Secrecy Rate of the Cooperative RSMA-Aided UAV Downlink Relying on Optimal Relay Selection

Hamed Bastami, Majid Moradikia, Hamid Behroozi, Member, IEEE, and Lajos Hanzo, Life Fellow, IEEE

Abstract—The Cooperative Rate-Splitting (CRS) scheme, proposed evolves from conventional Rate Splitting (RS) and relies on forwarding a portion of the RS message by the relaying users. In terms of secrecy enhancement, it has been shown that CRS outperforms its non-cooperative counterpart for a two-user Multiple Input Single Output (MISO) Broadcast Channel (BC). Given the massive connectivity requirement of 6G, we have generalized the existing secure two-user CRS framework to the multi-user framework, where the highest-security users must be selected as the relay nodes. This paper addresses the problem of maximizing the Worst-Case Secrecy Rate (WCSR) in a UAV-aided downlink network where a multi-antenna UAV Base-Station (UAV-BS) serves a group of users in the presence of an external eavesdropper (Eve). We consider a practical scenario in which only imperfect channel state information of Eve is available at the UAV-BS. Accordingly, we conceive a robust and secure resource allocation algorithm, which maximizes the WCSR by jointly optimizing both the Secure Relaying User Selection (SRUS) and the network parameter allocation problem, including the RS transmit precoders, message splitting variables, time slot sharing and power allocation. To circumvent the resultant non-convexity owing to the discrete variables imposed by SRUS, we propose a two-stage algorithm where the SRUS and network parameter allocation are accomplished in two consecutive stages. With regard to the SRUS, we study both centralized and distributed protocols. On the other hand, for jointly optimizing the network parameter allocation we resort to the Sequential Parametric Convex Approximation (SPCA) algorithm. Our numerical results show that the proposed solution significantly outperforms the existing benchmarks for a wide range of network loads in terms of the WCSR.

Index Terms—Rate-splitting, Physical layer security, Robust beamforming, Secure relay selection, Imperfect CSIT, Worst-case optimization, Cellular UAV networks.

I. INTRODUCTION

6G wireless communications are envisioned to support the heterogeneous services of a massive number of connected users with ultra-reliability, e.g., $1000\times$ higher mobile data volume per geographical area, as well as $10 \sim 100\times$ more connected devices, offered at efficient resources usage [1], [2]. These indicative parameters are known as Key Performance Indicators (KPIs) of 6G. Upon growing the dimension of the network and the number of connected users over the limited shared spectrum, the problems of Inter-User Interference (IUI) become exacerbated. To address these concerns, efficient Multiple Access (MA) technologies, such as Rate-Splitting Multiple Access (RSMA), have to be utilized [3], [4], [5]. RSMA may be viewed as a generalized generalized Non-Orthogonal Multiple Access (NOMA) and Space-Division Multiple Access (SDMA) framework that is resilient against outdated Channel State Information (CSI) [4], [5].

Given the open nature of the wireless medium, Multi-User (MU) systems are susceptible to especially security breaches, when a massive number of connected users intend to utilize the same spectrum. Traditionally, secure communication is achieved by employing cryptography encryption, which somewhat optimistically assumes limited computational capabilities for the eavesdroppers (Eves), as well as perfectly secure key transfers over the wireless medium. Yet, with the emergence of powerful quantum computers, a persistent and sophisticated Eve will be able to extract important confidential information. To circumvent this concern, Physical Layer (PHY)-Security (PLS), which relies on opportunistically exploiting the random nature of the fading channels, has gained significant attention [6], [7], [8]. A pair of potent PLS designs rely on: 1) Optimizing the active transmit precoder (beamformer) of a multi-antenna transmitter, aimed at focusing the transmit power in the directions of legitimate users, while minimizing the energy leakage to Eves [9], [10]; 2) intentionally broadcasting specifically designed Artificial Noise (AN) everywhere except for focusing any potential Eve [11]. However, both the performance and the design of the aforementioned PLS schemes significantly depends on the accuracy of the knowledge about the Eve’s CSI at the legitimate transmitter (E-CSIT) [9], [12].

To meet the demanding KPIs of 6G while securing the confidentiality of the transmitted MUs’ messages, RSMA was recently shown to be one of the most effective PLS techniques [12]-[17]. By relying on a secure RSMA Transmit Precoder (TPC) a common message which is constituted by a specific portion of the transmitted message, is introduced at source with a twin-fold mission. More explicitly, apart from serving as the desired message, it also acts as AN without consuming extra power [17]. This is in stark contrast to the conventional AN design, where some portion of the transmit power budget is allocated to AN, hence leading to inefficient usage of the available power budget. Additionally, by optimizing the RSMA TPC at the Base-Station (BS), we can deal with the effects of realistic imperfect channel estimation at the Tx [4], [5], [18]. As a beneficial extension of RS, two-user Cooperative Rate-Splitting (CRS) has been proposed in [19] that outperforms its non-cooperative version [18] in terms of both its reliability [20] and security [12], [16]. Briefly, the CRS framework benefits from the cooperation of the legitimate users, which are allowed to opportunistically forward their
TABLE I
OVERVIEW OF EXISTING LITERATURE

| References⇒ | Proposed Approach | [3] | [4] | [8] | [9] | [10] | [11] | [12] | [13] | [15] | [16] | [17] | [18] | [19] | [22] | [25] | [28] |
|-------------|-------------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| PLS         | ✓                 | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   |
| Beamformer  |                   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   |
| Design      |                   |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| Unknown Eve |                   | ✓   |     |     |     |     |     |     |     |     |     |     |     |     |     |     |
| FJ Design   |                   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   |
| SSRM        |                   | ✓   | ✓   | ✓   |     |     |     |     |     |     |     |     |     |     |     |     |
| UAV-BS      |                   | ✓   | ✓   |     |     |     |     |     |     |     |     |     |     |     |     |     |
| NOMA        |                   | ✓   |     | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   |
| I-CSIT      |                   | ✓   |     |     | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   |
| SOPM        |                   | ✓   |     |     |     | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   |
| RSMA        |                   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   |
| CRS         |                   | ✓   | ✓   | ✓   |     | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   |
| WCSRM       |                   | ✓   | ✓   | ✓   |     |     | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   |
| I-ECSIT     |                   | ✓   | ✓   |     | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   |
| SRUS        |                   | ✓   |     |     |     | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   | ✓   |
| MU-CRS      |                   | ✓   |     |     |     |     |     |     |     |     |     |     |     |     |     |     |

References⇒ Keywords⇒

• By relying on the two-stage multi-user C-RSMA philosophy, we follow the secrecy policy of [12] for safeguarding the first cooperative phase through the secure design of the common RSMA TPC. Interestingly, by decoding and forwarding the common stream, two opportunities are provided to take full advantage of the common

Recent flawlessly decoded common message to the distant user in two subsequent time-slots.

Recently, Unmanned Aerial Vehicle (UAV)-aided communications have attracted significant research interest [22], [23], [24], thanks to their, on-demand coverage, and the availability of the Line of Sight (LoS) links. In particular, the PLS attained may be readily improved by UAVs upon detecting the Eve’s location via the UAV-mounted cameras or radar [22]. In practice, only imperfect E-CSIT may be available and thus the conventional PLS schemes no longer perform at their best [12], [17]. Some of the associated challenges have been addressed by the robust PLS solutions designed for UAV-enabled scenarios in [25], [26]. Recently, secure RS and CRS-aided UAV networks relying on realistic imperfect CSIT have been studied respectively in [12], [27]. However, the solutions proposed in [12] and [27] are not applicable for multi-user networks, where secure Relaying Users Selection (SRUS) protocols are necessitated for security reasons. In other words, since all users may act potential candidates for forwarding the common stream during the relaying phase, the question arises: "How to beneficially select the relaying users with the objective of enhancing the security?" None of the above secure UAV-RSMA designs have addressed this important research question. Hence our objective is to close this knowledge gap. Furthermore, to circumvent the deleterious impact of imperfect CSIT, in contrast to [21], we have conceived the worst-case robust designs as well. Explicitly, this is the first work that investigates the robust and secure design of the generalized multi-user C-RSMA downlink of UAV networks. To gain deeper insights, the novelty of the proposed approach is boldly and explicitly contrasted to the state-of-the-art in Table I at a glance. Table II provides a list of acronyms used in this paper.

Against this background, the detailed contributions of our work are summarized as follows:

- TABLE II
LIST OF ACRONYMS AND ABBREVIATIONS

| Acronym | Description                          |
|---------|--------------------------------------|
| PLS     | Physical Layer Security              |
| FJ      | Friendly Jammer                      |
| UAV-BS  | Unmanned Aerial Vehicle Base-Station  |
| SIC     | Successive Interference Cancellation |
| I-ESIT  | Imperfect Eve’s Channel State Inform |
| RSMA    | Rate-Splitting Multiple Access       |
| MU-CRS  | Multi User Cooperative Rate-Splitting|
| NRS     | Non-Cooperative Rate-Splitting       |
| NOMA    | Non-Orthogonal Multiple Access       |
| SDMA    | Space Division Multiple Access       |
| EIR     | Estimated Information Rates          |
| WCSRM   | Worst Case Secrecy Rate Maximization |
| ACC     | Actual Channel Capacities            |
| AN      | Artificial Noise                     |
| CEU     | Cell Edge Users                      |
| CCU     | Cell Center Users                    |
| WCSR    | Worst-Case Secrecy Rate              |
| IUI     | Inter-User Interference              |
| LoS     | Line of Sight                        |
| MISO-BC | Multi-Input Single-Output Broadcast Channel |
| TPC     | Transmit Precoder                    |
| MA      | Multiple Access                      |
| SPCA    | Sequential Parametric Convex Approximation |
| SURS    | Secure Relaying Users Selection      |


The rest of this paper is organized as follows. The system model, signal representation, corresponding achievable information rate and other preliminaries are provided in Section II. Section III formulates our robust WCSR maximization problem and optimal SRUS protocol. The proposed SPCA-based solution, the associated feasible initialization procedures, and our complexity as well as convergence analysis are provided in Section IV. In Section V, our simulation results are presented and conclude in Section VI. Finally, the Appendices and proofs of the lemmas are provided.

Notation: Vectors and matrices are denoted by lower-case and upper-case boldface symbols, respectively; $(\cdot)^T$, $(\cdot)^*$, $(\cdot)^H$, and $(\cdot)^{-1}$ denote the transpose, conjugate, conjugate transpose, and inverse of a matrix respectively; $\Re(\cdot)$ denote the real part of a complex variable, and $\Im(\cdot)$ denote the imaginary part of a complex variable; We use $\mathbb{E}\{\cdot\}$ and $\mathbb{E}$ to denote the expectation and definition operations, respectively: A complex Gaussian random variable with mean $\mu$ and variance $\sigma^2$ reads as $\mathcal{CN}(\mu, \sigma^2)$; The notation $\mathbf{I}_N$ denotes the $N \times N$ identity matrix; $\mathbb{R}^{N \times 1}$ and $\mathbb{C}^{N \times 1}$ denote the set of $N$-dimensional standard real and complex Gaussian random variable, respectively; $\mathbb{C}^{N \times N}$ stands for an $N \times N$ element standard complex Gaussian random matrix whose real and imaginary parts are independent normally distributed random variables with mean zero and variance $\frac{1}{2}$; Finally, the entry in the $i$-th row and $j$-th column of a matrix $\mathbf{H}$ is represented by $\mathbf{H}[i,j]$.

II. System Model and Preliminaries

We commence by introducing the principles of C-RSMA and the channel models. The system model considered is illustrated in Fig. 1, in which a multi-antenna UAV-BS aims for concurrently serving $K$ legitimate users on the ground indexed by the set $\mathcal{K} = \{1, 2, ..., K\}$ in the presence of an $\mathcal{E}ve$, who silently engages in covert wiretapping. While the UAV-BS is equipped with $N_t$ transmit antennas, the terrestrial nodes are assumed to be single-antenna devices. For simultaneously serving multiple users, the UAV-BS is supported by RSMA. Note that, as it will be discussed later in detail, to take full advantage of RSMA, we exploit the more sophisticated C-RSMA technique in this paper, in which two groups of users are considered for each transmission slot. Thus, the users are divided into two different groups: Cell Center Users (CCU) indexed by the set $\mathcal{K}_1$, and Cell Edge Users (CEU) indexed by the set $\mathcal{K}_2$, so that we have $\mathcal{K}_1 \cup \mathcal{K}_2 = \mathcal{K}$. We assume furthermore that the channel conditions of the users of $\mathcal{K}_1$ are superior to the channels of those belonging to $\mathcal{K}_2$.

A. Principles of C-RSMA

Based on the principle of C-RSMA, the signal transmission is completed in two consecutive phases:

1) Broadcasting Phase (BP), where the UAV-BS transmits the RSMA precoded signal towards the terrestrial nodes through the typical Multiple Input Single Output (MISO) Downlink (DL) channels, i.e., represented by $\text{UAV-BS} \rightarrow \{U_k|_{k \in \mathcal{K}_1}, \mathcal{E}ve\}$.

2) Relaying Phase (RP), where users within $\mathcal{K}_1$, cooperatively forward the signals to CEUs, i.e., $\{U_k|_{k \in \mathcal{K}_1}\} \rightarrow \{U_k|_{k \in \mathcal{K}_2}, \mathcal{E}ve\}$.
user is expected to be able to decode $s_c$ as a part of its original message, the corresponding common TPC, i.e., $p_c$, must be designed for ensuring that $s_c$ simultaneously plays the role of undecodable jamming signal at Eve. Since the UAV-BS is idle during the RP, we assume that it serves as a friendly jammer during this phase to further enhance the secrecy.

### B. Channel Models

We focus on a quasi-static fading environment and denote the channel coefficients of the links spanning from the UAV-BS to terrestrial legitimate nodes and Eve respectively by $h_k \in \mathbb{C}^{N_t \times 1}$ and $h_e \in \mathbb{C}^{N_t \times 1}$. These channels are modeled as $h_n \triangleq PL(d_n) n_n, \forall n \in \{K, e\}$, where $PL(d_n)$ represent the path-loss characterized by the Aerial-to-Ground (A2G) distance $d_n$, and $n_n \sim \mathcal{CN}(0, I_{N_t})$ represents the corresponding small-scale fading. Similarly, $h_{j,i} \triangleq PL(d_{j,i}) n_{j,i, \forall j \in \{K_1\}, \forall i \in \{K_2, e\}$ stands for the Single Input Single Output (SISO) channel from CCUs and CEUs as well as Eve during RP.

Since large-scale fading varies smoothly, we suppose that the UAV-BS can obtain the path-loss variable perfectly for the entire links. Additionally, for the A2G legitimate links $UA V \rightarrow \{U_k|k \in K\}$, we assume that the small-scale fading component can be obtained accurately by frequently sending handshaking signals. However, concerning the Eve, as an untrustworthy subscriber who does not regularly interact with the UAV-BS, its CSI would be outdated at the UAV-BS owing to signaling delays, i.e., Imperfect E-CSIT, although $Eve$ might be able to perfectly estimate its corresponding channels in the worst-case secrecy scenario. Thus, for the illegitimate links during both phases $\{UA V, U_k|k \in K\} \rightarrow Eve$, we assume that the large-scale fading can be estimated perfectly, and imperfection can only contaminate the small-scale fading component. To characterize the imperfect E-CSIT, we utilize the worst-case model of [28], [29], by which the small-scale fading coefficients of the UAV $UA V \rightarrow Eve$ and $\{U_k|k \in K\} \rightarrow Eve$ channels are formulated as follows:

$$n_e \triangleq \hat{n}_e + \Delta n_e, \Theta_e = \{\Delta n_e \in \mathbb{C}^{N_t \times 1}: \|\Delta n_e\|^2 \leq N\zeta^2\},$$

$$n_{j,e} \triangleq \hat{n}_{j,e} + \Delta n_{j,e}, \Theta_{n_{j,e}} = \{\Delta n_{j,e} : \|\Delta n_{j,e}\|^2 \leq \zeta^2\},$$

for $\forall j \in K_1$, where $n_e$ and $\hat{n}_e$ are respectively the estimated small-scale fading of $Eve$ available for the UAV-BS. Furthermore, $U_j|j \in K_1$, and $\Delta n_e$ and $\Delta n_{j,e}$ respectively stand for the unknown channel uncertainty corresponding to $n_e$ and $n_{j,e}$. Still referring to (2), $\zeta$ specifies the radius of the bounded error regions of $\Delta n_{j,e}$, whilst for $\Delta n_e$ the error is a region bounded with radius $\sqrt{N\zeta}$. Specifically, $\zeta > 0$ denotes the size of the uncertainty region of the small-scale fading estimate of the $Eve$. Therefore, the estimated gains of the UAV $\rightarrow Eve$ and $U_j|j \in K_1 \rightarrow Eve$ channel are $\hat{n}_e = PL(d_e) \hat{n}_e$ and $\hat{n}_{j,e} = PL(d_{j,e}) \hat{n}_{j,e}$.

### C. Performance Metrics and Constraints

In this section, we derive the Achievable Secrecy Rate (ASR) as the objective function considered followed by the
constraints imposed, which must be taken into account in our design. Before proceeding, we have provided a flow-diagram in Fig. 2 to show the flow of the analysis described in the sequel. Again, the worst-case secrecy scenario is considered in this paper, where only imperfect E-CSIT is available at the UAV-BS. Given this perspective, while Eve can achieve the actual channel capacity, the UAV-BS is only capable of achieving the estimated information rate. In the following, we derive the Actual Channel Capacities (ACC) as well as the Estimated Information Rates (EIR).

1) Received Signal Models: During the BP, the UAV-BS broadcasts the RSMA signal $x^{(1)}$ and the terrestrial nodes, i.e., $\{U_k|k\in\mathcal{K}\}$ and Eve, will respectively receive the following signals:

$$
y_k^{(1)} = h_k^H x^{(1)} + z_k^{(1)}, \quad \forall k \in \mathcal{K}
$$

$$
y_e^{(1)} = h_e^H x^{(1)} + z_e^{(1)},
$$

where $z_k^{(1)} \sim \mathcal{CN}(0, \sigma_k^2)$ and $z_e^{(1)} \sim \mathcal{CN}(0, \sigma_e^2)$ respectively stand for the Additive White Gaussian Noise (AWGN). During the BP, the $j$-th CCU re-encodes the $s_c$ and forwards it towards the CEUs at a power of $p_j$. Concurrently, using the estimated channel $h_j$, the UAV-BS assigns the beamforming vector $\hat{p}_z \triangleq \frac{h_j^H}{\|h_j\|}$ directed towards the Eve with the power of $p_z$ to cover the transmission of $s_c$ against Eve. Hence, the signals transmitted during the BP respectively from the UAV-BS and the $j$-th CCU are given by:

$$
x_z^{(2)} = \sqrt{p_z} \hat{p}_z z, \quad \text{and} \quad x_j^{(2)} = \sqrt{p_j} s_c, \quad \forall j \in \mathcal{K}_1.
$$

Subsequently, the signals received by $k$-th CEU and Eve in the RP become:

$$
y_k^{(2)} = \sum_{j \in \mathcal{K}_1} h_{j,k}^H x_j^{(2)} + \sqrt{p_z} h_j^H \hat{p}_z z + z_k^{(2)}, \quad \forall k \in \mathcal{K}_2
$$

$$
y_e^{(2)} = \sum_{j \in \mathcal{K}_1} h_{j,e}^H x_j^{(2)} + \sqrt{p_z} h_j^H \hat{p}_z z + z_e^{(2)},
$$

where $z_k^{(2)} \sim \mathcal{CN}(0, \sigma_k^2)$ and $z_e^{(2)} \sim \mathcal{CN}(0, \sigma_e^2)$ are the AWGN at the legitimate user $\{U_k|k\in\mathcal{K}_2\}$ and Eve, respectively.

2) ACC and EIR Analysis: The CCUs first decode $s_c$, while treating the signals corresponding to all the private messages as noise. Accordingly, the channel capacities achieved by $\{U_k|k\in\mathcal{K}\}$ and Eve in decoding $s_c$ during the BP is given by:

$$
R_{c,k}^{(1)} = \theta \log_2 \left( 1 + \frac{|h_k^H p_c|^2}{\sum_{j \in \mathcal{K}} |h_k^H p_j|^2 + \sigma_k^2} \right),
$$

$$
R_{c,e}^{(1)} = \theta \log_2 \left( 1 + \frac{|h_e^H p_c|^2}{\sum_{j \in \mathcal{K}} |h_e^H p_j|^2 + \sigma_e^2} \right),
$$

where $\forall k \in \mathcal{K}$. Under the assumption of perfect SIC, the decoded common message is fully eliminated from the received signal and then each user decodes the intended private message by treating the remaining interference inflicted by the other private messages as a noise. Therefore, only the unintended private stream can be considered as interference and the ACC of decoding the private message by $\{U_k|k\in\mathcal{K}\}$ is calculated as:

$$
R_{p,k} = \theta \log_2 \left( 1 + \frac{|h_k^H p_k|^2}{\sum_{j \in \mathcal{K}, j \neq k} |h_k^H p_j|^2 + \sigma_k^2} \right),
$$

where $\forall k \in \mathcal{K}$. Upon using the RSMA technique, an appropriate secrecy policy is to design the common TPC for ensuring that Eve is unable to decode $s_c$. By doing so, $s_c$ can no longer be eliminated through the preceding SIC block and its corresponding term is considered as interference at Eve. Thus, considering that Eve has a single chance of deciphering the private messages during the first phase, the SINR associated with the detection of the private stream of $U_k|k\in\mathcal{K}$, while treating the private stream of the other users $U_j|j\in\mathcal{K}, j \neq k$ as well as the common stream as interference, may be expressed as:

$$
R_{k,c} = \theta \log_2 \left( 1 + \frac{|h_c^H p_c|^2}{\sum_{j \in \mathcal{K}, j \neq k} |h_c^H p_j|^2 + \sigma_c^2} \right),
$$

During the RP, the ACC in decoding the $s_c$ at $U_k|k\in\mathcal{K}_2$ and Eve are respectively given by:

$$
R_{c,k}^{(2)} = (1 - \theta) \log_2 \left( 1 + \frac{\sum_{j \in \mathcal{K}_1} |h_{j,k}|^2}{p_z \|h_j^H \hat{p}_z\|^2 + \sigma_k^2} \right),
$$

$$
R_{c,e}^{(2)} = (1 - \theta) \log_2 \left( 1 + \frac{\sum_{j \in \mathcal{K}_1} |h_{j,e}|^2}{p_z \|h_j^H \hat{p}_z\|^2 + \sigma_e^2} \right).
$$

Notably, the users in $\mathcal{K}_2$ and Eve combine the decoded common message in both phases. However, while the achievable capacity of decoding the common message at all $U_k|k\in\mathcal{K}$ is limited by the worst-case user, i.e., by user receiving at the minimum SINR in detecting $s_c$ during both phases, Eve tries to infer $s_c$ up to the sum-capacity of both phases. Accordingly, the achievable rate of decoding $s_c$ at $U_k|k\in\mathcal{K}$ and Eve are given as:

$$
R_c = \min \left\{ R_{c,k}^{(1)} \bigg| \forall k \in \mathcal{K}_1, \sum_{k \in \mathcal{K}_2} \left( R_{c,k}^{(1)} + R_{c,k}^{(2)} \right) \bigg| k \in \mathcal{K}_2 \right\}
$$

$$
= \min \left\{ R_{c,k_1}, R_{c,k_2} \right\}.
$$

Then, due to the deleterious impact of imperfect E-CSIT, the EIR corresponding to the Eve’s link from the UAV-BS...
viewpoint is formulated as follows:

\[ \hat{R}_{c,e}(1) = \theta \log_2 \left( 1 + \frac{\left| h^H p_c \right|^2}{\sum_{j \in K} \left| h^H p_j \right|^2 + \sigma_e^2} \right), \]

\[ \hat{R}_{c,e}(2) = (1 - \theta) \log_2 \left( 1 + \frac{\sum_{j \in K} p_j \left| h^H p_j \right|^2}{\left| h^H p_e \right|^2 + \sigma_e^2} \right), \]

\[ \hat{R}_{k,c} = \theta \log_2 \left( 1 + \frac{\left| h^H p_k \right|^2}{\sum_{j \in K, j \neq k} \left| h^H p_j \right|^2 + \sigma_e^2} \right). \]

Remark 1 (Secrecy Policy). To ensure that the common message is decodable for each legitimate user, the actual transmission rate of the common message \( r_c \) should satisfy the condition \( r_c \leq R_c \). On the other hand, the system’s objective is to maximize the minimum ASR among all users to see whether the condition \( C_1 \) is satisfied. For this purpose, we have to satisfy another condition, namely \( r_c > R_{c,e} \). As a result, the corresponding SINR of the private message at the Eve is degraded by the interference caused by the undecodable common message.

Remark 2 (Common Message Considerations). \( R_c \) is shared among all users to see whether the condition \( C_1 \), pointed out in Remark 1, is satisfied or not. Thus, the rate contributions of each user in transmitting \( W_k \), denoted by \( C_k \), should be tuned at the UAV-BS so that we have \( R_c = \sum_{k \in K} C_k \). The weighting factors \( p_k \) are associated with \( \sum_{k \in K} p_k = 1 \) enable us to flexibly adjust the significance of each user as part of the common secrecy rate enhancement.

The total achievable secrecy rate of \( k \)-th user is given by \( R_{e,k}^\text{sec} = R_{e,k}^\text{sec,c} + R_{e,k}^\text{sec,p} \), where \( R_{e,k}^\text{sec,c} = x_k [R_c - R_{c,e}]^+ \) and \( R_{e,k}^\text{sec,p} = [R_{p,k} - R_{k,c}]^+ \) represent the achievable secrecy rate of the common message and private message transmitted to the \( k \)-th user, respectively.

III. PROPOSED JOINT RESOURCE ALLOCATION AND SRUS

Under the realistic imperfect CSIT assumption, the performance of the MRT beamformer \( p_c \) is degraded. To mitigate this deleterious impact and to guarantee a robust design, we will aim for maximizing the minimum ASR over all possible CSI uncertainties. On the other hand, the system’s objective is to maximize the minimum ASR among all legitimate users, with the objective of maintaining secrecy fairness.

A. Optimization Problem

Based on the above discussion, the proposed joint resource allocation design comprises of jointly optimizing the TPC, the common message split, the time slot allocation, and SRUS with the objective of maximizing the minimum ASR among all users subject to a transmit power constraint at the UAV-BS as well as the RSMA secrecy constraints is formulated by:

\[ \max_{p, \theta, \lambda, K_c, p_e} \left( \min_{k \in K_c} \left( \min_{j \in K} \left( \Delta n, \{ R_{e,k}^\text{sec} \} \right) \right) \right) \]

s.t.

\[ C_1 : r_c \leq R_c, \]

\[ C_2 : R_c = \min \{ R_{c,K}, R_{c,K_2} \}, \]

\[ C_3 : r_c \geq \max \{ R_{c,K}, R_{c,K_2} \}, \]

\[ C_4 : \chi \triangleq [x_1, \ldots, x_K], \] and \( P_t \) stands for the transmit power budget at the UAV-BS. Note that, once \( K_1 \) is determined by solving the optimization problem, \( K_2 \) becomes specified, and thus only \( K_1 \) is considered as an optimization variable. The problem formulated is a mixed integer non-convex problem due to the discontinuous nature of the variable \( K_1 \). The optimal SRUS problem itself imposes high computational complexity and the resultant cost increases upon growing the number of users. To circumvent this difficulty, we propose a low-cost algorithm including the following two main steps. Firstly, SRUS protocol is performed to find optimum \( K_1^* \) and \( K_2^* \). In the next step, based on the \( K_1^* \) and \( K_2^* \), we jointly optimize the other network parameters.

B. Optimal SRUS

The SRUS protocol must address two questions:

- How do we select the relaying users?
- How many relaying users are needed?

In order to address these research questions, we turn to the following proposition.

Proposition 3. At the global by optimal point \( \left( P^*; \theta^*; \lambda^*, K_1^*; p_e^* \right) \) of problem (18), the common secrecy rates achieved by the users in the set \( K_1^* \), i.e., \( R_{e,K_1}^\text{sec} \), and set \( K_2^* \), i.e., \( R_{e,K_2}^\text{sec} \), are equal which can be formulated as:

\[ \min_{k \in K_1^*} \left\{ R_{e,k}^\text{sec}(1) \right\} = \min_{k \in K_2^*} \left\{ R_{e,k}^\text{sec}(1) + R_{e,k}^\text{sec}(2) \right\}, \]

Proof: See Appendix A.

Remark 4. It can be an be readily concluded from Proposition 3 that the optimal secure relaying user grouping obeys the following rule, when \( 0 < \theta^* < 1 \):

\[ \min_{k \in K_1^*} \left\{ R_{e,k}^\text{sec}(1) \right\} > \min_{k \in K_2^*} \left\{ R_{e,k}^\text{sec}(2) \right\}, \]

\[ \min_{k \in K_1^*} \left\{ R_{e,k}^\text{sec}(1) \right\} > \min_{k \in K_2^*} \left\{ R_{e,k}^\text{sec}(1) \right\}. \]
Given the insight inferred from Proposition 3, to enhance the common secrecy rate, the users having larger $R_{c,k}^{sec}(1)$ in BP and smaller RP leakage tend to be clustered in $K_1$, while the users with lower $R_{c,k}^{sec}(1)$ in BP and larger RP leakage tend to fall into $K_2$. Since the $R_{c,k}^{sec}(1)$ and RP leakage respectively depends on $\|h_k\|_2$ and $|h_{c,k}|$, an intuitive and simple selection algorithm is based on the simple metric $\frac{|h_{c,k}|}{\|h_k\|_2}$. In the following a pair of relaying protocols (centralized and distributed) based on this metric are presented.

- **Centralized relaying protocol**: Since the UAV-BS needs all the CSIs for its TPC design, one option is to perform SRUS by the UAV-BS. The proposed centralized SRUS algorithm is presented in Algorithm 1, where the process of channel estimation is performed through the classic Request-To-Send (RTS)/Clear-To-Send (CTS) collision avoidance mechanism.

- **Distributed relaying protocol**: In the above centralized protocol, the RTS packet is transmitted through a common downlink pilot channel, while the CTS packets are fed back through individual uplink pilot channels dedicated to each user. Because of this difference between the uplink and downlink centralized techniques are more susceptible to channel imperfections and thus, distributed selection is preferred. More explicitly, while the centralized protocol needs the CSIT for all users at the UAV-BS to select the best secure relaying users, the distributed protocol allows users to select their secure relaying partners based on the CSI estimated at the Receiver (CSIR). This may be readily obtained from the common downlink pilot channels. The proposed distributed SRUS algorithm is presented in Algorithm 2.

### IV. NETWORK PARAMETER OPTIMIZATION

**Algorithm 1 Centralized SRUS Protocol**

**Initialization** $n = 0$, $K_1 = \emptyset$, and $K_2 = K$.

**Step 1** Channel estimation of Users at UAV-BS: First UAV-BS inform all users about $|K_1| = K_1$ through a RTS packet and then they respond through a CTS packet by which their channel is estimated at UA V-BS.

**Step 2** Ordering the users based on the channel strength $\frac{|h_{c,k}|}{\|h_k\|_2}$.

**Step 3** UAV-BS finds $K_1$ secure relaying user as follows. Repeat:

1. $k^* = \max_{k} \left\{ \frac{|h_{c,k}|}{\|h_k\|_2} \right\}$
2. $K_1 \leftarrow K_1 \cup \{k^*\}$
3. $K_2 \leftarrow K_2 \setminus \{k^*\}$

Until $|K_1| = K_1$.

**Output**: UAV-BS transmits a "flag" packet containing the selection results to all users.

After relaxing the problem from the discontinuous variables $K_1^*$ and $K_2^*$, in this stage, we aim for optimizing the remaining variables comprised in the set $\{\mathbf{P}, \theta, \chi, \{p_j\}_{j \in K_1}, \rho_c\}$.
us to reformulate (22) into:

$$
\max_{P, \theta, \chi, \kappa, (p_j)_{j \in \kappa}} P, \theta, \chi, \kappa, (p_j)_{j \in \kappa}, \beta_{c, e}, \rho_{c, e} \text{ s.t.}
$$

$$
C_1: \quad x_k (R_c - \alpha_{c, e}) + \theta (\alpha_{p, k} - \alpha_{c, e}) \geq r_{sec}, \quad \forall k \in \kappa \\
C_2: \quad \theta_{c, e, j} \geq R_c, \quad \forall j \in \kappa \\
C_3: \quad \theta_{c, e, k} + R_{c, k}^{(2)} \geq R_c, \quad \forall k \in \kappa \\
C_4: \quad \sum_{j \in \kappa, j \neq k} |H_{k, j}|^2 |p_j|^2 \geq \rho_{c, k}, \quad \forall k \in \kappa \\
C_5: \quad \sum_{j \in \kappa} |H_{k, j}|^2 |p_j|^2 \geq \rho_{c, k}, \quad \forall k \in \kappa \\
C_6: \quad 1 + \rho_{c, k}^{(1)} - 2 \theta_{c, k}^{(1)} \geq 0, \quad \forall k \in \kappa \\
C_7: \quad 1 + \rho_{c, k} - 2 \theta_{c, k} \geq 0, \quad \forall k \in \kappa \\
C_8: \quad R_c \geq r_e, \\
C_9: \quad R_c \geq \alpha_{c, e}, \quad \forall k \in \kappa \\
C_{10}: \quad r_e \geq \max_{\Delta n_e, \{P_{c, e}\}_{j \in \kappa}} R_{c, e} \\
C_{11}: \quad \alpha_{c, e} \geq \max_{\Delta n_e, \{P_{c, e}\}_{j \in \kappa}} R_{c, e} \\
C_{12}: \quad \alpha_{c, e} \geq \max_{\Delta n_e, \{P_{c, e}\}_{j \in \kappa}} R_{c, e} \\
C_{13}: \quad \sum_{j \in \kappa} x_k = 1, \quad 0 \leq x_k \leq 1, \quad \forall k \in \kappa.
$$

Despite this linearization, by invoking the definitions of rates, the constraints (23-C1 : C5) and (23-C10 : C12) are still non-convex. To handle the non-convexity of these constraints we construct a suitable convex inner subset for approximating the non-convex feasible solution set. Given this perspective, we first try to circumvent the bilinear factor $\theta_{p, k}$ that appeared in (23-C1 : C5) which can be equivalently reformulated with the aim of linearization as $\theta_{p, k} = \frac{1}{4} (\theta + \beta_{p, k})^{(1)} - \frac{1}{4} (\theta - \beta_{p, k})^{(2)}$. Using its first-order Taylor expansion counterpart, at the $m$-th iteration, $\theta_{p, k}$ is approximated at the point $(\theta^{(m)}, \beta_{p, k}^{(m)})$ as follows:

$$
\theta_{p, k} \geq \Theta^{(m)} (\theta, \beta_{p, k}), \quad (24)
$$

$$
\Theta^{(m)} (\theta, \beta_{p, k}) = \max \left\{ \frac{1}{2} \left( \theta^{(m)} + \beta_{p, k}^{(m)} \right) (\theta + \beta_{p, k})^{(1)} - \frac{1}{4} (\theta^{(m)} + \beta_{p, k}^{(m)})^2 - \frac{1}{4} (\theta - \beta_{p, k})^{(2)} \right\}.
$$

Similarly, to acquire the lower bound of $\theta_{p, k}$, we approximate the term $(\theta - \beta_{p, k})^2$, which appeared in its expanded form, around $(\theta^{(m)}, \beta_{p, k}^{(m)})$ as follows:

$$
\theta_{p, k} \leq \Theta^{(m)} (\theta, \beta_{p, k}) \quad (25)
$$

$$
\Theta^{(m)} (\theta, \beta_{p, k}) = \min \left\{ \frac{1}{4} (\theta^{(m)} - \beta_{p, k}^{(m)} \right\} (\theta + \beta_{p, k})^{(1)} + \frac{1}{4} (\theta^{(m)} - \beta_{p, k}^{(m)})^2 - \frac{1}{2} (\theta^{(m)} - \beta_{p, k}^{(m)}) (\theta - \beta_{p, k}).
$$

By substituting the affine approximation terms obtained in (24) and (25), the constraints (23-C1 : C3) around the point $(\theta^{(m)}, \beta_{p, k}^{(m)}, \beta_{c, e}^{(m)}, \beta_{c, e}^{(1)(m)})$ are approximated as follows:

$$
C_k - \alpha_{c, e} + \Theta^{(m)} (\theta, \beta_{p, k}) - \Theta^{(m)} (\theta, \beta_{p, k}) \geq r_{sec}, \quad \forall k \in \kappa, \quad (26)
$$

$$
\Theta^{(m)} (\theta, \beta_{c, e}^{(1)}) + \Theta^{(m)} (1 - \theta, \beta_{c, e}^{(2)}) \leq \alpha_{c, e}, \quad (36)
$$

$$
1 + \rho_{c, e}^{(j)} - \Gamma^{(m)} (\beta_{c, e}^{(j)}) \leq 0, \quad j \in \{1, 2\}, \quad (37)
$$

$$
\sum_{k \in \kappa} |h_{e, k}|^2 p_k^2 \leq \rho_{c, e}^{(1)} \quad (38)
$$

As for the constraints (23-C4 : C5), they can be equivalently expressed through the Difference-of-Convex (DC) decomposition [37], given by:

$$
\sum_{k \in \kappa} |h_{k, H}^j p_j|^2 + \sigma_{k}^2 \leq 0, \quad \forall k \in \kappa. \quad (29)
$$

$$
\sum_{k \in \kappa} |h_{k, H}^j p_j|^2 + \sigma_{k}^2 \leq 0, \quad \forall k \in \kappa. \quad (30)
$$

As it can be observed, the non-convexities of (29) and (30) are caused by the concave terms $B_{p, k}$ and $C_{p, k}$. Therefore, we replace them by their affine approximation counterparts obtained by the first-order Taylor expansion around the point $(\mu_{c, k}^{(m)}, \mu_{p, k}^{(m)}, \mu_{c, e}^{(1)(m)}, \mu_{p, k}^{(m)})$ and obtain the convex approximations of (29) and (30) as follows:

$$
\sum_{k \in \kappa} |h_{k, H}^j p_j|^2 + \sigma_{k}^2 - \Psi^{(m)} (p_k, \rho_{c, k}; \ h_k) \leq 0, \quad \forall k \in \kappa. \quad (31)
$$

$$
\sum_{k \in \kappa} |h_{k, H}^j p_j|^2 + \sigma_{k}^2 - \Psi^{(m)} (\mu_{c, k}^{(m)}, \rho_{c, k}^{(1)}; \ h_k) \leq 0, \quad \forall k \in \kappa. \quad (32)
$$

where

$$
\Psi^{(m)} (u, x; \ h) \triangleq \frac{2Re}{x^{(m)}} \left\{ (u^{(m)})^H h h^H u - |h^H u^{(m)}|^2 x \right\}. \quad (33)
$$

Now, with the objective of convexifying (23-C10 : C11), we can equivalently write them as follows:

$$
\alpha_{c, e} \geq \alpha_{c, e}, \quad (34)
$$

$$
\alpha_{c, e} \geq R_{c, e}, \quad \forall \Delta n_e \in \Theta_e, \quad \forall \{\Delta n_{j,e} \in \Theta_{h_{j,e}}\}_{j \in \kappa_1}. \quad (35)
$$

However, (35) is still non-convex, which enforces us to introduce the new auxiliary variables $\beta_{c, e}^{(1)}, \rho_{c, e}^{(2)}, \beta_{c, e}^{(2)}$, representing the SINR, as well as the rate of the common streams associated with first and second phases at Eve, respectively. After some routine mathematical manipulations, (35) can be recast as:

$$
\Theta^{(m)} (\theta, \beta_{c, e}^{(1)}) + \Theta^{(m)} (1 - \theta, \beta_{c, e}^{(2)}) \leq \alpha_{c, e}, \quad (36)
$$

$$
1 + \rho_{c, e}^{(j)} - \Gamma^{(m)} (\beta_{c, e}^{(j)}) \leq 0, \quad j \in \{1, 2\}, \quad (37)
$$

$$
\sum_{k \in \kappa} |h_{e, k}|^2 p_k^2 \leq \rho_{c, e}^{(1)}, \quad \forall \Delta n_e \in \Theta_e. \quad (38)$$
\[
\sum_{j \in K_1} p_j |h_{j,e}|^2 \\
p_z \left| \hat{h}_e H \hat{p}_z \right|^2 + \sigma_e^2 \leq \rho_{e,c}^{(2)}, \quad \forall \Delta n_e \in \Theta_e, \forall \{ \Delta n_{j,e} \in \Theta_{h_{j,e}} \},
\]

where \( \Gamma^{[m]}(x) \triangleq 2^{x^{[m]}} [1 + \ln(2) (x - x^{[m]})] \).

Here, (38) and (39) are still non-convex, which enforces us to define the new auxiliary variables \( \{ x_{e,c}, \{ u_{k,c,e} \}_{k \in K}, \{ y_{j,c,e} \}_{j \in K}, v_{c,e} \} \), by which we can reformulate (38) and (39) as follows:

\[
\begin{align*}
\min_{\Delta n_{e} \in \Theta_{e}} & \left( \hat{h}_e + \Delta n_{e} \right)^H P_e \leq x_{c,e}, \\
\min_{\Delta n_{j,e} \in \Theta_{h_{j,e}}} & \left( \hat{h}_{j,e} + \Delta n_{j,e} \right)^H p_k \geq u_{k,c,e}, \quad \forall k \in K, \\
\min_{\Delta n_{j,e} \in \Theta_{h_{j,e}}} & \left( \hat{h}_{j,e} + \Delta n_{j,e} \right)^H p_k \geq v_{c,e}, \quad \forall j \in K_1, \\
\end{align*}
\]

where \( \delta_j \triangleq \sqrt{\rho_{j,e}} \). Next, we adopt the SPCA method to convert the non-convex constraints (40)-(41) into convex constraints. In this regard, we introduce the auxiliary variables \( \{ d_{e,c}, d_{c,e} \} \) into the constraints (40)-(41), leading to:

\[
\begin{align*}
\sum_{k \in K} u_{k,c,e} + \sigma_e^2 & \geq d_{e,c}^{(1)}, \\
\frac{\sigma_{e,c}^2}{d_{e,c}^{(1)}} & \leq \rho_{e,c}^{(1)}, \\
v_{c,e} + \sigma_e^2 & \geq d_{c,e}^{(2)}, \\
\sum_{j \in K_1} y_{j,c,e} + \sigma_e^2 & \leq \rho_{c,e}^{(2)}.
\end{align*}
\]

Using the interior-point methods of [37], we can solve the problem in (20), which is a convex Quadratically Constrained Quadratic Program (QCQP) [37].

### A. Feasible Initial Point Search Algorithm

Note that, if (50) is initialized by random points, it may fail at the very beginning, because of infeasibility [1], [5], [10]. To circumvent this issue, we now conceive a feasible initial point search algorithm (FIPSA) in this section. In this regard, we aim for minimizing an infeasibility indicator parameter \( \vartheta > 0 \), to flag up any violation of the constraints of (50). Hence we have to rewrite all the constraints of problem (50) in the form of \( \mathcal{G}_i(x) \mid_{i=1}^{16} \leq \vartheta \), where \( x \triangleq \{ P, \theta, \chi, K \}, \{ p_j \}_{j \in K_1}, \{ p_e \}, \{ p_{c,e} \}, \{ p_{c,e} \} \) and \( \mathcal{G}_i(x) \) stands for the reshaped format of the \( i \)-th constraint and all the terms at the left-side of the less than or equal to zero. Then we reformulate the feasibility problem as follows:

\[
\min_{x} \vartheta \quad \text{s.t.} \quad \mathcal{G}_i(x) \mid_{i=1}^{16} \leq \vartheta.
\]

This approach has been previously proposed in [9], [12] as a low-complexity technique of finding feasible initial points. Overall, the proposed FIPSA runs at the first step and then the initial points (IPs) calculated are fed to (50). As a starting point, FIPSA commences with following IPs and the algorithm is halted if either the stopping criterion is satisfied or the maximum number of affordable iterations is reached. In this regard, the TPCs of the proposed FIPSA algorithm are initialized by using MRT combined with Singular Value Decomposition (SVD). The TPC \( \{ P^{[0]} \}_{v \in K} \) constructed for the private stream \( \{ s_k \}_{v \in K} \) is initialized as \( \sqrt{\omega} \frac{h_{v,k}}{h_{v,k}} \), where \( 0 < \omega < 1 \). The TPC \( p^{[0]}_z \) for the common message \( s_c \) is initialized as \( \sqrt{(1 - \omega)} P \hat{u}_e \), and \( u_e \) is the largest left singular vector of the channel matrix \( A \triangleq [h_1, h_2, \ldots, h_K] \). It is calculated by \( u_e \triangleq U_e (:, 1) \) where \( A \triangleq \text{USV} \). Also we have initialized the iterative variables as \( \beta^{[0]} = 0.5 \), \( p^{[0]}_z = \omega_z P_z \), \( p^{[0]}_j = \omega_j P_j \) where \( 0 < \{ \omega_j, \omega_z \} < 1 \), \( \rho^{(1)}_{c,k} \), \( \rho^{(2)}_{c,k} \), \( \beta^{(1)}_{c,k} \), \( \beta^{(2)}_{c,k} \), \( \beta^{(n)}_{c,k} \), \( \lambda^{(1)}_{c,k} \) and \( \lambda^{(n)}_{c,k} \), which are defined as:

\[
\begin{align*}
\rho^{(1)}_{c,k} & = \frac{\| h_{c,k}^{[0]} p^{[0]}_z \|^2}{\sum_{j \in K} \| h_{c,k}^{[0]} p^{[0]}_j \|^2 + \sigma_e^2}, \\
\rho^{(2)}_{c,k} & = \frac{\sum_{j \in K} p^{[0]}_j |h_{j,k}^{[0]}|^2}{\| h_{c,k}^{[0]} p^{[0]}_z \|^2 + \sigma_e^2}, \\
\beta^{(1)}_{c,k} & = \log_2 \left( 1 + \rho^{(1)}_{c,k} \right), \\
\beta^{(2)}_{c,k} & = \log_2 \left( 1 + \rho^{(2)}_{c,k} \right), \\
\beta^{(n)}_{c,k} & = \log_2 \left( 1 - \beta^{(n-1)}_{c,k} \right), \\
\vartheta & = 1 - \beta^{(n)}_{c,k}, \\
\lambda^{(1)}_{c,k} & = \frac{1}{\vartheta} \sum_{j \in K} \{ p^{(1)}_j \}, \\
\lambda^{(n)}_{c,k} & = \frac{1}{\vartheta} \sum_{j \in K} \{ p^{(n)}_j \}.
\end{align*}
\]
B. Convergence Analysis

The proposed SPCA-based algorithm iteratively solves the approximated problem (23) until convergence is reached, where $\delta$ represents the convergence tolerance. In this regard, we formulate the following proposition.

Proposition 5. The proposed SPCA-based algorithm guarantees convergence to a stationary point of problem (22) for any feasible initial point.

Proof: See Appendix B.

C. Complexity Analysis

The SPCA-based solution suggested solves the convex subproblem (50) in each iteration. Problem (50) is a generalized nonlinear convex program due to the exponential cone constraints $(23-C_6 : C_7)$. In order to approximate $(23-C_6 : C_7)$, a sequence of Second Order Cones (SOCs) would be more efficient [38]. Hence, we can use one of the MATLAB optimization Toolbox solvers, such as cvx or fmincon. Considering the computational complexity of interior-point methods, i.e., $O\left([KN_t]^{3.5}\right)$, it is possible to solve the resultant SOC program. The total number of iterations required for achieving convergence may be shown to be on the order of $O\left(-\log(\zeta)\right)$. Therefore, the worst-case computational complexity is $O\left(-\log(\delta) \times [KN_t]^{3.5}\right)$.

V. NUMERICAL RESULTS

In this section, we present numerical results for characterizing our proposed framework using the following simulation setting, unless stated otherwise. The simulation results are averaged over $10^2$ random realizations of the proposed scheme. Through this section, a maximum of 25 iterations are considered for our proposed secrecy fairness maximization problem to converge. Moreover, we set the maximum convergence tolerance to be $\delta = 10^{-2}$. In contrast to the fading model between users, the path loss model of our UAV network includes both LoS and NLoS in conjunction with the path-loss exponents $L_{n,k}^i = 2$ and $N_{n,k}^i = 3.5$, respectively. We assume that the transmit power obeys $P_j = P_z = P_t^i$, $\forall k \in K_1$ and $P_t = 40\text{dBm}$. The UAV is assumed to serve users within a radius of $R = 300\text{ m}$ at an altitude of $H = 130\text{ m}$ with $N_t = 4$. Furthermore, the $K = 4$ users are randomly located within the coverage area of each UAV-BS. A channel estimation error variance of $\zeta = 10^{-3}$ is assumed and the additive noise at the receivers is considered to have a normalized power of $\sigma^2 = \sigma_e^2 = 0\text{ dBm}$, and the minimum required transmission rate $r_c = 1$. For simplicity, we collect all the simulation parameters in table III. We compare the following SRUS protocols for the design of $K_1$ and $K_2$:

- **Scheme 1:** 1 Optimal Relay (1OR): the optimal relaying protocol where the SRUS is carried out centrally at the UAV-BS by enumerating all possible relaying user combinations. The scheduling scheme having the highest max-min secrecy rate is selected. It achieves the upper bound of the max-min secrecy rate of all relaying protocols but has the highest selection complexity.

- **Scheme 2:** 1 Best Relay (1BR): the proposed SRUS protocols when $|K_1| = 1$.

- **Scheme 3:** $\frac{|K_1|}{2}$ Best Relays ($\frac{|K_1|}{2}$BR): the proposed SRUS when $|K_1| = |K_2|$.

- **Scheme 4:** 1 Random Relay (1RR): the UAV-BS randomly selects one user from $K$ and broadcasts the decision to all users via the “RTS” packet. It has the lowest selection complexity.

After SRUS both $K_1$ and $K_2$ are determined. Then we compare the following TPC, message split and time resource allocation algorithms:

- **Algorithm 1:** CRS-SPCA: the CRS model proposed in Section II and the proposed SPCA-based algorithm is adopted to solve problem (50).

- **Algorithm 2:** CRS-WMMSE: the CRS model proposed in Section II, but the optimization problem (50) is solved using the WMMSE algorithm of [19] employing one-dimensional exhaustive search for $\theta$.

- **Algorithm 3:** NRS-SPCA: Non-CRS is also a specific instance of the CRS-SPCA scheme, when $\theta$ is fixed to 1. This is the RS scheme that has been investigated in [19], [32] for MISO BC without cooperative transmission. The transmission is completed at the end of the direct transmission phase and the cooperative transmission is blocked.

- **Algorithm 4:** WMMSE-TPC: the traditional multi-user linear TPC-based beamformer investigated in [36]. There is no RS and no cooperative transmission (i.e., $\|p_c\| = 0$)

![Fig. 3. Evaluating of convergence speed of the proposed FIPSA versus the number of iterations, $P_t = 40\text{ dBm}, N_t = 4$ and $K = 4$.

| Parameter | Value | Parameter | Value |
|-----------|-------|-----------|-------|
| $\delta$  | $10^{-2}$ | $K$       | 4     |
| $L_{n,k}^i$ | 2    | $\zeta$   | $10^{-3}$ |
| $N_{n,k}^i$ | 3.5  | $\sigma^2 = \sigma_e^2$ | 0 dBm |
| $P_t$     | 40 dBm | $r_c$     | 1     |
| $R$       | 300 m  | #Iterations | 25 |
| $H$       | 130 m  | $N_t$     | 4     |
and $\theta = 1$).

The TPC initialization of the WMMSE algorithm is the same as that of the proposed SPCA-based algorithm, where $\theta$ is searched with increment $\Delta \theta = 0.1$ in the CRS, WMMSE algorithm. Therefore, the precoders and message split are optimized by using the WMMSE algorithm 10 times for each value of $\theta$ selected from the set $\{0.1, 0.2, ..., 1\}$. The MATLAB Toolbox cvx is used to solve the problem (50).

Fig. 3 depicts the average convergence of the proposed FIPSA for CRS-SPCA, CRS-WMMSE, WMMSE-TPC, and NRS-SPCA algorithms using the OF value of (51), $\bar{\vartheta}$ versus the number of iterations. As observed, the average convergence speed of all algorithm are fast and converge within a few iterations. Though the proposed FIPSA algorithm is able to converge quickly within a few iterations. This is similar to the convergence speed of WMMSE.

Fig. 4 and 5 show the WCSR, $r_{sec}$ achieved by the different strategies versus the total power budget $P_t$ for $N_t = 4$ and 8 UAV-BS transmit antennas. As expected $r_{sec}$ is increased with $P_t$. We can also observe in Fig. 4 that given a total power becomes high, the $r_{sec}$ is increased. We can also observe that given a specific total power budget $P_t$, BR has almost the same performance for the proposed CRS-SPCA algorithm as OR. A comparison shows that $\frac{2}{K}$-BR, which is the same as 2BR when $K = 4$, does have a negative effect on WCSR and has a similar performance to the baseline 1RR. To enhance the WCSR among users, reducing the size of $K_1$ is preferred, because then more users can benefit from the cooperative transmission. Under the given 1BR scheduling protocol, we compare the algorithms of optimizing the RSMA TPCs, message split variables, time slot sharing and power allocation. Fig. 4 shows that the proposed CRS-SPCA algorithm performs similarly or even better in terms of WCSR than all the existing transmission schemes.

According to Fig. 5, for $N_t = 8$ the relative WCSR gain of the proposed CRS-SPCA increases, because CRS provides improved interference management capabilities, when the multiuser interference is strong.

Additionally, we see that when the number of transmit antennas $N_t$ gets decreased, the WCSR difference between the suggested CRS-SPCA (with 1BR) and WMMSE-TPC increases, which it implies that TPC-based beamformer is only appropriate for under-loaded conditions. As $N_t$ decreases, it is unable to handle the multi-user interference caused by all other users. In comparison, as RS-aided transmission approaches can partially decode the interference and partially treat interference as noise, they are more tolerant to the network load. A higher disparity in channel strength results in a more severe loss of common rate. By re-transmitting the $s_c$ to the worst-case user in CRS, improves $C_{\xi}$ considerably. Therefore, $\theta$ is substantially closer to 1 when user channel strength disparities are negligible. As a result, the advantages of using CRS over NRS decrease.

Fig. 6 depicts the WCSR $r_{sec}$ versus the number of users $K$. Since $\sum_{k=1}^{K} \binom{K}{k}$ scheduling groups must be considered for obtaining the optimal SRUS, the complexity escalates as $K$ increases. We observe that in the $K$-user CRS-assisted transmission network using a single SRUS-based protocol would suffice. As shown in Fig. 6, the gap rate between NRS and CRS clearly increases as the number of users increases. It follows that as the number of users grows, the ideal theta decreases. This is
due to the fact that the multi-user interference increases with the number of users, and a larger portion of the user messages \(\mathcal{W}_k\) is transmitted via the common stream \(s_c\). On the other hand, then \(Eve\) is more likely to eavesdrop successfully on the common stream which leads to a lower WCSR.

To illustrate the robustness of our proposed framework against imperfect E-CSIT, we have produced Fig. 7, where the average WCSR is depicted versus the E-CSIT estimation error \(\zeta\). Observe that regardless of the value of \(\zeta\), comparing the WCSR of the proposed CRS-SPCA scheme to that of WMMSE-TPC demonstrates the superiority of the CRS-aided transmission scheme over traditional linear TPC-based beamformer. Additionally, the WCSR performances of the various scheduling relaying protocols are similar to each other for low E-CSIT estimation error of \(\zeta\), but at high values of \(\zeta\), \(\frac{K}{2}\) BR performs about 50% worse than "1BR."

Finally, Fig. 8 shows the WCSR achieved by the proposed framework versus the \(\theta\) using the "1BR" method. In this experiment we aim for observing the impact of the UAV-BS altitude \(H\) and \(\theta\) on the achievable WCSR \(r_{sec}\). It is interesting to note that the \(r_{sec}\) vs. \(\theta\) curve is concave, and there is an optimum \(\theta^*\) at which the \(r_{sec}\) will be maximized. This figure also indicates that the WCSR critically depends on the altitude of the UAV-BS. As the height of the UAV-BS increases, the value of \(\theta\) becomes closer to 1. This is because, owing to the LoS links, the quality of the common signal received at CEU is good enough at the optimal altitude \(H^*\). Hence no cooperation is needed for relaying the common stream. In Fig. 8, increasing the height \(H\) and moving away from the optimal altitude \(H^*\) results in approximately similar distances between the UAV-BS and all users, hence the WCSR is reduced due to its higher path-loss component. By contrast, when the height of the UAV-BS is reduced from its optimal value, \(\theta^*\) decreases as well due to the emergence of fading. As a result, the CEU’s common signal is adversely affected, and reliance on the cooperative phase becomes essential.

VI. CONCLUSION

To conclude, we studied the robust and secure max-min fairness of cooperative multi-user RSMA in a MISO-BC UAV network downlink where only imperfect E-CSIT is available. We formulated the problem of maximizing the WCSR by jointly optimizing the SRUS and the network’s resources allocation, including the TPCs, time slot sharing and power allocation. To circumvent the non-convexity resulting from the discrete nature of the SRUS, we proposed a two-stage algorithm, where the SRUS and network resources optimization were performed in two consecutive stages. As for the SRUS, we analytically showed that we only need the ratio of the UAV-BS to \(\{U_k\}_{k\in\mathcal{K}}\) and \(\{Eve\} \rightarrow \{Eve\}\) channel gains for two type of centralized and distributed protocols. On the other hand, an SPCA-based solution has been proposed to cope with the resultant non-convexity imposed by the network resource allocation. Our numerical results show that by applying the proposed solution, the WCSR is substantially boosted over that of the benchmarks. Thus, we conclude that our cooperative multi-user RSMA framework is capable of improving the confidentiality of 6G networks.

APPENDIX A

PROOF OF PROPOSITION 3

We first prove the equivalence of the common secrecy rate achieved by users in \(K_1\) and \(K_2\) at the globally optimal point (19) by the method of contradiction. By assuming that \(k_{1,\min}\) and \(k_{2,\min}\) are the two users that respectively achieve the worst common secrecy rate in \(K_1\) and \(K_2\) at the globally optimal point \((P^*, \theta^*, \chi^*, K_1^*, \{p^*_j\}_{j\in K_1^*}, p^*_z)\), we obtain (52), where

\[
\gamma_{c,n}^{(1)}(P^*) \triangleq \log_2 \left(1 + \frac{|h_n^H P_n^*|^2}{\sum_{k \in \mathcal{K}} |h_n^H P_k^*|^2 + \sigma_n^2}\right),
\]

\[
\gamma_{c,n}^{(2)}(\{p^*_j\}_{j\in K_1^*}, P^*_z) \triangleq \log_2 \left(1 + \frac{\sum_{j \in K_1^*} |p^{*}_{h,j,n}|^2}{|p^*_z h_n^H \hat{p}_z| + |\hat{p}_z|^2 + \sigma_n^2}\right).
\]

Note that for the weakest legitimate user in \(K_2\), i.e., \(U_{k_{2,\min}}\), we must have \(\gamma_{c,k_{2,\min}}^{(1)}(P^*) < \)
\[ R_{c,k_1}^{\text{sec}} \triangleq \theta^* \left[ \gamma_{c,k_1,\min}^{(1)} (P^*) - \gamma_{c,c}^{(1)} \right] = \theta^* \gamma_{c,k_1,\min}^{(1)} (P^*), \]  
\[ R_{c,k_2}^{\text{sec}} \triangleq \theta^* \left[ \gamma_{c,k_2,\min}^{(1)} (P^*) - \gamma_{c,c}^{(1)} \right] + (1 - \theta^*) \gamma_{c,k_2,\min}^{(2)} \left( \{(p^*_j)_{j \in K_1^c} \}, p^*_2, \kappa^*_1 \right) - \gamma_{c,c}^{(2)} \]  
\[ = \theta^* \gamma_{c,k_2,\min}^{(1)} (P^*) + (1 - \theta^*) \gamma_{c,k_2,\min}^{(2)} \left( \{(p^*_j)_{j \in K_1^c} \}, p^*_2, \kappa^*_1 \right), \]  
\[ = \theta^* \left[ \gamma_{c,k_2,\min}^{(1)} (P^*) - \gamma_{c,c}^{(1)} \right] + \gamma_{c,k_2,\min}^{(2)} \left( \{(p^*_j)_{j \in K_1^c} \}, p^*_2, \kappa^*_1 \right), \]  
\[ \theta^* > \theta^* \left[ \gamma_{c,k_1,\min}^{(1)} (P^*) - \gamma_{c,c}^{(1)} \right] + \gamma_{c,k_2,\min}^{(2)} \left( \{(p^*_j)_{j \in K_1^c} \}, p^*_2, \kappa^*_1 \right), \]  
\[ \Rightarrow \theta^* > \frac{\gamma_{c,k_2,\min}^{(1)} (P^*) - \gamma_{c,c}^{(1)}}{\gamma_{c,k_2,\min}^{(1)} (P^*)} = \tilde{\theta}, \]  
\[ \theta^* \left[ \gamma_{c,k_1,\min}^{(1)} (P^*) - \gamma_{c,c}^{(1)} \right] = (1 - \theta^*) \left[ \gamma_{c,k_2,\min}^{(2)} \left( \{(p^*_j)_{j \in K_1^c} \}, p^*_2, \kappa^*_1 \right) - \gamma_{c,c}^{(2)} \right], \]  
\[ R_{c,k_1}^{\text{sec}} - R_{c,k_2}^{\text{sec}} = R_{c,k_2}^{\text{sec}} \]  
Based on (19), we have \( R_{c,k_1}^{\text{sec}} > \min_{k \in K_2^c} \{ R_{c,k}^{\text{sec}} \} \) when \( \theta^* < 1 \) and the proof of proposition 1 is completed.

**APPENDIX B**

**PROOF OF PROPOSITION 5**

SPCA ensures monotonic improvement of \( r_{\text{sec}} \), i.e., \( r_{\text{sec}}^{[n]} \geq r_{\text{sec}}^{[n+1]} \). This is due to the fact that the solution generated by solving problem (23) at iteration \([n-1]\) is a feasible point of problem (23) at iteration \([n]\). Due to the transmit power constraint ((18)-(23), the sequence \( \{r_{\text{sec}}^{[n]}\}_{n=1}^{\infty} \) is bounded above, which implies that the convergence of the proposed SPCA-based algorithm is guaranteed. Next, we show that the sequence \( \left\{ (\tilde{p}_j, \tilde{\theta}, \tilde{\kappa}, (\tilde{P}_j)_{j \in K_1^c}, \tilde{p}_2, \tilde{\kappa}_1) \right\}_{n=1}^{\infty} \) converges to the set of stationary points of problem (23). The proposed SPCA-based algorithm is in fact an inner approximation algorithm of the non-convex optimization literature [30], [31]. This is proved by showing the equivalence of the KKT conditions of problem (22) and problem (23) when the solution \( \left\{ (P_j, \theta_j, \chi_j, (P_j)_{j \in K_1^c}, \beta_j, \rho_j, \alpha_j) \right\}_{j \in K_1^c} \) is equal to \( \left\{ (\tilde{P}_j, \tilde{\theta}_j, \tilde{\kappa}_j, (\tilde{P}_j)_{j \in K_1^c}, \tilde{p}_2, \tilde{\kappa}_1) \right\} \). Combined with the fact that the Taylor approximations made in (23) are asymptotically tight as \( n \to \infty \) [31], we can see that the solution of the proposed SPCA-based algorithm converges to the set of stationary points of problem (22).

**REFERENCES**

[1] M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, “6g wireless communication systems: Applications, requirements, technolo-
