Latency Minimization for Secure Intelligent Reflecting Surface Enhanced Virtual Reality Delivery Systems

Yi Zhou, Cunhua Pan, Phee Lep Yeoh, Kezhi Wang, Zheng Ma, Branka Vucetic and Yonghui Li

***Abstract*—This letter investigates a virtual reality (VR) delivery system, where the original VR contents requested by all users are stored at the macro base station (MBS). To reduce latency, MBS can either transmit the original VR data or the computed VR data to multiple users aided by an intelligent reflecting surface (IRS) to prevent attacks from an eavesdropper with imperfect channel state information (CSI). We jointly optimize the transmission policies, MBS transmit power, IRS phase shift and computing frequency to minimize the latency over all users subject to security constraint. Numerical results validate the robustness of our proposed algorithm.**

I. Introduction

Virtual reality (VR) has gained increasing popularity due to its potential to provide highly immersive VR environments. However, realizing low-latency VR applications is extremely difficult due to the limited computing capabilities of VR users. To address the latency bottlenecks, mobile edge computing (MEC), which is capable of providing sufficient computing resource at the network edge has been envisioned as one promising solution to achieve low-latency communications [1]–[3]. In [4], the latency of an unmanned aerial vehicle (UAV) VR delivery system was minimized by jointly optimizing the user association, communication and computing resources.

On the other hand, the intelligent reflecting surface (IRS) which consists of a large number of passive reflecting elements is a novel enabler for enhancing the spectral- and energy-efficiency due to its capability of reconfiguring the wireless propagation environment [5]–[7]. In [8], the authors proposed an efficient algorithm to maximize the sum rate of all users in an IRS-assisted non-orthogonal multiple access (NOMA) network. In [9], a transmit power minimization problem of an IRS-aided multiuser multiple-input single-output (MU-MISO) system was investigated. Recently, the amalgamation of IRS and MEC has received significant attention in the literature. In [10], an efficient algorithm was designed to reduce the computational latency in an IRS-assisted MEC network.

The work of Y. Zhou was supported by the Fundamental Research Funds for the Central Universities under Grant 2682021ZTPY117 and 2682022CX020. The work of P. L. Yeoh was supported by ARC under Grant DP190100770. The work of Z. Ma was supported by Sichuan Science and Technology Program under Grant 2020YFH0111. The work of Y. Li was supported by ARC under Grant DP190101988 and DP210103410. The work of B. Vucetic was partially supported by ARC Laureate Fellowship under Grant FL160100032. *(Corresponding author: Zheng Ma.)*

Y. Zhou and Z. Ma are with the Key Lab of Information Coding, and Transmission, Southwest Jiaotong University, Chengdu 610031, China. (e-mail:yizhou@swjtu.edu.cn;zma@home.swjtu.edu.cn).

C. Pan is with the National Mobile Communications Research Laboratory, Southeast University, China. (e-mail:cpan@seu.edu.cn).

P. L. Yeoh, B. Vucetic, and Y. Li are with the School of Electrical and Information Engineering, University of Sydney, NSW 2006, Australia. (e-mail: phee.yeoh@sydney.edu.au; branka.vucetic@sydney.edu.au; yonghui.li@sydney.edu.au).

K. Wang is with the Department of Computer and Information Sciences, Northumbria University, Newcastle NE2 1XE, U.K. (e-mail: kezhi.wang@northumbria.ac.uk).

Due to the broadcast nature of wireless transmissions, it is important to consider the security performance since the legitimate communication can be readily overheard by nearby eavesdroppers [11]–[13]. To the best of our knowledge, the research of IRS-enhanced VR delivery network with latency and security considerations is still in its infancy, thus strongly motivating this work.

In this letter, we propose a novel secure framework with the aim of minimizing the overall latency of an IRS-enhanced VR delivery system where the macro base station (MBS) can either transmit the original VR data or the computed VR data to multiple users in the presence of one eavesdropper with imperfect channel state information (CSI). Since the eavesdropper cannot decompress and decode the original VR data, we consider that the secrecy is perfectly guaranteed when original VR data is transmitted. We summarize our contributions as follows:

- We derive a mathematically tractable expression of lower bound secrecy capacity with imperfect eavesdropper's CSI and formulate a latency minimization problem of an IRS-enhanced VR delivery system subject to security constraint.
- We propose an efficient algorithm to solve this non-convex optimization problem by applying the alternating optimization (AO), **S**-Procedure and semi-definite relaxation (SDR) methods.
- Simulation results validate the effectiveness and robustness of our proposed strategy.

Notations: For a complex-valued vector $\boldsymbol{x}$, $\boldsymbol{x}^{\boldsymbol{T}}$, $\boldsymbol{x}^{\boldsymbol{H}}$ and diag$(\boldsymbol{x})$ represent its transpose, Hermitian transpose and diagonalization, respectively. For a matrix $\boldsymbol{M}$, rank$(\boldsymbol{M})$, $\boldsymbol{M}_{i,j}$ and Tr$(\boldsymbol{M})$ denote its rank, the $(i,j)th$ element and trace, respectively.

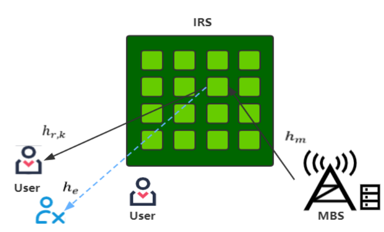

Fig. 1. An IRS-enhanced secure VR delivery system.

II. System Model

As depicted in Fig. 1, we consider an IRS-enhanced VR delivery system where the original VR data requested by K users is stored at the MBS. We assume that both the MBS and the users are equipped with computing resources which allow them to compute the original VR data. To reduce latency, MBS can either transmit the original VR data for user computing or the computed VR data after being processed at the itself to all users. Due to unfavorable blockages and obstacles, the direct transmissions between the MBS and the users are assumed to be unavailable [8]. Thus, an IRS which comprises N reflecting elements is deployed to assist the communications via frequency division multiple access (FDMA). Denote the sets of users and IRS reflecting elements as $\mathcal{K}$ and $\mathcal{N}$, respectively. Let $\mathbf{\Phi} = \mathrm{diag}\{\boldsymbol{\theta}\}$ denote the diagonal phase shift matrix for the IRS, where $\boldsymbol{\theta} = [e^{j\varpi_1}, e^{j\varpi_2}, \cdots, e^{j\varpi_N}]$ and $|\theta_n| = |e^{j\varpi_n}| = 1, \forall n \in \mathcal{N}$.

We denote I_k and O_k as the volumes of the original and computed VR data requested by the k-th user, respectively. To achieve an immersive VR environment, the computed VR data is usually modeled as three-dimensional (3D) video data while the original VR data is in two-dimensional (2D) form. Thus, the ratio between O_k and I_k is set as $\beta_k = \frac{O_k}{I_k} \geq 2$ in order to create a stereoscopic vision [3], [4].

We denote $\boldsymbol{c} \triangleq \{c_k, \forall k \in \mathcal{K}\}$ as the set of transmission policies where $c_k = 1$ implies that the MBS computes the original VR data I_k at itself and transmits the computed VR data O_k to the k-th user. Conversely, $c_k = 0$ represents that the MBS transmits the original VR data I_k to the k-th user, which needs to be processed locally. We further denote $\mathcal{K}_{mbs} = \{c_k = 1, \forall k \in \mathcal{K}\}$ as the set of users whose computed VR data will be transmitted from the MBS and K_{mbs} as the size of set $\mathcal{K}_{mbs}$.

A. Computing Model

1) MBS Computing Mode: Denote f_m as the central processing unit (CPU) cycle frequency of the MBS, which is fixed for the VR data computing [14], thus, the corresponding computing time is $t_k^{m,com} = \frac{I_k F_k}{f_m}$, where F_k denotes the number of CPU cycles required to compute one bit of I_k.

Since the computed VR data O_k will be transmitted after I_k being processed at the MBS, the corresponding transmission time is $t_k^{m,tr} = \frac{O_k}{BR_k}$, where B is the transmission bandwidth and R_k denotes the transmission rate between the MBS and the k-th user via the IRS, which is shown in (3).

2) User Computing Mode: In this mode, the MBS transmits the original VR data I_k to the k-th user for local computing. Denote f_k as the local computing resource at the k-th user. Thus, the transmission and local computing latency can be given by $t_k^{u,tr} = \frac{I_k}{BR_k}$ and $t_k^{u,com} = \frac{I_k F_k}{f_k}$, respectively.

Due to the limited battery at each user, the computing power consumed at the k-th user should be bounded by a maximum budget p_{max}, which is given by [1]

$$\kappa f_k^3 \leq p_{max}, \forall k \in \mathcal{K} \setminus \mathcal{K}_{mbs}, \tag{1}$$

where κ is a constant depends on the chip architecture.

As such, the latency consumed at the k-th user for completing the VR task is given by

$$\begin{aligned} t_k &= c_k(t_k^{m,tr} + t_k^{m,com}) + (1 - c_k)(t_k^{u,tr} + t_k^{u,com}) \\ &= c_k \left(\frac{O_k}{BR_k} + \frac{I_k F_k}{f_m} \right) + (1 - c_k) \left(\frac{I_k}{BR_k} + \frac{I_k F_k}{f_k} \right). \end{aligned} \tag{2}$$

B. Communication Model

We define the equivalent channels from the MBS to the IRS and from the IRS to the k-th user as $\boldsymbol{h}_m \in \mathbb{C}^{N \times 1}$ and $\boldsymbol{h}_{r,k} \in \mathbb{C}^{N \times 1}$, respectively. Thus, the achievable rate (bps/Hz) for the k-th user is given by

$$R_k = \log_2 \left(1 + \frac{p|\boldsymbol{h}_{r,k}^{\boldsymbol{H}} \mathbf{\Phi} \boldsymbol{h}_m|^2}{\sigma^2} \right), \forall k \in \mathcal{K}, \tag{3}$$

where p is the transmit power at the MBS and σ^2 is the noise power.

We consider that the CSI from the IRS to the eavesdropper $\boldsymbol{h}_e \in \mathbb{C}^{N \times 1}$ is imperfectly known, which can be characterized as $\boldsymbol{h_e} = \tilde{\boldsymbol{h_e}} + \Delta \boldsymbol{h_e}$, where $\tilde{\boldsymbol{h_e}}$ is the estimated CSI and $\Delta \boldsymbol{h_e}$ is the corresponding estimation error that is included in the continuous set Ω with a maximum uncertainty region ϵ, i.e., $\Omega \triangleq \{\Delta \boldsymbol{h_e} \in \mathbb{C}^{N \times 1} : ||\Delta \boldsymbol{h_e}|| \leq \epsilon\}$.

Since the eavesdropper cannot decompress and decode the original VR data, thus, the secrecy is perfectly guaranteed when the original VR data is transmitted, resulting in a zero eavesdropping rate, i.e., $R_{k,e} = 0, \forall k \in \mathcal{K} \setminus \mathcal{K}_{mbs}$. While for $k \in \mathcal{K}_{mbs}$, the corresponding eavesdropping rate is given by

$$\underset{\Delta \boldsymbol{h}_e \in \Omega}{R_{k,e}} = \log_2 \left(1 + \frac{p|\boldsymbol{h}_e^{\boldsymbol{H}} \mathbf{\Phi} \boldsymbol{h}_m|^2}{\sigma^2} \right), \forall k \in \mathcal{K}_{mbs}. \tag{4}$$

Based on (3) and (4), the secrecy capacity of the k-th user is given by $R_{k,sec} = [R_k - R_{k,e}]^+, \forall k \in \mathcal{K}$, where $[x]^+ \triangleq \max(x, 0)$.

III. Problem Formulation and Proposed Solution

In this letter, we aim to minimize the overall latency among all users subject to secrecy constraint. We jointly optimize the transmission policies $\boldsymbol{c}$, MBS transmit power p, IRS phase shift $\boldsymbol{\theta} \triangleq \{\theta_n, \forall n \in \mathcal{N}\}$ and computing frequency $\boldsymbol{F} \triangleq \{f_k, \forall k \in \mathcal{K} \setminus \mathcal{K}_{mbs}\}$. Thus, the optimization problem can be formulated as

$$\begin{aligned} &\underset{\boldsymbol{c}, p, \boldsymbol{\theta}, \boldsymbol{F}}{\text{minimize}} \quad \sum_{k=1}^{K} t_k && \text{(5a)} \\ &\text{s.t.} \quad \underset{\Delta \boldsymbol{h}_e \in \Omega}{R_{k,sec}} \geq R_{th}, \forall k \in \mathcal{K} && \text{(5b)} \\ &\quad |\theta_n| = 1, \forall n \in \mathcal{N} && \text{(5c)} \\ &\quad \kappa f_k^3 \leq p_{max}, \forall k \in \mathcal{K} \setminus \mathcal{K}_{mbs} && \text{(5d)} \\ &\quad 0 \leq f_k \leq f_{max}, \forall k \in \mathcal{K} \setminus \mathcal{K}_{mbs} && \text{(5e)} \\ &\quad 0 \leq p \leq p_{max}^{mbs} && \text{(5f)} \\ &\quad c_k = \{0, 1\}, \forall k \in \mathcal{K} && \text{(5g)} \\ &\quad ||\Delta \boldsymbol{h_e}|| \leq \epsilon. && \text{(5h)} \end{aligned}$$

It is worth noting that Problem (5) is non-convex since the unit-modulus constraint of the IRS phase shift variables $\boldsymbol{\theta}$ are non-convex. Moreover, the CSI uncertainty of the eavesdropper in constraint (5h) also makes Problem (5) very challenging to solve. To deal with Problem (5), we apply the AO method and solve $\boldsymbol{c}, p, \boldsymbol{\theta}, \boldsymbol{F}$ alternately.

A. Solving Transmission Policies and MBS Transmit Power

Before solving transmission policies and MBS transmit power, we first address the CSI uncertainty of the eavesdropper and derive a mathematically tractable expression of lower bound secrecy capacity . We note that $|\boldsymbol{h}_e^{\boldsymbol{H}}\boldsymbol{\Phi}\boldsymbol{h}_m| = |(\tilde{\boldsymbol{h}_e} + \Delta\boldsymbol{h_e})^{\boldsymbol{H}}\boldsymbol{\Phi}\boldsymbol{h}_m| \leq |\tilde{\boldsymbol{h}_e}^{\boldsymbol{H}}\boldsymbol{\Phi}\boldsymbol{h}_m| + |\Delta\boldsymbol{h}_e{}^{\boldsymbol{H}}\boldsymbol{\Phi}\boldsymbol{h}_m|$, where the last equality holds when

$$\arg(\tilde{\boldsymbol{h}_e}^{\boldsymbol{H}}\boldsymbol{\Phi}\boldsymbol{h}_m) = \arg(\Delta\boldsymbol{h}_e{}^{\boldsymbol{H}}\boldsymbol{\Phi}\boldsymbol{h}_m), \tag{6}$$

with $\arg(\cdot)$ represents the phase angle vector.

When $|\boldsymbol{h}_e^{\boldsymbol{H}}\boldsymbol{\Phi}\boldsymbol{h}_m| = |\tilde{\boldsymbol{h}_e}^{\boldsymbol{H}}\boldsymbol{\Phi}\boldsymbol{h}_m| + |\Delta\boldsymbol{h}_e{}^{\boldsymbol{H}}\boldsymbol{\Phi}\boldsymbol{h}_m|$, we have $|\boldsymbol{h_e^H}\boldsymbol{\Phi}\boldsymbol{h}_m|^2 = |\tilde{\boldsymbol{h_e}}^{\boldsymbol{H}}\boldsymbol{\Phi}\boldsymbol{h}_m|^2 + |\Delta\boldsymbol{h_e^H}\boldsymbol{\Phi}\boldsymbol{h}_m|^2 + 2|\tilde{\boldsymbol{h_e}}^{\boldsymbol{H}}\boldsymbol{\Phi}\boldsymbol{h}_m|(|\boldsymbol{h_e^H}\boldsymbol{\Phi}\boldsymbol{h}_m| - |\tilde{\boldsymbol{h}_e}^{\boldsymbol{H}}\boldsymbol{\Phi}\boldsymbol{h}_m|)$. To derive an upper bound of $R_{k,e}$, we consider the CSI of the eavesdropper that results in the maximum $|\Delta\boldsymbol{h_e^H}\boldsymbol{\Phi}\boldsymbol{h}_m|^2$.

Denote $\Delta h_{e,n}$ and ω_n as the magnitude and phase angle of the n-th element of $\Delta\boldsymbol{h}_e$, respectively. Thus, we have $\Delta\boldsymbol{h}_e = [|\Delta h_{e,1}|e^{j\omega_1}, |\Delta h_{e,2}|e^{j\omega_2}, \cdots, |\Delta h_{e,n}|e^{j\omega_n}]^{\boldsymbol{T}}$. We further denote $\boldsymbol{r} = \boldsymbol{\Phi}\boldsymbol{h}_m = [|r_1|e^{j\psi_1}, |r_2|e^{j\psi_2}, \cdots, |r_n|e^{j\psi_n}]^{\boldsymbol{T}}$, where r_n and ψ_n are the magnitude and phase angle of the n-th element of $\boldsymbol{r}$, respectively. Thus, $\Delta\boldsymbol{h}_e{}^{\boldsymbol{H}}\boldsymbol{\Phi}\boldsymbol{h}_m$ can be re-expressed as

$$\Delta\boldsymbol{h}_e{}^{\boldsymbol{H}}\boldsymbol{\Phi}\boldsymbol{h}_m = \Delta\boldsymbol{h}_e{}^{\boldsymbol{H}}\boldsymbol{r} = \sum_{n=1}^{N} |\Delta h_{e,n} r_n| e^{j(\psi_n - \omega_n)}. \tag{7}$$

We note that the maximum $|\Delta\boldsymbol{h}_e{}^{\boldsymbol{H}}\boldsymbol{\Phi}\boldsymbol{h}_m|$ can be achieved when phase angles of N reflecting elements are coherently combined, i.e., $\psi_1 - \omega_1 = \cdots = \psi_n - \omega_n$. With (6), the optimal phase angle that maximizes $|\Delta\boldsymbol{h}_e{}^{\boldsymbol{H}}\boldsymbol{\Phi}\boldsymbol{h}_m|$ is given by

$$\omega_n^* = \psi_n - \arg(\tilde{\boldsymbol{h}_e}^{\boldsymbol{H}}\boldsymbol{\Phi}\boldsymbol{h}_m). \tag{8}$$

Next, the magnitude part of $\Delta\boldsymbol{h}_e$ is addressed. We denote $\boldsymbol{q} = [|\Delta h_{e,1}|, |\Delta h_{e,2}|, \cdots, |\Delta h_{e,n}|]$ and $\boldsymbol{w} = [|r_1|, |r_2|, \cdots, |r_n|]$. To derive an upper bound of $R_{k,e}$, the corresponding magnitude subproblem is given as

$$\max_{\boldsymbol{q}} \quad |\boldsymbol{q}\boldsymbol{w}^{\boldsymbol{T}}|^2 \quad \text{s.t. } ||\boldsymbol{q}|| \leq \epsilon. \tag{9}$$

For Problem (9), the optimal $\boldsymbol{q}^*$ is given by [12]

$$\boldsymbol{q}^* = \epsilon\boldsymbol{w}/||\boldsymbol{w}||. \tag{10}$$

Denote $\Delta\boldsymbol{h}_e^{op}$ as the vector that results in the maximum $|\Delta\boldsymbol{h_e^H}\boldsymbol{\Phi}\boldsymbol{h}_m|^2$. Based on (8) and (10), we have $\Delta\boldsymbol{h}_e^{op} = \text{diag}[e^{j\omega_1^*}, e^{j\omega_2^*}, \cdots, e^{j\omega_n^*}]\boldsymbol{q}^{*\boldsymbol{T}}$. Thus, a lower bound secrecy capacity can be derived as

$$R_{k,sec}^{lower} = R_k - \log 2\left(1 + p|(\tilde{\boldsymbol{h}_e} + \Delta\boldsymbol{h}_e^{op})^{\boldsymbol{H}}\boldsymbol{\Phi}\boldsymbol{h}_m|^2/\sigma^2\right). \tag{11}$$

Next, we proceed to solve transmission policies and MBS transmit power. For given $\{\boldsymbol{\theta}, \boldsymbol{F}\}$, the transmission policies and MBS transmit power can be optimized by solving the following problem

$$\begin{aligned}
\underset{\boldsymbol{c},p}{\text{minimize}} \; & \sum_{k=1}^{K} c_k\left(\frac{O_k}{B\log_2(1+p\mathcal{A}_k)} + \frac{I_k F_k}{f_m}\right) \\
& + \sum_{k=1}^{K}(1-c_k)\left(\frac{I_k}{B\log_2(1+p\mathcal{A}_k)} + \frac{I_k F_k}{f_k}\right) && \text{(12a)} \\
\text{s.t. } & c_k R_{k,sec}^{lower} + (1-c_k)R_k \geq R_{th}, \forall k \in \mathcal{K} && \text{(12b)} \\
& c_k = \{0,1\}, \forall k \in \mathcal{K} && \text{(12c)} \\
& 0 \leq p \leq p_{max}^{mbs}, && \text{(12d)}
\end{aligned}$$

where $\mathcal{A}_k = |\boldsymbol{h}_{r,k}^{\boldsymbol{H}}\boldsymbol{\Phi}\boldsymbol{h}_m|^2/\sigma^2$. Since the latency for either MBS computing or user computing is inversely proportional to p, we note that the objective function in (12a) decreases with increasing p. Thus, with the aim of minimizing overall latency, the optimal MBS transmit power is given by

$$p^* = p_{max}^{mbs}. \tag{13}$$

With given p^*, we note that the optimal transmission policies are made on comparison of $t_k^m = \frac{O_k}{B\log_2(1+p\mathcal{A}_k)} + \frac{I_k F_k}{f_m}$ and $t_k^u = \frac{I_k}{B\log_2(1+p\mathcal{A}_k)} + \frac{I_k F_k}{f_k}$ with security consideration. Specifically, the MBS chooses to compute the original VR data and $c_k = 1$ if $t_k^m < t_k^u$ and $R_{k,sec}^{lower} \geq R_{th}$ are jointly satisfied, where $t_k^m < t_k^u$ corresponds to

$$p^* \geq \frac{2^{\mathcal{L}_k} - 1}{\mathcal{A}_k} \text{ where } \mathcal{L}_k = \frac{O_k - I_k}{B(\frac{I_k F_k}{f_k} - \frac{I_k F_k}{f_m})}, \tag{14}$$

since $O_k > I_k$ and MBS is equipped with sufficient computing frequency which is greater than that of local user, i.e., $f_m > f_k$, thus, $\mathcal{L}_k$ is a positive number. Moreover, the security constraint $R_{k,sec}^{lower} \geq R_{th}$ holds when

$$p^* \geq \frac{2^{R_{th}} - 1}{\mathcal{A}_k - 2^{R_{th}}\mathcal{A}_e} \text{ with } \mathcal{A}_k > 2^{R_{th}}\mathcal{A}_e, \tag{15}$$

where $\mathcal{A}_e = |(\tilde{\boldsymbol{h}_e} + \Delta\boldsymbol{h}_e^{op})^{\boldsymbol{H}}\boldsymbol{\Phi}\boldsymbol{h}_m|^2/\sigma^2$. Thus, the transmission policies are given by

$$c_k = \begin{cases} 1, & \text{if (14) and (15) are jointly satisfied} \\ 0, & \text{Otherwise.} \end{cases} \tag{16}$$

B. Solving IRS Phase Shift

With fixed $\{\boldsymbol{c}, p, \boldsymbol{F}\}$, by introducing a relaxed variable ξ as the upper bound of eavesdropper's signal-to-noise ratio (SNR), the IRS phase shift problem can be formulated as

$$\begin{aligned}
\underset{\boldsymbol{\theta},\boldsymbol{T},\xi}{\text{minimize}} \quad & \sum_{k=1}^{K} T_k && \text{(17a)} \\
\text{s.t. } & \log_2\left(1 + p|\boldsymbol{h}_{r,k}^{\boldsymbol{H}}\boldsymbol{\Phi}\boldsymbol{h}_m|^2/\sigma^2\right) \geq \frac{\mathcal{I}_{0,k}}{T_k - \mathcal{I}_{1,k}}, \forall k \in \mathcal{K} && \text{(17b)} \\
& \log_2\left(1 + p|\boldsymbol{h}_{r,k}^{\boldsymbol{H}}\boldsymbol{\Phi}\boldsymbol{h}_m|^2/\sigma^2\right) - \log_2(1+\xi) \geq R_{th}, \forall k \in \mathcal{K}_{mbs} && \text{(17c)} \\
& \log_2\left(1 + p|\boldsymbol{h}_{r,k}^{\boldsymbol{H}}\boldsymbol{\Phi}\boldsymbol{h}_m|^2/\sigma^2\right) \geq R_{th}, \forall \mathcal{K} \setminus \mathcal{K}_{mbs} && \text{(17d)} \\
& p|\boldsymbol{h}_e^{\boldsymbol{H}}\boldsymbol{\Phi}\boldsymbol{h}_m|^2/\sigma^2 \leq \xi && \text{(17e)} \\
& \text{(5c), (5h),}
\end{aligned}$$

where $\mathcal{I}_{0,k} = c_k O_k/B + (1-c_k)I_k/B$ and $\mathcal{I}_{1,k} = c_k I_k F_k/f_m + (1-c_k)I_k F_k/f_k$. Since $\mathcal{I}_{1,k}$ only represents the computing latency of the k-th user, $T_k > \mathcal{I}_{1,k}$ is guaranteed. Due to the infinitely possible CSIs at the eavesdropper in (5h) and the unit-modulus constraint in (5c), solving Problem (17) is very challenging. To tackle these issues, we let $\boldsymbol{v} = [\theta_1, \cdots, \theta_n]^{\boldsymbol{H}}, \forall n \in \mathcal{N}$. Thus, the unit-modulus constraint can be re-expressed as $|v_n|^2 = 1$. Since $\boldsymbol{h}_{r,k}^{\boldsymbol{H}}\boldsymbol{\Phi}\boldsymbol{h}_m = \boldsymbol{\Psi}_k\boldsymbol{v}$, where $\boldsymbol{\Psi}_k = \boldsymbol{h}_{r,k}^{\boldsymbol{H}}\text{diag}(\boldsymbol{h}_m)$, we have $|\boldsymbol{h}_{r,k}^{\boldsymbol{H}}\boldsymbol{\Phi}\boldsymbol{h}_m|^2 = |\boldsymbol{\Psi}_k\boldsymbol{v}|^2$. Note that $|\boldsymbol{\Psi}_k\boldsymbol{v}|^2 = \boldsymbol{\Psi}_k\boldsymbol{v}\boldsymbol{v}^{\boldsymbol{H}}\boldsymbol{\Psi}_k^{\boldsymbol{H}} = \boldsymbol{\Psi}_k\boldsymbol{V}\boldsymbol{\Psi}_k^{\boldsymbol{H}} = \text{Tr}(\boldsymbol{\Psi}_k\boldsymbol{V}\boldsymbol{\Psi}_k^{\boldsymbol{H}}) = \text{Tr}(\boldsymbol{V}\boldsymbol{\Psi}_k^{\boldsymbol{H}}\boldsymbol{\Psi}_k) = \text{Tr}(\boldsymbol{V}\boldsymbol{Q}_k)$, where $\boldsymbol{V} = \boldsymbol{v}\boldsymbol{v}^{\boldsymbol{H}}$ which needs to satisfy $\boldsymbol{V} \succeq 0$ and $\text{rank}(\boldsymbol{V}) = 1$. Moreover, $\boldsymbol{Q}_k = \boldsymbol{\Psi}_k^{\boldsymbol{H}}\boldsymbol{\Psi}_k$.

Similarly, with $\boldsymbol{h}_e^{\boldsymbol{H}}\boldsymbol{\Phi}\boldsymbol{h}_m = \boldsymbol{h}_e^{\boldsymbol{H}}\text{diag}(\boldsymbol{h}_m)\boldsymbol{v}$, (17e) can be transformed as

$$\boldsymbol{h}_e^{\boldsymbol{H}}\text{diag}(\boldsymbol{h}_m)\boldsymbol{V}\text{diag}(\boldsymbol{h}_m)^{\boldsymbol{H}}\boldsymbol{h}_e \leq \mathcal{I}_3 = \xi\sigma^2/p. \tag{18}$$

To address the CSI uncertainty of the eavesdropper, similar to [12], [15], we adopt the **S**-Procedure method to transform constraints (5h) and (18) into linear matrix inequalities (LMIs) with following lemma.

Lemma 1. *Define a function $g_k(x), k \in \{1, 2\}, x \in \mathbb{C}^{N\times 1}$ as*

$$g_k(x) = x^{\boldsymbol{H}} \boldsymbol{D}_k x + 2Re\{\boldsymbol{q}_k^{\boldsymbol{H}} x\} + r_k, \tag{19}$$

where $\boldsymbol{D}_k \in \mathbb{H}^N$, $\boldsymbol{q}_k \in \mathbb{C}^{N\times 1}$, and $r_k \in \mathbb{R}^{1\times 1}$. Then, the implication $g_1(x) \le 0 \Rightarrow g_2(x) \le 0$ holds if and only if there exists a $\eta \ge 0$ such that

$$\eta \begin{bmatrix} \boldsymbol{D}_1 & \boldsymbol{q}_1 \\ \boldsymbol{q}_1^{\boldsymbol{H}} & r_1 \end{bmatrix} - \begin{bmatrix} \boldsymbol{D}_2 & \boldsymbol{q}_2 \\ \boldsymbol{q}_2^{\boldsymbol{H}} & r_2 \end{bmatrix} \succeq 0, \tag{20}$$

provided that there exists a point $\hat{x}$ such that $f_k(\hat{x}) < 0$.

As such, after several mathematical manipulations, we first rewrite (5h) and (18) as

$$(5h) \Rightarrow \Delta\boldsymbol{h}_e^{\boldsymbol{H}} \Delta\boldsymbol{h}_e - \epsilon^2 \le 0 \tag{21a}$$

$$(18) \Rightarrow \Delta\boldsymbol{h}_e^{\boldsymbol{H}} \boldsymbol{S} \Delta\boldsymbol{h}_e + 2\text{Re}\{\tilde{\boldsymbol{h}}_e^{\boldsymbol{H}} \boldsymbol{S} \Delta\boldsymbol{h}_e\} + \tilde{\boldsymbol{h}}_e^{\boldsymbol{H}} \boldsymbol{S} \tilde{\boldsymbol{h}}_e - \mathcal{I}_3 \le 0, \tag{21b}$$

where $\boldsymbol{S} = \text{diag}(\boldsymbol{h}_m)\boldsymbol{V}\text{diag}(\boldsymbol{h}_m)^{\boldsymbol{H}}$.

By applying Lemma 1, constraints (21a) and (21b) can be transformed as

$$\begin{bmatrix} \eta \boldsymbol{I}_N & \boldsymbol{0}^{N\times 1} \\ \boldsymbol{0}^{1\times N} & -\eta\epsilon^2 + \mathcal{I}_3 \end{bmatrix} - \begin{bmatrix} \boldsymbol{S} & \boldsymbol{S}^{\boldsymbol{H}} \tilde{\boldsymbol{h}}_e \\ \tilde{\boldsymbol{h}}_e^{\boldsymbol{H}} \boldsymbol{S} & \tilde{\boldsymbol{h}}_e^{\boldsymbol{H}} \boldsymbol{S} \tilde{\boldsymbol{h}}_e \end{bmatrix} \succeq 0, \tag{22}$$

where $\boldsymbol{I}_N$ denotes a $N \times N$ identity matrix.

Thus, by relaxing the rank-one constraint rank$(\boldsymbol{V}) = 1$, the IRS phase shift subproblem can be reformulated as

$$\underset{\boldsymbol{V},\boldsymbol{T},\xi,\eta}{\text{minimize}} \quad \sum_{k=1}^{K} T_k \tag{23a}$$

$$\text{s.t.} \quad p\text{Tr}(\boldsymbol{V}\boldsymbol{Q}_k)/\sigma^2 \ge 2^{\frac{\mathcal{I}_{0,k}}{T_k - \mathcal{I}_{1,k}}} - 1, \forall k \in \mathcal{K} \tag{23b}$$

$$p\text{Tr}(\boldsymbol{V}\boldsymbol{Q}_k)/\sigma^2 \ge 2^{R_{th}}(1+\xi) - 1, \forall k \in \mathcal{K}_{mbs} \tag{23c}$$

$$p\text{Tr}(\boldsymbol{V}\boldsymbol{Q}_k)/\sigma^2 \ge 2^{R_{th}} - 1, \forall k \in \mathcal{K} \setminus \mathcal{K}_{mbs} \tag{23d}$$

$$[\boldsymbol{V}]_{n,n} = 1, \forall n \in \mathcal{N} \tag{23e}$$

$$\boldsymbol{V} \succeq 0 \tag{23f}$$

$$(22).$$

It can be easily verified that Problem (23) is a semi-definite programming (SDP) problem which can be solved by standard convex optimization solvers with a complexity of $\mathcal{O}\left(\lceil \frac{\log(N/t^0\chi)}{\log(\iota)} \rceil \left(\frac{N(\iota - 1\log(\iota))}{\gamma} + l\right)\right)$, where $\{t^0, \iota, \gamma, l\}$ are parameters which are set to guarantee the precision and χ is the accepted duality gap [7]. We note that the optimal $\boldsymbol{V}$ in (23) is not guaranteed to be rank-one in general. To tackle this issue, we apply the similar randomization process as [6], [7] to extract the suboptimal rank-one solution and thus omitted here for brevity.

C. Solving Computing Frequency

We note that the objective function (5a) is inversely proportional to f_k. With the aim of minimizing latency, the optimal computing frequency at the k-th user is either bounded by the power constraint (5d) or the computing frequency constraint (5e), which is given by

$$f_k^* = \min\left(\sqrt[3]{\frac{p_{max}}{\kappa}}, f_{max}\right). \tag{24}$$

D. Proposed Latency Minimization Algorithm

We summarize the proposed latency minimization solution in Algorithm 1, where all variables are optimized alternately until convergence. We note that the complexity of Algorithm 1 is dominated by solving IRS phase shift, which can be given as $\mathcal{O}\left(\lceil \frac{\log(N/t^0\chi)}{\log(\iota)} \rceil \left(\frac{N(\iota - 1\log(\iota))}{\gamma} + l\right)\right)$.

Algorithm 1 Proposed Latency Minimization Algorithm

initialize: Set $\{\boldsymbol{c}^0, p^0, \boldsymbol{\theta}^0, \boldsymbol{F}^0\}$ and $t = 1$.
repeat
  Given $\{\boldsymbol{\theta}^{t-1}, \boldsymbol{F}^{t-1}\}$, solving MBS transmit power p^t and transmission policies $\boldsymbol{c}^t$ based on (13) and (16), respectively;
  Given $\{\boldsymbol{c}^t, p^t, \boldsymbol{F}^{t-1}\}$, solving IRS phase shift $\boldsymbol{\theta}^t$ based on (23);
  Given $\{\boldsymbol{c}^t, p^t, \boldsymbol{\theta}^t\}$, solving computing frequency $\boldsymbol{F}^t$ based on (24);
  Update the iterative number $t = t + 1$;
until convergence.

IV. Simulation Results

In this section, numerical results are provided to validate the effectiveness of our proposed algorithm. We consider $K = 4$ users that are distributed randomly on a circle centered at $(0, 0)$ with radius 5 m while the MBS and the eavesdropper are located at $(100, 0)$ and $(-30, 0)$, respectively. The IRS with $N = 16$ elements is deployed at $(50, 10)$. We generate the entries of $\boldsymbol{h}_{r,k}, \boldsymbol{h}_m, \boldsymbol{h}_e$ independently from a Rician distribution with Rician factor 5. The large-scale path loss is $-30 - 10\alpha\log_{10}(d)$ dB, where α is the path loss factor and d is the distance in meters. The CSI error bound is set as $\epsilon = 10\%||\tilde{\boldsymbol{h}}_{\boldsymbol{e}}||$. The path loss factors for all channels are set as $\alpha_{r,k} = \alpha_m = \alpha_e = 2.2$. We set the computing frequency at the MBS as $f_m = 2$ GHz. The maximum computing frequency and power budget at each user are set as $f_{max} = 0.8$ GHz and $p_{max} = 0.6$ W. We set $\kappa = 10^{-27}$ and $p_{max}^{mbs} = 1$ W. The volume of original VR data follows $I_k \sim U[20, 50]$ KB and the ratio between O and I is set as $\beta_k \sim U[2, 3]$. Moreover, $F_k \sim U[500, 800]$ cycles/bit. We set the transmission bandwidth and noise power as $B = 2$ MHz and $\sigma^2 = -100$ dBm, respectively. The minimum secrecy capacity is set as $R_{th} = 2$ bps/Hz. Initially, we set $p^0 = 0.05$ W, $f_k^0 = \min\left(\sqrt[3]{\frac{p_{max}}{\kappa}}, f_{max}\right)$, $\theta_n^0 = 1, \forall n \in \mathcal{N}$ and $c_k^0 = 1$ when the initial secrecy capacity constraint at the k-th user is satisfied. For comparison, two benchmark schemes are considered as follows: 1) "All local computing": All users execute their original VR data locally and all other variables are optimized using Algorithm 1; 2) "Fixed IRS phase shift": We set $\theta_n = 1, \forall n \in \mathcal{N}$ and all other variables are optimized using Algorithm 1.

The convergence of Algorithm 1 is shown in Fig. 2 by plotting the latency versus number of iterations with different

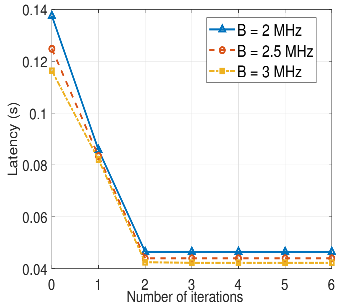

Fig. 2. Latency versus number of iterations

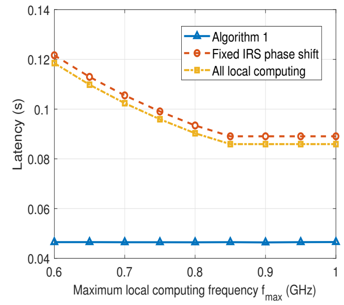

Fig. 3. Latency versus maximum local computing frequency f_{max}.

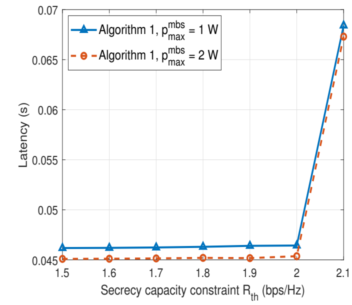

Fig. 4. Latency versus minimum secrecy capacity R_{th}

bandwidth B. It can be seen that our proposed algorithm quickly converges to a minimum latency within six iterations when B ranges from 2 MHz to 3 MHz. When $B = 2$ MHz, the latency reduces 65.94% from 0.138 s to 0.047 s by adopting proposed Algorithm 1, which verifies the effectiveness of our proposed solution.

Fig. 3 compares Algorithm 1 and other baseline schemes in reducing latency with a wide range of f_{max}. Several interesting observations can be found in Fig. 3. First, we observe that our proposed Algorithm 1 achieves the minimum latency among all strategies. Moreover, the latency of our proposed algorithm 1 keeps unchanged when f_{max} varies. This is because with our proposed joint optimization solution, the secrecy capacity constraint for all users are satisfied and $c_k = 1, \forall k \in \mathcal{K}$, resulting in an unchanged latency when f_{max} varies. We also observe that the latency of benchmark schemes decreases when f_{max} ranges from 0.6 GHz to 0.85 GHz since some users have to compute their original VR data locally caused by the security constraint. When f_{max} increases from 0.85 GHz to 1 GHz, the latency of two benchmark schemes keeps unchanged since the local computing frequency is bounded by the more strict power constraint.

Fig. 4 shows the relation between latency and minimum secrecy capacity constraint R_{th} with different maximum MBS transmit power p_{max}^{mbs} by adopting Algorithm 1. Interestingly, we observe that the latency increases with the increase of R_{th} and the remarkable jump point, i.e., when $R_{th} = 2.1$ bps/Hz, corresponds to an increase in the number of local computing user. Specifically, when $p_{max}^{mbs} = 1$ W, the original VR data of all users is computed at the MBS when R_{th} ranges from 1.5 bps/Hz to 2 bps/Hz. While when R_{th} increases to 2.1 bps/Hz, only two users satisfy the strict security constraint and the other two users have to compute their original VR data locally, resulting in an increased latency since the computing frequency at each user is limited. We also observe that increasing the feasible range of MBS transmit power is helpful to reduce latency when the number of local computing user is unchanged.

V. Conclusions

We proposed a new secure IRS-enhanced VR delivery framework to minimize the latency subject to security constraint by jointly optimizing the transmission policies, MBS transmit power, IRS phase shift and computing frequency. Numerical results confirmed that our proposed algorithm outperforms baseline schemes and highlighted a trade-off between the latency and security in IRS-enhanced VR delivery systems.

References

[1] Y. Zhou, C. Pan, P. L. Yeoh, K. Wang, M. Elkashlan, B. Vucetic, and Y. Li, "Secure Communications for UAV-Enabled Mobile Edge Computing Systems," in *IEEE Trans. Commun.,* vol. 68, no. 1, pp. 376-388, Jan. 2020.

[2] Y. Zhang, B. Di, P. Wang, J. Lin, and L. Song, "HetMEC: Heterogeneous Multi-Layer Mobile Edge Computing in the 6G Era," in *IEEE Trans. Veh. Technol.* vol. 69, no. 4, pp. 4388-4400, April 2020.

[3] Y. Sun, Z. Chen, M. Tao, and H. Liu, "Communications, Caching, and Computing for Mobile Virtual Reality: Modeling and Tradeoff," in *IEEE Trans. Commun.,* vol. 67, no. 11, pp. 7573-7586, Nov. 2019.

[4] Y. Zhou, C. Pan, P. L. Yeoh, K. Wang, M. Elkashlan, B. Vucetic, and Y. Li, "Communication-and-Computing Latency Minimization for UAV-Enabled Virtual Reality Delivery Systems," in *IEEE Trans. Commun.,* vol. 69, no. 3, pp. 1723-1735, March 2021.

[5] Q. Wu and R. Zhang, "Intelligent Reflecting Surface Enhanced Wireless Network via Joint Active and Passive Beamforming," in *IEEE Trans. Wireless Commun.,* vol. 18, no. 11, pp. 5394-5409, Nov. 2019.

[6] W. Yan, X. Yuan, and X. Kuai, "Passive Beamforming and Information Transfer via Large Intelligent Surface," in *IEEE Wireless Commun. Lett.,* vol. 9, no. 4, pp. 533-537, April 2020.

[7] Z. Ma, Y. Wu, M. Xiao, G. Liu, and Z. Zhang, "Interference Suppression for Railway Wireless Communication Systems: A Reconfigurable Intelligent Surface Approach," in *IEEE Trans. Veh. Technol.* vol. 70, no. 11, pp. 11593-11603, Nov. 2021

[8] M. Zeng, X. Li, G. Li, W. Hao, and O. A. Dobre, "Sum Rate Maximization for IRS-Assisted Uplink NOMA," in *IEEE Commun. Lett.,* vol. 25, no. 1, pp. 234-238, Jan. 2021.

[9] G. Zhou, C. Pan, H. Ren, K. Wang, M. D. Renzo and A. Nallanathan, "Robust Beamforming Design for Intelligent Reflecting Surface Aided MISO Communication Systems," in *IEEE Wireless Commun. Lett.,* vol. 9, no. 10, pp. 1658-1662, Oct. 2020.

[10] T. Bai, C. Pan, Y. Deng, M. Elkashlan, A. Nallanathan, and L. Hanzo, "Latency Minimization for Intelligent Reflecting Surface Aided Mobile Edge Computing," in *IEEE J. Sel. Areas Commun.,* vol. 38, no. 11, pp. 2666-2682, Nov. 2020.

[11] Y. Zhou, P. L. Yeoh, H. Chen, Y. Li, R. Schober, L. Zhuo, and B. Vucetic, "Improving physical layer security via a UAV friendly jammer for unknown eavesdropper location," in *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 11280-11284, Nov 2018.

[12] S. Li, B. Duo, M. D. Renzo, M. Tao, and X. Yuan, "Robust Secure UAV Communications With the Aid of Reconfigurable Intelligent Surfaces," in *IEEE Trans. Wireless Commun.,* vol. 20, no. 10, pp. 6402-6417, Oct. 2021.

[13] M. Cui, G. Zhang, and R. Zhang, "Secure Wireless Communication via Intelligent Reflecting Surface," in *IEEE Wireless Commun. Lett.,* vol. 8, no. 5, pp. 1410-1414, Oct. 2019.

[14] J. Zhang et al., "Energy-Latency Tradeoff for Energy-Aware Offloading in Mobile Edge Computing Networks," in *IEEE Internet Things J.,* vol. 5, no. 4, pp. 2633-2645, Aug. 2018.

[15] D. W. K. Ng, E. S. Lo, and R. Schober, "Robust Beamforming for Secure Communication in Systems With Wireless Information and Power Transfer," in *IEEE Trans. Wireless Commun.,* vol. 13, no. 8, pp. 4599-4615, Aug. 2014.