Computer Modeling in Engineering & Sciences

Tech Science Press

DOI: 10.32604/cmes.2023.029234

ARTICLE

IRS Assisted UAV Communications against Proactive Eavesdropping in Mobile Edge Computing Networks

Ying Zhang[1,*], Weiming Niu[2] and Leibing Yan[1]

[1]School of Electronic Information Engineering, Henan Institute of Technology, Xinxiang, 453003, China

[2]Houde College, Henan Institute of Technology, Xinxiang, 453003, China

*Corresponding Author: Ying Zhang. Email: zhangyingnssc@163.com

Received: 08 February 2023 Accepted: 27 April 2023 Published: 22 September 2023

ABSTRACT

In this paper, we consider mobile edge computing (MEC) networks against proactive eavesdropping. To maximize the transmission rate, IRS assisted UAV communications are applied. We take the joint design of the trajectory of UAV, the transmitting beamforming of users, and the phase shift matrix of IRS. The original problem is strong non-convex and difficult to solve. We first propose two basic modes of the proactive eavesdropper, and obtain the closed-form solution for the boundary conditions of the two modes. Then we transform the original problem into an equivalent one and propose an alternating optimization (AO) based method to obtain a local optimal solution. The convergence of the algorithm is illustrated by numerical results. Further, we propose a zero forcing (ZF) based method as sub-optimal solution, and the simulation section shows that the proposed two schemes could obtain better performance compared with traditional schemes.

KEYWORDS

Mobile edge computing (MEC); unmanned aerial vehicle (UAV); intelligent reflecting surface (IRS); zero forcing (ZF)

1 Introduction

With the development of communication technology, security issues have received more attention [1–3]. Due to the broadcast characteristics of wireless channel, the information transmitted can be easily obtained by non target users [4–6]. Due to its unique advantages, namely mobility and flexibility, UAV communication plays a very important role in supporting safe communication. Where traditional base stations cannot cover, UAVs can use their flexibility to provide more effective services [7,8].

Traditional physical layer security technologies focus on improving the confidentiality of received information [9,10], for example, by changing the coding method, using redundant information in the coding to check and interfere, or changing the amplitude and phase of the transmission signal to carry additional information [11–13]. Physical layer security technology can improve the security transmission rate of information through pre-designed policies. In recent years, researchers have become more and more aware of possible eavesdroppers in communication scenarios [14–16]. More and more eavesdroppers are studying physical layer security technology. At this time, the ability of the

eavesdropper is limited to (1) eavesdropping channel; (2) the transmission rate of the sender. As the research on security continues to expand, eavesdroppers have more forms.

However, the security of communication does not only include the above parts, but also the ability of eavesdroppers is evolving. In recent research, the concept of active monitoring was first proposed in [17,18], which aimed to improve the eavesdropping rate through the transmission of Gaussian noise by the eavesdropper; Huang et al. [19] further proposed that the eavesdropper can choose to send Gaussian noise to improve its eavesdropping ability. For the situation of the above intelligent eavesdroppers, a lot of research has not been carried out to counter them [20,21].

IRS is a passive device, which can reconstruct the sender's signal and enhance or weaken the specific user by changing the channel parameters [22,23]. Because of the excellent characteristics of IRS, it has been widely used and studied in secure communication. For example, in [24], the authors proposed to use IRS to assist multi-user communication. By designing the transmission beam and IRS phase shift matrix, the minimum secrecy rate among users was improved. In [25], the authors considered that the IRS would recode the new source transmission signal, that is, the user's receiving rate and the eavesdropper's receiving rate could be improved at the same time, it broken through the traditional upper bound of safe rate [26,27].

IRS assisted UAV communication also has a wide range of application scenarios. When UAV is used as air base station, IRS can be used as a ground equipment to improve the effective speed between UAV and users; When the UAV is used as a relay, the communication rate can be improved by adjusting the flight path of the UAV and the phase shift matrix of the IRS.

In this paper, we consider using IRS assisted UAVs to promote the safe communication of ground users. The specific contributions of this paper are as follows:

1. We consider the security in mobile edge computing. We use the IRS auxiliary computing tasks carried by UAV to unload, with the goal of reducing the system delay on the premise of ensuring safe transmission.
2. We preset the working mode of the eavesdropper and propose to control the eavesdropper's transmitting beam in the form of maximum ratio transmission through the joint design of the transmitting beam of the base station, the flight path of the UAV, and the phase shift matrix of the IRS.
3. We propose an algorithm based on interior point method and alternate optimization, and propose a sub-optimal scheme based on zeroing method with low complexity.
4. In the simulation section, we set a communication environment based on Rayleigh channel, and the positions of users and eavesdroppers are randomly set in each simulation. Simulation results show that the proposed scheme can effectively reduce the latency of mobile edge computing.

In the second section, we establish the original optimization problem; In the third section, we first estimate the transmission strategy of the eavesdropper, and transform the original optimization problem; In the fourth section, we solve the transformed optimization problem and obtain the design scheme by using the interior point method and alternative optimization; In the fifth section, we carry out the simulation experiments, and then the sixth chapter summarizes the full text.

2 System Model and Problem Formulation

In this section, we first introduce the system model, then take the secrecy rate as our optimization goal, and establish the original optimization problem.

2.1 System Model

We consider that the system consists of one user, one proactive eavesdropper, a UAV and an IRS. As shown in Fig. 1, the user and the eavesdropper are both equipped with multi-antennas. For the sake of generality, we assume that the channel between UAV and ground users is the superposition of LOS channel and NLOS channel. The IRS contains N IRS elements, each of which can be designed independently to change the channel of the IRS to the user; It is worth noting that the information transmitted by the UAV to each ground user is dual: the UAV itself will forward signals from the user; The IRS will also reflect the signal. The specific expression is proposed as follows:

$$\mathbf{y}_u = \left(\mathbf{h}_u^H + \mathbf{h}_{iu}^H\right)\mathbf{w}, \tag{1}$$

where $\mathbf{y}_u$ refers to the signal received at UAV. $\mathbf{h}_u$ and $\mathbf{h}_{iu}$ specifically represent the direct channels from user to UAV and the reflecting link, which defined as follows:

$$\mathbf{h}_u = \alpha_e P_{LOS}\mathbf{h}_{LOS} + (1-\alpha_e)P_{LOS}\mathbf{h}_{LOS}, \tag{2}$$

$$\mathbf{h}_{iu} = \mathbf{h}_{u,1}{}^H\mathbf{G}\mathbf{h}_{u,2}, \tag{3}$$

where α_u represents to the proportion of LOS channels in mixed channels for the user, $\mathbf{h}_{u,1}$ and $\mathbf{h}_{u,2}$ respectively refer to the channel from the user to IRS and that from IRS to UAV, and $\mathbf{G}$ is the phase shift matrix of IRS expressed as

$$\mathbf{G} = \begin{bmatrix} \theta_1 & & \\ & \ddots & \\ & & \theta_N \end{bmatrix}. \tag{4}$$

The gain of the LOS channel is only related to the physical distance between users and UAV, which conforms to the general assumption that the farther the distance is, the smaller the channel gain is. The specific formula is as follows:

$$L_{i,u} = a_u + 10b_u\log_{10}d_{i,u}. \tag{5}$$

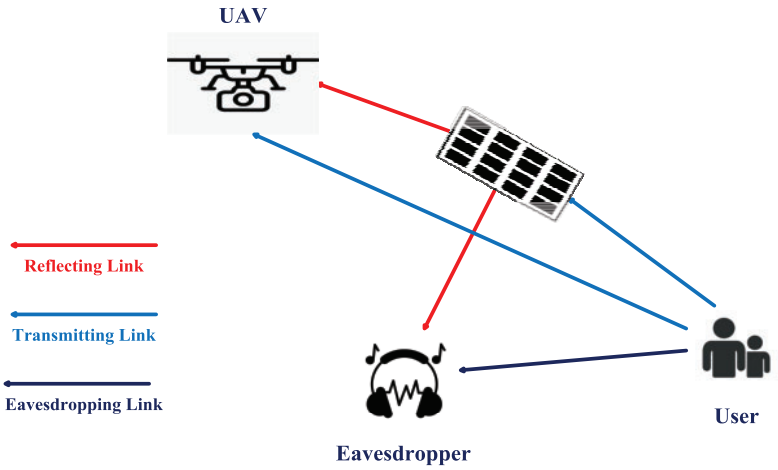

Figure 1: System model

Similarly, the channel between the physical distance is calculated as follows:

$$d_{iu} = \sqrt{(x_u - x_i)^2 + (y_u - y_i)^2 + H^2}, \tag{6}$$

$$d_{ie} = \sqrt{(x_e - x_i)^2 + (y_e - y_i)^2 + H^2}. \tag{7}$$

where (x_i, y_i) represents the position of UAV at time slot i, (x_u, y_u) represents the user position, and (x_e, y_e) represents the eavesdropper position. It is worth noting that the UAV can identify the exact location of users and eavesdroppers through cameras and other external devices, but the channels between users and eavesdroppers is NLOS channel, which is caused by ground shelters.

2.2 Problem Formulation

According to Shannon's theorem, we can first obtain the user's reception rate, which can be expressed as

$$R_{i,u} = \log_2\left(1 + \frac{\left\|\mathbf{h}_{i,u}^H \mathbf{w}\right\|^2}{\sigma_u^2}\right). \tag{8}$$

The eavesdropper's eavesdropping ability can be expressed by its eavesdropping rate, which is defined as

$$R_{i,e} = \log_2\left(1 + \frac{\left\|\mathbf{h}_{i,e}^H \mathbf{w}\right\|^2}{\sigma_e^2}\right), \tag{9}$$

Here, it could be assumed that the information intercepted by the eavesdropper is redundant information used to fill in the received code, i.e., the secrecy rate could be expressed as

$$R_{i,s} = [R_{i,u} - R_{i,e}]^+. \tag{10}$$

Based on the above discussion, we formulate the optimization problem as

$$\begin{aligned} &\max_{M_i, \mathbf{w}_i, \theta} \sum_{i \in I} R_{i,s} \\ &s.t.\ \ 0 \le \theta_n \le 2\pi, \\ &\quad \|\mathbf{w}_i\|^2 \le P_{\max}, \\ &\quad \|M_{i+1} - M_i\| \le L_{\max}, \\ &\quad \sum_{i \in I} \|\mathbf{w}_i\|^2 \le P_{sum}. \end{aligned} \tag{11}$$

The first constraint indicates that the element dependencies of the IRS should satisfy the legitimacy. The second constraint restricts the transmission power of the base station in each time slot, and the total consumed power of the time slot in the entire communication cycle should also meet the constraint, which is shown in the last constraint. In addition, UAVs will also be constrained by their flight speed.

3 Proposed Solution

In this section, we first want to obtain the transmission strategy of the eavesdropper, that is, the relationship between the transmission vector of the eavesdropper and the optimization variables we propose (the transmission vector of the base station, the flight path of the UAV, and the dependency matrix of the IRS), and then substitute the closed expression into the original problem to realize the conversion of the equivalent problem; then, we solve the original problem by using the interior point method and alternative optimization method.

3.1 Active Eavesdropping Strategy Acquisition

In this section, we simulate the strategies taken by eavesdroppers. Note that we cannot directly design the strategy of the eavesdropper, because we cannot directly interfere with the strategy of the eavesdropper. However, we can potentially affect the sending strategy of the eavesdropper by changing the receiving state of the eavesdropper.

Lemma 1: The transmission beam of the eavesdropper conforms to the following form:

$$\mathbf{v} = \alpha\widehat{\mathbf{h}}_{i,e} + \beta\mathbf{h}_{\perp}, \tag{12}$$

where $\widehat{h}_{i,e}$ is the channel with unit gain and $h_{\perp}$ represents the channel orthogonal to $\widehat{h}_{i,e}$, which are defined as

$$\widehat{\mathbf{h}}_{i,e} = \frac{\mathbf{h}_{i,e} + \mathbf{h}_{e}}{\left\|\mathbf{h}_{i,e} + \mathbf{h}_{e}\right\|}, \tag{13}$$

$$\mathbf{h}_{\perp} = \mathbf{h}_{i,u} - \widehat{\mathbf{h}}_{i,e}\mathbf{h}_{i,u}, \tag{14}$$

α and β are both parameters and could be obtained via the following equations:

$$\alpha = \sqrt{\frac{P_{e}}{\left\|\mathbf{h}_{i,e}\right\|}}\alpha_0, \tag{15}$$

$$\beta = \sqrt{\frac{P_{e}}{\left\|\mathbf{h}_{i,e}\right\|}}\beta_0. \tag{16}$$

The eavesdropping rate is thus expressed as

$$R_{e} = \begin{cases} R_{i,e} - R_{i,u}, & if\ R_{i,e} > R_{i,u}, \\ 0, & otherwise. \end{cases} \tag{17}$$

Proof. Please refer to Theorem 1 in [18].

According to Lemma 1, it is obvious that the transmission rate of the eavesdropper depends on the received signal and the channel from the UAV to the eavesdropper. When the eavesdropper has a chance to eavesdrop successfully, it maximizes the eavesdropping rate while ensuring the transmission rate; When the eavesdropper is unable to eavesdrop, it will maximize the user's reception rate, and then the eavesdropper will degenerate into a malicious attacker.

By substituting the results in Lemma 1 into the original problem, we construct the following problem:

$$\begin{aligned} &\max_{M_i,\mathbf{w}_i,\theta} \sum_{i\in I} R_{i,s} \\ &s.t.\ \ \log_2\left(1 + \frac{\left\|\mathbf{h}_{i,e}^{H}\mathbf{w}_i\right\|^2}{\sigma^2}\right) > \log_2\left(1 + \frac{\left\|\mathbf{h}_{i,u}^{H}\mathbf{w}_i\right\|^2}{\sigma^2}\right), \\ &\quad 0 \le \theta_n \le 2\pi, \\ &\quad \|\mathbf{w}_i\|^2 \le P_{\max}, \\ &\quad \|M_{i+1} - M_i\| \le L_{\max}, \\ &\quad \sum_{i\in I} \|\mathbf{w}_i\|^2 \le P_{sum} \end{aligned} \tag{18}$$

In (18), the eavesdropper could successfully eavesdrop on this MEC network. Meanwhile, the user's secrecy rate is 0.

$$\begin{aligned}
&\max_{M_i,\mathbf{w}_i,\theta} \sum_{i\in I} R_{i,s} \\
&s.t.\ \ \log_2\left(1+\frac{\left\|\mathbf{h}_{i,e}^H\mathbf{w}_i\right\|^2}{\sigma_e^2}\right) \le \log_2\left(1+\frac{\left\|\mathbf{h}_{i,u}^H\mathbf{w}_i\right\|^2}{\sigma_u^2}\right), \\
&\quad 0 \le \theta_n \le 2\pi, \\
&\quad \|\mathbf{w}_i\|^2 \le P_{\max}, \\
&\quad \|M_{i+1}-M_i\| \le L_{\max}, \\
&\quad \sum_{i\in I} \|\mathbf{w}_i\|^2 \le P_{sum}
\end{aligned} \tag{19}$$

In the above two problems, we also pay attention to two different situations. The first is that we cannot prevent eavesdroppers from acquiring information. This extreme situation occurs when the channel quality of eavesdroppers is much higher than the receiving channel, and the number of IRS elements is small. Normally, this kind of situation will not happen. Because as long as the transmission beam is controlled in the null space of the eavesdropping channel, eavesdroppers can be completely avoided. Therefore, we will only discuss such cases briefly and then focus on the second case, namely maximizing the security transmission rate.

3.2 Trajectory Design

In this section, we focus on the trajectory design of the UAV when the IRS phase shift matrix and the transmitting beam of the base station are fixed. Let's first transform the question into the following format:

$$\begin{aligned}
&\max_{M_i} \sum_{i\in I} R_{i,s} \\
&s.t.\ \ 0 \le \theta_n \le 2\pi, \\
&\quad \|M_{i+1}-M_i\| \le L_{\max}, \\
&\quad \sum_{i\in I} \|\mathbf{w}_i\|^2 \le P_{sum}
\end{aligned} \tag{20}$$

Note that we can solve the problem iteratively. To be specific, we first set up an initial trajectory, such as the constant speed straight flight of UAV. Then on this basis, we optimize the trajectory step by step, and the iteration method is proposed as follows:

$$\log A_i[n] + \frac{B_i[n]}{A_i[n]\ln 2} + \frac{C_i[n]}{A_i[n]\ln 2}\left(\mathbf{w}_i[n]-w_{i-1}[n]\right), \tag{21}$$

where

$$A_i[n] = \sum_{j=1}^{i} p_j[n]\left(\mathbf{w}_i[n]-\mathbf{w}_{i-1}[n]\right)^2 + \sigma^2. \tag{22}$$

Then the original problem could be solved by iterations.

3.3 Beamforming Matrices Design

In this subsection, we would like to obtain the beamforming matrix design for the base station. In specific, we set the trajectory of the UAV and the phase shift matrix of the IRS as fixed setting, and put forward the following problem:

$$\begin{aligned} &\max_{w_i} \sum_{i\in I} R_{i,s} \\ &s.t. \quad \|M_{i+1} - M_i\| \le L_{\max}, \\ &\quad \sum_{i\in I} \|\mathbf{w}_i\|^2 \le P_{sum} \end{aligned} \tag{23}$$

We introduce two variables defined as

$$l_1 = \sqrt{\left(1 + \mathbf{w}_1 + \frac{\alpha C}{t}\right)\frac{t^2}{3k_1}} \tag{24}$$

$$l_2 = \sqrt{\left(\mathbf{w}_1 + \beta + \frac{\alpha C}{t}\right)\frac{t^2}{3k_2}} \tag{25}$$

The power send by the user could be expressed as

$$p[n] = \frac{tB}{\alpha \ln 2}\left(\frac{h[n]^2}{h[n+1] - h[n]^2} - \frac{h[n-1]^2}{h[n] - h[n-1]^2}\right) \tag{26}$$

where $h[n]$ refers to the channel gain in nth time slot.

$$\begin{aligned} &\max_{\mathbf{w}_i} \sum_{i\in I} R_{i,s} \\ &s.t. \quad \|\mathbf{w}_i\|^2 \le P_{\max}, \end{aligned} \tag{27}$$

(27) is convex and could be solved by CVX [28].

3.4 Phase-Shift Matrix Design

In this section, we optimize the transmitting beam of the user. We first transform the following problem:

$$\begin{aligned} &\max_{\theta} \sum_{i\in I} R_{i,s} \\ &s.t. \quad 0 \le \theta_n \le 2\pi, \\ &\quad \log_2\left(1 + \frac{\left\|\mathbf{h}_{i,e}^H \mathbf{w}_i\right\|^2}{\sigma_e^2}\right) \le \log_2\left(1 + \frac{\left\|\mathbf{h}_{i,u}^H \mathbf{w}_i\right\|^2}{\sigma_u^2}\right), \end{aligned} \tag{28}$$

In addition, the above problem is a non-convex objective function composed of coupling variables. In order to convert the molecules of the objective function into concave functions, we consider introducing relaxation variables and using the SCA method. By introducing relaxation variables, the throughput can be rewritten as

$$\max_{\theta} \sum_{i \in I} Tr\left(\mathbf{G}_i \mathbf{W}_i \mathbf{G}_i^H\right)$$

$$s.t.\ \ 0 \le \theta_n \le 2\pi,$$

$$\log_2\left(1 + \frac{\left\|\mathbf{h}_{i,e}^H \mathbf{W}_i \mathbf{h}_{i,e}\right\|^2}{\sigma_e^2}\right) \le \log_2\left(1 + \frac{\left\|\mathbf{h}_{i,e}^H \mathbf{W}_i \mathbf{h}_{i,e}\right\|^2}{\sigma_u^2}\right). \tag{29}$$

Algorithm 3.1: Proposed algorithm

Input: Estimation error ζ_e^2 and ζ_p^2.
Input: Maximum power P_{max}, Channel state information $\mathbf{G}$, $\mathbf{H}_{k_1}$ and $\mathbf{H}_{k_2}$.
Output: Beamforming matrix $\mathbf{W}_k$, covariance matrix $\mathbf{G}$, and shift matrix $\mathbf{G}$,

function TRAJECTORY DESIGN
  Initial $\mathbf{W}_k = P_{max}\mathbf{I}$ and the shift matrix $\mathbf{G} = \mathbf{I}$, the index $n = 0$
  for $n \le N$ **do**
    Compute the next state according to the current $p_k[n]$
    Calculate $\mathbf{W}_k^{(n+1)}$ and P_k for given $\mathbf{G}^{(n)}$
    $n = n + 1$
  end for
end function

function ALTERNATIVE ALGORITHM
  Substituting the initial point the the constraints.
  repeat
    if $m > M$ **then**
      break;
    else ▷ Update the beamfroming
      Obtain $\mathbf{G}^{(H)}$ using the bisection method;
      for $k \le K$ **do**
        if $\left|f(\mathbf{w}_k^{(n+1)}, \mathbf{G}^{(n+1)}) - f(\mathbf{w}_k^{(n)}, \mathbf{G}^{(n)})\right| \le \varepsilon$ **then**
          continue;
        end if
      end for
      Update the beamforming vector
    end if
    The maximum secrecy rate $\eta_E^{n,opt}$ is obtained.
    if $m \le M$ **then**
      $m = m + 1$
    end if
  until $\|R_m - R_{m-1}\| \le e$
end function

Note that the problem (29) is still non-convex, we choose the lower bound of the optimization objective function [29]. At this time, the problem can be transformed into

$$f = -\sum_{i\in I} \log_2 \left(\mathrm{Tr}\left(\mathbf{G}_i \mathbf{W}_i \mathbf{G}_i^H\right) + \sigma_u\right) \tag{30}$$

$$g = -\sum_{i\in I} \log_2 \left(\mathrm{Tr}\left(\mathbf{G}_i \mathbf{H}_e \mathbf{G}_i^H\right) + \sigma_e^H\right) \tag{31}$$

$$\begin{aligned} &\max_{M_i,\theta} f \\ &s.t.\ \ 0 \le \theta_n \le 2\pi, \\ &\quad f \ge g. \end{aligned} \tag{32}$$

In order to solve the problem (32), we use the method of first order Taylor expansion and continuous convex approximation.

3.5 Alternate Optimization Algorithm Design

In this subsection, we summarize the above algorithm process and propose an overall algorithm based on alternative optimization. In our algorithm, we mainly include the nesting of three sub-problems. In the trajectory optimization of UAV, we use a small iterative method. After iterative convergence, it is added into the loop composed of the phase shift matrix of the IRS and the transmitting beam of the base station.

Due to the high coupling between variables, the convergence of the algorithm is given by simulation experiments.

4 Sub-Optimal Solution

In this section, we propose a suboptimal solution based on the zeroing method and analyze its computational complexity expenditure, which has a lower computational cost compared with the iterative algorithm.

4.1 Zeros-Force Method

In this subsection, we propose a suboptimal solution to the original problem, that is, by controlling the transmitting beam of the base station and the phase shift matrix of the IRS, the eavesdropper's receiving beam is limited to its zero space. At this point, an additional constraint needs to be added and the optimization problem needs to be rewritten as follows:

$$\begin{aligned} &\max_{M_i,\mathbf{w}_i,\theta} \sum_{i\in I} R_{i,s} \\ &s.t.\ \ \log_2\left(1 + \frac{\left\|\mathbf{h}_{i,e}^H \mathbf{w}_i\right\|^2}{\sigma_e^2}\right) \le \log_2\left(1 + \frac{\left\|\mathbf{h}_{i,u}^H \mathbf{w}_i\right\|^2}{\sigma_u^2}\right), \\ &\quad 0 \le \theta_n \le 2\pi, \\ &\quad \|\mathbf{w}_i\|^2 \le P_{\max}, \\ &\quad \|M_{i+1} - M_i\| \le L_{\max}, \\ &\quad \sum_{i\in I} \|\mathbf{w}_i\|^2 \le P_{sum} \end{aligned} \tag{33}$$

To solve this problem, we divide the problem into two sub-problems. In the first sub-problem, we focus on the design of the transmission beam of the base station and the phase shift matrix of the IRS, and rewrite it as

$$\mathbf{w}_e = p_e \mathbf{h}_{\perp}^{H} \tag{34}$$

In the second sub-problem, we focus on the flight path design of UAV. It is worth noting that we only need to pay attention to its impact on the safety rate when designing the flight path of UAV.

$$\begin{aligned} &\max_{M_i,\theta} \sum_{i\in I} R_{i,s} \\ &s.t.\ \log_2\left(1+\frac{\left\|\mathbf{h}_{i,e}^{H}\mathbf{w}_i\right\|^2}{\sigma_e^2}\right) \le \log_2\left(1+\frac{\left\|\mathbf{h}_{i,u}^{H}\mathbf{w}_i\right\|^2}{\sigma_u^2}\right), \\ &\quad 0 \le \theta_n \le 2\pi, \\ &\quad \|M_{i+1} - M_i\| \le L_{\max}. \end{aligned} \tag{35}$$

We finally get a simplified problem, and then we can use the interior point method to solve it by iteratively solve M_i and θ as in the AO-based scheme.

Further, we obtain the following algorithm with ZF based method.

5 Complexity Analysis

We focus on the complexity of proposed schemes and two traditional schemes: MRT scheme and OA algorithm. As shown in Table 1, note that MRT scheme gets the minimum complexity since it has a closed-form solution. The proposed sub-optimal get less complexity than the optimal scheme.

Table 1: Complexity analysis

Parameter	Complexity in each iteration	Overall complexity
Algorithm 3.1	$\mathcal{O}(M(P_1+P_2))$	$\mathcal{O}(M(P_1+P_2)P_1)$
Algorithm 4.1	$\mathcal{O}(M(P_1+1))$	$\mathcal{O}(M(P_1+1)P_2)$
MRT scheme	$\mathcal{O}(M)$	$\mathcal{O}(M)$
OA scheme	$\mathcal{O}(MP^2)$	$\mathcal{O}(MP^3)$

6 Discussion

We designed the transmission power of the base station, the flight path of the UAV, and the reflection matrix of the IRS to maximize the safety rate for scenarios with intelligent eavesdroppers. In view of the different working modes of the eavesdropper, we first analyze the rationality of the design scheme and then propose the scheme based on the interior point method and alternative optimization, as well as the sub-optimal scheme based on zero space.

The reason why we are targeting the scene of intelligent eavesdroppers is that with the development of communication technology, especially the widespread concern about secure communication, more and more emerging technologies may also be used by criminals. We need to guard against such active eavesdroppers.

Algorithm 4.1: Proposed algorithm

Input: estimation error ζ_e^2 and ζ_p^2.
Input: Maximum power P_{max}, Channel state information $\mathbf{G}$, $\mathbf{H}_{k_1}$ and $\mathbf{H}_{k_2}$.
Output: Beamforming matrix $\mathbf{W}_k$, covariance matrix $\mathbf{G}$, and shift matrix $\mathbf{G}$,

function TRAJECTORY DESIGN
  Initial $\mathbf{W}_k = P_{max}\mathbf{I}$ and the shift matrix $\mathbf{G} = \mathbf{I}$, the index $n = 0$
  for $n \leq N$ **do**
    Compute the next state according to the current $p_k[n]$
    Calculate $\mathbf{W}_k^{(n+1)}$ and P_k for given $\mathbf{G}^{(n)}$
    $n = n + 1$
  end for
end function

function ZF BASED ALGORITHM
  Substituting the initial point the the constraints.
  repeat
    The maximum secrecy rate $R_s^{n,opt}$ is obtained.
    if $m \leq M$ **then**
      $m = m + 1$
    end if
  until $\|R_m - R_{m-1}\| \leq e$
end function

There is still much to be learned about the confrontation of intelligent eavesdroppers. Although we only focus on some idealized scenarios in this article, we still put forward many constructive suggestions, such as adopting different strategies for the working mode of eavesdroppers and how to design a low-complexity scheme. With regard to multi-user design and more working modes of eavesdroppers, we leave the work for the future.

7 Numerical Results

In this section, we first list the parameters required for the simulation environment as shown in Fig. 2, then simulate the results under different settings, and analyze the advantages of the proposed algorithm.

7.1 Simulation Parameters

In this subsection, we build the simulation environment. The UAV flies at a fixed altitude, and its starting and ending points are fixed. The air-to-ground channel is composed of NLOS and LOS channels. The ground channel is NLOS channel, and the location of users and eavesdroppers is known. The specific parameters are shown in Table 2.

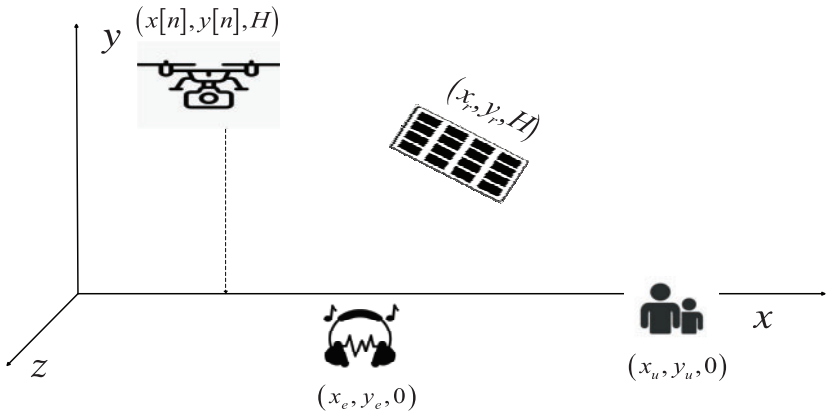

Figure 2: Simulation area

Table 2: Simulation parameters

Parameter	Symbol	Value
The total time of trajectory	T	10 s
Time slots	N	50
The gain of LOS channel for a reference distance $d_0 = 1$ m	ρ_0	−30 dB
The power of noise	N_0	−60 dB
Altitude of UAV	H	10 m
The maximum available speed of the UAV	V_{max}	10 m/s
The initial and final position of the UAV	$\mathbf{q_I}, \mathbf{q_F}$	(0, 0), (0,10)
The position of base station	$\mathbf{q_T}$	(0, 0)
The position of eavesdropper	$\mathbf{q_E}$	(0,10)
The position of user	$\mathbf{q_E}$	(0,10)

7.2 Simulation Results

In this section, we conducted simulation experiments on the proposed scheme, mainly including (1) the proposed scheme; (2) the proposed sub-optimal scheme; (3) the maximum rate scheme; (4) the scheme against potential eavesdroppers; (5) no IRS scheme; (6) the fixed IRS scheme. The specific results are as follows.

We first pay attention to the convergence of the proposed algorithm, that is, the proposed iterative algorithm. As we stated earlier, the convergence of the algorithm is obtained through simulation experiments. As shown in Fig. 3, the convergence rate of our proposed algorithm is slightly different at different initial points, but they all converge within 10 times. The convergence speed is equivalent to the scheme for dealing with silent listeners. However, the figure shows that the safety rate of convergence is higher than that of the comparison scheme. We will conduct more simulation experiments in the future to prove the superiority of our proposed scheme.

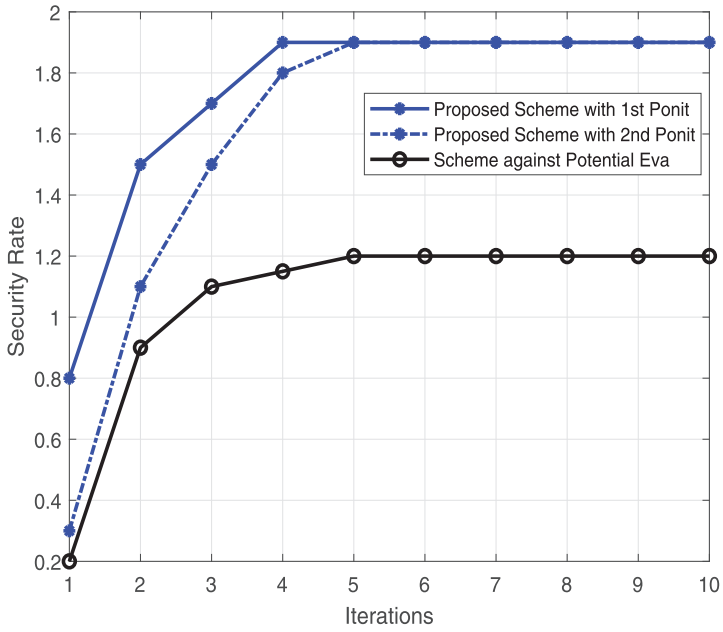

Figure 3: Convergence of the proposed algorithm

We focus on the flight path of the UAV in Fig. 4. Since the initial point and end point of the UAV are not the same points, we limit the UAV path to a straight line. At this time, the UAV is dense at some points and sparse at other places. Specifically, when the position of the UAV can be adapted to the phase control of the IRS, its flight speed will be reduced to extend the time it stays in the dominant area. It is worth noting that the UAV cannot stay at a certain point for a long time, and hovering will consume more energy and lose the ability to face multiple users.

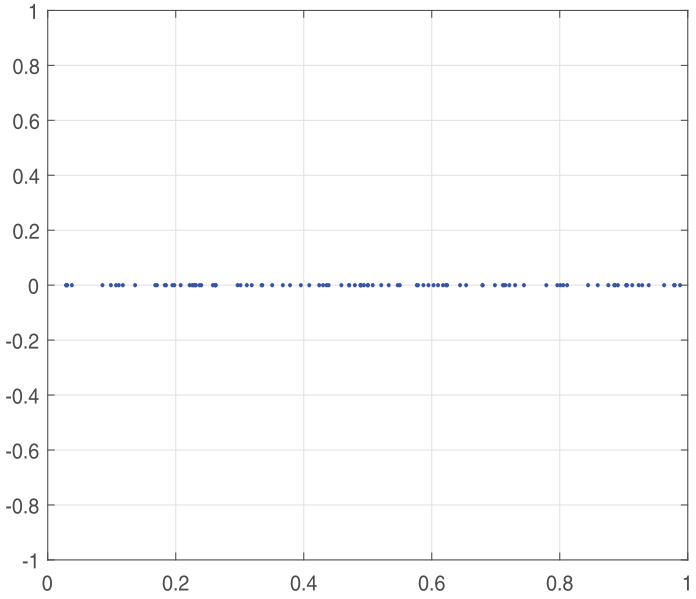

Figure 4: Trajectory of UAV

We also focused on the impact of the number of IRS elements on the security rate in Fig. 5. IRS plays a very important role in our proposed scheme. As an important indicator that directly affects the performance of IRS, the number of IRS elements deserves our further attention. Of course, the more elements of the IRS, the better. However, because there is a certain distance between the elements of the IRS, more elements may bring load pressure and security risks. We consider a reasonable range, that is when the number of IRS elements increases from 20 to 100.

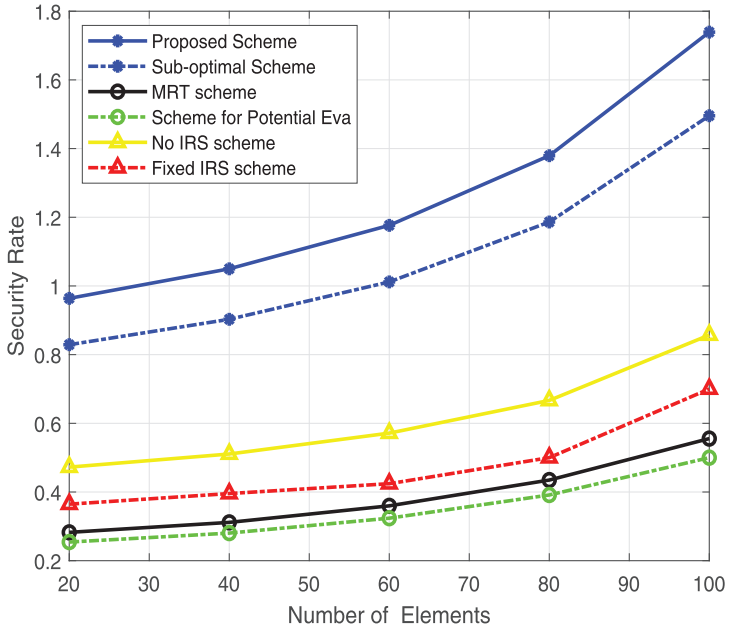

Figure 5: Security rate *vs*. the number of elements of IRS

In Fig. 6, we show the curve of the secrecy rate changing with user power. When the user power increases, the security rate also increases. It is worth noting that the MRT scheme in the curve crosses the curve without IRS. This is because when the user power is low, the MRT scheme can ensure a higher transmission rate, thus achieving better security. When the user power increases, the MRT scheme is not flexible enough. Although the scheme without IRS can not gain from IRS, it can gain ga by adjusting the user's transmitted beam.

We show the relationship between safety rate and noise power in Fig. 7. Noise power is the background white noise that cannot be avoided in the communication process. It will not only reduce the rate of legal communication but also reduce the eavesdropping ability of eavesdroppers. However, in our proposed scheme, with the increase of noise power, the decrease in secrecy rate is the smallest, which shows that our proposed scheme can still ensure a higher safety rate in a very noisy and harsh environment.

In traditional eavesdropping scenarios, the power of the eavesdropper is not concerned, because when the eavesdropper is silent, the power of the eavesdropper cannot affect the entire communication system. However, when the eavesdropper is proactive eavesdropping, the increase of eavesdropping power will reduce the security of the system. As shown in Fig. 8, with the increase in eavesdropper power, the security rate will also decrease. It is worth noting that when the power of the eavesdropper increases, it will increase the interference to the communication link, thus reducing the security rate.

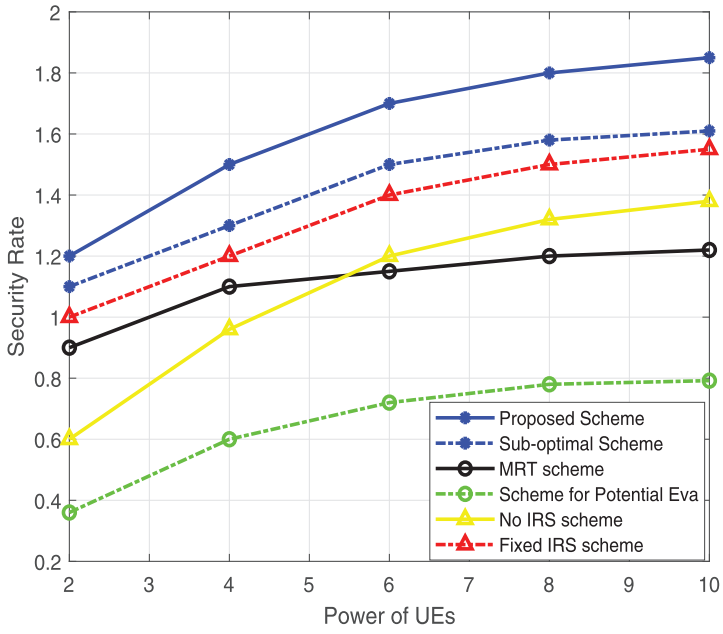

Figure 6: Security rate *vs.* power of base station

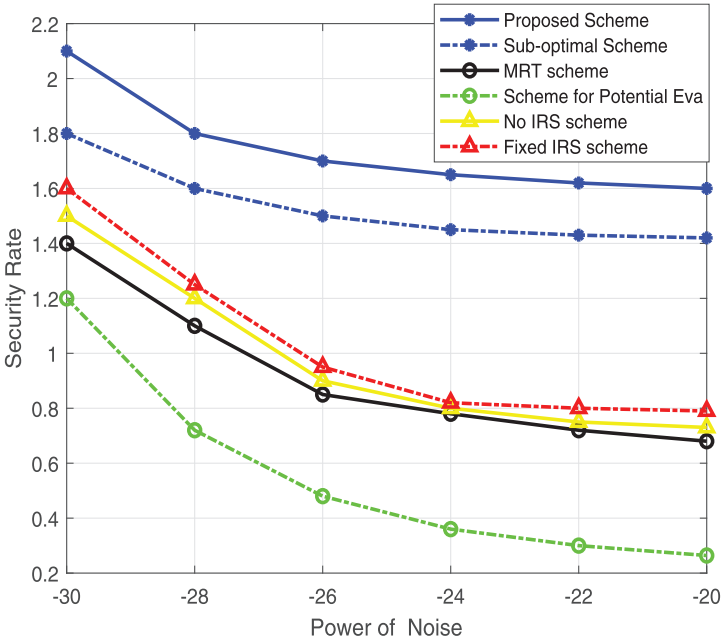

Figure 7: Security rate *vs.* power of noise

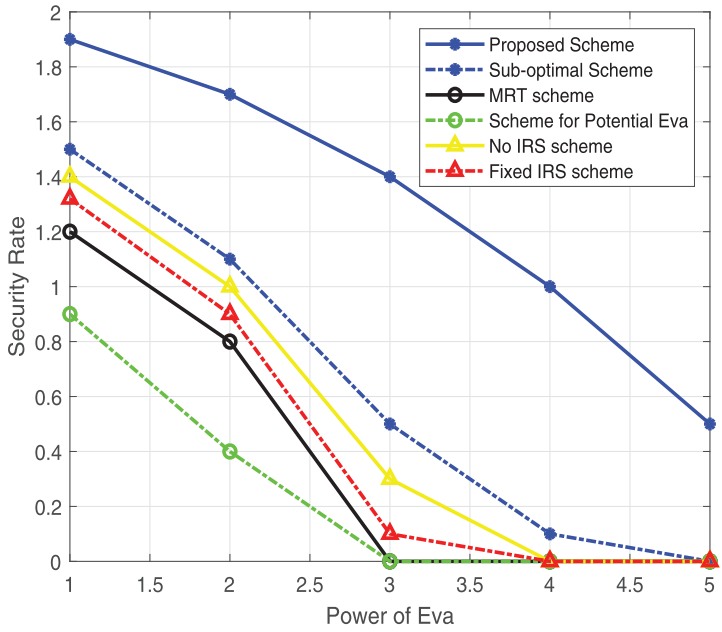

Figure 8: Security rate *vs*. power of eavesdropper

8 Conclusion

In this paper, we designed the transmitting beam of the user, the trajectory of the UAV, and the phase shift matrix of the IRS to maximize the user's secrecy rate. We analyzed the two working modes of the eavesdropper and potentially controlled its transmitting beam. We added the influence factor of the eavesdropper as an optimization variable into the design scheme and proposed a local optimization scheme based on the interior point method and alternative optimization. In addition, we designed a suboptimal scheme based on the zero forcing method to reduce the computational complexity. The simulation results showed that the proposed iterative scheme is superior to the suboptimal scheme and has a higher secrecy rate than the existing schemes.

Acknowledgement: The authors wish to express their appreciation to the reviewers for their helpful suggestions which greatly improved the presentation of this paper.

Funding Statement: This work was supported by the Key Scientific and Technological Project of Henan Province (Grant Number 222102210212), Doctoral Research Start Project of Henan Institute of Technology (Grant Number KQ2005) and Key Research Projects of Colleges and Universities in Henan Province (Grant Number 23B510006).

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Ying Zhang; data collection: Weiming Niu; analysis and interpretation of results: Leibing Yan. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: All data is synthesized using MATLAB and the generation method is described in detail in the simulation section.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

1. Zheng, L., Lops, M., Eldar, Y. C., Wang, X. (2019). Radar and communication coexistence: An overview: A review of recent methods. *IEEE Signal Processing Magazine, 36(5),* 85–99. https://doi.org/10.1109/MSP.2019.2907329
2. Griffiths, H., Cohen, L., Watts, S., Mokole, E., Baker, C. et al. (2015). Radar spectrum engineering and management: Technical and regulatory issues. *Proceedings of the IEEE, 103(1),* 85–102. https://doi.org/10.1109/JPROC.2014.2365517
3. Hu, X., Wong, K. K., Zhang, Y. (2020). Wireless-powered edge computing with cooperative UAV: Task, time scheduling and trajectory design. *IEEE Transactions on Wireless Communications, 19(12),* 8083–8098. https://doi.org/10.1109/TWC.2020.3019097
4. Patole, S. M., Torlak, M., Wang, D., Ali, M. (2017). Automotive radars: A review of signal processing techniques. *IEEE Signal Processing Magazine, 34(2),* 22–35. https://doi.org/10.1109/MSP.2016.2628914
5. Nartasilpa, N., Salim, A., Tuninetti, D., Devroye, N. (2018). Communications system performance and design in the presence of radar interference. *IEEE Transactions on Communications, 66(9),* 4170–4185. https://doi.org/10.1109/TCOMM.2018.2823764
6. Shi, Q., Razaviyayn, M., Luo, Z. Q., He, C. (2011). An iteratively weighted MMSE approach to distributed sum-utility maximization for a MIMO interfering broadcast channel. *IEEE Transactions on Signal Processing, 59(9),* 4331–4340. https://doi.org/10.1109/TSP.2011.2147784
7. Mishali, M., Eldar, Y. C. (2010). From theory to practice: Sub-nyquist sampling of sparse wideband analog signals. *IEEE Journal of Selected Topics in Signal Processing, 4(2),* 375–391. https://doi.org/10.1109/JSTSP.2010.2042414
8. Griffin, J. D., Durgin, G. D. (2009). Complete link budgets for backscatter-radio and RFID systems. *IEEE Antennas and Propagation Magazine, 51(2),* 11–25. https://doi.org/10.1109/MAP.2009.5162013
9. Grossi, E., Lops, M., Venturino, L., Zappone, A. (2018). Opportunistic radar in IEEE 802.11ad networks. *IEEE Transactions on Signal Processing, 66(9),* 2441–2454. https://doi.org/10.1109/TSP.2018.2813300
10. Wu, W., Wang, Z., Yuan, L., Zhou, F., Lang, F. et al. (2021). IRS-enhanced energy detection for spectrum sensing in cognitive radio networks. *IEEE Wireless Communications Letters, 10(10),* 2254–2258. https://doi.org/10.1109/LWC.2021.3099121
11. Farha, Y. A., Ismail, M. H. (2022). Design and optimization of a UAV-enabled non-orthogonal multiple access edge computing IoT system. *IEEE Access, 10,* 117385–117398. https://doi.org/10.1109/ACCESS.2022.3220264
12. Shirin Abkenar, F., Ramezani, P., Iranmanesh, S., Murali, S., Chulerttiyawong, D. et al. (2022). A survey on mobility of edge computing networks in IoT: State-of-the-art, architectures, and challenges. *IEEE Communications Surveys and Tutorials, 24(4),* 2329–2365. https://doi.org/10.1109/COMST.2022.3211462
13. Wu, W., Zhou, F., Hu, R. Q., Wang, B. (2020). Energy-efficient resource allocation for secure NOMA-enabled mobile edge computing networks. *IEEE Transactions on Communications, 68(1),* 493–505. https://doi.org/10.1109/TCOMM.2019.2949994
14. Lin, W., Ma, H., Li, L., Han, Z. (2022). Computing assistance from the sky: Decentralized computation efficiency optimization for air-ground integrated MEC networks. *IEEE Wireless Communications Letters, 11(11),* 2420–2424. https://doi.org/10.1109/LWC.2022.3205503
15. Mao, S., Liu, L., Zhang, N., Dong, M., Zhao, J. et al. (2022). Reconfigurable intelligent surface-assisted secure mobile edge computing networks. *IEEE Transactions on Vehicular Technology, 71(6),* 6647–6660. https://doi.org/10.1109/TVT.2022.3162044

16. Cui, J., Wang, L., Hu, B., Chen, S. (2022). Incidence control units selection scheme to enhance the stability of multiple UAVs network. *IEEE Internet of Things Journal, 9(15),* 13067–13076. https://doi.org/10.1109/JIOT.2021.3140066
17. Asim, M., Mashwani, W. K., Belhaouari, S. B., Hassan, S. (2021). A novel genetic trajectory planning algorithm with variable population size for multi-UAV-assisted mobile edge computing system. *IEEE Access, 9,* 125569–125579. https://doi.org/10.1109/ACCESS.2021.3111318
18. Wu, Q., Zhang, R. (2019). Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming. *IEEE Transactions on Wireless Communications, 18(11),* 5394–5409. https://doi.org/10.1109/TWC.2019.2936025
19. Huang, C., Zappone, A., Debbah, M., Yuen, C. (2018). Achievable rate maximization by passive intelligent mirrors. *ICASSP 2018—2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Calgary, AB, Canada.
20. Mishra, D., Johansson, H. (2019). Channel estimation and low-complexity beamforming design for passive intelligent surface assisted MISO wireless energy transfer. *ICASSP 2019—2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Brighton, UK.
21. Ning, Z., Dong, P., Kong, X., Xia, F. (2019). A cooperative partial computation offloading scheme for mobile edge computing enabled Internet of Things. *IEEE Internet of Things Journal, 6(3),* 4804–4814. https://doi.org/10.1109/JIOT.2018.2868616
22. Hum, S. V., Perruisseau-Carrier, J. (2014). Reconfigurable reflectarrays and array lenses for dynamic antenna beam control: A review. *IEEE Transactions on Antennas and Propagation, 62(1),* 183–198. https://doi.org/10.1109/TAP.2013.2287296
23. Di, B., Zhang, H., Song, L., Li, Y., Han, Z. et al. (2020). Hybrid beamforming for reconfigurable intelligent surface based multi-user communications: Achievable rates with limited discrete phase shifts. *IEEE Journal on Selected Areas in Communications, 38(8),* 1809–1822. https://doi.org/10.1109/JSAC.2020.3000813
24. Liu, Y., Zhao, J., Xiong, Z., Niyato, D., Chau, Y. et al. (2020). Intelligent reflecting surface meets mobile edge computing: Enhancing wireless communications for computation offloading. https://arxiv.org/abs/2001.07449
25. Ju, H., Lim, S., Kim, D., Poor, H. V., Hong, D. (2012). Full duplexity in beamforming-based multi-hop relay networks. *IEEE Journal on Selected Areas in Communications, 30(8),* 1554–1565. https://doi.org/10.1109/JSAC.2012.120922
26. Yu, X., Xu, D., Schober, R. (2019). MISO wireless communication systems via intelligent reflecting surfaces: (invited paper). *2019 IEEE/CIC International Conference on Communications in China (ICCC)*, Changchun, China.
27. Wu, W., Wang, X., Zhou, F., Wong, K. K., Li, C. et al. (2021). Resource allocation for enhancing offloading security in NOMA-enabled MEC networks. *IEEE Systems Journal, 15(3),* 3789–3792. https://doi.org/10.1109/JSYST.2020.3009723
28. Grant, M., Boyd, S. P. (2014). CVX: Matlab software for disciplined convex programming. http://cvxr.com/cvx/
29. Li, Z., Chen, W., Wu, Q., Wang, K., Li, J. (2022). Joint beamforming design and power splitting optimization in IRS-assisted swipt NOMA networks. *IEEE Transactions on Wireless Communications, 21(3),* 2019–2033. https://doi.org/10.1109/TWC.2021.3108901