Cell-Free Massive MIMO Networks: Optimal Power Control Against Active Eavesdropping

Tiep M. Hoang, *Student Member, IEEE*, Hien Quoc Ngo, Trung Q. Duong, *Senior Member, IEEE*, Hoang Duong Tuan, and Alan Marshall, *Senior Member, IEEE*

***Abstract*— This paper studies the security aspect of a recently introduced "cell-free massive MIMO" network under a pilot spoofing attack. First, a simple method to recognize the presence of this type of an active eavesdropping attack to a particular user is shown. In order to deal with this attack, we consider the problem of maximizing the achievable data rate of the attacked user or its achievable secrecy rate. The corresponding problems of minimizing the power consumption subject to security constraints are also considered in parallel. Path-following algorithms are developed to solve the posed optimization problems under different power allocation to access points (APs). Under equip-power allocation to APs, these optimization problems admit closed-form solutions. Numerical results show their efficiency.**

***Index Terms*— Cell-free, channel estimation, pilot spoofing attack, active eavesdropping, inner convex approximation.**

I. Introduction

A. Previous Works

1) Cell-Free Massive MIMO Networks: Cell-free massive MIMO has been recently introduced in [1]–[3]. These papers showed that by proper implementation, cell-free massive MIMO can provide a uniformly good service to all users in the network and outperform small-cell massive MIMO in terms of throughput, and handle the shadow fading correlation more efficiently. In a typical small-cell massive MIMO system, the channel from an access point (AP) to a user is a single scalar. In contrast, in a cell-free Massive MIMO system, all APs can liaise with each other via a central processing unit (CPU) to perform beamforming transmission tasks, and thus the effective channel (from an AP to a user) will take the form of an inner product between two vectors [2]. That inner product can converge to its mean when the length of each vector (equivalently, the number of APs) is large enough. As a result, the effective channel also converges to a constant and there is no need to estimate downlink channels in the massive MIMO systems using cell-free architecture, while the small-cell counterpart may require both downlink and uplink training for channel estimation.

Inspired by [1]–[3], cell-free massive MIMO has been further studied in [4]–[7]. Cell-free massive MIMO was modified in [4] to allow each AP serving only several users based on the strongest channels instead of serving all users. The joint user association and interference/power control to mitigate the interference and cell-edge effect was considered in [5]. The problem of designing zero-forcing precoders to maximize the energy efficiency for cell-free massive MIMO networks was considered in [6]. We are motivated to investigate the security aspect of cell-free massive MIMO as it was not considered in the current research.

2) Pilot Spoofing Attack: Recently, active eavesdropping has attracted the researchers' attention to physical layer security. It has been proved that active eavesdroppers are more dangerous than passive eavesdroppers because confidential information leaked to the active eavesdroppers is possibly higher [8]. Active eavesdropping is an interesting topic which has been emerging in recent years. For instance, active eavesdroppers are capable of jamming as well as eavesdropping [9]–[11] and/or they can send spoofing pilot sequences [8], [12], [13]. The latter scenario relates to the so-called *pilot spoofing attacks* [8], [12]. Eavesdropping attacks caused by an active eavesdropper is more harmful than passive ones. A feedback-based encoding scheme to improve the secrecy of transmission was proposed in [12]. On the contrary, from an eavesdropping point of view, [8] showed how an active eavesdropper achieves a satisfactory performance with the use of transmission energy.

Initialized by [8], pilot spoofing attacks in wireless security have been actively studied [13]–[18]. By assuming that an eavesdropper can attack a wireless communication system during training phase to gain the amount of leaked information, Kapetanovic *et al.* [13], Wu *et al.* [14], Im *et al.* [15], Tugnait [16], and Xiong *et al.* [17], [18] have studied pilot contamination attacks in distinct scenarios. Their results reveal that active eavesdropping poses an actual threat to different types of wireless systems in general. More specifically, the authors in [13] conducted a survey of detecting active

Manuscript received November 22, 2017; revised March 14, 2018 and May 6, 2018; accepted May 8, 2018. Date of publication May 16, 2018; date of current version October 16, 2018. This work was supported in part by the U.K. Royal Academy of Engineering Research Fellowship under Grant RF1415/14/22, by a U.K. Engineering and Physical Sciences Research Council under Grant EP/P019374/1, by a Research Environment Links, under the Newton Programme Vietnam Partnership Grant, ID 339568416, and Newton Prize 2017. The associate editor coordinating the review of this paper and approving it for publication was I. Krikidis. *(Corresponding author: Trung Q. Duong.)*

T. M. Hoang, H. Q. Ngo, and T. Q. Duong are with the School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, Belfast BT7 1NN, U.K. (e-mail: mhoang02@qub.ac.uk; hien.ngo@qub.ac.uk; trung.q.duong@qub.ac.uk).

H. D. Tuan is with the University of Technology Sydney, Ultimo, NSW 2007, Australia (e-mail: tuan.hoang@uts.edu.au).

A. Marshall is with the University of Liverpool, Liverpool L69 3GJ, U.K. (e-mail: alan.marshall@liverpool.ac.uk).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCOMM.2018.2837132

attacks on massive MIMO systems. Wu *et al.* [14] designed an artificial noise to cope with an active eavesdropper in a secure massive MIMO system. The use of artificial noise is not necessary in the present paper as our proposed optimization problems can also control beam steering towards intended destinations such that security constraints are met. Meanwhile, the consideration of Im *et al.* [15] [15] is a secret key generation, which is beyond the scope of our paper. In [16] a method called *minimum description length source enumeration* is employed to detect an active eavesdropping attack in a relaying network; however, the secure performance of the system (via metrics such as secrecy rate or secrecy outage probability) is not evaluated. Other detection techniques can be found in [17] and [18]. While [17] resort to the downlink phase to estimate channels and improve the system performance, we only use one training phase to detect a potential eavesdropper (which is presented in Appendix A). Our simple detection technique is similar to that in [18], which also compares the asymmetry of received signal power levels to detect eavesdroppers. The differences between [18] and our paper lie in modeling (massive MIMO networks versus cell-free networks) and optimization formulations. Although the eavesdropping attack detection methods in [16]–[18] are really attractive, we will not delve into similar methods and not consider such a method as a major contribution. Instead, we focus on solving optimization problems to provide specific solutions for cell-free systems in the case that a user is really suspected of being an eavesdropper.

B. Contributions

As discussed above, the introduction of a cell-free massive MIMO network can bring about a huge chance of improving throughput in comparison with small-cell networks. We thus study the security aspect of such a network and more importantly, this paper is the first work on the integration of security with the cell-free massive MIMO architecture. On the other hand, the analytical approach in this work is different from previous papers on security for massive MIMO. The major difference is that we do not use the law of large number to formulate approximate expressions for signal-to-noise (SNR) ratios. Instead, we consider lower- and upper- bounds for SNR expressions, thereby a lower-bound for secrecy rate is formulated and evaluated. This alternative approach, of course, holds true for general situations in which the number of nodes/antennas are not so many (and hence the term "massive" can be relatively understood and/or can be also removed).

In this paper, we examine a cell-free network in which an eavesdropper is actively involved in attacking the system during the training phase. We simply and shortly show that such an attack is dangerous but can be detected by a simple detection mechanism. Thereby, efforts to deal with active eavesdropping can be made and secure strategies can be prepared at APs during the next phase (i.e. the downlink phase). With these in mind and with the aim of keeping confidential information safe, we can realize beforehand which user is under attack and thus, we can propose optimization problems based on secrecy criteria to protect that user from being overhead. Our proposed optimization problems can be classified into 2 groups. For the first group, we design a matrix of power control coefficients

- to maximize the achievable data rate of the user who is under attack (see III-A)
- to maximize the achievable secrecy rate of user 1 (see III-B)
- to minimize the total power at all APs subject to the constraints on the data rate of each user, including all legitimate users and eavesdropper (see IV-A)
- to minimize the total power at all APs subject to the constraints on the achievable data rate and the data rates of other users (i.e. legitimate users not under attack) (see IV-B).

For the second group, we design a common power control coefficient for all APs and consider 4 optimization problems (V-A, V-B, V-C and V-D), which are similar and comparable to their counterparts in the first group. While the common goal of all maximization programs is achievable secrecy rate, that of all minimization programs is power consumption at APs. Taking control of power at each AP, we find the most suitable solutions to the proposed optimization problems and compare them in secure performance as well as energy.

The rest of the paper is organized as follows. In Section II, the system model is presented. In Section III, we propose two maximization problems to maximize achievable secrecy rate subject to several quality-of-service constraints. In parallel, Section IV provides two minimization problems to minimize the power consumption such that security constraints are still guaranteed. In Section V, special cases of the proposed optimization problems are given for comparison purposes. Simulation results and conclusions are given in Sections VI and VII, respectively.

Notation: $[\cdot]^T$, $[\cdot]^*$, and $[\cdot]^\dagger$ denote the transpose operator, conjugate operator, and Hermitian operator, respectively. $[\cdot]^{-1}$ and $[\cdot]^+$ denote the inverse operator and pseudo-inverse operator, respectively. Vectors and matrices are represented with lowercase boldface and uppercase boldface, respectively. $\mathbf{I}_n$ is the $n \times n$ identity matrix. $\|\cdot\|$ denotes the Euclidean norm. $\mathbb{E}\{\cdot\}$ denotes expectation. $\mathbf{z} \sim \mathscr{CN}_n(\bar{\mathbf{z}}, \mathbf{\Sigma})$ denotes a complex Gaussian vector $\mathbf{z} \in \mathbb{C}^{n\times 1}$ with mean vector $\bar{\mathbf{z}}$ and covariance matrix $\mathbf{\Sigma} \in \mathbb{C}^{n\times n}$.

II. Cell-Free System Model

We consider a system with *M* APs and *K* users in the presence of an active eavesdropper (Eve). Each node is equipped with a single antenna and all nodes are randomly positioned. Let $g_{mk} = \sqrt{\beta_{mk}} h_{mk} \sim \mathscr{CN}(0, \beta_{mk})$ be the downlink channel from the *m*th AP to the *k*th user.[1] We assume channel reciprocity between uplink and downlink. Similarly, let $g_{m\mathrm{E}} \sim \mathscr{CN}(0, \beta_{m\mathrm{E}})$ be the channel between the *m*th AP and Eve. Note that the desirable property of

[1]In the formulation $g_{mk} = \sqrt{\beta_{mk}} h_{mk}$, the term β_{mk} represents the large scale fading, while the term $h_{mk} \sim \mathscr{CN}(0, 1)$ implies the small scale fading. The value of β_{mk} is constant and is based on a particular rule of power degradation. This rule will be presented in Section VI, given that the Hata-COST231 propagation prediction model is used (see [19] and [20]).

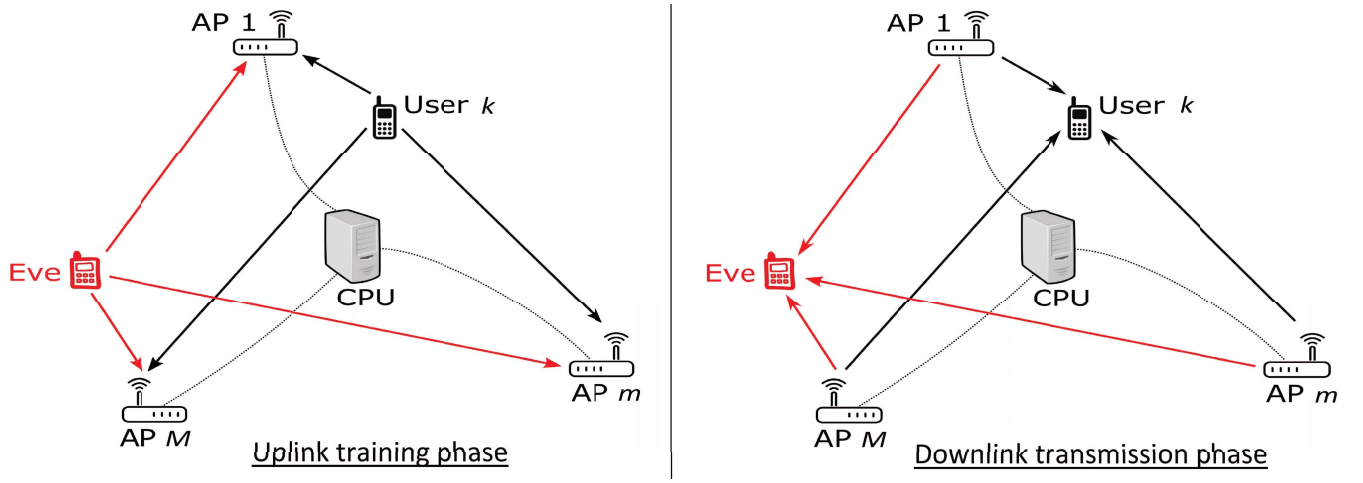


Fig. 1. A system model consisting of M APs, K legal users and one active eavesdropper Eve. The arrows point to the direction from transmitters to receivers. All directions, connected to Eve, are in red. In uplink training phase, all users and Eve send the pilots to the APs in order to request for the messages, which privately intended for them. Connected together through a CPU, the APs exchange information, estimate channels and detect abnormality in pilot sequences. In downlink transmission phase, the APs transmit their designed signals to users and Eve.

channel reciprocity requires the highly accurate calibration of hardware. In addition, the APs in cell-free massive MIMO systems are connected to a CPU via backhaul, thereby they can share information. We assume that the backhaul is perfect enough to consider error-free information only. Any limitation on capacity (caused by imperfect backhaul) will be left for future work.

The transmission includes 2 phases: Uplink training for channel estimation and downlink data transmission.

A. Uplink Training

In this phase, the kth user sends a certain pilot vector $\mathbf{p}_k \in \mathbb{C}^{T\times 1}$ to all APs where T is an integer number. If L_{int} denotes the coherence interval, then the first T symbols are for pilot training and the $(L_{int}-T)$ remaining symbols are for data transmission. In low-mobility environment, the coherence interval can take on large numbers. It is shown that if the vehicle speed is 5.4 km/h, the coherence interval L_{int} can approach 15000 symbols (see [21, p.23]). With such a large value of L_{int}, we can totally assign a sufficiently-large number to T such that the inequality $T \geq K$ holds true. For example, $(T, K) = (150, 100)$ is totally possible in practical situations (note that $T = 150$ accounts for only 0.1% of $L_{int} = 15000$). In short, we can totally have $T \geq K$ and then design K orthogonal pilot vectors such that $\mathbf{p}_k^\dagger \mathbf{p}_{k'} = 0$ for $k \neq k'$ and $\|\mathbf{p}_k\|^2 = 1$. In general, $\mathbf{p}_1, \ldots, \mathbf{p}_K$ are known to Eve because the pilot sequences of a system are standardized and public. Taking advantage of this, Eve also sends its pilot sequence $\mathbf{p}_{\mathrm{E}}$ to all APs. If Eve wants to detect the signal destined for the lth user, $\mathbf{p}_{\mathrm{E}}$ will be designed to be the same as $\mathbf{p}_l$ (see [8], [22], [23]). Without the loss of generality, let us consider the situation in which Eve aims to overhear the confidential messages intended for the 1st user, i.e. $\mathbf{p}_{\mathrm{E}} = \mathbf{p}_1$. At the mth AP, the received pilot vector is given by

$$\mathbf{y}_{p,m} = \sqrt{T\rho_u}\sum_{k=1}^{K} g_{mk}\mathbf{p}_k + \sqrt{T\rho_{\mathrm{E}}}g_{m\mathrm{E}}\mathbf{p}_1 + \mathbf{w}_m \qquad (1)$$

where $\rho_u \triangleq P_u/N_0$ and $\rho_{\mathrm{E}} \triangleq P_{\mathrm{E}}/N_0$. Herein, P_u and P_{E} are the average transmit power of each user and that of Eve, respectively; while N_0 is the average noise power per a receive antenna. $\mathbf{w}_m$ is an additive white Gaussian noise (AWGN) vector with $\mathbf{w}_m \sim \mathscr{CN}(\mathbf{0}, \mathbf{I})$. Projecting $\mathbf{y}_{p,m}$ onto $\mathbf{p}_k^\dagger$, we can write the post-processing signal $y_{km} = \mathbf{p}_k^\dagger \mathbf{y}_{p,m}$ as[2]

$$y_{km} = \begin{cases} \sqrt{T\rho_u}g_{mk} + \mathbf{p}_k^\dagger \mathbf{w}_m, & k \neq 1 \\ \sqrt{T\rho_u}g_{m1} + \sqrt{T\rho_{\mathrm{E}}}g_{m\mathrm{E}} + \mathbf{p}_1^\dagger \mathbf{w}_m, & k = 1. \end{cases} \qquad (2)$$

It is of crucial importance that all APs are not aware of an eavesdropping attack until they have realized an abnormal sign from the sequence of signals $\{y_{km}\}$ in (2). Based on that abnormal sign, APs can identify the pilot which might be harmed. Therefore, it is necessary for APs to have a method to observe abnormality from $\{y_{km}\}$. We describe such a method in Appendix A.

Besides, with the aim of estimating g_{mk} and $g_{m\mathrm{E}}$ from (2), the MMSE method is adopted at the mth AP, i.e.

$$\hat{g}_{mk} = \begin{cases} \dfrac{\sqrt{T\rho_u}\beta_{mk}}{T\rho_u\beta_{mk}+1} y_{km}, & k \neq 1 \\ \dfrac{\sqrt{T\rho_u}\beta_{m1}}{T\rho_u\beta_{m1} + T\rho_{\mathrm{E}}\beta_{m\mathrm{E}} + 1} y_{1m}, & k = 1 \end{cases} \qquad (3)$$

and

$$\hat{g}_{m\mathrm{E}} = \sqrt{\frac{\rho_{\mathrm{E}}}{\rho_u}}\frac{\beta_{m\mathrm{E}}}{\beta_{m1}}\hat{g}_{m1}. \qquad (4)$$

Let us denote

$$\gamma_{mk} \triangleq \mathbb{E}\left\{|\hat{g}_{mk}|^2\right\} = \begin{cases} \dfrac{T\rho_u\beta_{mk}^2}{T\rho_u\beta_{mk}+1}, & k \neq 1 \\ \dfrac{T\rho_u\beta_{m1}^2}{T\rho_u\beta_{m1} + T\rho_{\mathrm{E}}\beta_{m\mathrm{E}} + 1}, & k = 1 \end{cases}$$

[2]If we assumed $T < K$ (i.e. $\mathbf{p}_k^\dagger \mathbf{p}_{k'} \neq 0$ for $k \neq k'$), there would be the presence of the term $\sqrt{T\rho_u}\sum_{k'\neq k}^{K} g_{mk'}\mathbf{p}_k^\dagger \mathbf{p}_{k'}$ in (2). Other changes could also be made and the framework of this paper could be re-applied.

and $\gamma_{m\mathrm{E}} \triangleq \mathbb{E}\left\{|\hat{g}_{m\mathrm{E}}|^2\right\}$. Using (4), we can also rewrite

$$\gamma_{m\mathrm{E}} = \alpha_m \gamma_{m1}$$

with $\alpha_m = \left(\rho_{\mathrm{E}}\beta_{m\mathrm{E}}^2\right)/\left(\rho_u \beta_{m1}^2\right)$. In association with the above, we state the following proposition for later use in the rest of paper.

Proposition 1: $\hat{g}_{mk}$ and $\hat{g}_{mk'}$ are uncorrelated for $\forall k' \neq k$. At the same time, $\hat{g}_{mE}$ and $\hat{g}_{mk'}$ are uncorrelated for $\forall k' \neq 1$. Furthermore, we have

$$\mathbb{E}\left\{|\hat{g}_{mk}\hat{g}_{mk'}^*|^2\right\} = \begin{cases} \gamma_{mk}\gamma_{mk'}, & k' \neq k \\ 2\gamma_{mk}^2, & k' = k \end{cases}, \tag{5}$$

and

$$\mathbb{E}\left\{|\hat{g}_{mE}\hat{g}_{mk'}^*|^2\right\} = \begin{cases} \alpha_m\gamma_{m1}\gamma_{mk'}, & k' \neq 1 \\ 2\alpha_m\gamma_{m1}^2, & k' = 1. \end{cases} \tag{6}$$

Proof: It is straightforward to prove the uncorrelatedness by showing $\mathbb{E}\{\hat{g}_{mk}\hat{g}_{mk'}^*\} = 0$ for $\forall k' \neq k$ and $\mathbb{E}\{\hat{g}_{m\mathrm{E}}\hat{g}_{mk'}^*\} = 0$ for $\forall k' \neq 1$. Using these results, we can obtain (5) and (6) with the help of (2)–(4) and the definitions of γ_{mk} and $\gamma_{m\mathrm{E}}$. □

Note that the eavesdropper's attack against the 1st user during the training phase leads to the presence of ρ_{E} in the denominator of $\hat{g}_{m1}$ (which is called a pilot spoofing attack).

B. Downlink Transmisson

In this phase, the *m*th AP uses the estimate $\hat{g}_{mk}$ to perform beamforming technique. First, we denote s_k be the signal intended for the *k*th user and P_s be the average transmit power for a certain s_k. Then the signal transmitted by the *m*th AP can be designed (according to beamforming technique) as [2]

$$x_m = \sqrt{P_s}\sum_{k=1}^{K}\sqrt{\eta_{mk}}\hat{g}_{mk}^* s_k \tag{7}$$

with s_k being normalized such that $\mathbb{E}\left\{|s_k|^2\right\} = 1$. In (7), η_{mk} is the power control coefficient, which corresponds to the downlink channel from the *m*th AP to the *k*th user.

As such, the received signal at the *k*th user and Eve are, respectively, given by

$$z_k = \sqrt{\rho_s}\sum_{m=1}^{M} g_{mk}\left(\sum_{k=1}^{K}\sqrt{\eta_{mk}}\hat{g}_{mk}^* s_k\right) + n_k, \tag{8}$$

$$z_{\mathrm{E}} = \sqrt{\rho_s}\sum_{m=1}^{M} g_{m\mathrm{E}}\left(\sum_{k=1}^{K}\sqrt{\eta_{mk}}\hat{g}_{mk}^* s_k\right) + n_{\mathrm{E}} \tag{9}$$

where $\rho_s = P_s/N_0$, $n_k \sim \mathscr{CN}(0,1)$, and $n_{\mathrm{E}} \sim \mathscr{CN}(0,1)$.

1) The Lower-Bound for the Mutual Information Between s_k and z_k: We rewrite (8) as

$$z_k = \mathrm{DS}_k \times s_k + \underbrace{\mathrm{BU}_k \times s_k + \sum_{k'\neq k}^{K}\mathrm{UI}_{kk'} \times s_{k'} + n_k}_{\text{treated as aggregated noise}}, \tag{10}$$

where

$$\mathrm{DS}_k \triangleq \sqrt{\rho_s}\sum_{m=1}^{M}\mathbb{E}\{\sqrt{\eta_{mk}}g_{mk}\hat{g}_{mk}^*\},$$

$$\mathrm{BU}_k \triangleq \sqrt{\rho_s}\sum_{m=1}^{M}(\sqrt{\eta_{mk}}g_{mk}\hat{g}_{mk}^* - \mathbb{E}\{\sqrt{\eta_{mk}}g_{mk}\hat{g}_{mk}^*\}),$$

$$\mathrm{UI}_{kk'} \triangleq \sqrt{\rho_s}\sum_{m=1}^{M}\sqrt{\eta_{mk'}}g_{mk}\hat{g}_{mk'}^*$$

represent the strength of the desired signal s_k, the beamforming gain uncertainty, and the interference caused by the k'th user (with $k' \neq k$), respectively. It is proved that the terms DS_k, BU_k, $\mathrm{UI}_{kk'}$ and n_k in (10) are pair-wisely uncorrelated.

Lemma 1: Let U and V be complex-valued random variables with $U \sim \mathscr{CN}(0, var\{U\})$ and $\mathbb{E}\left\{|V|^2\right\} = var\{V\}$. Given that U and V are uncorrelated, then the mutual information $I(U;U+V)$ between U and $U+V$ is lower-bounded by $\log_2(1 + var\{U\}/var\{V\})$. Consequently, the lower-bound SNR can be given by $var\{U\}/var\{V\}$.

Proof: The reader is referred to [24] and [25] for detailed proofs in terms of information theory. □

Let $I_k(s_k; z_k)$ denote the mutual information between s_k and z_k. Considering the second, third, and fourth terms in (10) as noises, the lower-bound for $I_k(s_k; z_k)$ can be deduced from Lemma 1 as follows:

$$I_k(s_k; z_k) \geq \log_2(1 + \mathrm{snr_k}) \tag{11}$$

where

$$\mathrm{snr_k} = \frac{|\mathrm{DS}_k|^2}{\mathbb{E}\{|\mathrm{BU}_k|^2\} + \sum_{k'\neq k}^{K}\mathbb{E}\{|\mathrm{UI}_{kk'}|^2\} + 1} = \frac{\rho_s\left(\sum_{m=1}^{M}\sqrt{\eta_{mk}}\gamma_{mk}\right)^2}{\rho_s\sum_{k'=1}^{K}\sum_{m=1}^{M}\eta_{mk'}\gamma_{mk'}\beta_{mk} + 1}, \quad k \in \mathcal{K} \tag{12}$$

with $\mathcal{K} = \{1, 2, \ldots, K\}$. The derivation of (12) is available in [2, Appendix A]. The right hand side (RHS) of (11) is the achievable data rate of user *k*.

2) The Upper-Bound for the Mutual Information Between s_1 and z_E: We rewrite (9) as

$$z_{\mathrm{E}} = \mathrm{BU}_{\mathrm{E},1} \times s_1 + \underbrace{\sum_{k'\neq 1}^{K}\mathrm{UI}_{\mathrm{E},k'} \times s_{k'} + n_{\mathrm{E}}}_{\text{treated as aggregated noise}}. \tag{13}$$

where

$$\mathrm{BU}_{\mathrm{E},1} \triangleq \sqrt{\rho_s}\sum_{m=1}^{M}\sqrt{\eta_{m1}}g_{m\mathrm{E}}\hat{g}_{m1}^*,$$

$$\mathrm{UI}_{\mathrm{E},k'} \triangleq \sqrt{\rho_s}\sum_{m=1}^{M}\sqrt{\eta_{mk'}}g_{m\mathrm{E}}\hat{g}_{mk'}^*$$

respectively represent the strength of the desired signal s_1 (which Eve may want to overhear) and the interference caused by the remaining users (with $k' \neq k$). It is proved that the terms $\mathrm{BU}_{\mathrm{E},k}$, $\mathrm{UI}_{\mathrm{E},kk'}$ and n_{E} in (13) are pair-wisely uncorrelated. Thus, we can consider the second and third terms in (13) as noises.

Let $I_{\mathrm{E}}(s_1; z_{\mathrm{E}})$ denote the mutual information between s_1 and z_{E}. Then the upper-bound for $I_{\mathrm{E}}(s_k; z_{\mathrm{E}})$ can be formulated as follows:

$$\begin{aligned} I_{\mathrm{E}}(s_1; z_{\mathrm{E}}) &\overset{(a)}{\leq} I_{\mathrm{E}}\left(s_1; z_{\mathrm{E}} \middle| \{g_{mk}\}_{m,k}, \{\hat{g}_{mk}\}_{m,k}, \{g_{m\mathrm{E}}\}_m\right) \\ &= \mathbb{E}\left\{\log_2\left(1 + \frac{|\mathrm{BU}_{\mathrm{E},1}|^2}{\sum_{k'\neq 1}^{K}|\mathrm{UI}_{\mathrm{E},k'}|^2 + 1}\right)\right\} \\ &\overset{(b)}{\approx} \log_2(1 + \mathrm{snr}_{\mathrm{E}}) \end{aligned} \tag{14}$$

where

$$\mathrm{snr}_{\mathrm{E}} = \frac{\mathbb{E}\{|\mathrm{BU}_{\mathrm{E},1}|^2\}}{\sum_{k'\neq 1}^{K}\mathbb{E}\{|\mathrm{UI}_{\mathrm{E},k'}|^2\} + 1} \tag{15}$$

$$\overset{(c)}{=} \frac{\rho_s \sum_{m=1}^{M}\eta_{m1}\gamma_{m1}\left(\frac{\rho_{\mathrm{E}}\beta_{m\mathrm{E}}^2}{\rho_u\beta_{m1}^2}\gamma_{m1} + \beta_{m\mathrm{E}}\right)}{\rho_s\sum_{k'\neq 1}^{K}\sum_{m=1}^{M}\eta_{mk'}\gamma_{mk'}\beta_{m\mathrm{E}} + 1}. \tag{16}$$

The RHS of inequality (a) means that Eve perfectly knows channel gains. It also implies the worst case in terms of security. Meanwhile, the approximation (b) follows [26, Lemma 1]. Finally, the derivation of (c) is provided in Appendix B.

3) Achievable Secrecy Rate: From (11) and (14), we can define the achievable secrecy rate of user 1 as follows:

$$\begin{aligned} \Delta &= I_1(s_1; z_1) - I_{\mathrm{E}}(s_1; z_{\mathrm{E}}) \\ &\geq \log_2((1 + \mathrm{snr}_1)/(1 + \mathrm{snr}_{\mathrm{E}})) \triangleq R_{sec} \end{aligned} \tag{17}$$

in which the explicit expressions for snr_1 and $\mathrm{snr}_{\mathrm{E}}$ are presented in (12) and (16), respectively.

In order to facilitate further analysis in the rest of paper, we denote $\mathbf{\Psi}$ be the matrix in which the (m,k)th entry is $\mathbf{\Psi}(m,k) = \sqrt{\eta_{mk}}$. The kth column vector of $\mathbf{\Psi}$ is denoted as

$$\mathbf{u}_k = \mathbf{\Psi}(:,k) = [\sqrt{\eta_{1k}}, \sqrt{\eta_{2k}}, \ldots, \sqrt{\eta_{Mk}}]^T.$$

Besides, we also define the following matrices and vectors

$$\begin{aligned} \mathbf{a}_k &= \sqrt{\rho_s}[\gamma_{1k}, \gamma_{2k}, \ldots, \gamma_{Mk}]^T, \\ \mathbf{A}_{kk'} &= \sqrt{\rho_s}\mathrm{diag}\left(\sqrt{\beta_{1k}\gamma_{1k'}}, \ldots, \sqrt{\beta_{Mk}\gamma_{Mk'}}\right), \\ \mathbf{B}_{\mathrm{E}} &= \sqrt{\rho_s}\mathrm{diag}\left(\sqrt{\gamma_{11}(\gamma_{1\mathrm{E}}+\beta_{1\mathrm{E}})}, \ldots, \sqrt{\gamma_{M1}(\gamma_{M\mathrm{E}}+\beta_{M\mathrm{E}})}\right) \\ \mathbf{B}_{k'} &= \sqrt{\rho_s}\mathrm{diag}\left(\sqrt{\beta_{1\mathrm{E}}\gamma_{1k'}}, \ldots, \sqrt{\beta_{M\mathrm{E}}\gamma_{Mk'}}\right) \text{ with } k' \neq 1. \end{aligned}$$

Finally, the SNRs in (12) and (16) can be rewritten in a more elegant way as follows:

$$\mathrm{snr}_{\mathrm{k}} = \left(\mathbf{a}_k^T\mathbf{u}_k\right)^2 \Big/ \varphi_k(\mathbf{\Psi}), \tag{18}$$

$$\mathrm{snr}_{\mathrm{E}} = \|\mathbf{B}_{\mathrm{E}}\mathbf{u}_1\|^2 \Big/ \varphi_{\mathrm{E}}(\mathbf{\Psi}) \tag{19}$$

where

$$\varphi_k(\mathbf{\Psi}) = \sum_{k'=1}^{K}\|\mathbf{A}_{kk'}\mathbf{u}_{k'}\|^2 + 1, \quad k \in \mathcal{K}, \tag{20}$$

$$\varphi_{\mathrm{E}}(\mathbf{\Psi}) = \sum_{k'\neq 1}^{K}\|\mathbf{B}_{k'}\mathbf{u}_{k'}\|^2 + 1. \tag{21}$$

All SNR-related expressions are now presented as functions of Ψ instead of $\{\eta_{mk}\}_{m,k}$. Given that η_{mk} decides the amount of the *m*th AP's power destined for the *k* user, the (m,k)th entry of Ψ is also referred to as the factor deciding how much transmit power used by the *m*th AP and destined for the *k* user.

III. Secrecy Rate Maximization

In this section, we aim to design the matrix $\mathbf{\Psi}$ to maximize either the achievable data rate of user 1 (in nats/s/Hz), i.e. $\ln(1+\mathrm{snr}_1)$, or its achievable secrecy rate $\ln(1+\mathrm{snr}_1) - \ln(1+\mathrm{snr}_{\mathrm{E}1})$ in improving the secure performance of our system. Prior to performing these tasks, however, we need to impose a critical condition on the power at each AP. The power constraint is described as follows:

- Let P_{max} be the maximum transmit power of each AP, i.e. $P_{max} \geq \mathbb{E}\{|x_m|^2\}$. From (7), the average transmit power for the *m*th AP can be given by

$$\mathbb{E}\{|x_m|^2\} = P_s\sum_{k=1}^{K}\eta_{mk}\gamma_{mk}. \tag{22}$$

With the power constraint on every AP, we have

$$\sum_{k=1}^{K}\mathbf{\Psi}^2(m,k)\gamma_{mk} \leq \frac{\rho_{max}}{\rho_s}, \quad m \in \mathcal{M} \tag{23}$$

with $\mathcal{M} = \{1, \ldots, M\}$. Note that $\rho_{max} = P_{max}/N_0$ is viewed as the maximum possible ratio of the *m*th AP's average transmit power to the average noise power.

Now we begin with optimizing $\mathbf{\Psi}$ to maximize the achievable data rate of the 1st user (who is under attack), i.e.

$$(\mathbf{P1}) \quad \max_{\mathbf{\Psi}} \ \ln\left(1 + \left(\mathbf{a}_1^T\mathbf{u}_1\right)^2 \Big/ \varphi_1(\mathbf{\Psi})\right) \tag{24a}$$

$$\text{s.t. (23)}, \tag{24b}$$

$$\frac{\|\mathbf{B}_{\mathrm{E}}\mathbf{u}_1\|^2}{\varphi_{\mathrm{E}}(\mathbf{\Psi})} \leq \theta_{\mathrm{E}}, \tag{24c}$$

$$\frac{\left(\mathbf{a}_k^T\mathbf{u}_k\right)^2}{\varphi_k(\mathbf{\Psi})} \geq \theta_k, \quad k \in \mathcal{K}\backslash\{1\}. \tag{24d}$$

Herein, optimizing $\mathbf{\Psi}$ is equivalent to finding the optimal value of every power control coefficient η_{mk} (because of the relation $\mathbf{\Psi}(m,k) = \sqrt{\eta_{mk}}$).

The constraint (23) is to control the transmit power at each AP as previously described. The constraint (24c) requires that the *greatest* amount of information Eve can captures will not exceed some predetermined threshold, i.e. $\ln(1+\mathrm{snr}_{\mathrm{E}}) \leq \ln(1+\theta_{\mathrm{E}})$. Finally, the constraint (24d) guarantees that the achievable data rate of user $k \in \mathcal{K}\backslash\{1\}$ is equal to or greater than some target threshold, i.e. $\ln(1+\mathrm{snr}_{\mathrm{k}}) \geq \ln(1+\theta_k)$.

Similarly, we will optimize every η_{mk} (through optimizing the coefficient matrix $\mathbf{\Psi}$) to maximize the achievable secrecy rate of user 1, i.e.

$$(\mathbf{Q1}) \quad \max_{\mathbf{\Psi}} \ \ln\left(\frac{1 + \left(\mathbf{a}_1^T\mathbf{u}_1\right)^2 \Big/ \varphi_1(\mathbf{\Psi})}{1 + \|\mathbf{B}_{\mathrm{E}}\mathbf{u}_1\|^2 \Big/ \varphi_{\mathrm{E}}(\mathbf{\Psi})}\right) \tag{25a}$$

$$\text{s.t. (23), (24d)}. \tag{25b}$$

It should be noted that both problems **(P1)** and **(Q1)** has been considered in [27] and [28] in the context of conventional MIMO systems, information and energy transfer. Inspired by these two works, we also use path-following algorithms to solve non-convex optimization problems. As can be seen in the subsections below, each of the proposed path-following algorithms invokes only one simple convex quadratic program at each iteration and thus, at least a locally optimal solution can be found out.

A. Solving Problem (P1)

We can see that the constraint (23) is obviously convex, while (24d) is the following second-order cone (SOC) constraint and thus convex:

$$\frac{1}{\sqrt{\theta_k}}\mathbf{a}_k^T\mathbf{u}_k \geq \sqrt{\varphi_k(\mathbf{\Psi})}, \quad k \in \mathcal{K}\backslash\{1\}. \tag{26}$$

Besides, we observe that the objective function of (**P1**) can be replaced with $\left(\mathbf{a}_1^T\mathbf{u}_1\right)^2 \Big/ \varphi_1(\mathbf{\Psi})$. Let $\mathbf{\Psi}^{(\kappa)}$ be a feasible point for (**P1**) found from the $(\kappa-1)$th iteration. By using the inequality

$$\frac{x^2}{y} \geq 2\frac{\bar{x}}{\bar{y}}x - \frac{\bar{x}^2}{\bar{y}^2}y \quad \forall\ x>0,\ y>0,\ \bar{x}>0,\ \bar{y}>0 \tag{27}$$

we obtain

$$\frac{\left(\mathbf{a}_1^T\mathbf{u}_1\right)^2}{\varphi_1(\mathbf{\Psi})} \geq f_1^{(\kappa)}(\mathbf{\Psi}) \triangleq a^{(\kappa)}\mathbf{a}_1^T\mathbf{u}_1 - b^{(\kappa)}\varphi_1(\mathbf{\Psi}) \tag{28}$$

with

$$a^{(\kappa)} = 2\frac{\left(\mathbf{a}_1^T\mathbf{u}_1^{(\kappa)}\right)^2}{\varphi_1(\mathbf{\Psi}^{(\kappa)})}, \quad b^{(\kappa)} = (a^{(\kappa)}/2)^2. \tag{29}$$

As such, maximizing $\left(\mathbf{a}_1^T\mathbf{u}_1\right)^2 \Big/ \varphi_1(\mathbf{\Psi})$ is now equivalent to maximizing $f_1^{(\kappa)}(\mathbf{\Psi})$. Finally, considering the function $\varphi_{\mathrm{E}}(\mathbf{\Psi})$ in (24c), we find that it is convex quadratic and thus, the non-convex constraint (24c) is innerly approximated by the convex quadratic constraint[3]

$$\left\|\mathbf{B}_{\mathrm{E}}\mathbf{u}_1\right\|^2 \Big/ \theta_{\mathrm{E}} \leq \varphi_{\mathrm{E}}^{(\kappa)}(\mathbf{\Psi}) \tag{30}$$

for

$$\varphi_{\mathrm{E}}^{(\kappa)}(\mathbf{\Psi}) \triangleq \sum_{k\neq 1}^{K}\left[\mathbf{u}_k^{(\kappa)^T}\mathbf{B}_k^2\left(2\mathbf{u}_k - \mathbf{u}_k^{(\kappa)}\right)\right] + 1. \tag{31}$$

Having the approximations (28) and (30), at κ-th iteration we solve the following convex optimization to generate a feasible point $\mathbf{\Psi}^{(\kappa+1)}$:

$$\max_{\mathbf{\Psi}}\ f_1^{(\kappa)}(\mathbf{\Psi}) \text{s.t. } (23), (26), (30). \tag{32}$$

The problem (32) involves *MK* scalar real variables (because $\mathbf{\Psi}$ has *MK* entries) and $\epsilon = M + K$ quadratic constraints. According to [28], the per-iteration cost to solve (32) is $\mathcal{O}\left((MK)^2\epsilon^{2.5} + \epsilon^{3.5}\right)$.

[3]The right hand side of (30) is the first-order Taylor approximation of $\varphi_{\mathrm{E}}(\mathbf{\Psi})$ near $\mathbf{\Psi}^{(\kappa)}$. With $\varphi_{\mathrm{E}}(\mathbf{\Psi})$ being convex, we have $\varphi_{\mathrm{E}}^{(\kappa)}(\mathbf{\Psi}) \leq \varphi_{\mathrm{E}}(\mathbf{\Psi})$.

To find a feasible point for (**P1**) to initialize the above procedure, we address the problem

$$\min_{\mathbf{\Psi}}\ \left\|\mathbf{B}_{\mathrm{E}}\mathbf{u}_1\right\|^2 \Big/ \theta_{\mathrm{E}} - \varphi_{\mathrm{E}}(\mathbf{\Psi}) \quad \text{s.t. } (23), (26). \tag{33}$$

Initialized by any feasible point $\mathbf{\Psi}^{(0)}$ for convex constraints (23) and (26), we iterate the following optimization problem

$$\min_{\mathbf{\Psi}}\ \left\|\mathbf{B}_{\mathrm{E}}\mathbf{u}_1\right\|^2 \Big/ \theta_{\mathrm{E}} - \varphi_{\mathrm{E}}^{(\kappa)}(\mathbf{\Psi}) \quad \text{s.t. } (23), (26), \tag{34}$$

till

$$\left\|\mathbf{B}_{\mathrm{E}}\mathbf{u}_1^{(\kappa)}\right\|^2 \Big/ \theta_{\mathrm{E}} - \varphi_{\mathrm{E}}\left(\mathbf{\Psi}^{(\kappa)}\right) \leq 0, \tag{35}$$

so $\mathbf{\Psi}^{(\kappa)}$ is feasible for (**P1**). To sum up, we provide the following algorithm:

Algorithm 1 Path-Following Algorithm for Solving (**P1**)

1: **Initialization**: Set $\kappa = 0$ with a feasible point $\mathbf{\Psi}^{(0)}$ for (**P1**).
2: **repeat**
3: Solve (32) to obtain the optimal solution $\mathbf{\Psi}^{(\kappa+1)}$.
4: Reset $\kappa := \kappa + 1$.
5: **until** Converge.
6: **return** $\mathbf{\Psi}^{(\kappa)}$ as the desired result.

B. Solving Problem (Q1)

By using the inequality [29]

$$\ln\left(1+\frac{x^2}{y}\right) \geq \ln\left(1+\frac{\bar{x}^2}{\bar{y}}\right) + \frac{\frac{\bar{x}^2}{\bar{y}}}{1+\frac{\bar{x}^2}{\bar{y}}}\left(2 - \frac{\bar{x}}{2x-\bar{x}} - \frac{y}{\bar{y}}\right)$$
$$\text{for } \forall\ x>0,\ \bar{x}>0,\ y>0,\ \bar{y}>0,\ 2x>\bar{x} \tag{36}$$

we obtain

$$\ln\left(1+\frac{\left(\mathbf{a}_1^T\mathbf{u}_1\right)^2}{\varphi_1(\mathbf{\Psi})}\right)$$
$$\geq a^{(\kappa)} + b^{(\kappa)}\left(2 - \frac{\varphi_1(\mathbf{\Psi})}{\varphi_1(\mathbf{\Psi}^{(\kappa)})} - \frac{(\mathbf{a}_1^T\mathbf{u}_1^{(\kappa)})^2}{2\mathbf{a}_1^T\mathbf{u}_1^{(\kappa)}\mathbf{a}_1^T\mathbf{u}_1 - (\mathbf{a}_1^T\mathbf{u}_1^{(\kappa)})^2}\right)$$
$$\triangleq f^{(\kappa)}(\mathbf{\Psi}) \tag{37}$$

over the trust region

$$2\mathbf{a}_1^T\mathbf{u}_1^{(\kappa)}\mathbf{a}_1^T\mathbf{u}_1 - (\mathbf{a}_1^T\mathbf{u}_1^{(\kappa)})^2 > 0 \tag{38}$$

for

$$a^{(\kappa)} = \ln\left(1+t^{(\kappa)}\right),$$
$$b^{(\kappa)} = t^{(\kappa)}\Big/\left(1+t^{(\kappa)}\right),$$
$$t^{(\kappa)} = \left(\mathbf{a}_1^T\mathbf{u}_1^{(\kappa)}\right)^2\Big/\varphi_1\left(\mathbf{\Psi}^{(\kappa)}\right).$$

In addition, by respectively using the inequality [29]

$$\ln(1+x) \leq \ln(1+\bar{x}) - \frac{\bar{x}}{1+\bar{x}} + \frac{x}{\bar{x}+1}, \quad \forall\ x>0,\ \bar{x}>0 \tag{39}$$

and the fact that $\varphi_{\mathrm{E}}^{(\kappa)}(\mathbf{\Psi}) \leq \varphi_{\mathrm{E}}(\mathbf{\Psi})$ (please see Footnote 2), we obtain

$$\ln\left(1+\frac{\|\mathbf{B}_{\mathrm{E}}\mathbf{u}_1\|^2}{\varphi_{\mathrm{E}}(\mathbf{\Psi})}\right) \leq c^{(\kappa)} + d^{(\kappa)}\frac{\|\mathbf{B}_{\mathrm{E}}\mathbf{u}_1\|^2}{\varphi_{\mathrm{E}}(\mathbf{\Psi})} \leq c^{(\kappa)} + d^{(\kappa)}\frac{\|\mathbf{B}_{\mathrm{E}}\mathbf{u}_1\|^2}{\varphi_{\mathrm{E}}^{(\kappa)}(\mathbf{\Psi})} \triangleq g^{(\kappa)}(\mathbf{\Psi}) \quad (40)$$

over the trust region

$$\varphi_{\mathrm{E}}^{(\kappa)}(\mathbf{\Psi}) > 0 \quad (41)$$

for

$$c^{(\kappa)} = \ln(1+t_{\mathrm{E}}^{(\kappa)}) - t_{\mathrm{E}}^{(\kappa)} \Big/ \left(1+t_{\mathrm{E}}^{(\kappa)}\right),$$
$$d^{(\kappa)} = 1 \Big/ \left(1+t_{\mathrm{E}}^{(\kappa)}\right),$$
$$t_{\mathrm{E}}^{(\kappa)} = \left\|\mathbf{B}_{\mathrm{E}}\mathbf{u}_1^{(\kappa)}\right\|^2 \Big/ \varphi_{\mathrm{E}}\left(\mathbf{\Psi}^{(\kappa)}\right).$$

Initialized by a feasible point $\mathbf{\Psi}^{(0)}$ for the convex constraints (23) and (26), at κ-th iteration for $\kappa = 0, 1, \ldots$, we solve the following convex optimization problem to generate the next feasible point $\mathbf{\Psi}^{(\kappa+1)}$:

$$\max_{\mathbf{\Psi}} f^{(\kappa)}(\mathbf{\Psi}) - g^{(\kappa)}(\mathbf{\Psi}) \quad (42a)$$
$$\text{s.t. } (23), (26), (38), (41). \quad (42b)$$

With *MK* scalar real variables, 2 linear constraints and $(\epsilon-1)$ quadratic constraints, the per-iteration cost to solve (42) is $\mathcal{O}\left((MK)^2(\epsilon-1)^{2.5} + (\epsilon-1)^{3.5}\right)$.

As such, the problem (**Q1**) can be solved by using the following algorithm:

Algorithm 2 Path-Following Algorithm for Solving (**Q1**)

1: **Initialization**: Set $\kappa = 0$ with a feasible point $\mathbf{\Psi}^{(0)}$ for (**Q1**).
2: **repeat**
3: Solve (42) to obtain the optimal solution $\mathbf{\Psi}^{(\kappa+1)}$.
4: Reset $\kappa := \kappa + 1$.
5: **until** Converge.
6: **return** $\mathbf{\Psi}^{(\kappa)}$ as the desired result.

IV. Power Minimization

In this section, we aim to design the matrix $\mathbf{\Psi}$ to minimize the total average transmit power of all APs subject to security constraints as well as other SNR-based constraints:

$$(\mathbf{R1}) \quad \min_{\mathbf{\Psi}} \sum_{m=1}^{M}\sum_{k=1}^{K} \mathbf{\Psi}^2(m,k)\gamma_{mk} \quad (43a)$$
$$\text{s.t. } (23), (24c), \quad (43b)$$
$$\frac{\left(\mathbf{a}_k^T\mathbf{u}_k\right)^2}{\varphi_k(\mathbf{\Psi})} \geq \theta_k, \quad k \in \mathcal{K} \quad (43c)$$

and

$$(\mathbf{S1}) \quad \min_{\mathbf{\Psi}} \sum_{m=1}^{M}\sum_{k=1}^{K} \mathbf{\Psi}^2(m,k)\gamma_{mk} \quad (44a)$$
$$\text{s.t. } (23), (26), \quad (44b)$$
$$\ln\left(\frac{1+\left(\mathbf{a}_1^T\mathbf{u}_1\right)^2 \Big/ \varphi_1(\mathbf{\Psi})}{1+\|\mathbf{B}_{\mathrm{E}}\mathbf{u}_1\|^2 \Big/ \varphi_{\mathrm{E}}(\mathbf{\Psi})}\right) \geq r_\phi. \quad (44c)$$

Again, $\mathbf{\Psi}(m,k)$ is the (m,k)th entry of the matrix $\mathbf{\Psi}$. Due to the relation $\mathbf{\Psi}(m,k) = \sqrt{\eta_{mk}}$, finding $\mathbf{\Psi}$ is equivalent to finding every power control coefficient η_{mk} ($m \in \mathcal{M}$ and $k \in \mathcal{K}$).

In addition, the objective function is the total power *radiated* by the antennas of APs. The power consumed by other components (such as the backhaul and the CPU) is beyond the scope of this paper.

Note that (43c) is not exactly the same as (26) because (43c) contains one more constraint, i.e. $\text{snr}_1 \geq \theta_1$. Meanwhile, r_ϕ in the program (**S1**) is the given threshold which a designer may want to obtain. In general, we will have different results (which of course leads to different secure performances) when using (**R1**) and (**S1**). However, the obtained results can also be the same when using these programs, depending on the given values of θ_1, θ_{E} and r_ϕ.

A. Solving Problem (*R1*)

At κ-th iteration, we solve the following convex optimization problem to generalize the next iterative feasible point $\mathbf{\Psi}^{(\kappa+1)}$

$$\min_{\mathbf{\Psi}} \sum_{m=1}^{M}\sum_{k=1}^{K} \mathbf{\Psi}^2(m,k)\gamma_{mk} \quad (45a)$$
$$\text{s.t. } (23), (26), (30). \quad (45b)$$

Similar to (32), the computational complexity of solving (45) is also $\mathcal{O}\left((MK)^2\epsilon^{2.5} + \epsilon^{3.5}\right)$.

Note that a feasible point $\mathbf{\Psi}^{(0)}$ for (**R1**) can be found in the same way as (**P1**). Furthermore, the algorithm for solving (**R1**) is presented below.

Algorithm 3 Path-Following Algorithm for Solving (**R1**)

1: **Initialization**: Set $\kappa = 0$ with a feasible point $\mathbf{\Psi}^{(0)}$ for (**R1**).
2: **repeat**
3: Solve (45) to obtain the optimal solution $\mathbf{\Psi}^{(\kappa+1)}$.
4: Reset $\kappa := \kappa + 1$.
5: **until** Converge.
6: **return** $\mathbf{\Psi}^{(\kappa)}$ as the desired result.

B. Solving Problem (*S1*)

At κ-th iteration, we solve the following convex optimization problem to generalize the next iterative feasible

point $\mathbf{\Psi}^{(\kappa+1)}$:

$$\min_{\mathbf{\Psi}} \sum_{m=1}^{M}\sum_{k=1}^{K} \mathbf{\Psi}^2(m,k)\gamma_{mk} \tag{46a}$$
$$\text{s.t. } (23), (26), \tag{46b}$$
$$f^{(\kappa)}(\mathbf{\Psi}) - g^{(\kappa)}(\mathbf{\Psi}) \geq r_\phi. \tag{46c}$$

Similar to (32) and (45), the computational complexity of solving (46) is also $\mathcal{O}\left((MK)^2\epsilon^{2.5} + \epsilon^{3.5}\right)$.

Note that a feasible point $\mathbf{\Psi}^{(0)}$ for (**S1**) can be found like that for (**Q1**). Finally, we provide the detailed algorithm for solving (**S1**) as follows:

Algorithm 4 Path-Following Algorithm for Solving (**S1**)

1: **Initialization**: Set $\kappa = 0$ with a feasible point $\mathbf{\Psi}^{(0)}$ for (**S1**).
2: **repeat**
3: Solve (46) to obtain the optimal solution $\mathbf{\Psi}^{(\kappa+1)}$.
4: Reset $\kappa := \kappa + 1$.
5: **until** Converge.
6: **return** $\mathbf{\Psi}^{(\kappa)}$ as the desired result.

V. Optimization Under Equal Power Allocation at Access Points

In this section, we reconsider the proposed optimization problems with η_{mk} being equal to η (for all m and k) for comparison purposes.

Plugging $\eta_{mk} = \eta$ into (12)–(16), we obtain the special expressions for snr_k and snr_E as follows:

$$\text{snr}_\text{k}|_{\eta_{mk}=\eta} = \eta\omega_k / \left(\eta\breve{\omega}_k + 1\right), \tag{47}$$
$$\text{snr}_\text{E}|_{\eta_{mk}=\eta} = \frac{\eta\varpi}{\eta\breve{\varpi} + 1} \tag{48}$$

where

$$\omega_k = \rho_s \left(\sum_{m=1}^{M} \gamma_{mk}\right)^2,$$
$$\breve{\omega}_k = \rho_s \sum_{k'=1}^{K}\sum_{m=1}^{M} \gamma_{mk'}\beta_{mk},$$
$$\varpi = \rho_s \sum_{m=1}^{M} \gamma_{m1}\left(\frac{\rho_\text{E}\beta_{m\text{E}}^2}{\rho_u\beta_{m1}^2}\gamma_{m1} + \beta_{m\text{E}}\right),$$
$$\breve{\varpi} = \rho_s \sum_{k'\neq 1}^{K}\sum_{m=1}^{M} \gamma_{mk'}\beta_{m\text{E}}.$$

Then, problems (**P1**) and (**Q1**) reduce to

$$(\underline{\text{P1}}) \quad \max_{\eta} \ \eta\omega_1 / \left(\eta\breve{\omega}_1 + 1\right) \tag{49a}$$
$$\text{s.t. } \eta \leq \frac{\rho_{max}/\rho_s}{\sum_{k=1}^{K}\gamma_{mk}}, \quad m \in \mathcal{M} \tag{49b}$$
$$\eta\left(\varpi - \theta_\text{E}\breve{\varpi}\right) \leq \theta_\text{E}, \tag{49c}$$
$$\eta\left(\omega_k - \theta_k\breve{\omega}_k\right) \geq \theta_k, \quad k \in \mathcal{K}\backslash\{1\} \tag{49d}$$

and

$$(\underline{\text{Q1}}) \quad \max_{\eta} \ \left(1 + \frac{\eta\omega_1}{\eta\breve{\omega}_1 + 1}\right) \Big/ \left(1 + \frac{\eta\varpi}{\eta\breve{\varpi} + 1}\right) \tag{50a}$$
$$\text{s.t. } (49\text{b}), (49\text{d}). \tag{50b}$$

Similarly, problems (**R1**) and (**S1**) reduce to

$$(\underline{\text{R1}}) \quad \min_{\eta} \ \eta \tag{51a}$$
$$\text{s.t. } (49\text{b}), (49\text{c}), \tag{51b}$$
$$\frac{\eta\omega_k}{\left(\eta\breve{\omega}_k + 1\right)} \geq \theta_k, \ k \in \mathcal{K} \tag{51c}$$

and

$$(\underline{\text{S1}}) \quad \min_{\eta} \ \eta \tag{52a}$$
$$\text{s.t. } (49\text{b}), (49\text{d}), \tag{52b}$$
$$\frac{1 + \eta\omega_1 / \left(\eta\breve{\omega}_1 + 1\right)}{1 + \eta\varpi / \left(\eta\breve{\varpi} + 1\right)} \geq \phi. \tag{52c}$$

A. Closed-Form Solutions to (P1)

The objective function of (P1) increases in η. Hence, maximizing that objective function is equivalent to maximizing η. In other words, we will solve the following problem

$$(\underline{\text{P1}}) \quad \max_{\eta} \ \eta \tag{53a}$$
$$\text{s.t. } (49\text{b}), (49\text{c}), (49\text{d}). \tag{53b}$$

In order for (49d) to be meaningful, we need the condition

$$\left(\omega_k - \theta_k\breve{\omega}_k\right) > 0 \Leftrightarrow \theta_k < \omega_k/\breve{\omega}_k \tag{54}$$

with $k \in \mathcal{K}\backslash\{1\}$. If θ_k satisfies the above condition, we can infer from both (49b) and (49d) the following:

$$\underbrace{\max_{k\in\mathcal{K}\backslash\{1\}}\left\{\frac{\theta_k}{\omega_k - \theta_k\breve{\omega}_k}\right\}}_{\geq 0} \leq \eta \leq \underbrace{\min_{m\in\mathcal{M}} \ \left\{\frac{\rho_{max}/\rho_s}{\sum_{k=1}^{K}\gamma_{mk}}\right\}}_{>0}.$$

This also implies another necessary condition as follows:

$$\theta_k < \frac{\omega_k \min_{m\in\mathcal{M}} \ \left\{\frac{\rho_{max}/\rho_s}{\sum_{k=1}^{K}\gamma_{mk}}\right\}}{1 + \breve{\omega}_k \min_{m\in\mathcal{M}} \ \left\{\frac{\rho_{max}/\rho_s}{\sum_{k=1}^{K}\gamma_{mk}}\right\}} \tag{55}$$

for each $k \in \mathcal{K}\backslash\{1\}$. The two conditions (54) and (55) are now rewritten in the following form:

$$\theta_k < \min \ \left\{\frac{\omega_k}{\breve{\omega}_k}, \frac{\omega_k \min_{m\in\mathcal{M}} \ \left\{\frac{\rho_{max}/\rho_s}{\sum_{k=1}^{K}\gamma_{mk}}\right\}}{1 + \breve{\omega}_k \min_{m\in\mathcal{M}} \ \left\{\frac{\rho_{max}/\rho_s}{\sum_{k=1}^{K}\gamma_{mk}}\right\}}\right\} \tag{56}$$

with $k \in \mathcal{K}\backslash\{1\}$. Once (56) has been satisfied, the solution to (P1) can be given by

- either

$$\eta^\star_{(\underline{\text{P1}})} = \min_{m\in\mathcal{M}} \ \left\{\frac{\rho_{max}/\rho_s}{\sum_{k=1}^{K}\gamma_{mk}}\right\} \tag{57}$$

for

$$\theta_\text{E} \geq \varpi/\breve{\varpi} \tag{58}$$

- or

$$\eta^{\star}_{(\underline{\text{P1}})} = \min_{m\in\mathcal{M}} \left\{ \frac{\rho_{max}/\rho_s}{\sum_{k=1}^{K}\gamma_{mk}}, \frac{\theta_{\text{E}}}{(\varpi - \theta_{\text{E}}\breve{\varpi})} \right\} \tag{59}$$

for

$$\frac{\varpi \max_{k\in\mathcal{K}\setminus\{1\}} \left\{ \frac{\theta_k}{\omega_k - \theta_k\breve{\omega}_k} \right\}}{1 + \breve{\varpi}\max_{k\in\mathcal{K}\setminus\{1\}} \left\{ \frac{\theta_k}{\omega_k - \theta_k\breve{\omega}_k} \right\}} \leq \theta_{\text{E}} < \varpi/\breve{\varpi}. \tag{60}$$

B. Closed-Form Solution to (Q1)

As presented in the previous subsection, (56) is necessary in order that (Q1) can be solved. Then we can rewrite (Q1) as

$$(\underline{\text{Q1}}) \quad \max_{\chi} \; l(\chi) \tag{61a}$$

$$\text{s.t. } 0 \leq \chi \leq \overline{\alpha} \tag{61b}$$

where

$$\chi \triangleq \eta - \underline{\alpha},$$
$$\overline{\alpha} \triangleq \min_{m\in\mathcal{M}} \left\{ \frac{\rho_{max}/\rho_s}{\sum_{k=1}^{K}\gamma_{mk}} \right\} - \underline{\alpha},$$
$$\underline{\alpha} \triangleq \max_{k\in\mathcal{K}\setminus\{1\}} \left\{ \frac{\theta_k}{\omega_k - \theta_k\breve{\omega}_k} \right\}$$

and

$$l(\chi) = \frac{\chi(\omega_1 + \breve{\omega}_1) + \underline{\alpha}(\omega_1 + \breve{\omega}_1) + 1}{\chi\breve{\omega}_1 + \underline{\alpha}\breve{\omega}_1 + 1} \times \frac{\chi\breve{\varpi} + \underline{\alpha}\breve{\varpi} + 1}{\chi(\varpi + \breve{\varpi}) + \underline{\alpha}(\varpi + \breve{\varpi}) + 1}.$$

Introducing a new variable $\tau \geq 0$ and defining a Lagrangian function $\mathcal{L}(\chi,\tau) \triangleq l(\chi) - \tau(\chi - \overline{\alpha})$, we first consider two sub-cases:

- For $\tau = 0$, we solve $\frac{\partial l(\chi)}{\partial \chi} = 0$ to obtain two *positive-real* critical points $\chi = \chi_1$ and $\chi = \chi_2$ (if possible).
- For $\tau > 0$, we solve the system of two equations

$$\begin{cases} \dfrac{\partial \mathcal{L}(\chi,\tau)}{\partial \tau} = 0 \\ \dfrac{\partial \mathcal{L}(\chi,\tau)}{\partial \chi} = 0 \end{cases} \Leftrightarrow \begin{cases} \chi = \overline{\alpha} \\ \tau = \left.\dfrac{\partial l(\chi)}{\partial \chi}\right|_{\chi=\overline{\alpha}} \end{cases}$$

to obtain another critical point $\chi = \overline{\alpha} \triangleq \chi_3$.

Then the optimal solution to $\left(\underline{\text{Q1}}\right)$ can be given by

$$\eta^{\star}_{(\underline{\text{Q1}})} = \underline{\alpha} + \max_{\chi\in\{\chi_1,\chi_2,\chi_3\}} \; l(\chi). \tag{62}$$

C. Closed-Form Solution to (R1)

Similar to (P1), we first need the condition (56) with $k \in \{1,\ldots,K\}$ in order that (R1) can be solved. Then we can attain the solution to (R1), i.e.

$$\eta^{\star}_{(\underline{\text{R1}})} = \max_{k\in\mathcal{K}} \left\{ \frac{\theta_k}{\omega_k - \theta_k\breve{\omega}_k} \right\}, \tag{63}$$

in the case that either (58) or (60) is satisfied.

D. Closed-Form Solutions to (S1)

For (S1), the condition (56) (with $k \in \{2,\ldots,K\}$) is also required. The third constraint (52c) is rewritten in the form $\breve{a}\eta^2 + \breve{b}\eta + \breve{c} \geq 0$ with $\breve{a} = \breve{\varpi}(\omega_1 + \breve{\omega}_1) - \phi\breve{\omega}_1(\breve{\varpi} + \varpi)$, $\breve{b} = \omega_1 + \breve{\omega}_1 + \breve{\varpi} - \phi(\breve{\omega}_1 + \breve{\varpi} + \varpi)$ and $\breve{c} = 1 - \phi$. As such, there are two possibilities as follows:

- If $\breve{a} > 0$, then (52c) always holds for $\breve{b}^2 - 4\breve{a}\breve{c} \leq 0$. In this case, the solution to (S1) is given by

$$\eta^{\star}_{(\underline{\text{S1}})} = \max_{k\in\mathcal{K}\setminus\{1\}} \left\{ \frac{\theta_k}{\omega_k - \theta_k\breve{\omega}_k} \right\}. \tag{64}$$

- If $\breve{a} < 0$, then (52c) holds for $\breve{b}^2 - 4\breve{a}\breve{c} > 0$ and $\eta_1 \leq \eta \leq \eta_2$ given that η_1 and η_2 are the solutions to the quadratic equation $\breve{a}\eta^2 + \breve{b}\eta + \breve{c} = 0$. In this case, (S1) is infeasible if $\eta_2 < 0$; otherwise, the solution to (S1) is given by

$$\eta^{\star}_{(\underline{\text{S1}})} = \max_{k\in\mathcal{K}\setminus\{1\}} \left\{ \frac{\theta_k}{\omega_k - \theta_k\breve{\omega}_k}, \eta_1 \right\}. \tag{65}$$

VI. Numerical Results

In this section, we evaluate the secure performance and make comparisons for different scenarios. More specifically, we measure the secure performance by calculating R_{sec} (in nats/s/Hz) at

- $\mathbf{\Psi} = \mathbf{\Psi}^{\star}_{(\mathbf{P1})}$ (the solution to (**P1**));
- $\mathbf{\Psi} = \mathbf{\Psi}^{\star}_{(\mathbf{Q1})}$ (the solution to (**Q1**));
- $\mathbf{\Psi} = \mathbf{\Psi}^{\star}_{(\mathbf{R1})}$ (the solution to (**R1**));
- $\mathbf{\Psi} = \mathbf{\Psi}^{\star}_{(\mathbf{S1})}$ (the solution to (**S1**));
- $\eta^{\star}_{(\underline{\text{P1}})}$ (the solution to (P1));
- $\eta^{\star}_{(\underline{\text{Q1}})}$ (the solution to $\left(\underline{\text{Q1}}\right)$);
- $\eta^{\star}_{(\underline{\text{R1}})}$ (the solution to (R1));
- $\eta^{\star}_{(\underline{\text{S1}})}$ (the solution to (S1)).

For each case, the obtained value of R_{sec} will be denoted by $R_{sec}(\mathbf{P1})$, $R_{sec}(\mathbf{Q1})$, $R_{sec}(\mathbf{R1})$, $R_{sec}(\mathbf{S1})$, $R_{sec}(\underline{\text{P1}})$, $R_{sec}\left(\underline{\text{Q1}}\right)$, $R_{sec}(\underline{\text{R1}})$ and $R_{sec}(\underline{\text{S1}})$, respectively. Likewise, the notation $P_{tot}(\mathbf{R1})$, $P_{tot}(\mathbf{S1})$, $P_{tot}(\underline{\text{R1}})$, and $P_{tot}(\underline{\text{S1}})$ will stand for *" the total average transmit power of all APs at $\mathbf{\Psi} = \mathbf{\Psi}^{\star}_{(\mathbf{R1})}$, $\mathbf{\Psi} = \mathbf{\Psi}^{\star}_{(\mathbf{S1})}$, $\eta = \eta^{\star}_{(\underline{\text{R1}})}$, and $\eta = \eta^{\star}_{(\underline{\text{S1}})}$, respectively."*

As for simulation parameters, we use the Hata-COST231 model (see [2], [19] and [20]) to imitate the large scale fading coefficients, i.e.

$$\beta_{mk} = 10^{(\mathcal{S} + PL(d_{mk}))/10}, \tag{66}$$

$$\beta_{m\text{E}} = 10^{(\mathcal{S} + PL(d_{m\text{E}}))/10} \tag{67}$$

where $\mathcal{S} \sim \mathscr{CN}\left(0, \sigma^2_{\mathcal{S}}\right)$ presents the shadowing fading effect with the standard deviation $\sigma_{\mathcal{S}} = 8$ dB and

$$PL(d) = \begin{cases} -139.4 - 35\log_{10}(d) & \text{if } d > 0.05 \\ -119.9 - 20\log_{10}(d) & \text{if } d \in (0.01, 0.05] \\ -79.9 & \text{if } d \leq 0.01 \end{cases} \tag{68}$$

represents the path loss in dB with $d \equiv d_{mk}$ (or $d \equiv d_{m\text{E}}$) being the distance in km between the mth AP and user k

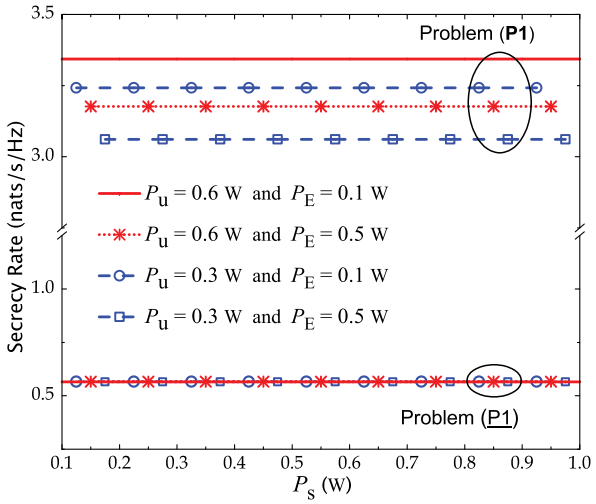


Fig. 2. Secrecy rate versus P_s (the average transmit power for a signal s_k). Other parameters: the average transmit power of each user is $P_u = \{0.3, 0.6\}$ W, the average transmit power of Eve is $P_E = \{0.1, 0.5\}$ W, $M = 50$, $K = 8$, $T = 12$, $\theta_E = 10^{-4}$, and $\theta_k = 2 \times 10^{-4}$ for $k = \{2, \ldots, K\}$.

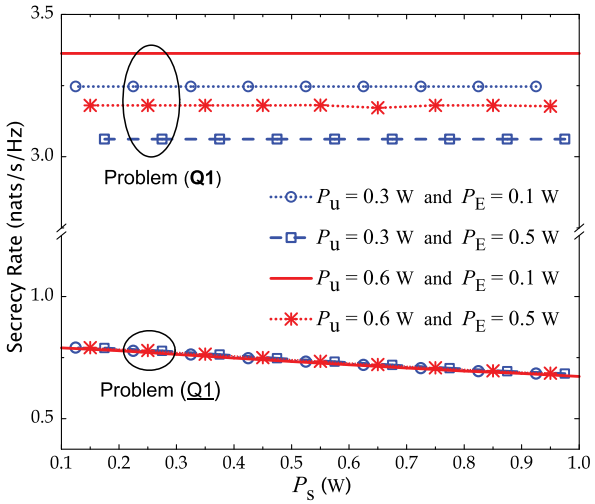


Fig. 3. Secrecy rate versus P_s (the average transmit power for a signal s_k). Other parameters: the average transmit power of each user is $P_u = \{0.3, 0.6\}$ W, the average transmit power of Eve is $P_E = \{0.1, 0.5\}$ W, $M = 50$, $K = 8$, $T = 12$ and $\theta_k = 2 \times 10^{-4}$ for $k = \{2, \ldots, K\}$.

(or Eve).[4] In addition, the maximum transmit power of each AP is $P_{max} = 1$ W. Meanwhile, the average noise power (in W) is given by

$$N_0 = \text{bandwidth} \times k_B \times T_0 \times \text{noise figure} \tag{69}$$

where $k_B = 1.38 \times 10^{-23}$ (Joule/Kelvin) is the Boltzmann constant, and $T_0 = 290$ (Kelvin) is the noise temperature. In all simulation results, we suppose that the bandwidth is 20 MHz and the noise figure is 9 dB. Finally, other parameters will be mentioned whenever they are used.

In Figure 2, we show the achievable secrecy rate (in nats/s/Hz) in 2 different cases: i) $\mathbf{\Psi} = \mathbf{\Psi}^{\star}_{(\mathbf{P1})}$ and ii) $\eta = \eta^{\star}_{(\underline{\text{P1}})}$. For each case, 3 different sub-cases of (P_u, P_E) are considered. It is observed that $R_{sec}\,(\mathbf{P1})$ is significantly higher than $R_{sec}\,(\underline{\text{P1}})$. In fact, the obtained values of $R_{sec}\,(\underline{\text{P1}})$ fall within the interval $(0.55, 0.57)$ nats/s/Hz. In other words, having $\eta_{mk} = \eta^{\star}$ (for all m and k) will lead to very poor performance in terms of security. Furthermore, the secure performance increases with P_u and reduces with P_E (the average transmit power of Eve).

Figure 3 shows the achievable secrecy rate versus P_s in two cases: i) $\mathbf{\Psi} = \mathbf{\Psi}^{\star}_{(\mathbf{Q1})}$ and ii) $\eta = \eta^{\star}_{(\underline{\text{Q1}})}$. The secure performance in the first case is significantly higher than the second case. Moreover, the changes in the value of $R_{sec}\,(\underline{\text{Q1}})$ are minor, i.e. $R_{sec}\,(\underline{\text{Q1}})$ falls within (0.67, 0.79) nats/s/Hz. We also observe that $R_{sec}\,(\mathbf{Q1})$ is improved with increasing P_u and is impaired with P_E. Meanwhile, $R_{sec}\,(\underline{\text{Q1}})$ slightly decreases with P_u.

In Figures 4 and 5, the achievable secrecy rates $R_{sec}\,(\mathbf{P1})$ and $R_{sec}\,(\mathbf{Q1})$ are depicted as functions of M. We can see

[4]Other presentations for $PL(d)$ are also available in literature. Herein, (68) is suggested for a practical scenario in which the carrier frequency is 1900 MHz, the heigh of each AP antenna is 20 m, the heigh of each user antenna (as well as that of Eve antenna) is 1.5 m and all nodes (APs, users and Eve) are randomly dispersed over a square of size 1×1 km^2 [2, eqs. (52) and (53)].

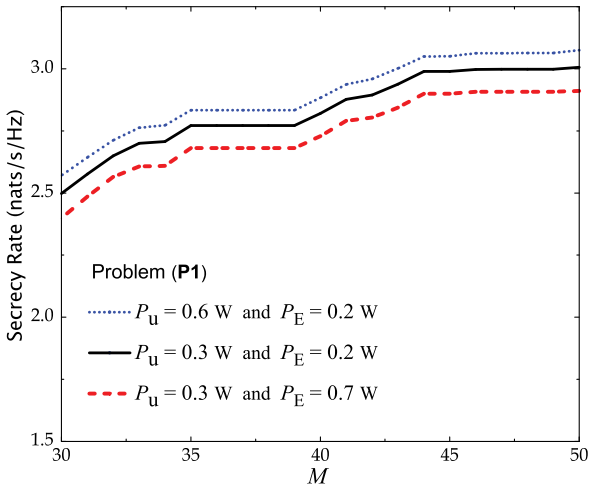


Fig. 4. Secrecy rate versus M. Other parameters: the average transmit power for a signal s_k is $P_s = 0.8$ W, the average transmit power of each user is $P_u = \{0.3, 0.6\}$ W, the average transmit power of Eve is $P_E = \{0.2, 0.7\}$ W, $K = 8$, $T = 12$, $\theta_k = 2 \times 10^{-4}$ for $k = \{2, \ldots, K\}$ and $\theta_E = \theta_k/50$.

that both of them increase with M. It implies that the more service APs we have, the higher secure performance we gain. Finally, $R_{sec}\,(\mathbf{P1})$ as well as $R_{sec}\,(\mathbf{Q1})$ increases with P_u and decreases with P_E. With the chosen parameters, $(\mathbf{Q1})$ appears better than $(\mathbf{P1})$ in terms of secrecy rate. Overall, P_E represents the strength of an actively eavesdropping attack; thus, we can observe that the secure performance is degraded when P_E grows as shown in Figures 2–5.

Figure 6 shows that $P_{tot}\,(\underline{\text{R1}})$ is much higher than $P_{tot}\,(\mathbf{R1})$ which is around 0.003 mW with every P_s. It means that the solution $\mathbf{\Psi}^{\star}_{(\mathbf{R1})}$ is much better than the solution $\eta^{\star}_{(\underline{\text{P1}})}$ in terms of energy, because the APs do not have to consume too much energy to meet security requirements. Besides, the figure also shows that $P_{tot}\,(\underline{\text{R1}})$ inversely decreases with P_s and is lowest at $P_s = P_{max}$. Finally, we observe that

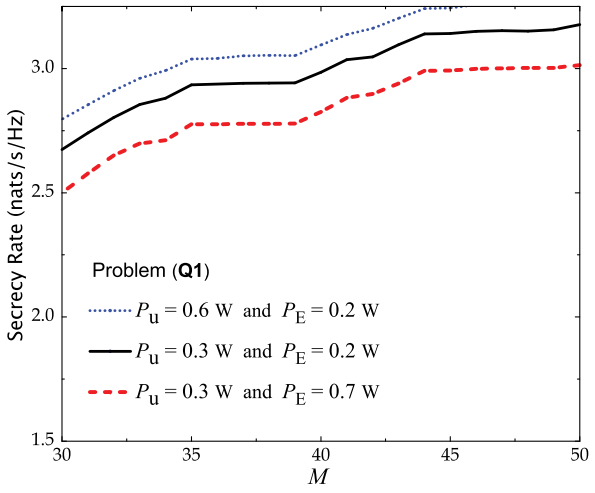


Fig. 5. Secrecy rate versus M. Other parameters: the average transmit power for a signal s_k is $P_s = 0.8$ W, the average transmit power of each user is $P_u = \{0.3, 0.6\}$ W, the average transmit power of Eve is $P_E = \{0.2, 0.7\}$ W, $K = 8$, $T = 12$ and $\theta_k = 2 \times 10^{-4}$ for $k = \{2, \ldots, K\}$.

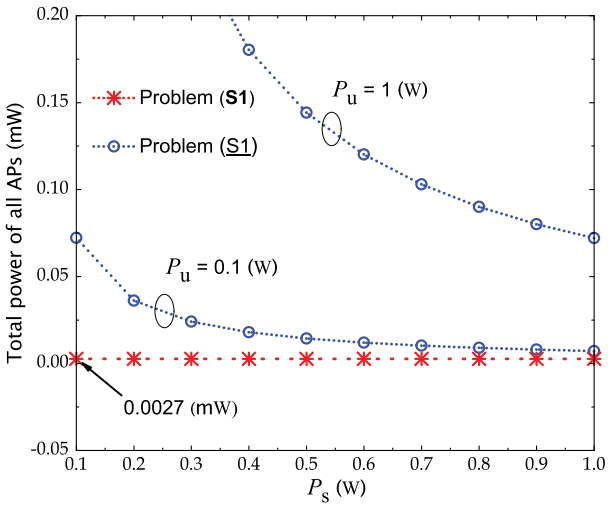


Fig. 7. Total power of all APs (in mW) versus P_s (the average transmit power for a signal s_k). Other parameters: the average transmit power of each user is $P_u = \{0.1, 1\}$ W, the average transmit power of Eve is $P_E = 0.5$ W, $M = 50$, $K = 8$, $T = 12$, $\theta_k = 0.02$ for $k = \{2, \ldots, K\}$ and $\phi = 1$.

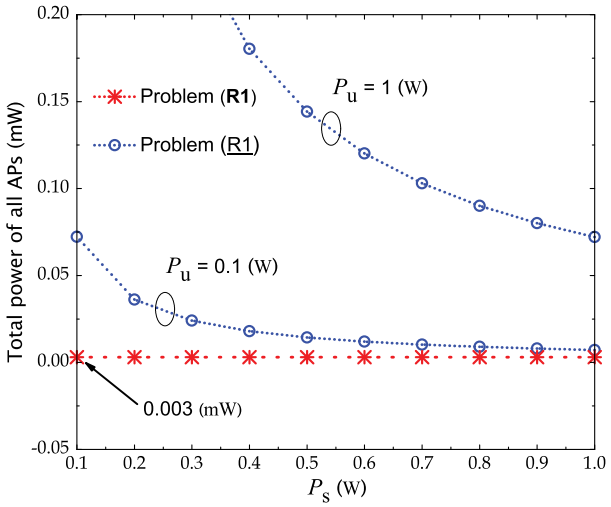


Fig. 6. Total power of all APs (in mW) versus P_s (the average transmit power for a signal s_k). Other parameters: the average transmit power of each user is $P_u = \{0.1, 1\}$ W, the average transmit power of Eve is $P_E = 0.5$ W, $M = 50$, $K = 8$, $T = 12$, $\theta_1 = 0.1$, $\theta_k = 0.02$ for $k = \{2, \ldots, K\}$ and $\theta_E = \theta_1/50$.

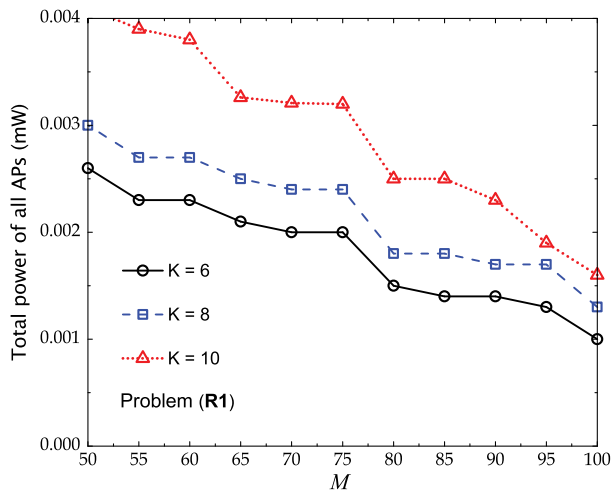


Fig. 8. Total power of all APs (in mW) versus M. Other parameters: the average transmit power for a signal s_k is $P_s = 0.7$ W, the average transmit power of each user is $P_u = 0.4$ W, the average transmit power of Eve is $P_E = 0.5$ W, $K = \{6, 8, 10\}$, $T = 12$, $\theta_1 = 0.1$, $\theta_k = 0.02$ for $k = \{2, \ldots, K\}$ and $\theta_E = \theta_1/50$.

when P_s changes, R_{sec} (**R1**) $\approx$ 0.0953 nats/s/Hz remains almost constant; meanwhile, R_{sec} (R1) $\approx$ 0.5386 nats/s/Hz with $P_u = 0.1$ W and 0.5091 nats/s/Hz with $P_u = 1$ W.

Figure 7 shows that P_{tot} (S1) is much higher than P_{tot} (**S1**) which is around 0.0027 mW at each considered value of P_s. This result also reveals that (**R1**) is the better program in terms of energy, because there is really less energy required for security. Besides, the figure also shows that P_{tot} (S1) inversely decreases with P_s and is lowest at $P_s = P_{max}$. Finally, we record that R_{sec} (**S1**) $\approx 0^+$ nats/s/Hz when P_s changes. In contrast, R_{sec} (S1) $\approx$ 0.4619 nats/s/Hz with $P_u = 0.1$ W and 0.4521 nats/s/Hz with $P_u = 1$W.

Figure 8 depicts P_{tot} (**R1**) as a function of M. With 3 different values of K, we observe that the total power consumption reduces with M but increases with K. We can see that (**R1**) can be solved with many different values of (M, K). Among them, the best choice is to choose M as large as possible while K should be as small as possible. For example, the system with $(M, K) = (70, 6)$ will require less power consumption (at APs) than the system with $(M, K) = (50, 10)$, while the security constraints remain guaranteed.

Figure 9 depicts P_{tot} (**S1**) as a function of M. Our observation of this figure is similar to Figure 8. We should choose M as large as possible and K as small as possible in order to attain the best performance (as long as the security constraints are satisfied). When M is large enough, the total power consumption is nearly zero and yet, the secrecy rate is also around zero (with the chosen parameters).

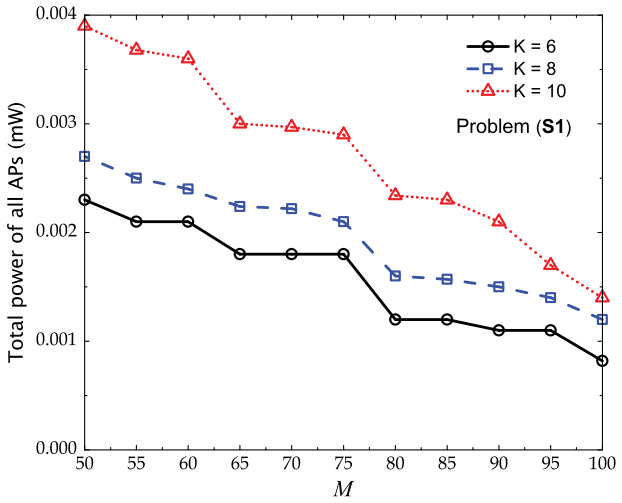


Fig. 9. Total power of all APs (in mW) versus M. Other parameters: the average transmit power for a signal s_k is $P_s = 0.7$ W, the average transmit power of each user is $P_u = 0.4$ W, the average transmit power of Eve is $P_{\rm E} = 0.5$ W, $K = \{6, 8, 10\}$, $T = 12$, $\theta_k = 0.02$ for $k = \{2, \ldots, K\}$ and $\phi = 1$.

In comparison between Figure 8 and Figure 9, one can find the two differences: i) the presence of $\theta_{\rm E}$ and the absence of ϕ in Figure 8; and ii) the absence of $\theta_{\rm E}$ and the absence of ϕ in Figure 9. It is because of the fact that (**R1**) and (**S1**) have different security constraints. With the setup parameters, (**S1**) offers better performance than (**R1**) because the required power consumption is lower (i.e., the curves in Figure 9 is slightly lower than those in Figure 8).

VII. Conclusions

In this paper, we have considered a cell-free MIMO network in the presence of an active eavesdropper. We have suggested maximization problems to maximize the achievable secrecy rate subject to quality-of-service constraints. Also, minimization problems have been provided to minimize power consumption as long as security requirements are still guaranteed. In finding the optimal values of the power control coefficients $\{\eta_{mk}\}_{m,k}$, we have considered two different cases: i) η_{mk} changes with m and k; and ii) $\eta_{mk} = \eta$ for all m and k. Through numerical results, we have found that the case of $\eta_{mk} = \eta$ will lead to far worse performance than the other case. Based on numerical results and intuitive observations, a trade-off problem between secrecy rate and energy consumption may be considered for cell-free networks in the future. Besides, preventing Eve's intrusion into the pilot training will be also worth considering.

Appendix

A. A Simple Method to Identify Abnormality in Pilot Training

As presented in Subsection II.A, the mth AP receives the array of signals $\{y_{km}\}_{k=1}^{K}$ after calculating the Hermitian inner product between $\mathbf{y}_{p,m}$ and $\mathbf{p}_k$. Then all APs (through the CPU) exchange information and make a calculation of

$$\mathcal{Y} \triangleq \sum_{m=1}^{M} \mathbb{E}\left\{|y_{1m}|^2\right\}$$

to check if Eve tries to overhear the signal transmitted from APs to user 1. If $\mathcal{H}_0$ denotes the hypothesis that there is no active eavesdropping and $\mathcal{H}_1$ denotes the opposite, then two possibly obtained values of $\mathcal{Y}$ are

$$\mathcal{Y}|_{\mathcal{H}_0} = T\rho_u \sum_{m=1}^{M} \beta_{m1} + M,$$
$$\mathcal{Y}|_{\mathcal{H}_1} = T\rho_u \sum_{m=1}^{M} \beta_{m1} + T\rho_{\rm E} \sum_{m=1}^{M} \beta_{m{\rm E}} + M.$$

It is clear that $\mathcal{Y}|_{\mathcal{H}_1} > \mathcal{Y}|_{\mathcal{H}_0}$ always holds for $\rho_{\rm E} > 0$. Therefore, APs simply compare $\mathcal{Y}$ with $\mathcal{Y}|_{\mathcal{H}_0}$ to make the decision, i.e.

- $\mathcal{Y} = \mathcal{Y}|_{\mathcal{H}_0} \Leftrightarrow$ No active eavesdropping.
- $\mathcal{Y} > \mathcal{Y}|_{\mathcal{H}_0} \Leftrightarrow$ Eve is seeking to attack the system.

Note that $\mathcal{Y}|_{\mathcal{H}_0}$ is a *known* value and is referred to as the only threshold (which APs need) to check any abnormality in pilot training related to the pilot $\mathbf{p}_1$.

In fact, the above-mentioned detection method can be performed without knowing the value of $\rho_{\rm E}$. However, $\rho_{\rm E}$ can also be predicted by

$$\rho_{\rm E} = \frac{\mathcal{Y} - \mathcal{Y}|_{\mathcal{H}_0}}{T\sum_{m=1}^{M} \beta_{m{\rm E}}}$$

in the case that active eavesdropping occurs.

B. Explicit Expression for snr_E

We first calculate

$$\begin{aligned}
&\mathbb{E}\left\{|{\rm BU}_{{\rm E},1}|^2\right\} \\
&= \rho_s \sum_{m=1}^{M} \eta_{m1}\, \mathbb{E}\left\{\left|g_{m{\rm E}}\hat{g}_{m1}^*\right|^2\right\} \\
&\overset{(a)}{=} \rho_s \sum_{m=1}^{M} \eta_{m1}\, \mathbb{E}\left\{\left|\left(e_{m{\rm E}} + \hat{g}_{m{\rm E}}\right)\hat{g}_{m1}^*\right|^2\right\} \\
&= \rho_s \sum_{m=1}^{M} \eta_{m1} \left(\mathbb{E}\left\{\left|\hat{g}_{m{\rm E}}\hat{g}_{m1}^*\right|^2\right\} + \mathbb{E}\left\{\left|e_{m{\rm E}}\right|^2 \left|\hat{g}_{m1}^*\right|^2\right\}\right) \\
&\overset{(b)}{=} \rho_s \sum_{m=1}^{M} \eta_{m1} \left[2\alpha_m\gamma_{m1}^2 + \left(\beta_{m{\rm E}} - \gamma_{m{\rm E}}\right)\gamma_{m1}\right] \\
&\overset{(c)}{=} \rho_s \sum_{m=1}^{M} \eta_{m1} \left(\alpha_m\gamma_{m1}^2 + \beta_{m{\rm E}}\gamma_{m1}\right) \\
&= \rho_s \sum_{m=1}^{M} \eta_{m1} \left[\left(\frac{\rho_{\rm E}\beta_{m{\rm E}}^2}{\rho_u\beta_{m1}^2}\right)\gamma_{m1}^2 + \beta_{m{\rm E}}\gamma_{m1}\right]
\end{aligned} \tag{70}$$

where (a) is obtained by substituting $g_{m{\rm E}} = e_{m{\rm E}} + \hat{g}_{m{\rm E}}$ with $e_{m{\rm E}} \triangleq g_{m{\rm E}} - \hat{g}_{m{\rm E}}$ being the channel estimation error for the link between the mth AP and Eve. In deriving (a), we also use the fact that $e_{m{\rm E}} \sim \mathcal{CN}\left(0, \beta_{m{\rm E}} - \gamma_{m{\rm E}}\right)$ is independent of $\hat{g}_{m{\rm E}}$. The equality (b) is obtained by using (6). Meanwhile, (c) results from the substitution of $\gamma_{m{\rm E}} = \alpha_m\gamma_{m1}$.

Similarly, for $k' \neq 1$, we calculate

$$\begin{aligned}
&\mathbb{E}\left\{|\mathrm{UI}_{\mathrm{E},k'}|^2\right\} \\
&= \rho_s \,\mathbb{E}\left\{\left|\sum_{m=1}^{M} \sqrt{\eta_{mk'}}\, g_{m\mathrm{E}} \hat{g}_{mk'}^*\right|^2\right\} \\
&= \rho_s \sum_{m=1}^{M} \eta_{mk'} \left(\mathbb{E}\left\{|\hat{g}_{m\mathrm{E}} \hat{g}_{mk'}^*|^2\right\} + \mathbb{E}\left\{|e_{m\mathrm{E}} \hat{g}_{mk'}^*|^2\right\}\right) \\
&\overset{(a)}{=} \rho_s \sum_{m=1}^{M} \eta_{mk'} \left(\alpha_m \,\mathbb{E}\left\{|\hat{g}_{m1} \hat{g}_{mk'}^*|^2\right\} + \mathbb{E}\left\{|e_{m\mathrm{E}}|^2 \,|\hat{g}_{mk'}^*|^2\right\}\right) \\
&\overset{(b)}{=} \rho_s \sum_{m=1}^{M} \eta_{mk'} \left[\alpha_m \gamma_{m1} \gamma_{mk'} + \left(\beta_{m\mathrm{E}} - \alpha_m \gamma_{m1}\right) \gamma_{mk'}\right] \\
&= \rho_s \sum_{m=1}^{M} \eta_{mk'} \beta_{m\mathrm{E}} \gamma_{mk'} \qquad (71)
\end{aligned}$$

where (a) is obtained by using (4) and (b) results from the substitution of (5).

Finally, substituting (70) and (71) into (15) yields (16).

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 16th Int. Workshop Signal Process. Adv. Wireless Commun. (SPAWC)*, Stockholm, Sweden, Jul. 2015, pp. 201–205.

[2] 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.

[3] H. Q. Ngo, L.-N. Tran, T. Q. Duong, M. Matthaiou, and E. G. Larsson, "On the total energy efficiency of cell-free massive MIMO," *IEEE Trans. Green Commun. Netw.*, vol. 2, no. 1, pp. 25–39, Mar. 2018.

[4] S. Buzzi and C. D'Andrea, "Cell-free massive MIMO: User-centric approach," *IEEE Wireless Commun. Lett.*, vol. 6, no. 6, pp. 706–709, Dec. 2017.

[5] A. Liu and V. K. N. Lau, "Joint BS-user association, power allocation, and user-side interference cancellation in cell-free heterogeneous networks," *IEEE Trans. Signal Process.*, vol. 65, no. 2, pp. 335–345, Jan. 2017.

[6] L. D. Nguyen, T. Q. Duong, H. Q. Ngo, and K. Tourki, "Energy efficiency in cell-free massive MIMO with zero-forcing precoding design," *IEEE Commun. Lett.*, vol. 21, no. 8, pp. 1871–1874, Aug. 2017.

[7] T. X. Doan, H. Q. Ngo, T. Q. Duong, and K. Tourki, "On the performance of multigroup multicast cell-free massive MIMO," *IEEE Commun. Lett.*, vol. 21, no. 12, pp. 2642–2645, Dec. 2017.

[8] 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.

[9] M. R. Abedi, N. Mokari, H. Saeedi, and H. Yanikomeroglu, "Robust resource allocation to enhance physical layer security in systems with full-duplex receivers: Active adversary," *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 885–899, Feb. 2017.

[10] L. Li, A. P. Petropulu, and Z. Chen, "MIMO secret communications against an active eavesdropper," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 10, pp. 2387–2401, Oct. 2017.

[11] A. Mukherjee and A. L. Swindlehurst, "Jamming games in the MIMO wiretap channel with an active eavesdropper," *IEEE Trans. Signal Process.*, vol. 61, no. 1, pp. 82–91, Jan. 2013.

[12] G. T. Amariucai and S. Wei, "Half-duplex active eavesdropping in fast-fading channels: A block-Markov wyner secrecy encoding scheme," *IEEE Trans. Inf. Theory*, vol. 58, no. 7, pp. 4660–4677, Jul. 2012.

[13] D. Kapetanovic, 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.

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

[15] S. Im, H. Jeon, J. Choi, and J. Ha, "Secret key agreement with large antenna arrays under the pilot contamination attack," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 6579–6594, Dec. 2015.

[16] J. K. Tugnait, "Detection of active eavesdropping attack by spoofing relay in multiple antenna systems," *IEEE Wireless Commun. Lett.*, vol. 5, no. 5, pp. 460–463, Oct. 2016.

[17] Q. Xiong, Y.-C. Liang, K. H. Li, Y. Gong, and S. Han, "Secure transmission against pilot spoofing attack: A two-way training-based scheme," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 5, pp. 1017–1026, May 2016.

[18] Q. Xiong, Y.-C. Liang, K. H. Li, and Y. Gong, "An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 5, pp. 932–940, May 2015.

[19] T. S. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 2002.

[20] Y. H. Chen and K. L. Hsieh, "A dual least-square approach of tuning optimal propagation model for existing 3G radio network," in *Proc. IEEE 63rd Veh. Technol. Conf.*, Melbourne, FL, Australia, May 2006, pp. 2942–2946.

[21] T. L. Marzetta, E. G. Larsson, H. Yang, and H. Q. Ngo, *Fundamentals of Massive MIMO*. Cambridge, U.K.: Cambridge Univ. Press, 2016.

[22] D. Kapetanovic, G. Zheng, K.-K. Wong, and B. Ottersten, "Detection of pilot contamination attack using random training and massive MIMO," in *Proc. IEEE 24th Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, London, U.K., Sep. 2013, pp. 13–18.

[23] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission in the presence of an active eavesdropper," in *Proc. IEEE Int. Conf. Commun. (ICC)*, London, U.K., Jun. 2015, pp. 1434–1440.

[24] A. Lapidoth and S. Shamai (Shitz), "Fading channels: How perfect need 'perfect side information' be?" *IEEE Trans. Inf. Theory*, vol. 48, no. 5, pp. 1118–1134, May 2002.

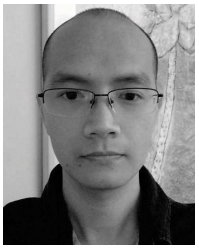
[25] T. Yoo and A. Goldsmith, "Capacity and power allocation for fading MIMO channels with channel estimation error," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2203–2214, May 2006.

[26] 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.

[27] A. A. Nasir, H. D. Tuan, T. Q. Duong, and H. V. Poor, "Secrecy rate beamforming for multicell networks with information and energy harvesting," *IEEE Trans. Signal Process.*, vol. 65, no. 3, pp. 677–689, Feb. 2017.

[28] N. T. Nghia, H. D. Tuan, T. Q. Duong, and H. V. Poor, "MIMO beamforming for secure and energy-efficient wireless communication," *IEEE Signal Process. Lett.*, vol. 24, no. 2, pp. 236–239, Feb. 2107.

[29] H. Tuy, *Convex Analysis and Global Optimization*, 2nd ed. Cham, Switzerland: Springer, 2016.



Tiep M. Hoang received the B.S. degree in electronics and electrical engineering from the Ho Chi Minh City University of Technology, Vietnam, in 2012, and the M.S. degree in electronics and radio engineering from Kyung Hee University, South Korea, in 2014. He is currently pursuing the Ph.D. degree with the School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, U.K. He was a Research Assistant with Duy Tan University, Vietnam, in 2015. His current research interests include wireless security, massive MIMO, stochastic geometry, and convex optimization.

Hien Quoc Ngo received the B.S. degree in electrical engineering from the Ho Chi Minh City University of Technology, Vietnam, in 2007, the M.S. degree in electronics and radio engineering from Kyung Hee University, South Korea, in 2010, and the Ph.D. degree in communication systems from Linköping University (LiU), Sweden, in 2015. In 2014, he visited Nokia Bell Labs, Murray Hill, NJ, USA. From 2016 to 2017, he was a VR Researcher with the Department of Electrical Engineering, LiU. He was also a Visiting Research Fellow with the School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, U.K., funded by the Swedish Research Council.

He is currently a Lecturer with Queen's University Belfast, U.K. He has co-authored many research papers in wireless communications and co-authored the textbook *Fundamentals of Massive MIMO* (Cambridge University Press, 2016). His main research interests include massive (large-scale) MIMO systems, cell-free massive MIMO, physical layer security, and cooperative communications.

Dr. Ngo has been a member of the technical program committees for several IEEE conferences, such as ICC, GLOBECOM, WCNC, VTC, WCSP, ISWCS, ATC, and ComManTel. He received the IEEE ComSoc Stephen O. Rice Prize in Communications Theory in 2015 and the IEEE ComSoc Leonard G. Abraham Prize in 2017. He also received the IEEE Sweden VT-COM-IT Joint Chapter Best Student Journal Paper Award in 2015. He was an Exemplary Reviewer for the IEEE COMMUNICATIONS LETTERS in 2014, the IEEE TRANSACTIONS ON COMMUNICATIONS in 2015, and the IEEE WIRELESS COMMUNICATIONS LETTERS in 2016. He was a Guest Editor of *IET Communications*, special issue on Recent Advances on 5G Communications and a Guest Editor of the IEEE ACCESS, special issue on Modelling, Analysis, and Design of 5G Ultra-Dense Networks, in 2017. He currently serves as an Editor for the IEEE WIRELESS COMMUNICATIONS LETTERS, *Digital Signal Processing*, and the *REV Journal on Electronics and Communications*.

Trung Q. Duong (S'05–M'12–SM'13) received the Ph.D. degree in telecommunications systems from the Blekinge Institute of Technology, Sweden, in 2012. He was a Lecturer (Assistant Professor) with Queen's University Belfast, U.K., from 2013 to 2017, where he has been a Reader (Associate Professor) since 2018. He has authored or co-authored 290 technical papers published in scientific journals (165 articles) and presented at the international conferences (125 papers). His current research interests include the Internet of Things, wireless communications, molecular communications, and signal processing.

Dr. Duong received the Best Paper Award from the IEEE Vehicular Technology Conference (Spring) in 2013, the IEEE International Conference on Communications 2014, the IEEE Global Communications Conference 2016, and the IEEE Digital Signal Processing Conference 2017. He was a recipient of the prestigious Royal Academy of Engineering Research Fellowship from 2016 to 2021 and the prestigious Newton Prize 2017. He currently serves as an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE TRANSACTIONS ON COMMUNICATIONS, and IET COMMUNICATIONS, and a Lead Senior Editor for the IEEE COMMUNICATIONS LETTERS.

Hoang Duong Tuan received the Diploma (Hons.) and Ph.D. degrees in applied mathematics from Odessa State University, Odessa, Ukraine, in 1987 and 1991, respectively. He spent nine academic years as an Assistant Professor with the Department of Electronic-Mechanical Engineering, Nagoya University, Nagoya, Japan, from 1994 to 1999, and then as an Associate Professor with the Department of Electrical and Computer Engineering, Toyota Technological Institute, Nagoya, from 1999 to 2003. He was a Professor with the School of Electrical Engineering and Telecommunications, University of New South Wales, Australia, from 2003 to 2011. He is currently a Professor with the Centre for Health Technologies, University of Technology Sydney, Australia. He has been involved in research in the areas of optimization, control, signal processing, wireless communication, and biomedical engineering for over 20 years.

Alan Marshall (M'88–SM'00) has spent over 24 years involved in the telecommunications and defense industries. He has formed a successful spin-out company Traffic Observation and Management Ltd. He holds the Chair in communications networks with the University of Liverpool, where he is the Director of the Advanced Networks Group and the Head of the Department. He has published over 200 scientific papers and holds a number of joint patents in the areas of communications and network security. His research interests include network architectures and protocols, mobile and wireless networks, network security, high-speed packet switching, QoS/QoE architectures, and multisensory communications, including haptics and olfaction. He is a fellow of the Institution of Engineering and Technology and a Senior Fellow of the Higher Education Academy. He is currently a Section Editor of *The Computer Journal* of the British Computer Society and an Editorial Board Member of the *Journal of Networks*.