

Privacy-Preserving Uplink Beamforming for Low-Altitude Wireless Networks

Jun Wu[†], Jinpeng Xu[‡], Qingqing Cheng[§], Wenchao Liu[‡], Xin Xie[¶], Tse-Tin Chan^{†*}

[†]Department of Mathematics and Information Technology, The Education University of Hong Kong, Hong Kong, China

[‡]Southern University of Science and Technology, Shenzhen, China

[§]Queensland University of Technology, Brisbane, Australia

[¶]Chongqing University of Posts and Telecommunications, Chongqing, China

*E-mail: tsetinchan@eduhk.hk

Abstract—This paper studies source-identity privacy in uplink low-altitude wireless networks (LAWNs), where multiple ground users simultaneously transmit messages to an unmanned aerial vehicle (UAV) in the presence of an eavesdropper. Unlike conventional physical-layer security designs that primarily prevent information decoding, we consider an eavesdropper who separates individual signal components from the composite uplink observation and infers the originating users from spatial statistical characteristics. To hinder such source identification, we develop a privacy-preserving uplink Jensen-Shannon divergence that quantifies the pairwise distinguishability between the separated signal components. A full-duplex UAV is further employed to transmit artificial noise (AN) while receiving the uplink signals. We formulate a worst-case privacy-preserving design that jointly optimizes the uplink beamforming and the AN covariance. An iterative algorithm is developed to obtain a suboptimal solution. Simulation results demonstrate the effectiveness of the proposed design in reducing source distinguishability.

Index Terms—Low-altitude wireless networks, physical-layer privacy, uplink beamforming.

I. INTRODUCTION

Low-altitude wireless networks (LAWNs) are expected to provide flexible three-dimensional coverage and ubiquitous connectivity for emerging low-altitude applications, including aerial logistics, environmental monitoring, and intelligent transportation [1], [2]. Owing to their mobility, rapid deployment capability, and favorable air-ground propagation conditions, unmanned aerial vehicles (UAVs) can serve as aerial base stations (BSs) or data collectors for widely distributed ground users.

Despite these advantages, the open propagation environment of LAWNs also introduces substantial physical-layer security risks. The broadcast nature of wireless transmission, together with strong air-ground line-of-sight (LoS) links, allows unauthorized receivers to intercept signals. Toward this end, existing physical-layer security studies have mainly addressed this issue by protecting the confidentiality of the transmitted information [3], [4]. Typical approaches include secrecy rate optimization and artificial noise (AN) transmission. For example, UAV-enabled cooperative jamming was

investigated to suppress the reception capability of an eavesdropper and improve the secrecy performance of a ground wiretap channel [5], [6]. In [7], the UAV simultaneously served as a downlink transmitter and radar receiver to track and predict a legitimate user's state. It optimized its trajectory in real time to maximize the secrecy rate. Beyond information confidentiality, covert communication has been introduced to conceal the occurrence of wireless transmission itself [8], [9]. In UAV-assisted networks, the UAV trajectory and transmit scheduling can be jointly designed to reduce the detection capability of unauthorized observers. In [10], the authors studied UAV-enabled covert wireless data collection by allowing a full-duplex (FD) UAV to receive uplink data while emitting artificial noise to hide the scheduled user's transmission from other ground nodes. Compared with conventional secure communication, covert communication provides an additional level of protection by making the existence of a transmission difficult to detect [11].

However, secure and covert transmission designs can not fully eliminate physical-layer privacy leakage [12]. Once a transmission is detected, or when an eavesdropper can observe and separate multiple simultaneously transmitted signal components, user-dependent physical features may still reveal the origin of each component. This issue is particularly important in multiuser uplink LAWNs, where users occupy different locations and experience distinct spatial channels toward the eavesdropper. Consequently, their received signal components may exhibit different statistical features even when the payloads and protocol-level identity fields are encrypted. By exploiting these differences, an eavesdropper may associate an observed component with a particular user and infer sensitive information, such as user activity, communication status, and location association. Therefore, preventing message decoding or transmission detection alone does not directly guarantee source-identity privacy.

Motivated by the above, this paper investigates source-identity protection in an uplink multiuser LAWN. We consider multiple multi-antenna ground users that simultaneously transmit to a multi-antenna UAV in the presence of a multi-antenna eavesdropper. The eavesdropper is assumed to separate user-

This work was supported in part by the Research Matching Grant Scheme from the Research Grants Council of Hong Kong. (Corresponding author: Tse-Tin Chan.)

dependent signal components from its composite observation and identify their sources according to their spatial covariance characteristics. Our design objective is to maintain reliable multiuser uplink transmission at the UAV while making the conditional observations associated with different users statistically indistinguishable at the eavesdropper.

To this end, we develop a privacy-preserving uplink beamforming framework assisted by FD UAV jamming. A covariance-based Jensen-Shannon divergence surrogate is derived to characterize the pairwise distinguishability of the user-induced observations at the eavesdropper. The users' transmit covariance matrices and the UAV's AN covariance matrix are then jointly optimized. To address the resulting non-convex problem, we construct a tractable upper approximation of the Jensen-Shannon divergence and develop an iterative algorithm based on successive convex approximation (SCA) techniques. Simulation results validate the effectiveness of the proposed design.

Notations: Boldface lowercase and uppercase letters denote vectors and matrices, respectively. The operators $(\cdot)^H$, $(\cdot)^{-1}$, $\text{tr}(\cdot)$, $\det(\cdot)$, and $\text{rank}(\cdot)$ denote the Hermitian transpose, matrix inverse, trace, determinant, and rank, respectively. The notation $\mathbf{X} \succeq \mathbf{0}$ indicates that $\mathbf{X}$ is positive semidefinite, and $\mathbf{I}_N$ denotes the $N \times N$ identity matrix. Moreover, $\|\cdot\|$ denotes the Euclidean norm, $\mathbb{E}[\cdot]$ denotes expectation, and $\mathcal{CN}(\boldsymbol{\mu}, \mathbf{R})$ denotes a circularly symmetric complex Gaussian distribution with mean $\boldsymbol{\mu}$ and covariance $\mathbf{R}$.

II. SYSTEM MODEL

As illustrated in Fig. 1, we consider an uplink LAWN system in which multiple ground users transmit information to a UAV-enabled aerial BS in the presence of a passive eavesdropper, referred to as Eve. The UAV operates in full-duplex mode, such that it can receive the desired uplink signals and simultaneously emit AN to perturb Eve's observation. This work aims to protect source-identity privacy by preventing Eve from distinguishing user-dependent spatial statistical signatures.

The network consists of K ground users, one full-duplex UAV, and one Eve. The user set is denoted by $\mathcal{K} = \{1, 2, \dots, K\}$. Each ground user and Eve are equipped with N_t and N_e antennas, respectively, whereas the full-duplex UAV utilizes separate transmit and receive arrays, each comprising N_u antennas. All users share the same time-frequency resource and transmit independent uplink streams to the UAV. Let $s_k \sim \mathcal{CN}(0, 1)$ denote the information symbol of user k , satisfying

$$\mathbb{E}[|s_k|^2] = 1, \quad \mathbb{E}[s_i s_j^*] = 0, \quad i \neq j. \quad (1)$$

The transmit beamforming vector of user k is denoted by $\mathbf{f}_k \in \mathbb{C}^{N_t \times 1}$. Hence, the transmitted signal of user k can be expressed as $\mathbf{x}_k = \mathbf{f}_k s_k$. Furthermore, the transmit power of each user is constrained by

$$\|\mathbf{f}_k\|^2 \leq P_k^{\max}, \quad \forall k \in \mathcal{K}. \quad (2)$$

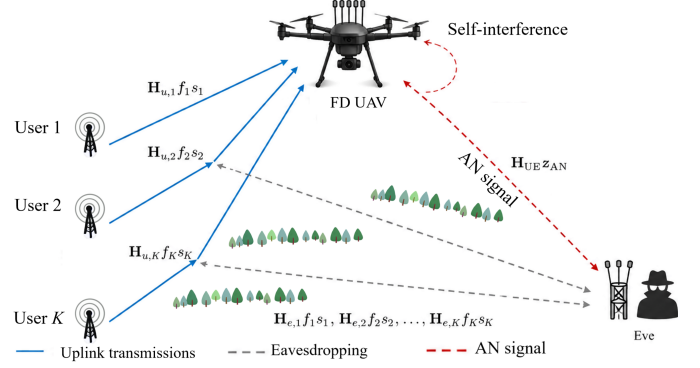


Fig. 1. The considered privacy-preserving uplink LAWN scenario.

To enhance source-identity privacy, the UAV emits AN during uplink reception to mask user-dependent spatial features at Eve. The AN signal is modeled as $\mathbf{z}_{\text{AN}} \sim \mathcal{CN}(\mathbf{0}, \mathbf{R}_{\text{AN}})$, where $\mathbf{R}_{\text{AN}} \succeq \mathbf{0}$ denotes the AN covariance matrix. The AN transmit power at the UAV is subject to

$$\text{tr}(\mathbf{R}_{\text{AN}}) \leq P_u^{\max}. \quad (3)$$

We first model the signal received by the legitimate UAV. Due to full-duplex operation, the emitted AN leaks into the UAV receiver. Let $\mathbf{H}_{u,k} \in \mathbb{C}^{N_u \times N_t}$ denote the uplink channel from user k to the UAV and $\mathbf{H}_{\text{SI}} \in \mathbb{C}^{N_u \times N_u}$ denote the self-interference channel. The received signal at the UAV is expressed as

$$\mathbf{y}_u = \sum_{k=1}^K \mathbf{H}_{u,k} \mathbf{f}_k s_k + \sqrt{\rho_{\text{SI}}} \mathbf{H}_{\text{SI}} \mathbf{z}_{\text{AN}} + \mathbf{n}_u, \quad (4)$$

where $\mathbf{n}_u \sim \mathcal{CN}(\mathbf{0}, \sigma_u^2 \mathbf{I}_{N_u})$ denotes the additive white Gaussian noise (AWGN) at the UAV. In (4), the coefficient $0 \leq \rho_{\text{SI}} \leq 1$ characterizes the residual self-interference level after self-interference cancellation.

The UAV adopts linear multiuser detection to recover the users' uplink streams [13]. When decoding the stream of user k , the signals from the remaining users and the residual self-interference induced by full-duplex AN transmission are treated as interference. The corresponding interference-plus-noise covariance matrix is

$$\mathbf{C}_k = \sum_{j \neq k} \mathbf{H}_{u,j} \mathbf{f}_j \mathbf{f}_j^H \mathbf{H}_{u,j}^H + \rho_{\text{SI}} \mathbf{H}_{\text{SI}} \mathbf{R}_{\text{AN}} \mathbf{H}_{\text{SI}}^H + \sigma_u^2 \mathbf{I}_{N_u}. \quad (5)$$

The minimum mean-squared error (MMSE) receive beamforming direction for user k is given by [14]

$$\mathbf{u}_k = \mathbf{C}_k^{-1} \mathbf{H}_{u,k} \mathbf{f}_k. \quad (6)$$

The resulting post-combining SINR is

$$\gamma_k^{\text{MMSE}} = \mathbf{f}_k^H \mathbf{H}_{u,k} \mathbf{C}_k^{-1} \mathbf{H}_{u,k} \mathbf{f}_k. \quad (7)$$

To guarantee reliable uplink communication performance, each user is required to satisfy the following quality-of-service (QoS) constraint:

$$\gamma_k^{\text{MMSE}} \geq \Gamma_k, \quad \forall k \in \mathcal{K}, \quad (8)$$

with Γ_k being the preset SINR threshold. We next model the composite signal observed by Eve. Let $\mathbf{H}_{e,k} \in \mathbb{C}^{N_e \times N_t}$ denote the channel from user k to Eve, and let $\mathbf{H}_{UE} \in \mathbb{C}^{N_e \times N_u}$ denote the channel from the UAV to Eve. The received signal at Eve is

$$\mathbf{y}_e = \sum_{k=1}^K \mathbf{H}_{e,k} \mathbf{f}_k s_k + \mathbf{H}_{UE} \mathbf{z}_{AN} + \mathbf{n}_e, \quad (9)$$

where $\mathbf{n}_e$ denotes the AWGN at Eve.

III. PROBLEM FORMULATION

In this section, we formulate the privacy-preserving uplink transmission design problem. Based on the composite observation in (9), Eve may separate the individual signal components and subsequently infer their originating users from differences in the associated spatial statistics. Such inference becomes more reliable when the components generated by different users exhibit clearly distinguishable statistical characteristics. Therefore, the design objective is to reduce the statistical distinguishability among the extracted components observed by Eve, while guaranteeing reliable uplink reception at the UAV.

Assume that Eve can effectively suppress the signal contributions of the remaining users during the separation process, whereas the unknown AN transmitted by the UAV remains in the resulting observation. We focus on component-wise source identification, where Eve infers the source of each extracted component from its individual spatial statistics without exploiting the joint statistics among multiple separated components. Let $S \in \mathcal{K}$ denote the source identity of an extracted signal component. Conditioned on $S = k$, the corresponding separated observation at Eve is modeled as

$$\tilde{\mathbf{y}}_{e,k} = \mathbf{H}_{e,k} \mathbf{f}_k s_k + \mathbf{H}_{UE} \mathbf{z}_{AN} + \mathbf{v}_{e,k}, \quad (10)$$

where $\mathbf{v}_{e,k}$ is the disturbance following $\mathbf{v}_{e,k} \sim \mathcal{CN}(0, \sigma_{e,k}^2 \mathbf{I}_{N_e})$. Therefore, the conditional probability density function (PDF) of the extracted observation can be straightforwardly expressed as [15]

$$p_{e,k}(\mathbf{y}) \triangleq p(\tilde{\mathbf{y}}_{e,k} = \mathbf{y} \mid S = k). \quad (11)$$

Under the Gaussian models introduced in Section II, $p_{e,k}(\mathbf{y})$ is a zero-mean circularly symmetric complex Gaussian distribution with covariance matrix

$$\mathbf{R}_{e,k} = \mathbf{H}_{e,k} \mathbf{f}_k \mathbf{f}_k^H \mathbf{H}_{e,k}^H + \mathbf{H}_{UE} \mathbf{R}_{AN} \mathbf{H}_{UE}^H + \sigma_{e,k}^2 \mathbf{I}_{N_e}, \quad (12)$$

which can be rewritten as $p_{e,k}(\mathbf{y}) = \mathcal{CN}(\mathbf{0}, \mathbf{R}_{e,k})$. The collection $\{p_{e,k}\}_{k \in \mathcal{K}}$ characterizes the statistical distributions of the signal components originating from different users. If $p_{e,i}$ and $p_{e,j}$ are well separated, Eve can more reliably determine whether an extracted component originates from user i or user j . Conversely, when these conditional distributions are close, inferring the physical source of an extracted component becomes challenging. As a consequence, reducing

the pairwise statistical distinguishability among $\{p_{e,k}\}_{k \in \mathcal{K}}$ improves source-identity privacy. To quantify the pairwise statistical distinguishability at Eve, we adopt the Jensen-Shannon (JS) divergence, which is a symmetric divergence measure between two probability distributions. In particular, for two users i and j , the JS divergence between $p_{e,i}$ and $p_{e,j}$ is defined as [16]

$$D_{JS}(i, j) = \frac{1}{2} D_{KL}(p_{e,i} \| m_{ij}) + \frac{1}{2} D_{KL}(p_{e,j} \| m_{ij}), \quad (13)$$

where

$$m_{ij}(\mathbf{y}) = \frac{1}{2} p_{e,i}(\mathbf{y}) + \frac{1}{2} p_{e,j}(\mathbf{y}), \quad (14)$$

is the equally weighted mixture distribution and $D_{KL}(\cdot \| \cdot)$ is the Kullback-Leibler (KL) divergence. Equivalently, (13) can be re-expressed as

$$D_{JS}(i, j) = h(m_{ij}) - \frac{1}{2} h(p_{e,i}) - \frac{1}{2} h(p_{e,j}), \quad (15)$$

where $h(\cdot)$ denotes differential entropy. The JS divergence is symmetric, non-negative, and equal to zero if and only if the two distributions are identical. In other words, if all conditional distributions $\{p_{e,k}\}_{k \in \mathcal{K}}$ are identical, the source index S is statistically independent of Eve's observation, and Eve cannot infer the transmitting user from this observation alone.

To facilitate the system design, we further define $\mathbf{F}_k = \mathbf{f}_k \mathbf{f}_k^H$, which follows that

$$\mathbf{F}_k \succeq \mathbf{0}, \quad \text{rank}(\mathbf{F}_k) = 1. \quad (16)$$

Then, the covariance matrix $\mathbf{R}_{e,k}$ can be simplified as

$$\mathbf{R}_{e,k} = \mathbf{H}_{e,k} \mathbf{F}_k \mathbf{H}_{e,k}^H + \mathbf{H}_{UE} \mathbf{R}_{AN} \mathbf{H}_{UE}^H + \sigma_{e,k}^2 \mathbf{I}_{N_e}. \quad (17)$$

Based on the above discussion, we minimize the worst-case pairwise statistical distinguishability at Eve, while satisfying the uplink QoS constraints in (8) and the power constraints in (2) and (3). The original problem is formulated as

$$\mathcal{P}_1 : \min_{\mathbf{F}_k, \mathbf{R}_{AN}} \max_{\substack{i, j \in \mathcal{K} \\ i < j}} D_{JS}(i, j) \quad (18a)$$

$$\text{s.t. } \gamma_k^{\text{MMSE}} \geq \Gamma_k, \quad \forall k \in \mathcal{K}, \quad (18b)$$

$$\text{tr}(\mathbf{F}_k) \leq P_k^{\max}, \quad \forall k \in \mathcal{K}, \quad (18c)$$

$$\mathbf{F}_k \succeq \mathbf{0}, \quad \text{rank}(\mathbf{F}_k) = 1, \quad \forall k \in \mathcal{K}, \quad (18d)$$

$$\text{tr}(\mathbf{R}_{AN}) \leq P_u^{\max}, \quad \mathbf{R}_{AN} \succeq \mathbf{0}, \quad (18e)$$

Problem $\mathcal{P}_1$ is non-convex and difficult to solve directly. The non-convexity arises from the rank-one constraints on $\mathbf{F}_k$ and the worst-case objective. Moreover, the SINR constraints are coupled with the transmit covariance matrices and the AN covariance. To address these challenges, we develop an iterative algorithm to obtain a suboptimal solution in what follows.

IV. PROPOSED ALGORITHMS

This section presents an iterative solution to $\mathcal{P}_1$. We first deal with the non-convex objective function. Notice that although $p_{e,i}$ and $p_{e,j}$ are Gaussian, the Gaussian mixture m_{ij} generally has no closed-form differential entropy expression. Therefore, directly optimizing (15) is challenging. To compromise, we now construct a covariance-based surrogate. It is evident that the mixture m_{ij} is zero mean and has covariance

$$\bar{\mathbf{R}}_{e,ij} = \frac{1}{2} (\mathbf{R}_{e,i} + \mathbf{R}_{e,j}). \quad (19)$$

In light of the maximum-entropy property [17], the entropy of m_{ij} is upper bounded by that of a zero-mean complex Gaussian distribution with covariance $\bar{\mathbf{R}}_{e,ij}$, i.e.,

$$h(m_{ij}) \leq \log \det (\pi e \bar{\mathbf{R}}_{e,ij}). \quad (20)$$

For each Gaussian component, we have [18]

$$h(p_{e,k}) = \log \det (\pi e \mathbf{R}_{e,k}). \quad (21)$$

Substituting (20) and (21) into (15), it follows that

$$\begin{aligned} D_{\text{JS}}(i, j) &\leq \tilde{D}_{\text{JS}}(i, j) = \log \det (\bar{\mathbf{R}}_{e,ij}) - \frac{1}{2} \log \det (\mathbf{R}_{e,i}) \\ &\quad - \frac{1}{2} \log \det (\mathbf{R}_{e,j}). \end{aligned} \quad (22)$$

It is evident that $\tilde{D}_{\text{JS}}(i, j) = 0$ when $\mathbf{R}_{e,i} = \mathbf{R}_{e,j}$. Under the zero-mean Gaussian model given by (11), $\tilde{D}_{\text{JS}}(i, j) = 0$ further indicates $p_{e,i} = p_{e,j}$. Hence, reducing $\tilde{D}_{\text{JS}}(i, j)$ makes the Eve's observations induced by users i and j statistically indistinguishable, thereby limiting Eve's ability to identify the transmitting user.

Although (22) is more manageable, the min-max structure is still intractable. To address this challenge, we introduce an auxiliary variable η to represent the worst-case privacy distinguishability among all user pairs. Then, we have the following problem $\mathcal{P}_2$:

$$\mathcal{P}_2: \min_{\mathbf{F}_k, \mathbf{R}_{\text{AN}}, \eta} \eta \quad (23a)$$

$$\text{s.t. } \tilde{D}_{\text{JS}}(i, j) \leq \eta, \forall i \neq j, \quad (23b)$$

$$(18b), (18c), (18d), (18e) \quad (23c)$$

It is observed that the term $\log \det (\bar{\mathbf{R}}_{e,ij})$ in (22) is concave with respect to $\bar{\mathbf{R}}_{e,ij}$, and thus admits a global affine upper bound via first-order Taylor expansion given a local point, which is given by

$$\begin{aligned} \log \det (\bar{\mathbf{R}}_{e,ij}) &\leq \log \det (\bar{\mathbf{R}}_{e,ij}^r) \\ &\quad + \text{tr} \left[(\bar{\mathbf{R}}_{e,ij}^r)^{-1} (\bar{\mathbf{R}}_{e,ij} - \bar{\mathbf{R}}_{e,ij}^r) \right] \triangleq \phi_{ij}^r, \end{aligned} \quad (24)$$

where $\bar{\mathbf{R}}_{e,ij}^r$ denotes the local point at the r -th iteration. Therefore, an upper approximation of the pairwise JS surrogate is

$$\hat{D}_{\text{JS}}^r(i, j) = \phi_{ij}^r - \frac{1}{2} \log \det (\mathbf{R}_{e,i}) - \frac{1}{2} \log \det (\mathbf{R}_{e,j}). \quad (25)$$

To handle the rank-one constraint, we leverage Schur's complement, such that (18d) can be represented by

$$\begin{bmatrix} \mathbf{F}_k & \mathbf{f}_k \\ \mathbf{f}_k^H & 1 \end{bmatrix} \succeq \mathbf{0}, \quad \forall k, \quad (26)$$

together with

$$\text{tr}(\mathbf{F}_k) - \mathbf{f}_k^H \mathbf{f}_k \leq 0, \quad \forall k. \quad (27)$$

The constraint in (27) is non-convex. At the r -th iteration, we obtain the first-order lower bound particularized as

$$\mathbf{f}_k^H \mathbf{f}_k \geq 2\Re\{(\mathbf{f}_k^r)^H \mathbf{f}_k\} - \|\mathbf{f}_k^r\|^2. \quad (28)$$

Then, (27) is conservatively approximated by

$$\text{tr}(\mathbf{F}_k) - 2\Re\{(\mathbf{f}_k^r)^H \mathbf{f}_k\} + \|\mathbf{f}_k^r\|^2 \leq 0, \quad \forall k. \quad (29)$$

We proceed to address the SINR constraint. Define $\mathbf{A}_{k,j} = \mathbf{H}_{u,j}^H \mathbf{u}_k \mathbf{u}_k^H \mathbf{H}_{u,j}$, and $\mathbf{B}_k = \mathbf{H}_{\text{SI}}^H \mathbf{u}_k \mathbf{u}_k^H \mathbf{H}_{\text{SI}}$, the SINR requirement (8) can be equivalently written as

$$\begin{aligned} &\text{tr}(\mathbf{A}_{k,k} \mathbf{F}_k) \\ &\geq \Gamma_k \left(\sum_{j \neq k} \text{tr}(\mathbf{A}_{k,j} \mathbf{F}_j) + \rho_{\text{SI}} \text{tr}(\mathbf{B}_k \mathbf{R}_{\text{AN}}) + \sigma_u^2 \|\mathbf{u}_k\|^2 \right). \end{aligned} \quad (30)$$

It is evident that (30) is now a linear constraint. Based on the above discussions, the original problem in iteration r can be approximated as the following problem:

$$\mathcal{P}_3 \quad \min_{\mathbf{F}_k, \mathbf{f}_k, \mathbf{R}_{\text{AN}}, \eta} \eta \quad (31a)$$

$$\text{s.t. } \hat{D}_{\text{JS}}^r(i, j) \leq \eta, \quad \forall i < j, \quad (31b)$$

$$\begin{bmatrix} \mathbf{F}_k & \mathbf{f}_k \\ \mathbf{f}_k^H & 1 \end{bmatrix} \succeq \mathbf{0}, \quad \forall k, \quad (31c)$$

$$\text{tr}(\mathbf{F}_k) - 2\Re\{(\mathbf{f}_k^r)^H \mathbf{f}_k\} + \|\mathbf{f}_k^r\|^2 \leq 0, \quad \forall k, \quad (31d)$$

$$\mathbf{F}_k \succeq \mathbf{0}, \mathbf{R}_{\text{AN}} \succeq \mathbf{0}, (18c), (18e), (30). \quad (31e)$$

However, the strict first-order Taylor approximation of the rank-one constraint can easily render the convexified problem $\mathcal{P}_3$ infeasible if the initialized $\mathbf{F}_k$ and $\mathbf{f}_k$ are not strictly aligned. To circumvent the difficulty of finding a specifically tailored initial point that satisfies this restrictive mathematical approximation, we adopt a penalty-based SCA method by introducing a non-negative slack variable $\xi_k \geq 0$ [19]. The resultant problem becomes

$$\mathcal{P}_4 \quad \min_{\mathbf{F}_k, \mathbf{f}_k, \mathbf{R}_{\text{AN}}, \eta, \xi_k} \eta + \tau^r \sum_k \xi_k \quad (32a)$$

$$\text{s.t. } \text{tr}(\mathbf{F}_k) - 2\Re\{(\mathbf{f}_k^r)^H \mathbf{f}_k\} + \|\mathbf{f}_k^r\|^2 \leq \xi_k, \quad \forall k, \quad (32b)$$

$$\xi_k \geq 0, \quad \forall k, \quad (32c)$$

$$(18c), (18e), (30), (31b), (31c). \quad (32d)$$

Here, $\tau^r > 0$ denotes the penalty coefficient at iteration r . It is updated according to $\tau^{r+1} = \min\{\chi \tau^r, \tau_{\text{max}}\}$, where $\chi > 1$ is the penalty growth factor and τ_{max} is the prescribed

Algorithm 1 Proposed Penalty-Based SCA Algorithm

Require: Channel matrices, power budgets, SINR thresholds, tolerances ϵ_1, ϵ_2 , and $\tau^0 > 0$.

Ensure: $\{\mathbf{f}_k^*\}$ and $\mathbf{R}_{\text{AN}}^*$.

- 1: Initialize $\{\mathbf{f}_k^0, \mathbf{F}_k^0\}$, $\mathbf{R}_{\text{AN}}^0$, and set $r = 0$.
 - 2: **repeat**
 - 3: Update the MMSE receive beamformers $\{\mathbf{u}_k^r\}$ according to (6).
 - 4: Compute $\{\mathbf{A}_{k,j}^r\}$, $\{\mathbf{B}_k^r\}$, and $\{\mathbf{R}_{e,k}^r\}$.
 - 5: Construct the upper bounds $\{\phi_{ij}^r\}$ according to (24).
 - 6: Solve $\mathcal{P}_4$ to obtain $\{\mathbf{F}_k^{r+1}, \mathbf{f}_k^{r+1}, \zeta_k^{r+1}, \mathbf{R}_{\text{AN}}^{r+1}, \eta^{r+1}\}$.
 - 7: Update $\tau^{r+1} = \min\{\chi\tau^r, \tau_{\max}\}$ and set $r \leftarrow r + 1$.
 - 8: **until** $|\eta^r - \eta^{r-1}|/|\eta^{r-1}| \leq \epsilon_1$ and $\max_k \zeta_k^r \leq \epsilon_2$
 - 9: **return** $\{\mathbf{f}_k^r\}$ and $\mathbf{R}_{\text{AN}}^r$.
-

upper bound. Since the MMSE receiver depends on $\mathbf{F}_k$ and $\mathbf{R}_{\text{AN}}$, the receive beamformers $\mathbf{u}_k$ are updated according to (6) at each iteration. The optimization variables and receive beamformers are then alternately refined until the objective variation and the slack variables satisfy the prescribed tolerances. The overall procedure is summarized in Algorithm 1.

V. SIMULATION RESULTS

In this section, we present extensive numerical results to verify the effectiveness of the proposed privacy-preserving design. The considered system comprises $K = 4$ ground users, each equipped with $N_t = 4$ antennas. The FD-UAV utilizes $N_u = 8$ transmit and receive antennas. The eavesdropper is equipped with $N_e = 4$ antennas. Spatially, the UAV is positioned at (0, 0, 100) m and Eve at (80, 80, 0) m. The ground users are uniformly distributed within an area of $60 \times 60 \text{ m}^2$. All communication links, including the channels from the user to the UAV, the user to Eve, and the UAV to Eve, are modeled using Rician fading with a Rician factor of 10 dB. The large-scale channel power gain is characterized by $\beta(d) = \beta_0 d^{-\alpha}$ where $\beta_0 = -40 \text{ dB}$ represents the reference channel power gain at a distance of 1 m and $\alpha = 2.5$ is the path loss exponent [20]. The noise power at both the UAV and Eve is set to -100 dBm , and the residual self-interference coefficient is fixed at $\rho_{\text{SI}} = -60 \text{ dB}$. Furthermore, the maximum transmit power for each ground user is capped at $P_k^{\max} = 5 \text{ dBm}$. The optimization algorithm is configured with a convergence tolerance of 10^{-4} .

To rigorously validate the performance of our proposed design, we compare two baseline schemes. The first benchmark is the isotropic AN scheme, in which the AN covariance is set to an isotropic emission defined as $\mathbf{R}_{\text{AN}} = (P_u^{\max}/N_u)\mathbf{I}_{N_u}$ and optimizes only the users' transmit covariance matrices. The second benchmark is the scheme without AN. It eliminates the use of artificial noise entirely by setting $\mathbf{R}_{\text{AN}} = \mathbf{0}$. Furthermore, privacy performance is quantified using the worst-case distinguishability metric, i.e., $D_{\max}^e = \max_{i < j} \tilde{D}_{\text{JS}}(i, j)$, where a diminished value indicates that

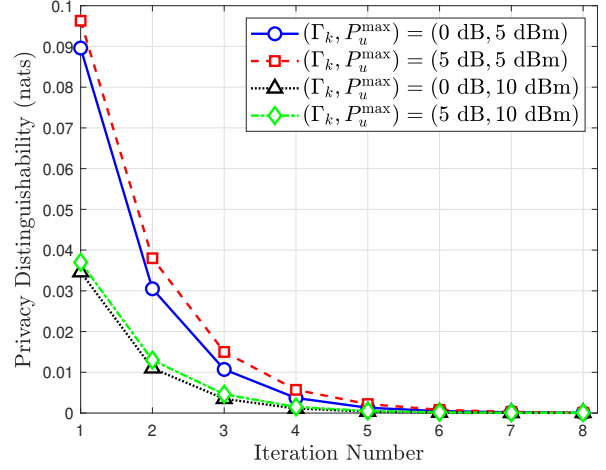


Fig. 2. The evaluation of convergence behavior.

the user-dependent observations at Eve are statistically less distinguishable.

Fig. 2 illustrates the convergence behavior of the proposed algorithm across four combinations of the required SINR Γ_k and the UAV AN power budget $P_u^{\max}$. Across all tested configurations, the privacy distinguishability metric exhibits a precipitous decline during the initial iterations and stabilizes after approximately six to eight iterations. For a given SINR requirement, increasing $P_u^{\max}$ from 5 dBm to 10 dBm yields a substantial reduction in privacy distinguishability throughout the optimization process. This is because a more generous AN power budget permits the UAV to inject a dominant covariance component into Eve's observations. This effectively masks the relative disparities among the users' spatial features. Conversely, for a fixed AN power budget, the curves associated with $\Gamma_k = 5 \text{ dB}$ consistently reside above those for $\Gamma_k = 0 \text{ dB}$. An elevated SINR constraint inherently restricts the feasible beamforming space. It necessitates that a greater proportion of spatial resources be dedicated to ensuring reliable uplink reception. Consequently, fewer degrees of freedom remain available for equalizing the statistical observations at the eavesdropper.

Fig. 3 plots the worst-case privacy distinguishability as a function of the required SINR. A uniform upward trend is observable across all schemes as Γ_k increases. This underscores a fundamental tradeoff between privacy and communication reliability. Under relaxed SINR constraints, the transmit covariance matrices possess sufficient flexibility to obscure the statistical differences among Eve's observations. However, as Γ_k increases, the users' transmission strategies must increasingly align with their legitimate channels to fulfill the QoS mandates. These highly specific beamforming alignments inadvertently generate more pronounced and distinguishable covariance signatures at Eve. Additionally, amplifying the AN exacerbates the residual self-interference at the FD UAV, which imposes a physical limit on AN design that can be viably deployed under strict SINR requirements.

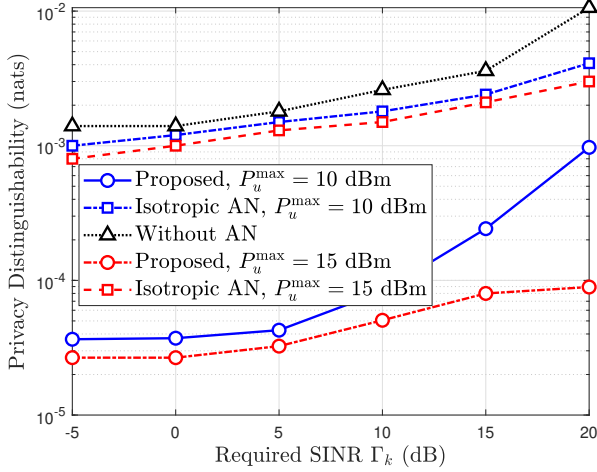


Fig. 3. The worst-case privacy distinguishability $D_{\max}^e$.

We further observe that the proposed joint design consistently yields the lowest $D_{\max}^e$ among all evaluated schemes. This superiority arises from the framework's ability to spatially shape the AN covariance toward the exact directions where user-induced observations exhibit the highest distinguishability. By contrast, isotropic AN disperses power uniformly across all spatial dimensions. This renders it inefficient at neutralizing the specific distinguishing features isolated by Eve. The isotropic approach still surpasses the baseline without AN, but its privacy enhancements are demonstrably inferior to those of the proposed joint design. Expanding the AN power budget from 10 dBm to 15 dBm further bolsters the proposed design's efficacy. This gain becomes especially pronounced under stringent SINR requirements. For instance, at $\Gamma_k = 20$ dB, the proposed framework with $P_u^{\max} = 15$ dBm achieves a privacy distinguishability on the order of 10^{-4} . In contrast, both the isotropic AN and the without AN schemes stagnate on the orders of 10^{-3} and 10^{-2} , respectively. Notably, the proposed curve operating at $P_u^{\max} = 10$ dBm rises sharply at elevated SINR levels. This reveals that this constrained AN budget is insufficient to counterbalance the loss of beamforming flexibility.

VI. CONCLUSION

This paper investigated source-identity privacy in uplink multiuser LAWNs, where an eavesdropper may infer the transmitting user by exploiting user-dependent spatial statistics. To address this challenge, we developed a full-duplex UAV-assisted privacy-preserving framework that jointly optimizes the users' uplink beamforming and the UAV's AN covariance. Specifically, a covariance-based Jensen-Shannon divergence surrogate was introduced to quantify the worst-case statistical distinguishability among the eavesdropper's conditional observations, thereby translating the source-identity protection objective into a tractable design metric. The resulting non-convex optimization problem was solved using an iterative SCA-based algorithm. Simulation results confirmed the rapid

convergence of the proposed method and revealed a fundamental tradeoff between source-identity privacy and uplink communication efficiency. Furthermore, the joint design was shown to consistently achieve lower privacy distinguishability than benchmark schemes, validating the effectiveness of the proposed approach.

REFERENCES

- [1] J. Wu *et al.*, "Low-altitude wireless networks: A comprehensive survey," *China Commun.*, vol. 23, no. 3, pp. 99–141, Mar. 2026.
- [2] W. Yuan *et al.*, "From ground to sky: Architectures, applications, and challenges shaping low-altitude wireless networks," 2025, *arXiv:2506.12308*.
- [3] L. Wang, Y. Chen, P. Wang, and Z. Yan, "Security threats and countermeasures of unmanned aerial vehicle communications," *IEEE Commun. Stand. Mag.*, vol. 5, no. 4, pp. 41–47, Dec. 2021.
- [4] N. Su *et al.*, "Integrating sensing and communications in 6G? Not until it is secure to do so," *IEEE Wireless Commun.*, early access, Jun. 2026, doi: 10.1109/MWC.2026.3703015.
- [5] C. Zhong, J. Yao, and J. Xu, "Secure UAV communication with cooperative jamming and trajectory control," *IEEE Commun. Lett.*, vol. 23, no. 2, pp. 286–289, Feb. 2019.
- [6] M. Wu *et al.*, "Energy-constrained multidimensional optimization for UAV-aided secure data collection with cooperative jamming," *IEEE Trans. Veh. Technol.*, vol. 74, no. 12, pp. 18 529–18 542, Dec. 2025.
- [7] J. Wu, W. Yuan, and L. Hanzo, "When UAVs meet ISAC: Real-time trajectory design for secure communications," *IEEE Trans. Veh. Technol.*, vol. 72, no. 12, pp. 16 766–16 771, Dec. 2023.
- [8] J. Xu, L. Bai, X. Xie, and L. Zhou, "Collaborative secret and covert communications for multi-user multi-antenna uplink UAV systems: Design and optimization," *IEEE Trans. Wireless Commun.*, vol. 24, no. 7, pp. 6020–6035, Jul. 2025.
- [9] J. Wu, X. Zhang, H. Pan, G. Zhao, D. I. Kim, and T.-T. Chan, "Integrating sensing into covert communications: Opportunities and challenges," 2026, *arXiv:2606.23073*.
- [10] X. Zhou, S. Yan, F. Shu, R. Chen, and J. Li, "UAV-enabled covert wireless data collection," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 11, pp. 3348–3362, Nov. 2021.
- [11] X. Chen *et al.*, "Covert communications: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 1173–1198, 2nd Quart., 2023.
- [12] C. Lin, D. He, N. Kumar, K.-K. R. Choo, A. Vinel, and X. Huang, "Security and privacy for the Internet of Drones: Challenges and solutions," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 64–69, Jan. 2018.
- [13] Z. Wang, J. Zhang, H. Q. Ngo, B. Ai, and M. Debbah, "Uplink precoding design for cell-free massive MIMO with iteratively weighted MMSE," *IEEE Trans. Commun.*, vol. 71, no. 3, pp. 1646–1664, Mar. 2023.
- [14] Y. Jiang, M. K. Varanasi, and J. Li, "Performance analysis of ZF and MMSE equalizers for MIMO systems: An in-depth study of the high SNR regime," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2008–2026, Apr. 2011.
- [15] R. M. Gray and L. D. Davisson, *An Introduction to Statistical Signal Processing*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
- [16] Y. Huang, Z. Zhu, Q. Cui, N. Wei, X. Tao, and P. Zhang, "ISAC privacy: Achieving signal indistinguishability via joint beamforming and perturbation," *IEEE Trans. Cogn. Commun. Netw.*, vol. 12, pp. 9790–9805, 2026.
- [17] E. T. Jaynes, "On the rationale of maximum-entropy methods," *Proc. IEEE*, vol. 70, no. 9, pp. 939–952, Sep. 1982.
- [18] A. Eskenazis, P. Nayar, and T. Tkocz, "Gaussian mixtures: Entropy and geometric inequalities," *Ann. Probab.*, vol. 46, no. 5, pp. 2908–2945, Sep. 2018.
- [19] C. Wang, Z. Li, H. Zhang, D. W. K. Ng, and N. Al-Dhahir, "Achieving covertness and security in broadcast channels with finite blocklength," *IEEE Trans. Wireless Commun.*, vol. 21, no. 9, pp. 7624–7640, Sep. 2022.
- [20] C. You and R. Zhang, "3D trajectory optimization in Rician fading for UAV-enabled data harvesting," *IEEE Trans. Wireless Commun.*, vol. 18, no. 6, pp. 3192–3207, Jun. 2019.