Secure Power Control for Downlink Cell-Free Massive MIMO With Passive Eavesdroppers

Junguk Park, Sangseok Yun, Member, IEEE, and Jeongseok Ha, Senior Member, IEEE

Abstract—This work studies secure communications for a cell-free massive multiple-input multiple-output (CF-mMIMO) network which is attacked by multiple passive eavesdroppers overhearing communications between access points (APs) and users in the network. It will be revealed that the distributed APs in CF-mMIMO allow not only legitimate users but also eavesdroppers to reap the diversity gain, which seriously degrades secrecy performance. In addition, by the principle of order statistics, the secrecy performance is further degraded as the number of eavesdroppers increases. Motivated by these, this work proposes an artificial noise-aided secure power control scheme for CF-mMIMO under passive eavesdropping aiming to achieve a higher secrecy rate and/or guaranteed secrecy performance, i.e., minimum secrecy rate. In particular, it will be demonstrated that the secure power control is especially important to guarantee the secrecy fairness. The performance of the proposed power control scheme is evaluated and compared with various power control schemes via numerical experiments, which clearly shows that the proposed power control scheme outperforms all the competing schemes.

Index Terms—Downlink cell-free massive MIMO, physical layer security, power control, spatially correlated Rician fading.

I. INTRODUCTION

Recently, cell-free massive multiple-input multiple-output (CF-mMIMO) has been gaining attention as a promising network structure for beyond 5G (B5G) networks, since it can provide uniformly high quality of service for all users throughout the coverage area [1], [2]. In contrast to conventional co-located massive MIMO (mMIMO) which co-locates a massive number of antennas at an access point (AP), CF-mMIMO has a massive number of APs distributed across a network. In addition, all APs in the network cooperatively serve all users. These features of CF-mMIMO provide the spatial diversity gain and the array gain resulting from the distributed APs and the cooperative beamforming, respectively [3].

The broadcast nature of wireless channels makes challenges in securing wireless communication systems. Physical layer security (PLS) has been considered as one of enabling technologies for constructing secure communication systems in B5G networks [4] including UAV-aided networks [5], [6] and UDN networks [7]. Unlike conventional security measures based on computational cryptography, PLS utilizes physical layer resources to achieve security goals. In addition, PLS builds on the information-theoretic security which brings inherent advantages, such as unconditionally perfect secrecy and scalability. Thus, there have been notable efforts to construct PLS-based secure CF-mMIMO systems, such as secure power control schemes [8], [9], [10], [11], [12], [13] and pilot spoofing attack detection [14].

In [8], the achievable secrecy rate in the presence of an active eavesdropper was analyzed. In particular, the authors proposed a power control scheme with artificial noise (AN) for maximizing the achievable secrecy rate of the user under attack. Meanwhile, the authors in [9] considered two different power control problems without AN in the presence of an active eavesdropper. They formulated optimization problems to maximize the secrecy rate of the attacked user and minimize the power consumption. In [10], the authors investigated the impact of hardware impairments on an achievable secrecy rate under pilot spoofing attack. It was also investigated the impact of Rician fading and low-resolution digital-to-analog converters on the secrecy performance under pilot spoofing attack in [11]. Secrecy performance in simultaneous wireless information and power transfer CF-mMIMO with an active eavesdropper has been studied in [12]. Recently, reconfigurable intelligent surface-assisted secure CF-mMIMO was investigated in [13]. The pilot spoofing attack detection with downlink training strategy was studied in [14].

The aforementioned studies of PLS for CF-mMIMO focus on an active eavesdropping attack called pilot spoofing/contamination attack [15] in which an active eavesdropper transmits the same pilot signal as the one for a target user to tilt the direction of the beamforming towards the attacker. Contrary to the active eavesdropper, a passive eavesdropper does not tamper with the signal of the target users, e.g., pilot signals, and instead passively overhears the transmitted signals to the target user. It is well known [16] that co-located mMIMO selectively provides the benefit of array gain to legitimate users, which allows the legitimate users to achieve secrecy capacity close to the capacity of ordinary communication without further effort for secrecy, e.g., AN signals.

It seems that a large number of transmit antennas in CF-mMIMO, while distributed across a network, also empower the legitimate parties to nullify the passive eavesdropping as observed in co-located mMIMO. This is in part why the passive eavesdropping in CF-mMIMO has not been touched yet. However, contrary to co-located mMIMO, as the number of APs in CF-mMIMO increases, not only legitimate users but also eavesdroppers can enjoy the benefit of the spatial diversity, which exposes legitimate users in CF-mMIMO to the threat of passive eavesdropping. In addition, by the principle of order statistics, the threat of passive eavesdropping is more exacerbated as the number of eavesdroppers increases. This challenge motivates us to investigate a novel secure power control scheme for CF-mMIMO under passive eavesdropping. In particular, we will demonstrate the vulnerability of CF-mMIMO to passive eavesdropping and also develop an AN-aided secure power control scheme for CF-mMIMO attacked by multiple passive eavesdroppers. To formulate the secure power control as an optimization problem, we derive a lower bound on the secrecy rate with AN in a closed-form under spatially correlated Rician fading. Then, we devise an AN-aided secure power control algorithm which maximizes the minimum secrecy rate among all users. The comprehensive performance comparisons reveal that the existing non-secure power control scheme [3] cannot guarantee the secrecy fairness, i.e., the minimum
This work investigates for the first time the vulnerability to single antenna users, 
and represent the non-line-of-sight (NLoS) component. In single 
where \( z_\tilde{m} = \sum_{m=1}^{M} g_{mk} \psi_k \), \( g_{mk} \) and \( \tilde{\psi}_k \) represent the channel realizations, i.e., \( g_{mk} \) and \( \tilde{\psi}_k \) are independent and identically distributed (i.i.d.) random variables in different coherence blocks. APs only know statistical channel state information (CSI), not the channel realizations.

In the uplink channel estimation phase, all users simultaneously transmit their own pilot signals. All pilot signals are assumed to be orthonormal to each other. When \( K > \tau_p \), the pilot contamination effect is caused by the reuse of orthogonal pilot signals already assigned to other users. For mitigating the pilot contamination, the random assignment scheme [3] is employed. Then, the received signal at the \( m \)th AP can be represented as

\[
Y_{p,m} = \sqrt{\tau_p P_p} \sum_{k=1}^{K} g_{mk} \psi_k + W_{p,m},
\]

where \( p_p, \psi_k \in \mathbb{C}^{L, r} \), and \( W_{p,m} \in \mathbb{C}^{L, r} \) respectively represent the pilot transmit power, the pilot signal of the \( k \)th user, and the thermal noise whose elements follow i.i.d. \( \mathcal{CN}(0, 1) \). Then, each AP separately estimates the channel between itself and each user based on the linear minimum mean square error (LMMSE) estimation with statistical CSI. The LMMSE estimate of \( g_{mk} \) is obtained by

\[
g_{mk} = \hat{g}_{mk} + c_{mk} y_{p,m}, \tag{1}
\]

where

\[
y_{p,m} = y_{p,m} \psi_k^H = \sqrt{\tau_p p_p} \sum_{k \in \mathcal{U}_k} g_{mk} \psi_k + W_{p,m},
\]

\[
c_{mk} = \sqrt{\tau_p p_p} R_{mk} \left( \tau_p p_p \sum_{k \in \mathcal{U}_k} R_{mk}^{\tau} + I_L \right)^{-1},
\]

where \( \mathcal{U}_k \) is the set of users who use the same pilot signal as the \( k \)th user. Note that \( \hat{g}_{mk} \) follows \( \mathcal{CN}(h_{mk}, C_{mk}) \) where \( C_{mk} = \sqrt{\tau_p p_p} \text{cov}(R_{mk}) \), and the estimation error vector, \( e_{mk} \), follows \( \mathcal{CN}(0, L, \text{diag}(R_{mk} - C_{mk})) \). These are shown at the bottom of the next page.

In the downlink data transmission phase, each AP transmits the data signals for all users with the conjugate beamforming for the data signals [3] and the random beamforming for AN signal [8], [11]. Then, the transmitted signal from the \( m \)th AP can be expressed as

\[
x_m = \sum_{k=1}^{K} \sqrt{p_{mk}} \hat{g}_{mk} x_k + \sqrt{p_{mv}} v_m,
\]

where \( p_{mk} \) and \( p_{mv} \) are the transmit powers of data for the \( k \)th user and AN at the \( m \)th AP, respectively. The data signal for the \( k \)th user and the AN signal at the \( m \)th AP are denoted by \( s_k \sim \mathcal{CN}(0, 1) \) and \( v_m \), whose elements follow i.i.d. \( \mathcal{CN}(0, 1) \), respectively. The total transmit power of the data and AN signals is limited in such a way that \( \mathbb{E}[||x_m||^2] \leq p_t \) for \( m \in \{1, 2, \ldots, M\} \).

Meanwhile, the received signals at the \( k \)th user and the \( j \)th Eve are respectively given by

\[
r_k = \sum_{m=1}^{M} \hat{g}_{mk} x_m + w_{d,k} = \sum_{k'=1}^{K} f_{kk'} s_{k'} + z_k + w_{d,k}, \tag{2}
\]

\[
r_j = \sum_{m=1}^{M} (g_{mj}^e)^H x_m + w_{j}^e = \sum_{k=1}^{K} f_{jk} s_k + z_j^e + w_{d,j}^e, \tag{3}
\]

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
TABLE I

| Symbol | Description |
|--------|-------------|
| $M$    | The number of APs |
| $L$    | The number of antennas per AP |
| $K$    | The number of users |
| $J$    | The number of eavesdroppers |
| $T_p$  | The length of plot signal |
| $p_{mk}$ | The transmit power of data for the $k$th user at the $m$th AP |
| $p_{mv}$ | The transmit power of AN at the $m$th AP |

and $w_{d,k}$ and $w_{a,j}$ are the thermal noises following $CN(0, 1)$. For convenience, the symbols frequently used in this work are summarized in Table I.

III. ARTIFICIAL NOISE-ASSISTED SECURE POWER CONTROL

In this section, we formulate an optimization problem which finds the optimal power control coefficients for the data and AN at each AP. In the formulation of the problem, we need an analytic expression of the secrecy rate, which however, to the best of our knowledge, is intractable to obtain. Thus, we instead derive a lower bound on the secrecy rate with a lower and upper bound on the leakage rate, respectively. For the rate of user $R_k$, we first apply the use-and-then-forget (UaTf) lower bound [18] to $R_k$, which results in a lower bound on $R_k$, denoted by $\bar{R}_k$ in (4). Meanwhile, for the leakage rate, $\bar{R}_{jk}^e$, we derive an upper bound, denoted by $\bar{R}_{jk}$, assuming the worst-case scenario that Eves perfectly know their channel gains [8], [9], [10], [11]. Then, we have the upper bound, $\bar{R}_{jk}$ in (5).

$$R_k \geq \bar{R}_k = \log_2 (1 + \Gamma_k) = \log_2 \left(1 + \frac{S_k}{IN_k}\right),$$

$$\bar{R}_{jk}^e \leq \bar{R}_{jk} = \log_2 (1 + \Gamma_{jk}^e) = \log_2 \left(1 + \frac{L_{jk}}{IN_{jk}}\right),$$

where $S_k$, $I_{1,k}$, $I_{2,k}$, $A_k$, $L_{jk}$, and $A_j^t$ are shown at the top of this page. The detailed derivations are provided in Appendix A. Finally, we obtain a lower bound on the secrecy rate as follows:

$R_{jk}^t = [\bar{R}_k - \bar{R}_{jk}]^+$, for $k \in \{1, 2, \ldots, K\}$ and $j \in \{1, 2, \ldots, J\}$, where $[x]^+$ is max$[0, x]$. The optimization problem for the secrecy fairness, i.e., maximizing the minimum secrecy rate of all users, can be formulated as

$$\max_{p_{mk}, p_{mv}=\omega_{jk}} \min \bar{R}_k - \bar{R}_{jk}^t$$

s.t. $\sum_{k=1}^{K}(p_{mk})^2 \gamma_{mk} + p_{mv} \leq P_t$, $\forall m$,

$$p_{mv} \geq 0, p_{mv} \geq 0, \forall m, \forall k,$$

where $p_{mk} = \sqrt{p_{mk}}$, and the constraints in (6b) comes from $E[x_m^2] \leq P_t$. By introducing slack variables $\bar{t}$ and $\omega_{jk}$ which represent the minimum secrecy rate and the leakage rate at the $j$th Eve for the $k$th user data, respectively, we can reformulate the optimization problem in (6) as follows:

$$\max \bar{t}$$

s.t. $\bar{R}_k - \omega_{jk} \geq \bar{t}$, $\forall k, \forall j$,

$$\bar{R}_{jk}^e \leq \omega_{jk}, \forall k, \forall j,$$

Unfortunately, the constraints in (7b) and (7c) are non-convex. To turn around the obstacle, we introduce slack variables $S_k$, $\bar{S}_k$, $\bar{I}_{N_k}$, $\bar{L}_{jk}$, $\bar{L}_{jk}$, and $\bar{I}_{N_{jk}}$, and then the optimization problem in (7) can be reformulated as

$$\max \bar{t}$$

s.t. $\log_2(1 + \bar{\Gamma}_k) \geq \bar{t} + \omega_{jk}$, $\forall k, \forall j$,

$$(\bar{S}_k)^2/\bar{I}_{N_k} \geq \bar{L}_{jk}, \forall k,$$

$\bar{S}_k \leq \sqrt{\bar{S}_k}, \forall k,$

$\bar{I}_{N_k} \geq \bar{I}_{N_k}, \forall k,$

$\log_2(1 + \bar{\Gamma}_{jk}^e) \leq \omega_{jk}, \forall k, \forall j,$

$L_{jk}/\bar{I}_{N_{jk}} \leq L_{jk}, \forall k, \forall j,$

$\bar{L}_{jk} \geq L_{jk}, \forall j, \forall k,$

$L_{jk} \leq \bar{I}_{N_{jk}}, \forall k, \forall j,$

$\bar{I}_{N_{jk}} \leq \bar{I}_{N_{jk}}, \forall k, \forall j,$

(6b), (6c).

Note that the constraints in (8c), (8e) $\sim$ (8i) are non-convex. To resolve the non-convexity, we will solve the optimization problem in (8) with an iterative method solving sequential convex problems in such a way replacing the non-convex constraints with their first-order Taylor approximation at each iteration. By the first-order Taylor expression, the constraints in (8c), (8e) $\sim$ (8i) at the $(n + 1)$th iteration can be expressed as

$$S_k = \left(\sum_{m=1}^{M} \sqrt{p_{mk}} \gamma_{mk}\right)^2,$$

$$I_{1,k} = \sum_{k'=1}^{K} \sum_{m=1}^{M} p_{mk}' \left(\bar{h}_{mk}' \bar{h}_{mk} \bar{h}_{mk} + \bar{h}_{mk}' \bar{R}_{mk} \bar{h}_{mk} + \text{tr}(\bar{C}_{mk} \bar{R}_{mk})\right),$$

$$I_{2,k} = \sum_{m=1}^{M} \sqrt{p_{mk}} I_{3,k} = \sum_{m=1}^{M} \sqrt{p_{mk}} I_{3,mk},$$

$$L_{1,mj} = \bar{h}_{mj}^H \bar{C}_{mj} \bar{h}_{mj} + \bar{h}_{mk}^H \bar{R}_{mk} \bar{h}_{mk} + \text{tr}(\bar{C}_{mk} \bar{R}_{mj}),$$

$$L_{2,mj} = \bar{h}_{mj}^H \bar{h}_{mk},$$

$$A_j^t = \sum_{m=1}^{M} p_{mv} \beta_{mj},$$

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply.
Algorithm 1: AN-Aided Secure Power Control Algorithm.

**input:** initial transmit power, \( \{p_{mk}^{[0]}, p_{mv}^{[0]}\} \); initial objective function value, \( f^{[0]} \); convergence constraint, \( \epsilon \).

**output:** optimized transmit power, \( \{p_{mk}^{[n]}, p_{mv}^{[n]}\} \).

1. **initialize:** \( n \leftarrow 0 \); update Eqs. (9) \( \sim \) (14) based on \( \{p_{mk}^{[0]}, p_{mv}^{[0]}\} \).

2. **repeat**

3. solve (15) and obtain \( t \) and \( \{p_{mk}, p_{mv}\} \).

4. \( n \leftarrow n + 1 \); \( \{p_{mk}^{[n]}, p_{mv}^{[n]}\} \leftarrow \{p_{mk}, p_{mv}\} \); update Eqs. (9) \( \sim \) (14) based on \( \{p_{mk}^{[n]}, p_{mv}^{[n]}\} \).

5. **until** \( |f^{[n]} - f^{[n-1]}| < \epsilon \).

respectively obtained as

\[
\frac{2S_k^{[n]}}{TN_k} \tilde{S}_k - \left( \frac{\tilde{c}_k^{[n]}}{TN_k} \right)^2 TN_k \geq \tilde{\Gamma}_k, \forall k, \quad (9)
\]

\[
TN_k \geq I_{1,k} + \sum_{k' \neq k} K_{2,k,k'} + A_k + 1, \quad (10)
\]

\[
\log_2 \left( 1 + \tilde{\Gamma}_k^{[n]} \right) + \frac{\tilde{\Gamma}_k^{[n]} - \tilde{\Gamma}_k^{[n-1]}}{\ln(2)} \leq \omega_k, \forall k, \forall j, \quad (11)
\]

\[
\frac{L_{j,k}^{[n]}}{TN_{j,k}^{[n]}} + \frac{\tilde{L}_{j,k}^{[n]} TN_{j,k}^{[n]}}{TN_{j,k}^{[n]}} \leq \tilde{\Gamma}_j, \forall k, \forall j, \quad (12)
\]

\[
L_{j,k} \geq \sum_{m=1}^{M} (\tilde{p}_{mk}^{[n]})^2 L_{1,m,j} + \tilde{L}_{2,j,k}, \forall k, \forall j, \quad (13)
\]

\[
TN_{j,k} \leq \sum_{k' \neq k} L_{j,k}' + A_j + 1, \forall k, \forall j, \quad (14)
\]

where

\[
\tilde{L}_{2,k,k'} = 2\Re \left( \sum_{m=1}^{M} p_{mk}^{[n]} L_{1,m,k} \right) \left( \sum_{m=1}^{M} \tilde{p}_{mk}^{[n]} L_{1,m,k} \right)^* \right)^2 - \left| \sum_{m=1}^{M} \tilde{p}_{mk}^{[n]} L_{1,m,k} \right|^2,
\]

\[
\tilde{L}_{2,j,k} = 2\Re \left( \sum_{m=1}^{M} p_{mk}^{[n]} L_{2,m,j} \right) \left( \sum_{m=1}^{M} \tilde{p}_{mk}^{[n]} L_{2,m,j} \right)^* \right)^2 - \left| \sum_{m=1}^{M} \tilde{p}_{mk}^{[n]} L_{2,m,j} \right|^2,
\]

\[
\tilde{L}_{j,k} = \sum_{m=1}^{M} \left( \tilde{p}_{mk}^{[n]} \right)^2 + 2\Re \left( \tilde{p}_{mk}^{[n]} - \tilde{p}_{mv}^{[n]} \right) L_{1,m,j} + \tilde{L}_{2,j,k}.
\]

Then, the optimization problem in (8) can be reformulated as the following optimization problem at the \((n+1)\)th iteration.

\[
\max_{p_{mk}, p_{mv}, \omega_k, \tilde{\Gamma}_k, \tilde{\Gamma}_j, TN_k} f_{\tilde{L}_{j,k}, \tilde{L}_{j,k}, TN_k, t}
\]

s.t. (6b), (6c), (6b), (8d), (9) \( \sim \) (14).

The reformulated optimization problem in (15) is now convex and can be solved by utilizing the convex optimization tools, e.g., CVX. At each iteration, we update the linear approximations, i.e., (9) \( \sim \) (14), based on the solutions at the previous iteration, until \( t \) converges to a fixed value, i.e., \( |f^{[n]} - f^{[n-1]}| < \epsilon \) where \( \epsilon \) is a convergence constraint. The proposed algorithm guarantees to converge since \( f^{[n+1]} \geq f^{[n]} \) will always hold, and the maximum value of \( t \) is bounded by the transmit power constraint in (6b). The proposed algorithm is outlined in Algorithm 1.

IV. SIMULATION RESULTS

In this section, we carry out Monte-Carlo simulations to evaluate and analyze the secrecy performance of the proposed AN-aided power control scheme. For the simulations, we consider a network in which \( M \) APs, \( K \) users, and \( J \) Eves are randomly distributed in a square area of \( 1 \times 1 \) km\(^2\). For path-loss model, the COST 321 multipath fading model, and the coverage area is the square area of \( 1 \times 1 \) km\(^2\). In our simulations, the COST 321 multipath fading model is used to model the multipath fading channel. The path-loss model is given by

\[
P_d = \frac{P_t}{d^\alpha},
\]

where \( P_t \) is the transmitted power, \( d \) is the distance between the transmitter and the receiver, and \( \alpha \) is the path-loss exponent.

The large-scale channel model is given by

\[
\mathbf{H} = \mathbf{H}_\text{LoS} \mathbf{H}_\text{NLoS},
\]

where \( \mathbf{H}_\text{LoS} \) and \( \mathbf{H}_\text{NLoS} \) are the large-scale channel matrices, respectively.

The received signal at the receiver can be expressed as

\[
r_i(t) = \sum_{j=1}^{J} \mathbf{H}_{i,j} \mathbf{X}_j(t) + n_i(t),
\]

where \( \mathbf{X}_j(t) \) is the transmitted signal from the \( j \)-th Eve, \( n_i(t) \) is the additive white Gaussian noise (AWGN) at the receiver.

The secrecy outage probability is defined as the probability that the secrecy rate is less than a certain threshold.

\[
P_{\text{out}} = \Pr \left[ \frac{R_s}{I_s} < R_0 \right],
\]

where \( R_s \) is the secrecy rate, and \( I_s \) is the interference rate.

The secrecy throughput is defined as the average secrecy rate over a long period of time.

\[
\text{Secrecy Throughput} = \frac{1}{T} \int_{0}^{T} R_s(t) dt,
\]

where \( T \) is the total transmission time.

The secrecy capacity is defined as the maximum achievable secrecy rate.

\[
C_s = \max_{P_t} \frac{R_s}{I_s}.
\]

The secrecy capacity is achieved when the transmitter selects the optimal transmit power such that the secrecy rate is maximized.

The simulation results are summarized in Table II.

| Parameter | Value |
|-----------|-------|
| Transmit power | \( T_s = 200 \) and \( T_d = 200 - T_p \) |
| Thermal noise power | \( P_n = 200 \) mW and \( P_p = 100 \) mW |
| Antenna spacing parameter | -94 dBm |
| Angular standard deviation | 0.5 (fraction of wavelength) |
| Convergence constraint | 15°, 0.1 |

Authorized licensed use limited to the terms of the applicable license agreement with IEEE. Restrictions apply. 
rate for 500 random realizations of the network deployment. For each realization, the minimum secrecy rate, i.e., \( \min_{k,j} R_{j,k}^\tau \), is obtained by calculating \( R_k \) and \( R_{j,k}^\tau \) with the proposed scheme and two competing schemes. Then, the cumulative distribution function (CDF) and the average minimum secrecy rate are obtained with the evaluations of minimum secrecy rate. Note that the smaller value of CDF at a minimum realization, the minimum secrecy rate, i.e., \( R_{j,k}^\tau \), increases, the performance of all schemes gets lowered, which is due to the fact that the maximum leakage rate among Eves increases by the principle of order statistics. One can find that the proposed AN-aided secure power control scheme always achieves the best secrecy performance and is robust against the growing number of Eves. It is also observed that the non-secure power control scheme can not guarantee the secrecy fairness, i.e., the minimum secrecy rate diminishes to zero. Specifically, the non-secure power control scheme suffers from the lower secrecy fairness performance than the heuristic power control scheme as \( J \) increases. The results in Fig. 2 clearly demonstrate the vulnerability of CF-mMIMO to passive eavesdropping when a carefully designed power control is not employed.

In Fig. 3, we repeat the experiment in Fig. 2 with different values of \( K \), i.e., the number of users. It is observed that the pilot contamination makes the secrecy performance of all schemes get deteriorated. This happens due to the fact that the transmit power per user with the increasing number of users decreases. It should be noted that the proposed AN-aided scheme, nevertheless, always has better secrecy performance than those of the competing schemes. In Fig. 4, we present the average minimum secrecy rate with different values of \( M \) and \( L \), i.e., the numbers of APs and antennas, respectively. As \( M \) increases, all schemes have better performance, and the same can be seen with the growing \( L \). As shown in Fig. 4, the proposed AN-aided secure power control scheme consistently outperforms the other competing schemes. From the comparisons, one can conclude that the proposed AN-aided secure power control scheme significantly improves the secrecy rate of the CF-mMIMO system under passive eavesdropping.

V. CONCLUSION

In this work, we investigated secure communications in CF-mMIMO under passive eavesdropping. For maximizing the minimum secrecy rate, we proposed the AN-aided secure power control scheme. By conducting performance comparisons, it was shown that the proposed AN-aided secure power control scheme significantly improves secrecy performance. As a future research direction, we will study the secrecy performance of CF-mMIMO with hardware impairments.

APPENDIX A

We first derive the data rate of the \( f \)th user from the received signal in (2). By applying the UatF lower bound [18], \( R_k \) is given by

\[
R_k = \log_2 \left( 1 + \frac{\mathbb{E}[f_{kk}]}{\mathbb{V}(f_{kk}) + \sum_{k' \neq k} \mathbb{E}[f_{k'k}]^2 + \mathbb{E}[|z_k|^2] + 1} \right),
\]

where \( \mathbb{V}(f_{kk}) = \mathbb{E}[|f_{kk} - \mathbb{E}[f_{kk}]|^2] \). By the definition of \( g_{mk} \) in (1), \( \mathbb{E}[f_{kk}] \) can be readily derived as \( \sum_{m=1}^{M} \sqrt{\mathbb{E}[g_{mk}^H g_{mk}]} = \|\mathbf{h}_{mk}\| + \text{tr}(\mathbf{C}_{mk}) \). Then, the derivation of \( \mathbb{V}(f_{kk}) \) can be obtained as the following equations.

\[
\mathbb{V}(f_{kk}) = \mathbb{E}[|f_{kk} - \mathbb{E}[f_{kk}]|^2] = \mathbb{E}[|f_{kk}|^2] - (\mathbb{E}[f_{kk}])^2
\]

\[
= \mathbb{E} \left[ \sum_{m=1}^{M} \sqrt{\mathbb{E}[g_{mk}^H g_{mk}]} \right]^2 + \sum_{m=1}^{M} \mathbb{E}[|e_{mk}^H g_{mk}|^2]
\]

\[- \sum_{m=1}^{M} \sum_{m'=1}^{M} \sqrt{\mathbb{E}[g_{mk}^H g_{mk}]} \gamma_{mk} \gamma_{m'k}
\]

\[= \sum_{m=1}^{M} \mathbb{E}[|e_{mk}^H g_{mk}|^2] + \sum_{m=1}^{M} \sum_{m'=1}^{M} \sqrt{\mathbb{E}[g_{mk}^H g_{mk}]} \gamma_{mk} \gamma_{m'k}
\]

\[+ \sum_{m=1}^{M} \mathbb{E}[|e_{mk}^H g_{mk}|^2] - \sum_{m=1}^{M} \sum_{m'=1}^{M} \sqrt{\mathbb{E}[g_{mk}^H g_{mk}]} \gamma_{mk} \gamma_{m'k}
\]

\[\left(a\right) \sum_{m=1}^{M} \mathbb{E}[|\hat{h}_{mk}^H (\hat{R}_{mk} + C_{mk}) \hat{h}_{mk} + \text{tr} (\hat{R}_{mk} C_{mk})|]
\]

where \( a \) is from applying [17, Lemma 5] (or [17, Lemma 4], resp.) to the first term (the third term, resp.). \( \mathbb{E}[|f_{kk}|^2] \) can be expressed as the
following equations after some algebraic manipulations.

\[
\mathbb{E}[|f_{jk}|^2] = \sum_{m=1}^{M} p_{mk} \left( \mathbb{E}\left[ g_{mk}^H g_{mk} \right] + \mathbb{E}\left[ |e_{mk}|^2 \right] \right) + \sum_{m'=1}^{M} \sum_{m''=1}^{M} \sqrt{p_{mk} p_{m''k}} \mathbb{E}\left[ g_{mk}^H g_{m''k} \left( g_{m''k}^* g_{mk} \right)^* \right].
\]

Then, we calculate \(\mathbb{E}[|f_{jk}|^2]\) separately for \(k' \notin \mathbb{P}_k\) and \(k' \in \mathbb{P}_k\). Firstly, \(\mathbb{E}[|f_{jk}|^2]\) for \(k' \notin \mathbb{P}_k\) can be obtained by applying [17, Lemma 4] to \(\mathbb{E}[g_{mk}^H g_{mk}^*]\) and \(\mathbb{E}[|e_{mk}|^2]\), and given by the following equations after some algebraic manipulations.

\[
\sum_{m=1}^{M} p_{mk} \left( \mathbb{E}\left[ g_{mk}^H g_{mk} \right] + \mathbb{E}\left[ |e_{mk}|^2 \right] + \text{tr} \left( \mathbb{E}\left[ \hat{C}_{mk} \right] \right) \right) + \sum_{m'=1}^{M} \sqrt{p_{mk} p_{m''k}} \mathbb{E}\left[ g_{mk}^H g_{m''k} \left( g_{m''k}^* g_{mk} \right)^* \right].
\]

Secondly, \(\mathbb{E}[|f_{jk}|^2]\) for \(k' \in \mathbb{P}_k\) can be obtained by applying [17, Lemma 5] ((17, Lemma 4), resp.) to \(\mathbb{E}[g_{mk}^H g_{mk}^*]\), \(\mathbb{E}[|e_{mk}|^2]\), and given by the following equations after some algebraic manipulations.

\[
\sum_{m=1}^{M} p_{mk} \left( \mathbb{E}\left[ g_{mk}^H g_{mk} \right] + \mathbb{E}\left[ |e_{mk}|^2 \right] + \text{tr} \left( \mathbb{E}\left[ \hat{C}_{mk} \right] \right) \right) + \sum_{m'=1}^{M} \sqrt{p_{mk} p_{m''k}} \mathbb{E}\left[ g_{mk}^H g_{m''k} \left( g_{m''k}^* g_{mk} \right)^* \right] .
\]

With the assumption that all Eves have perfect knowledge of the channels, the leakage rate of the \(k\)th user at the \(j\)th Eve, \(R_{jk}^e\), is given by

\[
R_{jk}^e \approx \log_2 \left( 1 + \frac{\mathbb{E}[|f_{jk}|^2]}{\sum_{k' \neq k} \mathbb{E}[|f_{jk}|^2] + \mathbb{E}[|z|^2] + 1} \right),
\]

where \((b)\) is from the approximation in [20, Lemma 1]. Similar to the derivation of \(\mathbb{E}[|z|^2]\) and \(\mathbb{E}[|z|^2]\), we can rewrite \(\sum_{m=1}^{M} p_{mk} \beta_{mk}\) as \(\sum_{m=1}^{M} p_{mk} \beta_{mk}\), where \(\beta_{mk} = \mathbb{E}[|g_{mk}|^2] = ||h_{mk}||^2 + \text{tr}(\mathbb{E}[\hat{C}_{mk}])\). Finally, \(\mathbb{E}[|f_{jk}|^2]\) is given by

\[
\mathbb{E}[|f_{jk}|^2] = \mathbb{E}\left[ \sum_{m=1}^{M} \sqrt{p_{mk}} \left( g_{mk}^H g_{mk} \right) \right]^2.
\]

By applying [17, Lemma 4] to \(\mathbb{E}[|g_{mk}^H g_{mk}^*|] \) in (21) and after some algebraic manipulations, the closed-form expression of \(\mathbb{E}[|f_{jk}|^2]\) in (20) can be obtained.

REFERENCES

[1] H. Q. Ngo, A. Ashikhmin, H. Yang, E. G. Larsson, and T. L. Marzetta, “Cell-free massive MIMO: Uniformly great service for everyone,” in Proc. IEEE Int. Workshop Signal Process. Adv. Wireless Commun., 2015, pp. 201–205.

[2] J. Zhang, S. Chen, Y. Lin, J. Zheng, B. Ai, and L. Hanzo, “Cell-free massive MIMO: A new next-generation paradigm,” IEEE Access, vol. 7, pp. 99878–99888, Jul. 2019.

[3] H. Q. Ngo, A. Ashikhmin, H. Yang, E. G. Larsson, and T. L. Marzetta, “Cell-free massive MIMO versus small cells,” IEEE Trans. Wireless Commun., vol. 16, no. 3, pp. 1834–1850, Mar. 2017.

[4] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, “Security and privacy for 6G: A survey on prospective technologies and challenges,” IEEE Commun. Surveys Tuts., vol. 23, no. 4, pp. 2384–2428, Fourthquarter 2021.

[5] F. Cheng, G. Gui, N. Zhao, Y. Chen, J. Tang, and H. Sari, “UAV-relaying-assisted secure transmission with caching,” IEEE Trans. Commun., vol. 67, no. 5, pp. 3140–3153, May 2019.

[6] H. Guo, Y. Wang, J. Liu, and C. Liu, “Multi-UAV cooperative task off-loading and resource allocation in 5G advanced and beyond,” IEEE Trans. Wireless Commun., early access, doi: 10.1109/TWC.2023.3277801.

[7] H. Guo, W. Huang, J. Liu, and Y. Wang, “Inter-server collaborative federated learning for ultra-dense edge computing,” IEEE Trans. Wireless Commun., vol. 21, no. 7, pp. 5191–5203, Jul. 2022.

[8] S. Timilsina, D. Kudathanthirige, and G. Amarasuriya, “Physical layer security in cell-free massive MIMO,” in Proc. IEEE Glob. Commun. Conf., 2018, pp. 1–7.

[9] 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 Trans. Commun., vol. 66, no. 10, pp. 4724–4737, Oct. 2018.

[10] X. Zhang, D. Guo, K. An, and B. Zhang, “Secure communications over cell-free massive MIMO networks with hardware impairments,” IEEE Syst. J., vol. 14, no. 2, pp. 1909–1920, Jun. 2020.

[11] Y. Zhang, W. Xia, G. Zheng, H. Zhao, L. Yang, and H. Zhu, “Secure transmission in cell-free massive MIMO with low-resolution DACs over Rician fading channels,” IEEE Trans. Commun., vol. 70, no. 4, pp. 2606–2621, Apr. 2022.

[12] M. Alaghi, A. Ikhlief, A. Alsfiany, M. A. M. Abdullah, G. Chen, and J. Chambers, “Optimal downlink transmission for cell-free SWIPT massive MIMO systems with active eavesdropping,” IEEE Trans. Inf. Forensics Secur., vol. 15, pp. 1993–1998, Nov. 2020.

[13] S. Elhoushy, M. Ibrahim, and W. Hamouda, “Exploiting RIS for limiting information leakage to active eavesdropper in cell-free massive MIMO,” IEEE Wireless Commun. Lett., vol. 11, no. 3, pp. 443–447, Mar. 2022.

[14] 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, Apr. 2019.

[15] X. Zhou, B. Maham, and A. Hjorungnes, “Pilot contamination for active eavesdropping,” IEEE Trans. Wireless Commun., vol. 11, no. 3, pp. 903–907, Mar. 2012.

[16] D. Kapetanović, G. Zheng, and F. Rusek, “Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks,” IEEE Commun. Mag., vol. 53, no. 6, pp. 21–27, Jun. 2015.

[17] Ö. Özdogan, E. Björnson, and E. G. Larsson, “Massive MIMO with spatially correlated rician fading channels,” IEEE Trans. Commun., vol. 67, no. 5, pp. 3234–3250, May 2019.

[18] E. Björnson, J. Hoydis, and L. Sanguinetti, Massive MIMO Networks: Spectral Energy, and Hardware Efficiency. Norwell, MA, USA: Now Found. Trends, 2017.

[19] G. Interdonato, P. Frenger, and E. G. Larsson, “Scalability aspects of cell-free massive MIMO,” in Proc. IEEE Int. Cont. Commun., 2019, pp. 1–6.

[20] Q. Zhang, S. Jin, K.-K. Wong, H. Zhu, and M. Matthaiou, “Power scaling of uplink massive MIMO systems with arbitrary-rank channel means,” IEEE J. Sel. Topics Signal Process., vol. 8, no. 5, pp. 966–981, Oct. 2014.