionalities. *IEEE Trans. Wirel. Commun.* **2021**, *20*, 83–95. [\[CrossRef\]](#)
12. Naser, M.; Alsabab, M.; Mahmmoud, B.; Noordin, N.; Abdhussain, S.; Baker, T. Downlink training design for FDD massive MIMO systems in the presence of colored noise. *Electronics* **2020**, *9*, 2155. [\[CrossRef\]](#)
13. Alsabab, M.; Naser, M.; Mahmmoud, B.; Noordin, N.; Abdhussain, S. Sum rate maximization versus MSE minimization in FDD massive MIMO systems with short coherence time. *IEEE Access* **2021**, *9*, 108793–108808. [\[CrossRef\]](#)
14. Zhang, X.; Wang, Z.; Zhang, H.; Yang, L. Near-field channel estimation for extremely large-scale array communications: A model-based deep learning approach. *IEEE Commun. Lett.* **2023**, *27*, 1155–1159. [\[CrossRef\]](#)
15. Zhang, X.; Zhang, H.; Zhang, J.; Li, C.; Huang, Y.; Yang, L. Codebook Design for Extremely Large-Scale MIMO Systems: Near-field and Far-field. *arXiv* **2021**, arXiv:2109.10143.
16. Wang, Z.; Mu, X.; Liu, Y. Near-field integrated sensing and communications. *IEEE Commun. Lett.* **2023**, *27*, 2048–2052. [\[CrossRef\]](#)
17. Zhang, H.; Shlezinger, N.; Guidi, F.; Dardari, D.; Eldar, Y.C. 6G Wireless Communications: From Far-Field Beam Steering to Near-Field Beam Focusing. *IEEE Commun. Mag.* **2023**, *61*, 72–77. [\[CrossRef\]](#)
18. Zhang, H.; Shlezinger, N.; Guidi, F.; Dardari, D.; Imani, M.F.; Eldar, Y.C. Beam focusing for near-field multiuser MIMO communications. *IEEE Trans. Wirel. Commun.* **2022**, *21*, 7476–7490. [\[CrossRef\]](#)
19. Guerra, A.; Guidi, F.; Dardari, D.; Djurić, P.M. Near-field tracking with large antenna arrays: Fundamental limits and practical algorithms. *IEEE Trans. Signal Process.* **2021**, *69*, 5723–5738. [\[CrossRef\]](#)
20. Hua, H.; Xu, J.; Han, T.X. Optimal transmit beamforming for integrated sensing and communication. *IEEE Trans. Veh. Technol.* **2023**, *72*, 10588–10603. [\[CrossRef\]](#)
21. Zhang, H.; Huang, Y.; Li, C.; Yang, L. Secure beamforming design for SWIPT in MISO broadcast channel with confidential messages and external eavesdroppers. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 7807–7819. [\[CrossRef\]](#)
22. Chang, T.-H.; Hsin, C.-W.; Ma, W.-K.; Chi, C.-Y. A linear fractional semidefinite relaxation approach to maximum-likelihood detection of higher-order QAM OSTBC in unknown channels. *IEEE Trans. Signal Process.* **2009**, *58*, 2315–2326. [\[CrossRef\]](#)
23. Grant, M.; Boyd, S. CVX: Matlab Software for Disciplined Convex Programming, Version 2.1. 2014. Available online: <http://cvxr.com/cvx/> (accessed on 25 December 2023).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.