Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 8462350, 15 pages
https://doi.org/10.1155/2022/8462350

Research Article

Reconfigurable Intelligent Surface-Aided Cell-Free Massive MIMO with Low-Resolution ADCs: Secrecy Performance Analysis and Optimization

Xianyu Zhang,[1] **Xiaoqiang Qiao**,[1] **Kang An**,[1] **Junquan Deng**,[1] **Tao Liang**,[1] **and Xiaoyu Wang**[2]

[1]*Sixty-Third/63rd Research Institute, National University of Defense Technology, Nanjing 210007, China*
[2]*College of Communication Engineering, Army Engineering University of PLA, Nanjing 210007, China*

Correspondence should be addressed to Xiaoqiang Qiao; qxq0527@163.com

Received 9 August 2022; Revised 29 September 2022; Accepted 15 October 2022; Published 3 November 2022

Academic Editor: Wence Zhang

The secure communication in reconfigurable intelligent surface-aided cell-free massive MIMO system is investigated with low-resolution ADCs and with the existence of an active eavesdropper. Specifically, an aggregated channel estimation approach is applied to decrease the overhead required to estimate the channels. Using the available imperfect channel state information (CSI), the conjugate beamforming and random beamforming are applied at the APs and the RIS for downlink data transmission, respectively. The closed-form expression of the achievable secrecy rate is acquired to appraise the achievable secrecy performance using only the channel statistics. With the achievable analytical results, the impacts of the quantization bit of ADCs, channel estimation error, the number of RIS elements, and the number of the APs can be unveiled. Aiming to maximize the minimum achievable rate of all legitimate users subject to security constraints, the power control optimization scheme is first formulated. To tackle this nonconvex property of the proposed optimization problem, a path-following algorithm is then utilized to solve the initial problem with continuous approximations and iterative optimization. Numerical results are presented to verify the achieved results along with availability of the presented power allocation approach.

1. Introduction

Cell-free massive MIMO and reconfigurable intelligent surface (RIS) are two conspicuous technologies which can meet the demanding coverage and massive connectivity request in the sixth generation (6G) and future wireless communication systems [1, 2]. As a serviceable and scalable implementation of the distributed antenna network, cell-free massive MIMO system exploits multitudinous access points (APs) to serve a smaller number of users [3, 4]. Besides, all APs are attached via backhaul links to a central processing unit (CPU) for information interaction. Due to the superiority of the distributed systems and network MIMO configurations, the cell-free massive MIMO system has obvious superiority in terms of 95%-likely network capacity [5–7]. RIS is an emerging technology which can beamform the electromagnetic waves without requiring digital signal processing techniques and without applying power amplifiers. RISs are programmable metasurfaces with many passive reflecting elements which can be independently designed to alter the phase shifts of the electromagnetic signal to turn the reflective wave beam to different orientations [8–10]. Recently, the attractive benefits of deploying RISs for various existing communication have been demonstrated in various scenarios, for instance, RIS-aided NOMA systems, RIS-aided mmWave communication, RIS-aided secure transmission system, and RIS-aided massive MIMO systems [11–14]. The results in these studies have shown that introducing RISs can provide an augmented performance while envisioning higher efficiency and lower cost than common

systems. Integration of the two aforesaid techniques can be defined as RIS-aided cell-free massive MIMO system [15]. The performance analysis of the downlink RIS-aided cell-free massive MIMO adopting a random beamforming scheme at the RIS has been considered and studied in [16]. Besides, the authors in [17] employed multiple RISs in cell-free massive MIMO system to acquire an evident performance gain. This letter also developed a hybrid beamforming (HBF) scheme and formulated a sum rate optimization problem. Then, the uplink and downlink performance of RIS-aided cell-free massive MIMO systems under the presence of spatially-correlated channels has been considered in [18], where various impact factors on the system performance have been analyzed in detail. Then, a new scenario called aerial IRS- (AIRS-) aided cell-free massive MIMO was studied in [19].

On the other hand, due to the increasing complexity of the communication environment and the imperative security of private information, communication security for protecting the confidential message transmission is crucially important in future wireless communication networks [20, 21]. Different from the traditional cryptographic encryption and decryption secure technique, physical layer security can provide good security performance by exploiting the properties of wireless communication channels without requiring secret key distribution, protection, and management [22, 23]. Thus, the physical layer security is more absorbing in academia and industry and has been widely studied in wireless communication scenarios. In particular, multiantenna wireless communication systems can enhance its secrecy in the physical layer by enlarging the signal quality difference of the target user and the eavesdropper [24, 25]. Hence, secrecy-enhancing techniques have been widely investigated in recent years, such as secrecy beamforming, artificial noise transmission, cooperative jammers, and power control. As a scalable MIMO system, massive MIMO can harvest all the advantages of conventional MIMO. Besides, the abundant transmit antennas can be used for secrecy improvement. Thus, application of the physical layer security in massive MIMO system is potential [26, 27]. In general, most studies in security in massive MIMO follow with interest colocated massive MIMO. Then, the secure communication in multicell massive MIMO systems was studied in [28]. Furthermore, the secure massive MIMO transmission along with a multiantenna active eavesdropper was studied in detail in [29]. Besides, the precoding, power control, relay systems, active attack detection, and hardware impairments in secure massive MIMO have also been investigated [30–33]. In addition, another practical deployment of massive MIMO is to employ a so-called distributed antenna architecture which can obtain a deterministic performance gain over the colocated massive MIMO system. Besides, the security performance analysis in multiuser massive MIMO was studied in detail in [34, 35]. The secure communication in cell-free massive MIMO system has been studied in some related works. The authors in [36] focused on the secure communication in the cell-free massive MIMO network. The security aspect in multigroup multicasting cell-free massive MIMO has been considered in [37]. Considering the impact of hardware impairments, the authors in [38] were concerned with the problem of secure communication in cell-free massive MIMO system.

All aforementioned works are based on a common assumption that all APs are installed with ideal ADCs. However, due to the increasing large number of the ADCs, the implementation with high-resolution ADCs may become more expensive and significantly bulkier. A feasible scheme is to make use of low-resolution ADCs for low-cost practical cell-free massive MIMO system. The authors in [39] presented a detailed analysis on the achievable performance of the cell-free massive MIMO system with low-resolution ADCs. The uplink achievable rate in cell-free massive MIMO considering the low-resolution ADCs and RF impairments has been studied in [40]. Then, considering the low-resolution DACs, the authors in [41] presented an investignation on the RIS-aided massive MIMO systems. In addition, facilitating physical layer secrecy in cell-free massive MIMO network with low-resolution ADCs is another critical concern and has received attention recently. Under the assumption of low-resolution ADCs, the secrecy performance analysis and the power control in cell-free massive MIMO have been investigated in detail in [42]. Besides, the authors in [43] analyzed the effect of the RF impairments and low-resolution ADCs/DACs in secure cell-free massive MIMO system, where some key parameters on the security performance have been stuided and been verified via numerical results.

With these above considerations in mind, the secure RIS-aided cell-free massive MIMO system with low-resolution ADCs at the users and the APs is studied in this paper. Different from the previous conference paper [44], the paper provides novel insights on secure performance analysis and power control scheme. The specific contributions of our article are summarized as follows:

(i) With the equipment of the low-resolution ADCs, the secure aspect in RIS-aided cell-free massive MIMO system has been firstly studied in this paper. The AQNM is advocated to model the ADC imperfections which can well simulate the quantization noise terms as Gaussian variable. Then, we present a channel estimation approach at the APs to estimate the aggregated channels comprising the direct and indirect links, instead of all individual channel coefficients

(ii) Using the imperfect CSI by channel estimation, the closed-form secrecy rate expression has been derived by using conjugate beamforming at the APs and the random beamforming at the RIS, which can provide an implement for quantitative analysis on the impacts of the channel estimation error, the quantization bit of coarse ADCs, the number of total antenna arrays, and the RIS's scattering elements

(iii) To ensure the user fairness and further improve the system performance, we aim to optimize the power

allocation coefficients to maximize the minimum achievable rate of the legitimate users subject to the achievable rate constraints of the active eavesdropper in parallel. With some continuous approximations, this formulated problem has been solved efficiently by an iterative manner under the path-following algorithms framework

The remainder of this article is as follows. Section 2 describes the secure communication in the considered RIS-aided cell-free massive MIMO system, including the uplink channel estimation and downlink data transmission. Section 3 details the achievable secrecy rate. Section 4 further provides a max–min power control optimization strategy with security constraint. Furthermore, Section 5 presents some simulation results. Finally, the conclusions of the paper are given in Section 6.

1.1. Notation. The matrices and vectors in the paper are represented as uppercase and lowercase boldface letters, respectively. Besides, the superscripts $(\cdot)^T$, $(\cdot)^*$, and $(\cdot)^H$ denote the transpose operator, conjugate operator, and Hermitian (conjugate transpose) operator, respectively. I_n represents the $n \times n$ identity matrix. The expectation is represented as $\mathbb{E}\{\cdot\}$. diag (x) refers to a diagonal matrix consisting of the entries in the main diagonal of vector x. $\log_2(\cdot)$ stands for the base-2 logarithm. $z \sim \mathrm{CN}(\bar{z}, \Sigma)$ represents a circularly symmetric complex Gaussian random vector $z \in \mathbb{C}^{N\times 1}$ with mean $\bar{z}$ and covariance matrix Σ. The notation $\mathbb{C}^{m\times n}$ indicates the $m \times n$ complex matrix space. Finally, $[x]^+$ is the nonnegative projection operation, i.e., $[x]^+ = \max\{x, 0\}$.

2. System Model

As depicted in Figure 1, we take into account a cell-free massive MIMO system consisting M single-antenna APs simultaneously communicating with K single-antenna legitimate users with the existence of an active single-antenna eavesdropper (Eve). All APs are connected to a central processing unit (CPU) via a backhaul link, thereby they can share information. Besides, all APs, all users, and the Eve are randomly located in the coverage area. Considering the scenario that the target users are located far away from the APs, a RIS that comprises N scattering elements is adopted to assist the communication by modifing the phases of the incident signals [18]. In this regard, it is important to unveil the achievable secrecy performance improvement in the considered RIS-aided system. In addition, a quasistatic block fading model is considered in this paper; that is, the transmission channels are frequency flat and static in each coherence interval comprising τ_c symbols. Furthermore, this topology adopts a time division duplex (TDD) protocol, thereby the channel reciprocity can be utilized for CSI estimation.

Then, the line-of-sight (LoS) channel between the kth user and the mth AP can be written as

$$h_{\mathrm{mk}}^d \sim \mathrm{CN}\left(0, \beta_{\mathrm{mk}}^d\right) \in \mathbb{C}^{1\times 1}, \tag{1}$$

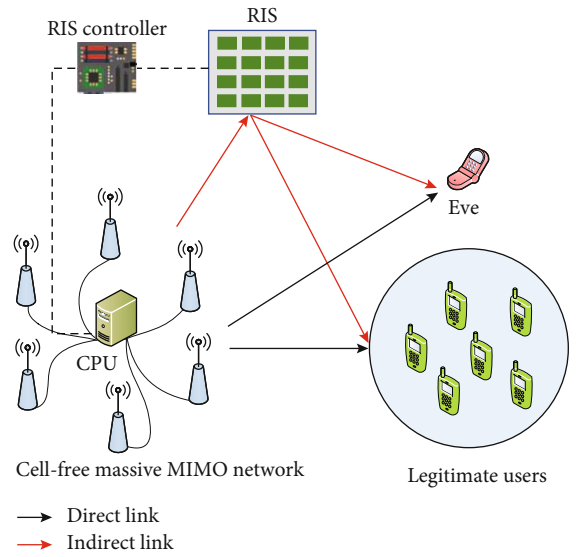

FIGURE 1: Illustration of the secure RIS-aided cell-free massive MIMO network.

where β_{mk}^d denotes the large-scale fading coefficient of the LoS link.

Since this paper considers a harsh propagation conditions with the existence of poor scattering environment or high attenuation as a result of large obstacles, we should consider the issue that the direct links will be unblocked with a given probability. Considering the harsh propagation environments, the large-scale fading coefficient β_{mk}^d is indicated as

$$\beta_{\mathrm{mk}}^d = a_{\mathrm{mk}} \bar{\beta}_{\mathrm{mk}}^d, \tag{2}$$

where large-scale fading coefficient $\bar{\beta}_{\mathrm{mk}}^d$ is composed of the shadow fading and the path loss and the binary variables a_{mk} is associated with the probability that the LoS links are resisted which can be formulated as [18]

$$a_{\mathrm{mk}} = \begin{cases} 1, \text{with a probability } P_r, \\ 0, \text{with a probability } 1 - P_r. \end{cases} \tag{3}$$

Similarly, the channel of the LoS link between the Eve and the mth AP can be denoted by

$$h_{\mathrm{mE}}^d \sim \mathrm{CN}\left(0, \beta_{\mathrm{mE}}^d\right) \in \mathbb{C}^{1\times 1}. \tag{4}$$

The channel between the RIS and the mth AP is expressed as

$$h_{1,m} = \sqrt{\beta_{1,m}}\left[h_{1,m,1}, \cdots, h_{1,m,N}\right] \in \mathbb{C}^{1\times N}, \tag{5}$$

where $\beta_{1,m}$ represents the channel attenuation coefficient and $h_{1,m,n}$, $n = 1, 2, \cdots, N$ represents the small-scale fading with elements being i.i.d. $\mathrm{CN}(0, 1)$ random variables.

Similarly, the channels between the kth user, the Eve, and the RIS can be represented as

$$\begin{aligned} h_{2,k} &= \sqrt{\beta_{2,k}}\left[h_{2,m,1}^{k},\cdots,h_{2,m,N}^{k}\right] \in \mathbb{C}^{1\times N}, \\ h_{2,E} &= \sqrt{\beta_{2,E}}\left[h_{2,m,1}^{E},\cdots,h_{2,m,N}^{E}\right] \in \mathbb{C}^{1\times N}, \end{aligned} \tag{6}$$

where $\beta_{2,k}(\beta_{2,E})$ and $h_{2,m,n}^{k}(h_{2,m,n}^{E})$ are the large-scale channel attenuation coefficient and small-scale attenuation coefficients, respectively.

Besides, the configuration matrix of the RIS can be represented as

$$\Phi = \text{diag}\ (v) \in \mathbb{C}^{N\times N}, \tag{7}$$

where vector v is the RIS reflect beamforming vector, which can be denoted by

$$v = [\xi_1 \exp\ (j\theta_1), \xi_2 \exp\ (j\theta_2),\cdots,\xi_N \exp\ (j\theta_N)] \in \mathbb{C}^{1\times N}, \tag{8}$$

where $\xi_i \in [0,1]$ and $\theta_i \in [0,2\pi]$ represent the amplitude reflection coefficient and phase shift of the ith element in the RIS. Specifically, to achieve the largest array reflection gain, we assume that $\xi_i = 1, \forall i$ in this paper.

This paper focuses on the secure downlink transmission. Consequently, each coherence interval contains two phases: uplink channel estimation and downlink data transmission.

2.1. Uplink Channel Estimation. Under the TDD protocol, the downlink transmission channel can be estimated by uplink training due to the channel reciprocity. The kth user transmits a certain pilot sequence $\sqrt{\tau_p}\varphi_k \in \mathbb{C}^{\tau_p\times 1}$ to the APs where τ_p is the length of uplink training duration and $\|\varphi_k\| = 1$ is the normalized pilot vector. In addition, it is required that $\tau_p < \tau_c$. To avoid the pilot contamination caused by the legitimate users, the system can exploit orthogonal pilot vectors such that $\varphi_{k'}^{H}\varphi_k = 0$ for $k \neq k'$ [45]. Since the used pilot symbols are publicly designed, an active eavesdropper can intervene the channel estimation by sending the same pilot symbols as the target user which is also called spoofing attack. Let $\sqrt{\tau_p}\varphi_E \in \mathbb{C}^{\tau_p\times 1}$ be the Eve's pilot sequence without the loss of generality, let the k_0th user be the target user, that is, $\varphi_E = \varphi_{k_0}$. Consequently, the receiving signal at the mth AP is indicated as

$$\begin{aligned} y_{p,m} = &\sqrt{\tau_p\rho_p}\sum_{k=1}^{K}\left(h_{mk}^{d} + h_{1,m}\boldsymbol{\Phi}\mathbf{h}_{2,k}^{H}\right)\varphi_k \\ &+ \sqrt{\tau_p\rho_p}\left(h_{\text{mE}}^{d} + h_{1,m}\boldsymbol{\Phi}\mathbf{h}_{2,E}^{H}\right)\varphi_E + w_m, \end{aligned} \tag{9}$$

where $w_m \in \mathbb{C}^{\tau_p\times 1}$ denotes the additive noise vector at the mth AP with the distribution as $w_m \sim \text{CN}(0, I_{\tau_p})$.

Due to the coexistence of direct and indirect links caused by the RIS, we aim to estimate the cascaded channel including the direct and indirect links [16]. Based on the above definitions, we define the total cascaded channel between the mth AP and the kth user as

$$g_{\text{mk}} = h_{\text{mk}}^{d} + h_{1,m}\Phi h_{2,k}^{H}. \tag{10}$$

Then, the cascaded channel between the mth AP and the Eve can be written as

$$g_{\text{mE}} = h_{\text{mE}}^{d} + h_{1,m}\Phi h_{2,E}^{H}. \tag{11}$$

According to the central limit theory of great numeral, the cascaded channels g_{mk} and g_{mE} are approximatively distributed as [16].

$$\begin{aligned} g_{\text{mk}} &\sim \text{CN}(0, \beta_{\text{mk}}), \\ g_{\text{mE}} &\sim \text{CN}(0, \beta_{\text{mE}}), \end{aligned} \tag{12}$$

where

$$\begin{aligned} \beta_{\text{mk}} &= \beta_{\text{mk}}^{d} + N\beta_{1,m}\beta_{2,k}, \\ \beta_{\text{mE}} &= \beta_{\text{mE}}^{d} + N\beta_{1,m}\beta_{2,E}. \end{aligned} \tag{13}$$

Besides, the additive quantization noise model (AQNM) could be exploited to evaluate the impact of the low-resolution ADCs at the APs [39, 40]. Hence, the output of the ADCs at the mth AP is expressed as

$$\begin{aligned} \tilde{y}_{p,m} \quad &= \alpha_A y_{p,m} + \tilde{w}_{p,m} = \alpha_A\sqrt{\tau_p\rho_p}\sum_{k=1}^{K} g_{\text{mk}}\varphi_k \\ &+ \alpha_A\sqrt{\tau_p\rho_E}g_{\text{mE}}\varphi_E + \alpha_A w_m + \tilde{w}_{p,m}, \end{aligned} \tag{14}$$

where α_A represents the quantization distortion factor which dictates the quantization precision of the ADC and is related to the number of quantization bits at the APs, b_a. When $b_a > 5$, α_A can be approximately expressed as

$$\alpha = \frac{\sqrt{3}\pi}{2}2^{-2b}. \tag{15}$$

Whereas for $b \leq 5$, the corresponding values of α are listed in Table 1 [40].

Besides, the last term in (14) denotes the additive Gaussian quantization noise component whose covariance matrix can be given by

$$R_{\tilde{w}_{p,m}} = \mathbb{E}\left\{\tilde{w}_{p,m}\tilde{w}_{p,m}^{H}\right\} = \alpha_A(1-\alpha_A)\ \text{diag}\left(\mathbb{E}\left\{\tilde{y}_{p,m}\tilde{y}_{p,m}^{H}\right\}\right). \tag{16}$$

Projecting $\tilde{y}_{p,m}$ onto φ_k^{H}, the postprocessing signal can be given by

$$\begin{aligned} \tilde{y}_{p,m} = &\alpha_A\sqrt{\tau_p\rho_p}g_{\text{mk}} + \alpha_A\sqrt{\tau_p\rho_E}g_{\text{mE}}\delta(k-k_0) \\ &+ \alpha_A\varphi_k^{H}w_m + \varphi_k^{H}\tilde{w}_{p,m}, \end{aligned} \tag{17}$$

Table 1: The corresponding quantization distortion factors for various quantization bits.

b	1	2	3	4	5
α	0.6366	0.8825	0.96546	0.990503	0.997501

where the function $\delta(k-k_0)$ is defined as

$$\delta(k-k_0)=\begin{cases}1, k=k_0,\\ 0, k\neq k_0.\end{cases} \tag{18}$$

Then, we can acquire the channel estimation results in Lemma 1 [46].

Lemma 1. *Based on $\tilde{y}_{p,m}$, the minimum mean-square (MMSE) method can be adopted at the mth AP to estimate the cascaded channel g_{mk} as*

$$\widehat{g}_{mk}=c_{mk}\tilde{y}_{mk}, \tag{19}$$

where

$$c_{mk}=\frac{\sqrt{\tau_p\rho_p}\beta_{mk}}{\tau_p\rho_p\beta_{mk}+\tau_p\rho_E\beta_{mE}\delta(k-k_0)+1}\tilde{y}_{mk}. \tag{20}$$

Also, we can obtain another estimated channel as

$$\widehat{g}_{\mathrm{mE}}=\frac{\sqrt{\rho_E}\beta_{\mathrm{mE}}}{\sqrt{\rho_d}\beta_{\mathrm{mk}_0}}\widehat{g}_{\mathrm{mk}_0}. \tag{21}$$

In addition, both the channel estimation $\widehat{g}_{\mathrm{mk}}$ and the estimation error $\tilde{g}_{\mathrm{mk}}$ are zero mean Gaussian variable with variances as

$$\begin{aligned}\lambda_{\mathrm{mk}}&=\mathbb{E}\{|\widehat{g}_{\mathrm{mk}}\widehat{g}^*_{\mathrm{mk}}|\}=\frac{\alpha_A\tau_p\rho_p\beta^2_{\mathrm{mk}}}{\tau_p\rho_p\beta_{\mathrm{mk}}+\tau_p\rho_E\beta_{\mathrm{mE}}\delta(k-k_0)+1},\\ \mathbb{E}\{|\tilde{g}_{\mathrm{mk}}\tilde{g}^*_{\mathrm{mk}}|\}&=\frac{\beta_{\mathrm{mk}}+(1-\alpha_A)\tau_p\rho_p\beta^2_{\mathrm{mk}}}{\tau_p\rho_p\beta_{\mathrm{mk}}+\tau_p\rho_E\beta_{\mathrm{mE}}\delta(k-k_0)+1}.\end{aligned} \tag{22}$$

Besides, we can define the variance of $\widehat{g}_{\mathrm{mE}}$ as

$$\lambda_{\mathrm{mE}}=\mathbb{E}\{|\widehat{g}_{\mathrm{mE}}\widehat{g}^*_{\mathrm{mE}}|\}=\frac{\rho_E\beta^2_{\mathrm{mE}}}{\rho_d\beta^2_{\mathrm{mk}_0}}\lambda_{\mathrm{mk}_0}. \tag{23}$$

Proof. Please refer to Appendix A. □

It is noted that $\Phi\Phi^H=I_N$. Thus, λ_{mk} and λ_{mE} are independent of RIS's phase shift matrix Φ under the considered system architecture and channel estimation method. Therefore, adopting a random phase shift design at the RIS can be considered as a suboptimal scenario in these settings [16].

Furthermore, the normalized minimum square error (NMSE) can be used to access the performance of the channel estimation which is written as [40]

$$E_N=\frac{\sum_{m=1}^{M}\sum_{k=1}^{K}\mathbb{E}\{\|\tilde{g}_{\mathrm{mk}}\|^2\}}{\sum_{m=1}^{M}\sum_{k=1}^{K}\mathbb{E}\{\|g_{\mathrm{mk}}\|^2\}}=\frac{\sum_{m=1}^{M}\sum_{k=1}^{K}(\beta_{\mathrm{mk}}-\lambda_{\mathrm{mk}})}{\sum_{m=1}^{M}\sum_{k=1}^{K}\beta_{\mathrm{mk}}}. \tag{24}$$

Then, since NMSE is the function of ρ_p, we can consider the asymptotic high-SNR regime as follows.

As $\rho_p\longrightarrow+\infty$, the NMSE converges to

$$\lim_{\rho_p\longrightarrow+\infty}E_N=\frac{\sum_{m=1}^{M}\sum_{k=1}^{K}\left(\beta_{\mathrm{mk}}-\lim_{\rho_p\longrightarrow+\infty}\lambda_{\mathrm{mk}}\right)}{\sum_{m=1}^{M}\sum_{k=1}^{K}\beta_{\mathrm{mk}}}=1-\alpha_A. \tag{25}$$

The above presented result indicates that the NMSE converges to a finite limit by increasing the pilot power of the legitimate users. That is, there will be a nonzero channel estimation error floor which is only determined by quantization distortion factor (quantization bits) of the low-resolution ADCs at the APs and cannot be mitigated by enlarging the number of the APs or enhancing the SNR.

2.2. Downlink Data Transmission. In this section, we shall pay attention to the downlink data transmission. The APs utilize the estimated channel state information to implement conjugate beamforming technique for data transmission. Let ρ_d be the average transmission power of the certain data signal. Besides, the downlink transmitted signal by the mth AP can be designed as

$$x_m=\sqrt{\rho_d}\sum_{k=1}^{K}\sqrt{\eta_{\mathrm{mk}}}\widehat{g}^*_{\mathrm{mk}}s_k, \tag{26}$$

where s_k is the normalized signal intended for the kth user, i.e., $\mathbb{E}\{|s_k|^2\}=1$. η_{mk} are the power control coefficients designed to satisfy the limited power budget constraint at each AP as follows

$$\sum_{k=1}^{K}\eta_{\mathrm{mk}}\lambda_{\mathrm{mk}}\leq 1. \tag{27}$$

As such, with superposition of all transmitted signals, the receiving signal at the kth user is expressed as

$$\begin{aligned}r_k=&\sum_{m=1}^{M}g^T_{\mathrm{mk}}x_m+w_k=\sqrt{\rho_d}\sum_{m=1}^{M}\sqrt{\eta_{\mathrm{mk}}}g_{\mathrm{mk}}\widehat{g}^*_{\mathrm{mk}}q_k\\ &+\sqrt{\rho_d}\sum_{k'\neq k}^{K}\sum_{m=1}^{M}\sqrt{\eta_{\mathrm{mk}'}}g_{\mathrm{mk}}\widehat{g}^*_{\mathrm{mk}'}q_{k'}+w_k,\end{aligned} \tag{28}$$

where $w_k\sim\mathrm{CN}(0,1)$ is the AWGN at the kth user. Furthermore, low-resolution ADCs are exploited at the legitimate

users. To appraise the impact of these low-resolution ADCs, the AQNM is used to describe the quantization processing. As a result, the output of the ADC at the kth user can be expressed as

$$\tilde{r}_k = \alpha_U r_k + \tilde{w}_k = \alpha_U \sqrt{\rho_d} \sum_{m=1}^{M} \sqrt{\eta_{\mathrm{mk}}} g_{\mathrm{mk}} \widehat{g}^*_{\mathrm{mk}} q_k + \alpha_U \sqrt{\rho_d} \sum_{k' \neq k}^{K} \sum_{m=1}^{M} \sqrt{\eta_{\mathrm{mk}'}} g_{\mathrm{mk}} \widehat{g}^*_{\mathrm{mk}'} q_{k'} + \alpha_U w_k + \tilde{w}_k, \tag{29}$$

where α_U indicates the quantization distortion factor of the ADCs, which is related to the relative accuracy of the ADCs, and b_u. $\tilde{w}_k$ denotes the quantization noise whose covariance can be modeled as

$$R_{\tilde{w}_k} = \mathbb{E}\left\{|\tilde{w}_k|^2\right\} = \alpha_U(1-\alpha_U)\mathbb{E}\left\{|r_k|^2\right\}. \tag{30}$$

An active malicious eavesdropper can boost its wiretapping performance by employing ideal hardware and perfect high-resolution ADCs. Since it is difficult for the system to achieve the configuration information of the Eve, this worst-case assumption is reasonable. Then, the receiving signal at the Eve is expressed as

$$r_E = \sum_{m=1}^{M} g^T_{\mathrm{mE}} x_m + w_E = \sqrt{\rho_d} \sum_{m=1}^{M} \sqrt{\eta_{\mathrm{mk}_0}} g_{\mathrm{mE}} \widehat{g}^*_{\mathrm{mk}_0} q_{k_0} + \sqrt{\rho_d} \sum_{k' \neq k_0}^{K} \sum_{m=1}^{M} \sqrt{\eta_{\mathrm{mk}'}} g_{\mathrm{mE}} \widehat{g}^*_{\mathrm{mk}'} q_{k'} + w_E, \tag{31}$$

where $w_E \sim \mathrm{CN}(0,1)$ denotes the additive Gaussian noise at the Eve.

3. Secrecy Performance Analysis

This paper assumes that the delay can be tolerable, and coding with various different independent channel realizations is possible. Therefore, this paper adopts the ergodic secrecy rate as the performance metric to assess the network's secrecy performance. The achievable ergodic secrecy rate is bounded by the difference of the target user's achievable rate and the information leakage to the Eve. Thus, the ergodic secrecy rate is indicated as [28, 29].

$$R^{\mathrm{sec}}_{k_0} = \left[R_{k_0} - C^{\mathrm{Eve}}_{k_0}\right]^+, \tag{32}$$

where R_{k_0} denotes the achievable rate of the target user and $C^{\mathrm{Eve}}_{k_0}$ represents the information capacity of the Eve.

Then, we present a detailed investigation on the achievable rate of the kth user. Considering a realistic case that the kth user only have the statistical effective CSI instead of instantaneous CSI to decode the desired data, the signal $\tilde{r}_k$ can be indicated as

$$\tilde{r}_k = \alpha_U \sqrt{\rho_d} \mathbb{E}\left\{\sum_{m=1}^{M} \sqrt{\eta_{\mathrm{mk}}} g_{\mathrm{mk}} \widehat{g}^*_{\mathrm{mk}}\right\} q_k + n^{\mathrm{eff}}_k, \tag{33}$$

where n^{eff}_k is the effective noise component whose expression is given by (34).

$$n^{\mathrm{eff}}_k = \alpha_U \sqrt{\rho_d} \left(\sum_{m=1}^{M} \sqrt{\eta_{\mathrm{mk}}} g_{\mathrm{mk}} \widehat{g}^*_{\mathrm{mk}} - \mathbb{E}\left\{\sum_{m=1}^{M} \sqrt{\eta_{\mathrm{mk}}} g_{\mathrm{mk}} \widehat{g}^*_{\mathrm{mk}}\right\}\right) q_k + \alpha_U \sqrt{\rho_d} \sum_{k' \neq k}^{K} \sum_{m=1}^{M} \sqrt{\eta_{\mathrm{mk}'}} g_{\mathrm{mk}} \widehat{g}^*_{\mathrm{mk}'} q_{k'} + \alpha_U w_k + \tilde{w}_k. \tag{34}$$

Since the transmitted symbols are intended for various users, the quantization noise and the AWGN component are mutually independent; the achievable rate of the kth user is provided by (35).

$$R_k = \left(1 - \frac{\tau_p}{\tau_c}\right) \log_2\left(1 + \frac{|\mathrm{DS}_k|^2}{\mathbb{E}\left\{|\mathrm{BU}_k|^2\right\} + \sum_{k' \neq k}^{K} \mathbb{E}\left\{|\mathrm{UI}_{k'k}|^2\right\} + \alpha_A^2 + R_{\tilde{w}_k}}\right), \tag{35}$$

where the terms can be given by

$$\mathrm{DS}_k = \alpha_U \sqrt{\rho_d} \mathbb{E}\left\{\sum_{m=1}^{M} \sqrt{\eta_{\mathrm{mk}}} g_{\mathrm{mk}} \widehat{g}^*_{\mathrm{mk}}\right\},$$

$$\mathrm{BU}_k = \alpha_U \sqrt{\rho_d} \cdot \left(\sum_{m=1}^{M} \sqrt{\eta_{\mathrm{mk}}} g_{\mathrm{mk}} \widehat{g}^*_{\mathrm{mk}} - \mathbb{E}\left\{\sum_{m=1}^{M} \sqrt{\eta_{\mathrm{mk}}} g_{\mathrm{mk}} \widehat{g}^*_{\mathrm{mk}}\right\}\right),$$

$$\mathrm{UI}_{k'k} = \alpha_U \sqrt{\rho_d} \sum_{m=1}^{M} \sqrt{\eta_{\mathrm{mk}'}} g_{\mathrm{mk}} \widehat{g}^*_{\mathrm{mk}'}. \tag{36}$$

Furthermore, we can provide the following theorem:

Theorem 2. *In the considered system, the achievable rate of the kth user via RIS with the low-resolution ADCs can be given by (37) listed on the top of the next page.*

$$R_k = \left(1 - \frac{\tau_p}{\tau_c}\right) \log_2\left(1 + \frac{\alpha_U \rho_d \left(\sum_{m=1}^{M} \sqrt{\eta_{\mathrm{mk}}} \lambda_{\mathrm{mk}}\right)^2}{1 + \rho_d \sum_{k'=1}^{K} \sum_{m=1}^{M} \eta_{\mathrm{mk}'} \lambda_{\mathrm{mk}'} \beta_{\mathrm{mk}} + (1-\alpha_U)\rho_d \left(\sum_{m=1}^{M} \sqrt{\eta_{\mathrm{mk}}} \lambda_{\mathrm{mk}}\right)^2}\right). \tag{37}$$

Proof. Please refer to Appendix B. □

Next, we consider the ergodic capacity of the Eve. To obtain some analytical results, we should make another assumption that the Eve can perfectly acknowledge its effective channel gains. The receipt signal at the Eve is expressed as

$$r_E = \sum_{m=1}^{M} g_{\mathrm{mE}}^T x_m + w_E = \mathrm{BU}_{E,k_0} \cdot q_{k_0} + \sum_{k' \neq k_0}^{K} \mathrm{UI}_{E,k'} \cdot q_{k'} + w_E, \tag{38}$$

with the terms being

$$\begin{aligned} \mathrm{BU}_{E,k_0} &= \sqrt{\rho_d} \sum_{m=1}^{M} \sqrt{\eta_{\mathrm{mk}_0}} g_{\mathrm{mE}} \widehat{g}_{\mathrm{mk}_0}^*, \\ \mathrm{UI}_{E,k'} &= \sqrt{\rho_d} \sum_{m=1}^{M} \sqrt{\eta_{\mathrm{mk}'}} g_{\mathrm{mE}} \widehat{g}_{\mathrm{mk}'}^*. \end{aligned} \tag{39}$$

The terms BU_{E,k_0} and $\mathrm{UI}_{E,k'}$ denote the strength of the desired signal and the interference caused by the other users, respectively. Besides, it is not hard to prove that the terms BU_{E,k_0}, $\mathrm{UI}_{E,k'}$, and w_E are pair-wisely uncorrelated. Hence, the ergodic capacity $C_{k_0}^{\mathrm{Eve}}$ can be given by

$$C_{k_0}^{\mathrm{Eve}} = \left(1 - \frac{\tau_p}{\tau_c}\right) \log_2 \left(1 + \frac{\mathbb{E}\left\{\left|\mathrm{BU}_{E,k_0}\right|^2\right\}}{\sum_{k' \neq k_0}^{K} \mathbb{E}\left\{\left|\mathrm{UI}_{E,k'}\right|^2\right\} + 1}\right). \tag{40}$$

Then, we can derive the following result:

Theorem 3. *With an assumptions that the Eve is an equipped ideal ADCs and can know the perfect instantaneous CSI and $C_{k_0}^{Eve}$ is formulated as (41).*

$$C_{k_0}^{Eve} = \left(1 - \frac{\tau_p}{\tau_c}\right) \log_2 \left(1 + \frac{\rho_d \sum_{m=1}^{M} \eta_{mk_0} \lambda_{mk_0} (\lambda_{mE} + \beta_{mE})}{\rho_d \sum_{k' \neq k_0}^{K} \sum_{m=1}^{M} \eta_{mk'} \lambda_{mk'} \beta_{mE} + 1}\right). \tag{41}$$

Proof. Please refer to Appendix C. □

Then, substituting (37) and (41) into (32) can yield the desired tractable expression of the system's achievable ergodic secrecy rate.

4. Power Control Optimization

Since all users are randomly located in the service region, there will be great difference of the achievable rates due to their geographic locations. Hence, adopting a uniform power allocation strategy would result in poor user fairness. With this above consideration, we work to design an optimal power control scheme at the APs by adopting the max–min power control principle which can guarantee the network fairness. Furthermore, to boost the security performance of the considered system, a critical condition restriction can be presented on the achievable rate of the Eve.

To facilitate further analysis in this section, we should define the following matrices and vectors as

$$\begin{aligned} u_k &= \left[\sqrt{\eta_{1k}}, \sqrt{\eta_{2k}}, \cdots, \sqrt{\eta_{\mathrm{Mk}}}\right]^T, \\ a_k &= \sqrt{\rho_d} \left[\lambda_{1k}, \lambda_{2k}, \cdots, \lambda_{\mathrm{Mk}}\right]^T, \\ A_{\mathrm{kk}'} &= \sqrt{\rho_d}\, \mathrm{diag}\left(\sqrt{\beta_{1k}\lambda_{1k'}}, \cdots, \sqrt{\beta_{\mathrm{Mk}}\lambda_{\mathrm{Mk}'}}\right), \\ B_{k'} &= \sqrt{\rho_d}\, \mathrm{diag}\left(\sqrt{\beta_{1E}\lambda_{1k'}}, \cdots, \sqrt{\beta_{\mathrm{ME}}\lambda_{\mathrm{Mk}'}}\right). \end{aligned} \tag{42}$$

Now, let us begin with designing the power allocation coefficients to maximize the minimum achievable ergodic rate of all legitimate users subject to security constraints. The optimization problem is formulated as

$$\begin{aligned} &\max_{\{\eta_{\mathrm{mk}}\}} \min_{k=1,\cdots,K} R_k, \\ &\text{s.t.} \sum_{k=1}^{K} \eta_{\mathrm{mk}} \lambda_{\mathrm{mk}} \leq 1, m = 1, 2, \cdots, M, \\ &\eta_{\mathrm{mk}} \geq 0, \\ &\mathrm{SINR}_E \leq \theta_E, \end{aligned} \tag{43}$$

where SINR means the signal-to-interference-plus-noise ratio and θ_E is the upper bound of the Eve's SINR.

Then, we can use the path-following algorithm to settle this nonconvex optimization problem.

Now, we define a function as

$$f(u_k) = \frac{\rho_d \left(\sum_{m=1}^{M} \sqrt{\eta_{\mathrm{mk}}} \lambda_{\mathrm{mk}}\right)^2}{1 + \rho_d \sum_{k'=1}^{K} \sum_{m=1}^{M} \eta_{\mathrm{mk}'} \lambda_{\mathrm{mk}'} \beta_{\mathrm{mk}}}. \tag{44}$$

It is noted that the objective function in (43) is monotonically increasing with $f(u_k)$. Hence, R_k can be replaced with $f(u_k)$.

Then, using the first-order Taylor approximation, the nonconvex constraint of SINR_E can be approximated by [36].

$$\frac{\left\|B_E u_{k_0}\right\|^2}{\theta_E} \leq \zeta_E^{(\kappa)}(u_k), \tag{45}$$

where the analytical form of the function $\zeta_E^{(\kappa)}(u_k)$ can be indicated as

$$\zeta_E^{(\kappa)}(u_k) \triangleq \sum_{k \neq k_0}^{K} u_k^{(\kappa)^T} B_k^2 \left(2u_k - u_k^{(\kappa)}\right) + 1. \tag{46}$$

(1) Initialization: set $\kappa = 0$, $t_{\min} \le p^*$, $t_{\max} \ge p^*$, and $\varepsilon > 0$, where p^* is the optimal value of the objective function in (47) and ε denotes the tolerance

(2) Set $t = (1/2)1/2(t_{\min} + t_{\max})$, then solve the following optimization problem

$$\max_{\{\eta_{\mathrm{mk}}\}} t,$$

$$\text{s.t.} \left(a_k^T u_k\right)^2 / 1 + \rho_d \sum_{m=1}^{M} \vartheta_m^2 \beta_{\mathrm{mk}} \ge t, k = 1, 2, \cdots, K,$$

$$\sum_{k=1}^{K} \eta_{\mathrm{mk}} \lambda_{\mathrm{mk}} \le \vartheta_m^2, m = 1, 2, \cdots, M,$$

$$0 \le \vartheta_m \le 1,$$

$$\eta_{\mathrm{mk}} \ge 0,$$

$$\left\| B_E u_{k_0} \right\|^2 / \theta_E \le \varphi_E^{(\kappa)}(u_k).$$

Then, update the $\kappa = \kappa + 1$; if the problem is feasible, set the $t_{\min} = t$, or else set that $t_{\max} = t$;

(3) Repeat 2 until the algorithm converges; that is, $t_{\max} - t_{\min} \le \varepsilon$; return $\{\eta_{\mathrm{mk}}\}$ as the optimal power control coefficients

Algorithm 1: Power control optimization algorithm.

Furthermore, we can introduce slack variables ϑ_m [39]. And optimization problem (43) is redescribed as

$$\begin{aligned} &\max_{\{\eta_{\mathrm{mk}}\}} \min_{k=1,\cdots,K} \frac{\left(a_k^T u_k\right)^2}{1 + \rho_d \sum_{m=1}^{M} \vartheta_m^2 \beta_{\mathrm{mk}}}, \\ &\text{s.t.} \sum_{k=1}^{K} \eta_{\mathrm{mk}} \lambda_{\mathrm{mk}} \le \vartheta_m^2, m = 1, 2, \cdots, M, \\ &0 \le \vartheta_m \le 1, \\ &\eta_{\mathrm{mk}} \ge 0, \\ &\frac{\left\| B_E u_{k_0} \right\|^2}{\theta_E} \le \varphi_E^{(\kappa)}(u_k). \end{aligned} \tag{47}$$

It can be noted that objective function in (47) is quasi-concave, and the constraints are convex. Hence, the bisection method can be utilized to resolve the optimization problem. With initialization by some feasible value, the next feasible point can be generated by convex optimization in each step. The optimal power control scheme can be obtained until the algorithm converges. For clarity, the detailed algorithm is presented in Algorithm 1.

Notably, the assumption on the Eve is stringent; since perfect CSI is practically unavailable at the APs. One straightforward extension is to consider the practical scenarios with the partial Eve's CSI or without knowledge of the Eve, which can be taken into account in future works.

5. Numerical and Simulation Results

This section presents some representative simulation results to assess the impact of various parameters on the secrecy performance of the considered secure RIS-aided cell-free massive MIMO system. Unless stated otherwise, some key system parameter settings are as follows: $M = N = 100$, $K = 10$, $\tau_c = 200$, $\tau_p = 10$, $\rho_p = 100$ mW, $\rho_E = 50$ mW, $\rho_d = 200$ mW, and $P_r = 0.2$. Since a harsh communication environment is mainly considered in this paper, the simulations can be operated in some special scenarios [18]. The geographic position of the APs, legitimate users, and the Eve are given in terms of (x, y) coordinates. The M APs are evenly distributed within the subregion, $x, y \in [-250, -250]$ m, while the Eve and the legitimate users are evenly distributed within the subregion, $x, y \in [150, 150]m$. And the RIS is situated at the coordinate origin, i.e., $(x, y) = (0, 0)$. The large-scale fading coefficients are subordinated to the following model as [5, 6]

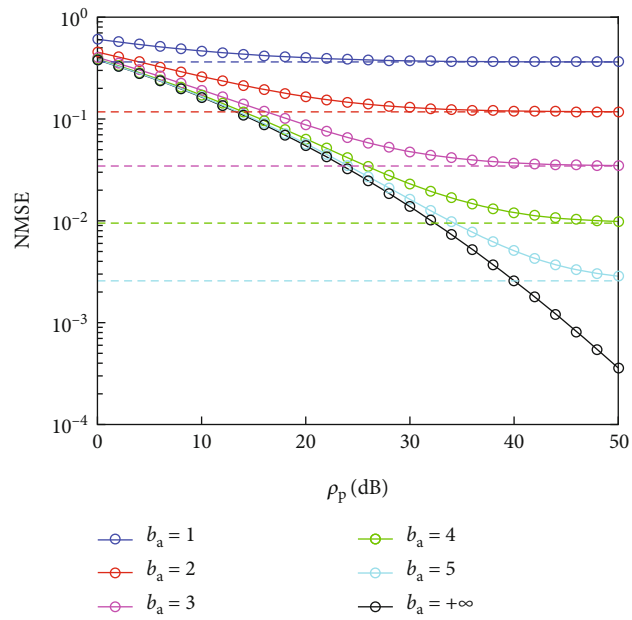

Figure 2: The NMSE of channel estimator versus the pilot power with different quantization bits b_a.

$$\beta = \mathrm{PL} \cdot 10^{(\delta_{\mathrm{sh}} z/10)}, \tag{48}$$

where PL means the path loss and $10^{(\delta_{\mathrm{sh}} z/10)}$ models the shadow fading with standard deviation $\delta_{\mathrm{sh}} = 8$ dB and $z \sim N(0, 1)$. Then, the three-slope model is utilized to simulate

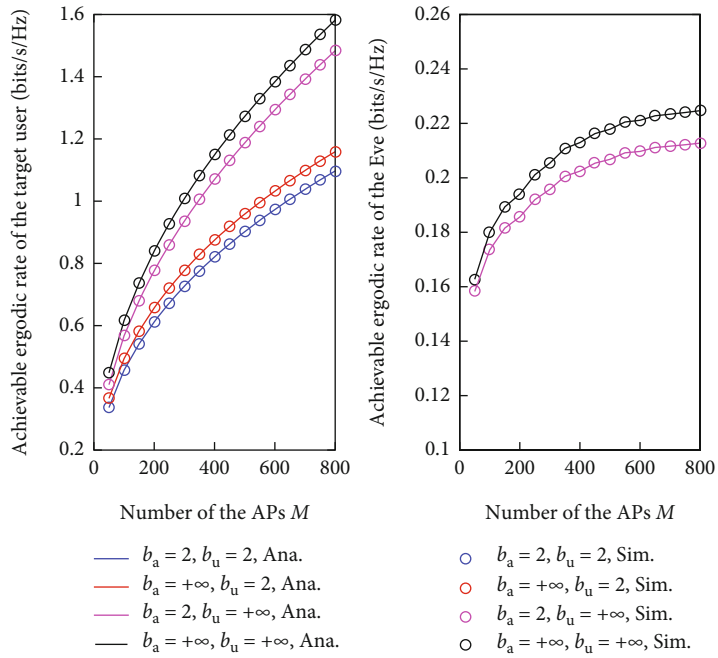

FIGURE 3: The simulated (Sim.) and analytical (Ana.) results versus M against quantization bits b_a and b_u.

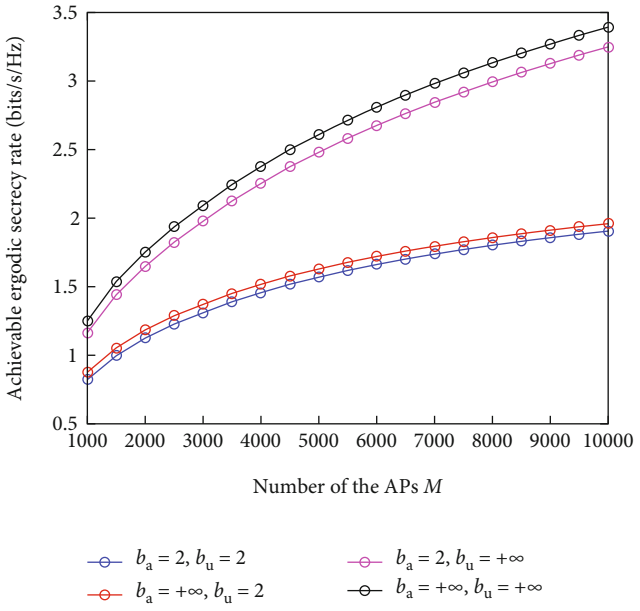

FIGURE 4: The achievable ergodic secrecy rates versus M against quantization bits b_a and b_u.

the path loss in dB, which can be given by

$$\mathrm{PL} = \begin{cases} -L - 35\log_{10}(d), \text{if } d > d_1, \\ -L - 15\log_{10}(d_1) - 20\log_{10}(d), \text{if } d_0 < d \le d_1, \\ -L - 15\log_{10}(d_1) - 20\log_{10}(d_0), \text{if } d \le d_0, \end{cases} \tag{49}$$

where $L = 140.7$ dB, $d_1 = 50$ m, and $d_0 = 10$ m.

Besides, the noise power in W can be expressed as

$$\text{noisepower} = \text{bandwidth} \cdot k_B \cdot T_0 \cdot \text{noisefigure}, \tag{50}$$

where $k_B = 1.381 \times 10^{-23}$(J/Kelvin) denotes the Boltzmann constant and $T_0 = 290$(Kelvin) means the noise temperature. Also, we can set that noisefigure = 9 dB and bandwidth = 20 MHz.

Figure 2 indicates the NMSE of the channel estimator versus the power of the legitimate users' uplink pilot against different quantization bits b_a. It is noted that employing imperfect ADCs at the APs causes higher NMSE, which indicates that implementing low-quality ADCs could give rise to a significant performance degradation in terms of the channel estimation error. Besides, as a result of the low-resolution ADC distortions, some error floors appear at high SNR cases. However, the error floors vanish when the APs are equipped perfect high-quality ADCs at the APs, i.e., $b_a = +\infty$, which means that employing perfect ADCs could achieve an error-free channel estimation with a considerably large ρ_d.

Figure 3 illustrates the achievable rates at the target legitimate user and the Eve of the "Simulated Result" and the "Analytical Result" against different M with different ADC configurations. The "Simulated Result" is obtained via the Monte Carlo simulations by averaging over 10^4 independent channel realizations. We could see that both the achievable rates at the target user and the Eve are monotonically increasing in M. Also, we could observe that the analytical results coincide with the numerical values for all considered cases with high tightness. These comparisons verify the validity of our derived analytical representations. For

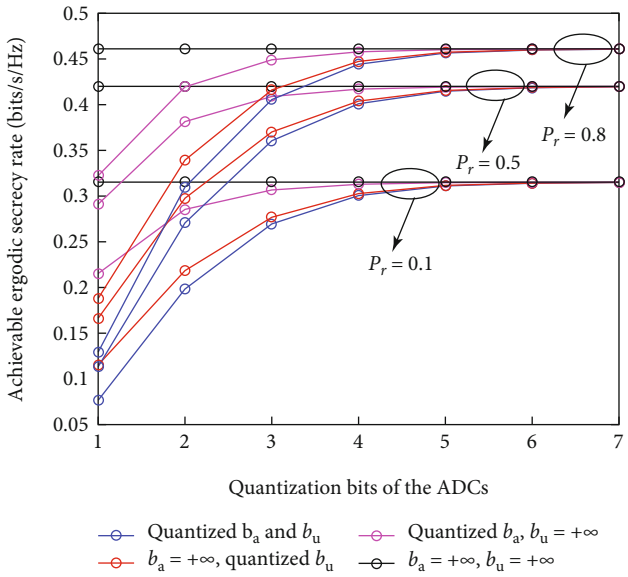

FIGURE 5: The achievable ergodic secrecy rates versus quantization bits.

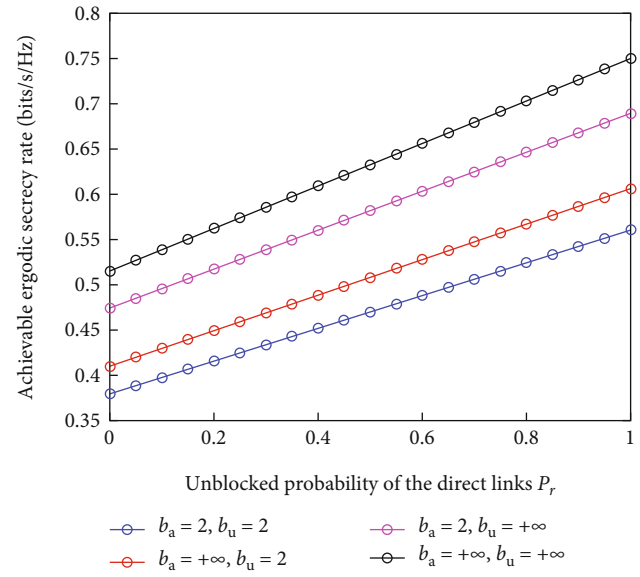

FIGURE 6: The achievable ergodic secrecy rates versus the unblocked probability of the direct links P_r.

simplification, the rest of the simulations can be operated by using the derived closed-form expressions in the paper.

Figure 4 illustrates the achievable ergodic secrecy rate versus M against four different ADC configurations. As expected, the increase of APs yields improved secrecy performance. Furthermore, the ADC configuration has apparent effect on secrecy rates. For instance, the configuration "$b_a = +\infty, b_u = +\infty$" produces the best performance, while the configuration "$b_a = 2, b_u = 2$" brings about the worst performance. Besides, it is clear to note that the system would suffer a trifling performance loss by using low-quality ADCs at the APs. However, the system performance is dominated by the ADC distortion at the users, which indicates that the ADC configuration bring a great effect on the system properties. In other words, low-resolution ADCs could be widely installed at the APs instead of at the user terminals in actual system configuration.

Figure 5 validates the effects of the ADCs' quantization bits on the ergodic secrecy rate against different ADC configuration. We could note that the ergodic secrecy rate increases with the rising of quantization bit and would finally converge to some fixed limit rates when $b \geq 5$, which implies that the 5-bit ADCs are sufficient to replace the ideal ADCs for practical system design. Besides, as expected, employing high-resolution ADCs at the users can achieve larger ergodic secrecy rate, which also verify the conclusion obtained from the Figure 4. These observations suggest that the system should implement low-resolution ADCs at the APs to cut the hardware costing while achieving appreciable performance. From the obtained results, it is observed that the probability P_r also has an imposed prominent effect on the achievable ergodic rate which monotonically increases with the increase of the probability P_r.

Figure 6 shows the influence of the probability P_r on the achievable ergodic secrecy rate. We could see that the

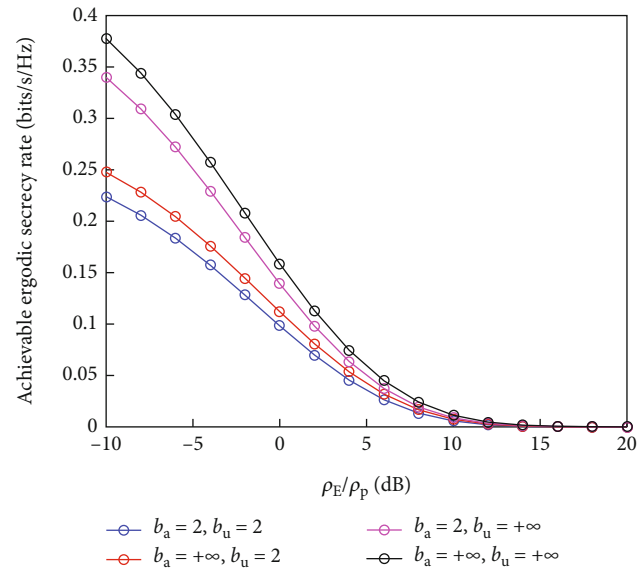

FIGURE 7: The achievable ergodic secrecy rates versus the power ratio between the uplink pilot power of the legitimate users and the Eve.

achievable ergodic secrecy rates increase with the increase of the unblocked probability of the direct links. We could note that the RIS-aided system setup furnishes the largest net throughput. The reason is that the system can conquer the nonexistence of the LoS links due to the existence of the RIS. If the direct links are blocked and unreliable, as expected, the information directly offered by the APs of the system tends to zero. In addition, we can find that the RIS-aided system setup can offer nonzero secrecy

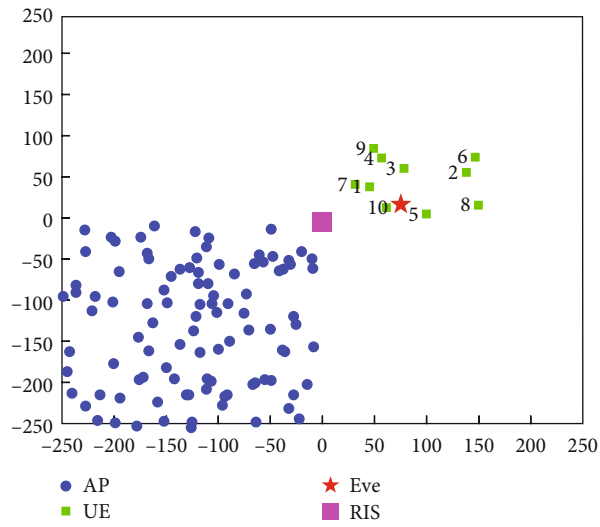

Figure 8: Illustration of the nodes' locations in the considered secure RIS-aided cell-free massive MIMO network.

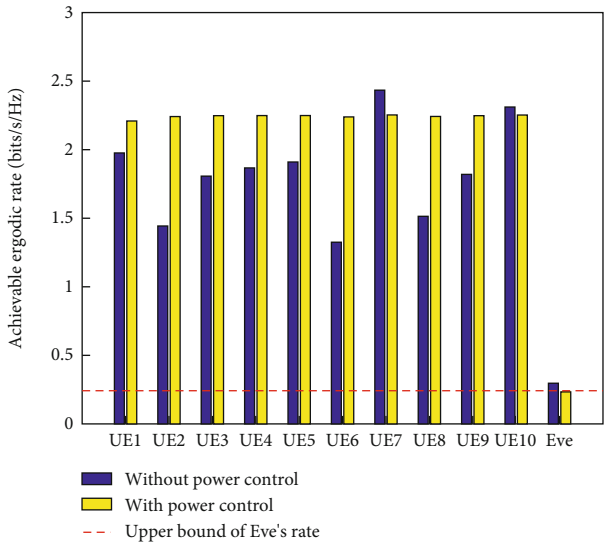

Figure 9: The achievable ergodic rate comparison between the proposed power control scheme and the equal coefficients allocation scheme.

throughput even in the worst scenario that all LoS links are obstructed, i.e., $P_r = 0$. Hence, the presence of the RIS is especially beneficial when P_r is small, since in this case the direct links are incapable to provide a high-information capacity. On this condition, the application of RIS in cell-free massive MIMO is able to offer a high-information throughput and reliable communication.

Figure 7 depicts the curves of the ergodic secrecy rate versus the power ratio between the uplink pilot power of the legitimate users and the Eve. Just as the prediction, the ergodic secrecy rate is decreasing in the power of the Eve and gradually approach zero with an appropriately larger ρ_E. That is, an active wiretapper can improve its eavesdropping ability by increasing its power of the pilot spoofing attack. In addition, the outcomes in Figure 7 indicate that the active eavesdropper leads to a significant degradation of the secrecy capacity and poses a prominent threat for secure communication of the concerned network. To alleviate the negative impact of the Eve, some measures can be operated in the secure communication system, such as active pilot spoofing attack detection, artificial noise aiding, and power control. This is beyond our consideration in this paper, which can be left for the future research.

To appraise the power allocation optimization algorithm, we consider a network configuration as depicted in Figure 8. All APs, the users, and the Eve are all located randomly in the subregions. For the sake of analysing, we assume that Eve is trying to intercept the private messages intended for the 1st user; that is, the first user is the target user. Figure 9 depicts the achievable information rates of the Eve and the users with and without power control. Besides, it is assumed that the users and the APs are all installed with low-quality ADCs ($b_a = b_u = 2$). For the situation without power control, we choose the constant power control coefficients, i.e., $\eta_{\mathrm{mk}} = (\sum_{k'=1}^{K} \lambda_{\mathrm{mk}})^{-1}$, $\forall k = 1, 2, \cdots, K$. From the obtained results, it is easy to observe that the fluctuation of the per user achievable rate with the suggested power allocation scheme has been greatly reduced. Moreover, the max–min power allocation method is operated to maintain the ergodic rate of the Eve under some fixed restriction. It signifies that adopting the max–min power control scheme can concentrate all per users ergodic rate around its median. Therefore, the proposed power control algorithm can maintain better fairness among the users with security constraints. These aforementioned observations can give perceptive insight for optimizing the power allocation in the considered system.

6. Conclusions

This paper studied the secure communication in RIS-aided cell-free massive MIMO system with low-resolution ADCs. To overcome the high overhead of uplink training, a simple and effective aggregated channel estimation scheme is presented to acquire the CSI at the APs. Using the estimated CSI, the conjugate beamforming has been operated at the APs. Under these settings, the tractable closed-form expression for downlink secrecy capacity has been provided in terms of only the channel statistics which is independent of the RIS phase configuration. The derived analytical expressions can be used to evaluate the effects of the CSI estimation error, the quantization bits of the ADCs, the number of APs, and the number of passive reflecting elements in RIS. Moreover, we proposed a power control technique aiming at maximizing the minimum achievable rate of all legitimate users subject to security constraints. Some numerical results have been offered to confirm the analytical conclusions and the efficiency of the power allocation algorithm.

Appendix

A. Proof of Lemma 1

On the basis of the MMSE estimation method, the estimate of the aggregate channel g_{mk} can be obtained as

$$\widehat{g}_{\mathrm{mk}} = \frac{\mathbb{E}\{\tilde{y}^*_{\mathrm{mk}} g_{\mathrm{mk}}\}}{\mathbb{E}\{\tilde{y}^*_{\mathrm{mk}} \tilde{y}_{\mathrm{mk}}\}} \tilde{y}_{\mathrm{mk}}. \tag{51}$$

First, due to the statistical characteristics of the channel g_{mk} and the terms of $\tilde{y}^*_{\mathrm{mk}}$, the expression $\mathbb{E}\{\tilde{y}^*_{\mathrm{mk}} g_{\mathrm{mk}}\}$ can be computed as

$$\mathbb{E}\{\tilde{y}^*_{\mathrm{mk}} g_{\mathrm{mk}}\} = \alpha_A \sqrt{\tau_p \rho_p}\, \mathbb{E}\{g^*_{\mathrm{mk}} g_{\mathrm{mk}}\} = \alpha_A \sqrt{\tau_p \rho_p}\, \beta_{\mathrm{mk}}. \tag{52}$$

Next, the term $\mathbb{E}\{\tilde{y}^*_{\mathrm{mk}} \tilde{y}_{\mathrm{mk}}\}$ can be calculated as

$$\begin{aligned}\mathbb{E}\{\tilde{y}^*_{\mathrm{mk}} \tilde{y}_{\mathrm{mk}}\} &= \alpha_A^2 \tau_p \rho_p \beta_{\mathrm{mk}} + \alpha_A^2 \tau_p \rho_E \beta_{\mathrm{mE}} \delta(k - k_0) \\ &\quad + \alpha_A^2 \mathbb{E}\left(\left|\varphi_k^H w_m\right|^2\right) + \mathbb{E}\left(\left|\varphi_k^H \tilde{w}_{p,m}\right|^2\right).\end{aligned} \tag{53}$$

Since the vector φ_k is a normalized vector, we can get that

$$\mathbb{E}\left(\left|\varphi_k^H w_m\right|^2\right) = 1. \tag{54}$$

According to [39], the covariance matrix of the quantization noise $\tilde{w}_{p,m}$ can be denoted as

$$\begin{aligned}R_{\tilde{w}_{p,m}} &= \alpha_A(1 - \alpha_A)\ \mathrm{diag}\left(\mathbb{E}\left\{\tilde{y}_{p,m} \tilde{y}^H_{p,m}\right\}\right) \\ &= \alpha_A(1 - \alpha_A)\mathbb{E}\left(y_{p,m} y^H_{p,m}\right)\ \mathrm{diag}\left(I_{\tau_p}\right),\end{aligned} \tag{55}$$

where the term $\mathbb{E}(y_{p,m} y^H_{p,m})$ can be given by

$$\mathbb{E}\left(y_{p,m} y^H_{p,m}\right) = \tau_p \rho_p \beta_{\mathrm{mk}} + \tau_p \rho_E \beta_{\mathrm{mE}} \delta(k - k_0) + 1. \tag{56}$$

Hence, substituting (52) and (56) into (51), we can obtain the channel estimate as

$$\widehat{g}_{\mathrm{mk}} = \frac{\sqrt{\tau_p \rho_p}\, \beta_{mk}}{\tau_p \rho_p \beta_{\mathrm{mk}} + \tau_p \rho_E \beta_{\mathrm{mE}} \delta(k - k_0) + 1} \tilde{y}_{\mathrm{mk}}. \tag{57}$$

Then, we can easily obtain that

$$\lambda_{\mathrm{mk}} = \frac{\alpha_A \tau_p \rho_p \beta^2_{\mathrm{mk}}}{\tau_p \rho_p \beta_{\mathrm{mk}} + \tau_p \rho_E \beta_{\mathrm{mE}} \delta(k - k_0) + 1}. \tag{58}$$

Now, we finish the proof.

B. Proof of Theorem 2

To acquire the analytical closed-form representation of R_k, the essential issue is to analyse the expressions of DS_k, $\mathbb{E}\{|\mathrm{BU}_k|^2\}$, $\mathbb{E}\{|\mathrm{UI}_{k'k}|^2\}$, and $R_{\tilde{w}_k}$, respectively.

First, we can calculate DS_k as

$$\begin{aligned}\mathrm{DS}_k &= \alpha_U \sqrt{\rho_d}\, \mathbb{E}\left\{\sum_{m=1}^{M} \sqrt{\eta_{\mathrm{mk}}} (\widehat{g}_{\mathrm{mk}} + \tilde{g}_{\mathrm{mk}}) \widehat{g}^*_{\mathrm{mk}}\right\} \\ &= \alpha_U \sqrt{\rho_d}\, \mathbb{E}\left\{\sum_{m=1}^{M} \sqrt{\eta_{\mathrm{mk}}} \widehat{g}_{\mathrm{mk}} \widehat{g}^*_{\mathrm{mk}}\right\} = \alpha_U \sqrt{\rho_d \eta_{\mathrm{mk}}}\, \lambda_{\mathrm{mk}}.\end{aligned} \tag{59}$$

Then, we compute $\mathbb{E}\{|\mathrm{BU}_k|^2\}$ as

$$\begin{aligned}\mathbb{E}\left\{|\mathrm{BU}_k|^2\right\} &= \alpha_U^2 \rho_d \mathbb{E}\left\{\left|\sum_{m=1}^{M} \sqrt{\eta_{\mathrm{mk}}} g_{\mathrm{mk}} \widehat{g}^*_{\mathrm{mk}}\right|^2\right\} \\ &\quad - \mathrm{DS}_k^2 = \alpha_U^2 \rho_d \sum_{m=1}^{M} \eta_{\mathrm{mk}} \mathbb{E}\{\widehat{g}_{\mathrm{mk}} g^*_{\mathrm{mk}} g_{\mathrm{mk}} \widehat{g}^*_{\mathrm{mk}}\} \\ &\quad + \alpha_U^2 \rho_d \sum_{m=1}^{M} \sum_{m' \neq m}^{M} \\ &\quad \sqrt{\eta_{\mathrm{mk}} \eta_{m'\mathrm{k}}}\, \mathbb{E}\left\{\widehat{g}_{\mathrm{mk}} g^*_{\mathrm{mk}} g_{m'k} \widehat{g}^*_{m'k}\right\} - \mathrm{DS}_k^2,\end{aligned} \tag{60}$$

where

$$\mathbb{E}\{\widehat{g}_{\mathrm{mk}} g^*_{\mathrm{mk}} g_{\mathrm{mk}} \widehat{g}^*_{\mathrm{mk}}\} = \lambda^2_{\mathrm{mk}} + \lambda_{\mathrm{mk}} \beta_{\mathrm{mk}}, \tag{61}$$

$$\mathbb{E}\left\{\widehat{g}_{\mathrm{mk}} g^*_{\mathrm{mk}} g_{m'k} \widehat{g}^*_{m'k}\right\} = \lambda_{\mathrm{mk}} \lambda_{m'k}. \tag{62}$$

Substituting (61) and (62) into (60), it is easy to get the expression as

$$\mathbb{E}\left\{|\mathrm{BU}_k|^2\right\} = \alpha_U^2 \rho_d \sum_{m=1}^{M} \eta_{\mathrm{mk}} \lambda_{\mathrm{mk}} \beta_{\mathrm{mk}}. \tag{63}$$

Next, we show solicitude for the evaluation of $\mathbb{E}\{|\mathrm{UI}_{k'k}|^2\}$ as

$$\begin{aligned}\mathbb{E}\left\{|\mathrm{UI}_{k'k}|^2\right\} &= \alpha_U^2 \rho_d \sum_{m=1}^{M} \eta_{\mathrm{mk}'} \mathbb{E}\left\{g_{\mathrm{mk}} \widehat{g}^*_{\mathrm{mk}'} \widehat{g}_{\mathrm{mk}'} g^*_{\mathrm{mk}}\right\} \\ &= \alpha_U^2 \rho_d \sum_{m=1}^{M} \eta_{\mathrm{mk}'} \lambda_{\mathrm{mk}'} \beta_{\mathrm{mk}}.\end{aligned} \tag{64}$$

We notice that the variance of the quantization noise component $\tilde{w}_k$ is written as

$$R_{\tilde{w}_k} = \alpha_U(1 - \alpha_U)(1 + \rho_d D_k), \tag{65}$$

where

$$D_k = \sum_{k'=1}^{K} \sum_{k''=1}^{K} \sum_{m=1}^{M} \sum_{m'=1}^{M} \sqrt{\eta_{\mathrm{mk}'} \eta_{m'k''}}\, \mathbb{E}\left\{g_{\mathrm{mk}} \widehat{g}^*_{\mathrm{mk}'} \widehat{g}_{m'k''} g^*_{m'k}\right\}. \tag{66}$$

Using some simple algebraic manipulations, it is not hard to obtain that

$$D_k = \sum_{k'=1}^{K}\sum_{m=1}^{M}\eta_{\mathrm{mk}'}\lambda_{\mathrm{mk}'}\beta_{\mathrm{mk}} + \sum_{m=1}^{M}\sum_{m'=1}^{M}\sqrt{\eta_{\mathrm{mk}}\eta_{m'k}}\lambda_{\mathrm{mk}}\lambda_{m'k}. \tag{67}$$

Finally, substituting (59), (63), (64), and (65) into (35), we can get the desired result as (37).

C. Proof of Theorem 3

At first we pay attention to the component $\mathbb{E}\{|\mathrm{BU}_{E,k_0}|^2\}$ as

$$\begin{aligned}\mathbb{E}\left\{\left|\mathrm{BU}_{E,k_0}\right|^2\right\} &= \rho_d\sum_{m=1}^{M}\eta_{\mathrm{mk}_0}\mathbb{E}\left\{\left|g_{\mathrm{mE}}\widehat{g}^*_{\mathrm{mk}_0}\right|^2\right\}\\ &= \rho_d\sum_{m=1}^{M}\eta_{\mathrm{mk}_0}\mathbb{E}\left\{\left|(\widehat{g}_{\mathrm{mE}}+\tilde{g}_{\mathrm{mE}})\widehat{g}^*_{\mathrm{mk}_0}\right|^2\right\}\\ &= \rho_d\sum_{m=1}^{M}\eta_{\mathrm{mk}_0}\left(\mathbb{E}\left\{\left|\widehat{g}_{\mathrm{mE}}\widehat{g}^*_{\mathrm{mk}_0}\right|^2\right\}+\mathbb{E}\left\{\left|\tilde{g}_{\mathrm{mE}}\widehat{g}^*_{\mathrm{mk}_0}\right|^2\right\}\right)\\ &= \rho_d\sum_{m=1}^{M}\eta_{\mathrm{mk}_0}\\ &\quad\left[2\lambda_{\mathrm{mk}_0}\lambda_{\mathrm{mE}}+(\beta_{\mathrm{mE}}-\lambda_{\mathrm{mE}})\lambda_{\mathrm{mk}_0}\right]\\ &= \rho_d\sum_{m=1}^{M}\eta_{\mathrm{mk}_0}\lambda_{\mathrm{mk}_0}(\lambda_{\mathrm{mE}}+\beta_{\mathrm{mE}}).\end{aligned} \tag{68}$$

Next, let us calculate the component $\mathbb{E}\{|\mathrm{UI}_{E,k'}|^2\}$ as

$$\begin{aligned}\mathbb{E}\left\{\left|\mathrm{UI}_{E,k'}\right|^2\right\} &= \rho_d\sum_{m=1}^{M}\eta_{\mathrm{mk}'}\mathbb{E}\left\{\left|g_{\mathrm{mE}}\widehat{g}^*_{\mathrm{mk}'}\right|^2\right\}\\ &= \rho_d\sum_{m=1}^{M}\eta_{\mathrm{mk}'}\mathbb{E}\left\{\left|(\widehat{g}_{\mathrm{mE}}+\tilde{g}_{\mathrm{mE}})\widehat{g}^*_{\mathrm{mk}'}\right|^2\right\}\\ &= \rho_d\sum_{m=1}^{M}\eta_{\mathrm{mk}'}\left(\mathbb{E}\left\{\left|\widehat{g}_{\mathrm{mE}}\widehat{g}^*_{\mathrm{mk}'}\right|^2\right\}+\mathbb{E}\left\{\left|\tilde{g}_{\mathrm{mE}}\widehat{g}^*_{\mathrm{mk}'}\right|^2\right\}\right)\\ &= \rho_d\sum_{m=1}^{M}\eta_{\mathrm{mk}'}[\lambda_{\mathrm{mE}}\lambda_{\mathrm{mk}'}+(\beta_{\mathrm{mE}}-\lambda_{\mathrm{mE}})\lambda_{\mathrm{mk}'}]\\ &= \rho_d\sum_{m=1}^{M}\eta_{\mathrm{mk}'}\beta_{\mathrm{mE}}\lambda_{\mathrm{mk}'}.\end{aligned} \tag{69}$$

Finally, substituting (68) and (69) into (40), we can obtain the expression as (41).

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the China Postdoctoral Science Foundation under Grant 2021MD703980 and in part by the National Natural Science Foundation of China under Grant 61901502 and 61901497.

References

[1] E. Shi, J. Zhang, S. Chen et al., "Wireless Energy Transfer in RIS-Aided Cell-Free Massive MIMO Systems: Opportunities and Challenges," *IEEE Communications Magazine*, vol. 60, no. 3, pp. 26–32, 2022.

[2] M. Matthaiou, O. Yurduseven, H. Q. Ngo, D. Morales-Jimenez, S. L. Cotton, and V. F. Fusco, "The road to 6G: ten physical layer challenges for communications engineers," *IEEE Communications Magazine*, vol. 59, no. 1, pp. 64–69, 2021.

[3] P. Liu, K. Luo, D. Chen, and T. Jiang, "Spectral efficiency analysis of cell-free massive MIMO systems with zero-forcing detector," *IEEE Transactions on Wireless Communications*, vol. 19, no. 2, pp. 795–807, 2020.

[4] S. Chen, J. Zhang, E. Björnson, J. Zhang, and B. Ai, "Structured massive access for scalable cell-free massive MIMO systems," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 4, pp. 1086–1100, 2021.

[5] H. Q. Ngo, A. Ashikhmin, H. Yang, E. G. Larsson, and T. L. Marzetta, "Cell-free massive MIMO versus small cells," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 1834–1850, 2017.

[6] H. Q. Ngo, L. Tran, T. Q. Duong, M. Matthaiou, and E. G. Larsson, "On the total energy efficiency of cell-free massive MIMO," *IEEE Transactions on Green Communications and Networking*, vol. 2, no. 1, pp. 25–39, 2018.

[7] D. Wang, M. Wang, P. Zhu, J. Li, J. Wang, and X. You, "Performance of network-assisted full-duplex for cell-free massive MIMO," *IEEE Transactions on Communications*, vol. 68, no. 3, pp. 1464–1478, 2020.

[8] E. Björnson, O. Özdogan, and E. G. Larsson, "Reconfigurable intelligent surfaces: three myths and two critical questions," *IEEE Communications Magazine*, vol. 58, no. 12, pp. 90–96, 2020.

[9] Z. Lin, H. Niu, K. An et al., "Refracting RIS-aided hybrid satellite-terrestrial relay networks: joint beamforming design and optimization," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 58, no. 4, pp. 3717–3724, 2022.

[10] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: intelligent reflecting surface aided wireless network," *IEEE Communications Magazine*, vol. 58, no. 1, pp. 106–112, 2020.

[11] Y. Li, M. Jiang, Q. Zhang, and J. Qin, "Joint beamforming design in multi-cluster MISO NOMA reconfigurable intelligent surface-aided downlink communication networks," *IEEE Transactions on Communications*, vol. 69, no. 1, pp. 664–674, 2021.

[12] H. Du, J. Zhang, J. Cheng, and B. Ai, "Millimeter wave communications with reconfigurable intelligent surfaces: performance analysis and optimization," *IEEE Transactions on Communications*, vol. 69, no. 4, pp. 2752–2768, 2021.

[13] S. Hong, C. Pan, H. Ren, K. Wang, K. K. Chai, and A. Nallanathan, "Robust transmission design for intelligent reflecting surface-aided secure communication systems with imperfect cascaded CSI," *IEEE Transactions on Wireless Communications*, vol. 20, no. 4, pp. 2487–2501, 2020.

[14] E. Björnson and L. Sanguinetti, "Power Scaling Laws and Near-Field Behaviors of Massive MIMO and Intelligent Reflecting Surfaces," *IEEE Open Journal of the Communications Society*, vol. 1, pp. 1306–1324, 2020.

[15] A. A. Khalil, M. Y. Selim, and M. A. Rahman, "CURE: enabling RF energy harvesting using cell-free massive MIMO UAVs assisted by RIS," in *Proc. 46th IEEE Conf. Local Comput. Netw. (LCN)*, pp. 533–540, Edmonton, AB, Canada, 2021.

[16] B. Al-Nahhas, M. Obeed, A. Chaaban, and M. J. Hossain, "RIS-aided cell-free massive MIMO: performance analysis and competitiveness," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, pp. 1–6, Montreal, QC, Canada, 2021.

[17] Y. Zhang, B. Di, H. Zhang, J. Lin, Y. Li, and L. Song, "Reconfigurable intelligent surface aided cell-free MIMO communications," *IEEE Wireless Communications Letters*, vol. 10, no. 4, pp. 775–779, 2021.

[18] T. Van Chien, H. Q. Ngo, S. Chatzinotas, M. Di Renzo, and B. Ottersten, "Reconfigurable intelligent surface-assisted cell-free massive MIMO systems over spatially-correlated channels," *IEEE Transactions on Wireless Communications*, vol. 21, no. 7, pp. 5106–5128, 2022.

[19] T. Zhou, K. Xu, X. Xia, W. Xie, and J. Xu, "Achievable rate optimization for aerial intelligent reflecting surface-aided cell-free massive MIMO system," *IEEE Access*, vol. 9, pp. 3828–3837, 2021.

[20] C. Feng and H. -M. Wang, "Secure Short-Packet Communications at the Physical Layer for 5G and Beyond," *IEEE Communications Standards Magazine*, vol. 5, no. 3, pp. 96–102, 2021.

[21] A. K. Yerrapragada, T. Eisman, and B. Kelley, "Physical layer security for beyond 5G: ultra secure low latency communications," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 2232–2242, 2021.

[22] K. An, M. Lin, J. Ouyang, and W. P. Zhu, "Secure transmission in cognitive satellite terrestrial networks," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 11, pp. 3025–3037, 2016.

[23] B. Li, Z. Fei, C. Zhou, and Y. Zhang, "Physical-layer security in space information networks: a survey," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 33–52, 2020.

[24] Z. Lin, K. An, H. Niu et al., "SLNR-based Secure Energy Efficient Beamforming in Multibeam Satellite Systems," *IEEE Transactions on Aerospace and Electronic Systems*, pp. 1–4, 2022.

[25] X. Chen, C. Zhong, C. Yuen, and H. Chen, "Multi-antenna relay aided wireless physical layer security," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 40–46, 2015.

[26] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: an overview on passive eavesdropping and active attacks," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 21–27, 2015.

[27] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20–27, 2015.

[28] J. Zhu, R. Schober, and V. K. Bhargava, "Secure transmission in multicell massive MIMO systems," *IEEE Transactions on Wireless Communications*, vol. 13, no. 9, pp. 4766–4781, 2014.

[29] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission with an active eavesdropper," *IEEE Transactions on Information Theory*, vol. 62, no. 7, pp. 3880–3900, 2016.

[30] J. Zhu, R. Schober, and V. K. Bhargava, "Linear precoding of data and artificial noise in secure massive MIMO systems," *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 2245–2261, 2016.

[31] X. Zhang, D. Guo, and K. Guo, "Secure performance analysis for multi-pair AF relaying massive MIMO systems in Ricean channels," *IEEE Access*, vol. 6, pp. 57708–57720, 2018.

[32] X. Zhang, D. Guo, K. Guo, and H. Niu, "Secure performance analysis and detection of pilot attack in massive multiple-input multiple-output system," *International Journal of Distributed Sensor Networks*, vol. 14, no. 5, Article ID 155014771877692, 2018.

[33] J. Zhu, D. W. K. Ng, N. Wang, R. Schober, and V. K. Bhargava, "Analysis and design of secure massive MIMO systems in the presence of hardware impairments," *IEEE Transactions on Wireless Communications*, vol. 16, no. 3, pp. 2001–2016, 2017.

[34] X. Zhang, D. Guo, K. An, W. Ma, and K. Guo, "Secure transmission and power allocation in multiuser distributed massive MIMO systems," *Wireless Networks*, vol. 26, no. 2, pp. 941–954, 2020.

[35] K. Guo, Y. Guo, and G. Ascheid, "Security-constrained power allocation in MU-massive-MIMO with distributed antennas," *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 8139–8153, 2016.

[36] T. M. Hoang, H. Q. Ngo, T. Q. Duong, H. D. Tuan, and A. Marshall, "Cell-free massive MIMO networks: optimal power control against active eavesdropping," *IEEE Transactions on Communications*, vol. 66, no. 10, pp. 4724–4737, 2018.

[37] X. Zhang, D. Guo, K. An, Z. Ding, and B. Zhang, "Secrecy analysis and active pilot spoofing attack detection for multigroup multicasting cell-free massive MIMO systems," *IEEE Access*, vol. 7, pp. 57332–57340, 2019.

[38] X. Zhang, D. Guo, K. An, and B. Zhang, "Secure communications over cell-free massive MIMO networks with hardware impairments," *IEEE Systems Journal*, vol. 14, no. 2, pp. 1909–1920, 2020.

[39] X. Hu, C. Zhong, X. Chen, W. Xu, H. Lin, and Z. Zhang, "Cell-free massive MIMO systems with low resolution ADCs," *IEEE Transactions on Communications*, vol. 67, no. 10, pp. 6844–6857, 2019.

[40] Y. Zhang, M. Zhou, Y. Cheng, L. Yang, and H. Zhu, "RF impairments and low-resolution ADCs for nonideal uplink cell-free massive MIMO systems," *IEEE Systems Journal*, vol. 15, no. 2, pp. 2519–2530, 2021.

[41] J. Dai, Y. Wang, C. Pan, K. Zhi, H. Ren, and K. Wang, "Reconfigurable intelligent surface aided massive MIMO systems with low-resolution DACs," *IEEE Communications Letters*, vol. 25, no. 9, pp. 3124–3128, 2021.

[42] X. Zhang, T. Liang, and K. An, "Secrecy performance analysis of cell-free massive MIMO in the presence of active eavesdropper with low resolution ADCs," *Wireless Networks*, vol. 27, no. 7, pp. 4839–4852, 2021.

[43] X. Zhang, T. Liang, K. An, G. Zheng, and S. Chatzinotas, "Secure transmission in cell-free massive MIMO with RF

impairments and low-resolution ADCs/DACs," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 9, pp. 8937–8949, 2021.

[44] X. Zhang, T. Liang, K. An, H. Yang, and C. Niu, "Secure Transmission in RIS-Assisted Cell-free Massive MIMO system with Low Resolution ADCs/DACs," in *2022 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 339–344, Austin, TX, USA, 2022.

[45] P. Liu, S. Jin, T. Jiang, Q. Zhang, and M. Matthaiou, "Pilot power allocation through user grouping in multi-cell massive MIMO systems," *IEEE Transactions on Communications*, vol. 65, no. 4, pp. 1561–1574, 2017.

[46] P. Liu and T. Jiang, "Channel estimation performance analysis of massive MIMO IoT systems with Ricean fading," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 6114–6126, 2021.