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.

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).

In [10], an efficient algorithm was designed to reduce the computational latency in an IRS-assisted MEC network. 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 $\mathbf{x}$, $\mathbf{x}^T$, $\mathbf{x}^H$ and $\text{diag}(\mathbf{x})$ represent its transpose, Hermitian transpose and diagonalization, respectively. For a matrix $\mathbf{M}$, $\text{rank}(\mathbf{M})$, $\mathbf{M}_{i,j}$ and $\text{Tr}(\mathbf{M})$ denote its rank, the $(i,j)\text{th}$ element and trace, respectively.

![Fig. 1. An IRS-enhanced secure VR delivery system.](image)
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 \( K \) and \( \mathcal{N} \), respectively. Let \( \Phi = \text{diag}\{\theta\} \) denote the diagonal phase shift matrix for the IRS, where \( \theta = [e^{j\pi_1}, e^{j\pi_2}, \ldots, e^{j\pi_N}] \) and \( |\theta_n| = |e^{j\pi_n}| = 1, \forall n \in \mathcal{N} \).

We denote \( I_k \) and \( R_k \) 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 \( \beta_k = \frac{O_k}{T_k} \geq 2 \) in order to create a stereoscopic vision [3, 4].

We denote \( c \triangleq \{c_k, \forall k \in K\} \) 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 \( \mathcal{K}_{\text{mbs}} = \{c_k = 1, \forall k \in K\} \) as the set of users whose computed VR data will be transmitted from the MBS and \( \mathcal{K}_{\text{mbs}} \) as the size of set \( \mathcal{K}_{\text{mbs}} \).

\section*{A. Computing Model}

\subsection*{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 \( t_{k,m,\text{com}}^{\text{m,com}} = \frac{I_k F_k}{F_k} \), 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 \( t_{k,m,\text{tr}}^{\text{m,com}} = \frac{O_k}{B R_k} \), 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).

\subsection*{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 \( t_{k,m,\text{tr}}^{\text{u,com}} = \frac{I_k F_k}{B R_k} \) and \( t_{k,m,\text{com}}^{\text{u,com}} = \frac{I_k F_k}{f_k} \), 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 \( p_{\text{max}} \), which is given by [1]

\[ \kappa f_k \leq p_{\text{max}}, \forall k \in K \setminus \mathcal{K}_{\text{mbs}}, \]

where \( \kappa \) 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

\[ t_k = c_k (t_{k,m,\text{tr}}^{\text{m,com}} + t_{k,m,\text{tr}}^{\text{u,com}}) + (1 - c_k) (t_{k,m,\text{tr}}^{\text{u,com}} + t_{k,m,\text{com}}^{\text{u,com}}) \]

\[ = c_k \left( \frac{O_k}{B R_k} + \frac{I_k F_k}{B R_k} \right) + (1 - c_k) \left( \frac{I_k F_k}{f_k} + \frac{I_k F_k}{f_k} \right). \]

\section*{B. Communication Model}

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

\[ R_k = \log_2 \left( 1 + \frac{p |h_{r,k}^H \Phi h_m|^2}{\sigma^2} \right), \forall k \in K, \]

where \( p \) is the transmit power at the MBS and \( \sigma^2 \) is the noise power.

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

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., \( R_{k,e} = 0, \forall k \in K \setminus \mathcal{K}_{\text{mbs}} \). While for \( k \in \mathcal{K}_{\text{mbs}} \), the corresponding eavesdropping rate is given by

\[ R_{k,e} = \log_2 \left( 1 + \frac{p |h_{r,k}^H \Phi h_m|^2}{\sigma^2} \right), \forall k \in K_{\text{mbs}}. \]

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

\section*{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 \( c \), MBS transmit power \( p \), IRS phase shift \( \theta \triangleq \{\theta_n, \forall n \in N\} \) and computing frequency \( F \triangleq \{f_k, \forall k \in K \setminus \mathcal{K}_{\text{mbs}}\} \). Thus, the optimization problem can be formulated as

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

It is worth noting that Problem (5) is non-convex since the unit-modulus constraint of the IRS phase shift variables \( \theta \) 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 \( c, p, \theta, F \) alternately.

\section*{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 $|h_e^H \Phi \Phi_m| = |\hat{h}_e + \Delta h_e^H \Phi \Phi_m| \leq |\hat{h}_e^H \Phi \Phi_m| + |\Delta h_e^H \Phi \Phi_m|$, where the last equality holds when

$$\arg(\hat{h}_e^H \Phi \Phi_m) = \arg(\Delta h_e^H \Phi \Phi_m),$$

(6)

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

When $|h_e^H \Phi \Phi_m| = |\hat{h}_e^H \Phi \Phi_m| + |\Delta h_e^H \Phi \Phi_m|$, we have $|h_e^H \Phi \Phi_m|^2 = |\hat{h}_e^H \Phi \Phi_m|^2 + |\Delta h_e^H \Phi \Phi_m|^2 + 2|\hat{h}_e^H \Phi \Phi_m||\Delta h_e^H \Phi \Phi_m|(\hat{h}_e^H \Phi \Phi_m - \hat{h}_e^H \Phi \Phi_m)$.

Denote $\Delta h_e, \omega_n$ as the magnitude and phase angle of the n-th element of $\Delta h_e$, respectively. Thus, we have $\Delta h_e = [\Delta h_{e,1}, \Delta h_{e,2}, \cdots, \Delta h_{e,n}]$. We further denote $r = \Phi \Phi_m = [r_1, r_2, \cdots, r_n]$. To derive an upper bound of $R_{k,e}$, the corresponding magnitude subproblem is given as

$$\Delta h_e^H \Phi \Phi_m = \Delta h_e^H r = \sum_{n=1}^{N} |\Delta h_{e,n} r_n| e^{j(\omega_n - \omega_n)}.$$  (7)

We note that the maximum $|\Delta h_e^H \Phi \Phi_m|$ 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 $|\Delta h_e^H \Phi \Phi_m|$ is given by

$$\omega_n^* = \psi_n - \arg(\hat{h}_e^H \Phi \Phi_m).$$

(8)

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

$$\max_q |qw|^2$$

s.t. $|q| \leq \epsilon$.  (9)

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

$$q^* = \epsilon w/||w||.$$  (10)

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

$$R_{k,sec} = R_k - \log(1 + p|\hat{h}_e + \Delta h^{op})^H \Phi \Phi_m|/\sigma^2).$$  (11)

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

$$\min_{\theta, F} \sum_{k=1}^{K} T_k$$

s.t. $\log_2 \left(1 + p|h_{r,k}^H \Phi \Phi_m|^2/\sigma^2\right) \geq \frac{J_{0,k}}{T_k - J_{1,k}}$, $\forall k \in K$  (17a)

$$\log_2 \left(1 + p|h_{r,k}^H \Phi \Phi_m|^2/\sigma^2\right) - \log_2(1 + \xi) \geq R_{th, k}, \forall k \in K_{mbs}$$.  (17b)

$$\log_2 \left(1 + p|h_{r,k}^H \Phi \Phi_m|^2/\sigma^2\right) \geq R_{th, k}, \forall k \in K_{mbs}$$.  (17c)

$$\xi = p|h_{r,k}^H \Phi \Phi_m|^2/\sigma^2 \leq \xi$$

(5c), (5h).

where $J_{0,k} = c_k O_k / B + (1 - c_k)I_k / B$ and $J_{1,k} = c_k I_k F_k / f_m + (1 - c_k) I_k F_k / f_k$. Since $J_{1,k}$ only represents the computing latency of the k-th user, $T_k > J_{1,k}$ 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 $v = [\theta_1, \cdots, \theta_n]$, $\forall n \in N$. Thus, the unit-modulus constraint can be re-expressed as $v_n = 1$. Since $h_{r,k}^H \Phi \Phi_m = \Psi_{k} \nu$, where $\Psi_{k} = h_{r,k}^H \Phi \Phi_m$, we have $|h_{r,k}^H \Phi \Phi_m|^2 = |\Psi_{k} \nu|^2$.

Note that $|\Psi_{k} \nu|^2 = \Psi_{k} \nu \Psi_{k}^H |\Psi_{k} \nu|^2 = \text{Tr}(V \Psi_{k}^H \Psi_{k}) = \text{Tr}(V Q_k)$, where $V = \nu \nu^H$ which needs to satisfy $V \geq 0$ and rank$(V) = 1$. Moreover, $Q_k = \Psi_{k} \Psi_{k}^H$.

Similarly, with $h_{e}^H \Phi \Phi_m = h_{e}^H \Phi \Phi_m$, (17e) can be transformed as

$$h_{e}^H \Phi \Phi_m \leq I_3 = \frac{\xi \sigma^2}{p}.$$  (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
\[
g_k(x) = x^H D_k x + 2 \text{Re} \{ q_k^H e \} + r_k,
\]
where \( D_k \in \mathbb{H}^N \), \( q_k \in \mathbb{C}^{N \times 1} \), and \( r_k \in \mathbb{R}^{1 \times 1} \). Then, the implication \( g_1(x) \leq 0 \) \( \Rightarrow \) \( g_2(x) \leq 0 \) holds if and only if there exists a \( \eta \geq 0 \) such that
\[
\eta \begin{bmatrix} D_1 & q_1 \\ q_1^H & r_1 \end{bmatrix} - \begin{bmatrix} D_2 & q_2 \\ q_2^H & r_2 \end{bmatrix} \succeq 0,
\]
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
\[
\begin{align*}
\text{(5h)} & \Rightarrow \Delta h_e^H \Delta h_e - e^2 \leq 0 \quad (21a) \\
\text{(18)} & \Rightarrow \Delta h_e^H S \Delta h_e + 2 \text{Re} \{ h_e^H S \Delta h_e \} + \hat{h}_e^H S \hat{h}_e - I_3 \leq 0, \quad (21b)
\end{align*}
\]
where \( S = \text{diag}(h_m)^V \text{diag}(h_m)^H \).

By applying Lemma 1, constraints (21a) and (21b) can be transformed as
\[
\begin{bmatrix} \eta I_N & 0_{N \times 1} \\ 0_{1 \times N} & -\eta e^2 + I_3 \end{bmatrix} - \begin{bmatrix} S & S^H \hat{h}_e \\ \hat{h}_e^H S - \hat{h}_e^H S \hat{h}_e \end{bmatrix} \succeq 0,
\]
where \( I_x \) denotes a \( N \times N \) identity matrix.

Thus, by relaxing the rank-one constraint rank(\( V \)) = 1, the IRS phase shift subproblem can be reformulated as
\[
\begin{align}
\text{minimize} & \quad \sum_{k=1}^K T_k \\
\text{s.t.} & \quad p \text{Tr}(V Q_k) / \sigma^2 \geq 2 \frac{\sigma_{\nu k}}{\nu + 1}, \forall k \in K \quad (23b) \\
& \quad p \text{Tr}(V Q_k) / \sigma^2 \geq 2 R_{th}(1 + \gamma) - 1, \forall k \in K_{\text{mbs}} \quad (23c) \\
& \quad p \text{Tr}(V Q_k) / \sigma^2 \geq 2 R_{th} - 1, \forall k \in K \setminus K_{\text{mbs}} \quad (23d) \\
& \quad |V|_{n,n} = 1, \forall n \in N \quad (23e) \\
& \quad V \succeq 0 \quad (23f).
\end{align}
\]

It can be easily verified that Problem (23) is a semi-definite programming (SDP) problem which can be solved by standard convex optimization solvers. The complexity of the optimization problem is given by \( O \left( \left( \log(N/f_{\text{max}}) \right)^2 \right) \), where \( \{\theta^0, \theta^1, \gamma, l\} \) are parameters which are set to guarantee the precision and \( \gamma \) is the accepted duality gap [7]. We note that the optimal \( V \) 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
\[
f^*_k = \min \left\{ \sqrt{\frac{p_{\text{max}}}{k}}, f_{\text{max}} \right\}.
\]

### 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 \( O \left( \frac{\log(N/q^0)}{\log(1)} \right) \left( \frac{(N - 1) \log(c_i)}{\gamma} + l \right) \).

**Algorithm 1** Proposed Latency Minimization Algorithm

1: initialize: Set \( \{e^0, p^0, \theta^0, F^0\} \) and \( t = 1 \).
2: repeat
3: \quad Given \( \{\theta^{t-1}, F^{t-1}\} \), solving MBS transmit power \( p^t \) and transmission policies \( c^t \) based on (13) and (16), respectively;
4: \quad Given \( \{c^t, p^t, F^{t-1}\} \), solving IRS phase shift \( \theta^t \) based on (23);
5: \quad Given \( \{c^t, p^t, F^t\} \), solving computing frequency \( F^t \) based on (24);
6: \quad Update the iterative number \( t = t + 1 \);
7: 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 \( h_{e,k}, h_{m,k}, h_{e} \) independently from a Rician distribution with Rician factor 5. The large-scale path loss is \( -30 - 10 \alpha \log_{10}(d) \) dB, where \( \alpha \) is the path loss factor and \( d \) is the distance in meters. The CSI error bound is set as \( \epsilon = 10\% \| h_{e} \| \). The path loss factors for all channels are set as \( \alpha_{e,k} = \alpha_m = \alpha_e = 2.2 \). 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 \( f_{\text{max}} = 0.8 \) GHz and \( p_{\text{max}} = 0.6 \) W. We set \( \kappa = 10^{-27} \) and \( p_{\text{mbs}}^0 = 1 \) W. The volume of original VR data follows \( L_k \sim U[20, 50] \) 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 maximum secrecy capacity is set as \( R_{th} = 2 \) bps/Hz. Initially, we set \( p^0 = 0.05 \) W, \( f^0_k = \min \left\{ \sqrt{\frac{p_{\text{max}}}{k}}, f_{\text{max}} \right\}, \theta^0_n = 1, \forall n \in N \) and \( c^0_k = 1 \) 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 \( \theta_n = 1, \forall n \in N \) 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
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 $c_k = 1, \forall k \in K$, 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**


