Secure Transmission in Massive MIMO System with Specular Component-based Beamforming and Artificial Noise over Ricean Fading Channel

Aiyan Qu, Xianyu Zhang, Kang An, Gan Zheng, *Fellow, IEEE,* and Symeon Chatzinotas, *Senior Member, IEEE*

***Abstract*—This paper investigates the secure transmission in a multi-user massive MIMO system over Ricean fading channel in the presence of a multi-antenna eavesdropper. In order to reduce the system complexity and the channel estimation overhead, a low-complexity beamforming (BF) scheme using only the specular component is presented. Moreover, the generation of artificial noise (AN) is employed at the base station (BS) for additional security enhancement. Specifically, a tractable closed-form lower bound for the achievable ergodic secrecy rate is derived. Furthermore, the optimal power allocation factor is obtained based on the asymptotic analysis to maximize the achievable ergodic secrecy rate. The analytical results reveal that the ergodic secrecy rate improves with the increase of Ricean K-factor and converges to a specific constant when increasing the number of antennas. The performance of the proposed scheme is evaluated through comprehensive simulations.**

***Index Terms*—Physical layer security, massive MIMO, specular component-based beamforming, artificial noise, ergodic secrecy rate.**

I. Introduction

As one of the promising technologies for emerging and future communication networks, massive MIMO makes use of a large number of antenna elements at the base station (BS) to provide increased spectral efficiency and energy efficiencies at low system complexity [1], [2]. However, due to the large antenna array, channel estimation occupies a large portion of a time slot as overhead [3], [4]. Moreover, many existing works show that the imperfect channel estimation and pilot contamination in masssive MIMO systems make the transmitter beamforming deviate from the desired directions, leading to severe system performance degradation [5], [6].

It is noted that security is a critical issue for future wireless systems due to the broadcast nature of the wireless medium [7], [8]. Since the abundance of antennas in massive MIMO systems have potential to boost the secrecy performance, the combination of physical layer security and massive MIMO has received significant attention in recent years [9], [10]. As one of the effective signal processing approaches, artificial noise has also been used in massive MIMO systems for secure transmission [11], [12]. However, most of the existing researches focusing on the physical layer security in massive MIMO are restricted to the Rayleigh fading channels, which falls short of capturing the propagation characteristics of highly directional line-of-sight (LOS) component, such as in mmWave communication, high altitude platform communication and etc [13]. It is noted that Ricean fading channel is the most suitable model for massive MIMO systems when there are specular components in received signals, i.e., indoor channels and mmWave channels [14], [15]. Moreover, secure transmission in multi-pair massive MIMO relaying over Ricean fading channels has been firstly investigated in [16], where beamforming was implemented based on the channel state information (CSI) estimated through uplink training.

Nevertheless, it should be noted that channel estimation will result in heavy overhead and pilot contamination which is a fundamental challenge in multi-user massive MIMO systems [11]. To reduce the overhead of channel estimation, beamformer can be designed only based on the specular component which can be conveniently estimated and achieved in Ricean fading channels [17], [18]. Hence, the channel estimation overhead and pilot contamination can be avoided or alleviated in massive MIMO systems. Motivated by the aforementioned observations, this paper investigates the secure transmission in a multi-user massive MIMO system in Ricean fading channel with specular component-based beamforming and artificial noise. A tight closed-form lower bound on the achievable ergodic secrecy rate is derived to evaluate the system performance. Furthermore, optimal power allocation is presented based on the asymptotic analysis. Numerical results were conducted to validate the analytical results.

Notations: Throughout this paper, the upper case boldface letters and lower case boldface letters denote matrices and vectors, e.g. $\mathbf{g}$, $\mathbf{G}$. $(\cdot)^*$, $(\cdot)^T$ and $(\cdot)^H$ indicate the matrix conjugate, transpose and Hermitian transpose, respectively. $\mathcal{CN}(\mathbf{0}, \mathbf{I})$ represents a circularly symmetric complex Gaussian random vector with mean $\mathbf{0}$ and covariance $\mathbf{I}$. $\mathbb{E}\{\cdot\}$ stands for the statistical expectation. $\mathbb{C}^{M\times N}$ means $M \times N$ dimensional complex space. Besides, i.i.d indicates the ab-

This work is supported by the National Natural Science Foundation of China under Grant U19B214 and 61901502, in part by the Foundation strengthening Plan Area Fund under Grant 2019-JCJQ-JJ-212 and Grant 2019-JCJQ-JJ226, in part by the National Postdoctoral Program for Innovative Talents under Grant BX20200101, and in part by the 18-QNCXJ-029. *(Corresponding author: Xianyu Zhang)*

A. Qu is with the Jinling Institute of Technology, Nanjing 211169, China (Email: quaiyan@jit.edu.cn).

X. Zhang and K. An are with the Sixty-Third Research Institute, National University of Defense Technology, Nanjing 210007, China (Email: zhangxy_sat@126.com; ankang89@nudt.edu.cn).

G. Zheng is with the Wolfson School of Mechanical, Electrical and Manufacturing Engineering, Loughborough University, Loughborough LE11 3TU, U.K. (e-mail: g.zheng@lboro.ac.uk).

S. Chatzinotas is with Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg, Luxembourg, L-1855, Luxembourg (e-mail: symeon.chatzinotas@uni.lu).

breviation of independent and identically distributed. Finally, $[x]^+ = \max\{0, x\}$.

II. System Model

We consider a multi-user massive MIMO system comprising an M-antenna BS and K single-antenna users, as shown in Fig. 1. Besides, there exists an eavesdropper (Eve) equipped with N_e antennas which seeks to intercept the information transmitted to the legitimate users.

For the propagation in Ricean fading environments, the fading channel consists of two parts, namely, a deterministic specular component and a Rayleigh distributed random scattered component. Hence, the channels between the BS and kth user, and between the BS and Eve can be expressed as

$$\begin{cases} \mathbf{g}_k = \sqrt{\beta_i \bar{\kappa}}\bar{\mathbf{h}}_k + \sqrt{\beta_i \tilde{\kappa}}\tilde{\mathbf{h}}_k \\ \mathbf{G}_e = \sqrt{\beta_e \bar{\kappa}}\bar{\mathbf{H}}_e + \sqrt{\beta_e \tilde{\kappa}}\tilde{\mathbf{H}}_e \end{cases}, \tag{1}$$

where $\beta_k\,(\beta_e)$ is large-scale fading coefficient, $\bar{\kappa} = \frac{K_a}{K_a+1}$, $\tilde{\kappa} = \frac{1}{K_a+1}$, and $K_a > 0$ represents the Ricean K-factor. $\tilde{\mathbf{h}}_k \in \mathbb{C}^{1\times M}$ and $\tilde{\mathbf{H}}_e \in \mathbb{C}^{N_e\times M}$ are the random vector and matrix, respectively, whose elements are independent and identically distributed (i.i.d.) Gaussian random variables with zero-mean and unit variance. Similar to [14] and [18], the specular component can be given by

$$\begin{cases} \bar{\mathbf{h}}_k = \mathbf{t}_{\theta_k} \\ \bar{\mathbf{H}}_e = \mathbf{r}_e^T \mathbf{t}_{\theta_e} \end{cases}, \tag{2}$$

where vectors $\mathbf{t}_\theta = \left[1, e^{j2\pi d_t \sin(\theta)}, \cdots, e^{j2\pi(M-1)d_t \sin(\theta)}\right]$ and $\mathbf{r}_e = \left[1, e^{j2\pi d_e \sin(\phi_e)}, \cdots, e^{j2\pi(N_e-1)d_e \sin(\phi_e)}\right]$ represent the specular array responses at the transmitter and receiver, $\theta_k\,(\theta_e)$ denotes the angle-of-departure (AoD) of kth user (Eve), ϕ_e is the angle-of-arrival (AoA) of Eve, d_t and d_e are the normalized antenna spacing in signal wavelength at the BS's transmitting and Eve's receiving antenna arrays.

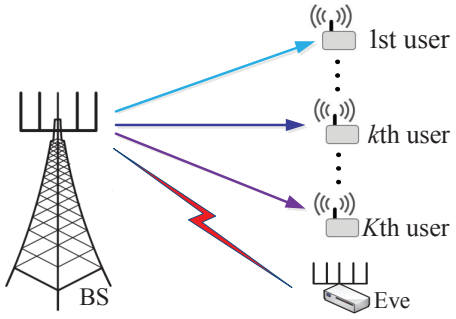

Fig. 1: System model for a multi-user massive MIMO network in the presence of a multi-antenna eavesdropper

To degrade Eve's decoding ability, BS can utilize the remaining $M-K$ degrees of freedom provided by the antennas array for emission of AN. Then, the transmitted signal vector at BS can be written as

$$\mathbf{x} = \sqrt{p}\mathbf{W}\mathbf{s} + \sqrt{q}\mathbf{V}\mathbf{z} = \sum_{i=1}^{K}\sqrt{p}\mathbf{w}_i s_i + \sum_{i=1}^{M-K}\sqrt{q}\mathbf{v}_i z_i, \tag{3}$$

where p and q are the transmit data power and AN signal power. Let P be the total transmit power. Then, p and q can be denoted by $p = \frac{\phi P}{K}$ and $q = \frac{(1-\phi)P}{M-K}$, respectively, and ϕ is the power allocation factor, $\mathbf{W} = [\mathbf{w}_1, \mathbf{w}_2, \cdots, \mathbf{w}_k] \in \mathbb{C}^{M\times K}$ is beamforming matrix with the beamformer vector $\mathbf{w}_i$ designed as $\mathbf{w}_i = \frac{\mathbf{t}_{\theta_i}^*}{\sqrt{M}}$, $\mathbf{V} = [\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_k] \in \mathbb{C}^{M\times(M-K)}$ is AN shaping matrix which lies in the null space of $\mathbf{W}$, i.e., $\mathbf{V}^T\mathbf{W} = \mathbf{0}$. Moreover, s_i and z_i represent the zero-mean normalized symbols, i.e., $\mathbb{E}\{s_i\} = \mathbb{E}\{z_i\} = 0$, $\mathbb{E}\{s_i^H s_i\} = \mathbb{E}\{z_i^H z_i\} = 1$. Accordingly, the received signals at the target user and Eve can be given by

$$\begin{aligned} y_k &= \mathbf{g}_k\mathbf{x}^T + n_k \\ &= \sqrt{p}\sum_{i=1}^{K}\mathbf{g}_k\mathbf{w}_i^T s_i + \sqrt{q}\sum_{i=1}^{M-K}\mathbf{g}_k\mathbf{v}_i^T z_i + n_k \\ &= \sqrt{p\beta_k\bar{\kappa}}\bar{\mathbf{h}}_k\mathbf{w}_k^T s_k + z_k, \end{aligned} \tag{4}$$

$$\begin{aligned} y_e &= \mathbf{r}_e\left(\sqrt{p}\sum_{i=1}^{K}\mathbf{G}_e\mathbf{w}_i^T s_i + \sqrt{q}\sum_{i=1}^{M-K}\mathbf{G}_e\mathbf{v}_i^T z_i + \mathbf{n}_e^T\right) \\ &= \mathbf{v}_e\left(\sqrt{p}\mathbf{G}_e\mathbf{w}_k^T s_k + \mathbf{z}_e\right), \end{aligned} \tag{5}$$

where $n_k \sim \mathcal{CN}\left(0, \delta^2\right)$ and $\mathbf{n}_e \in \mathcal{CN}\left(\mathbf{0}, \delta_e^2\mathbf{I}_{N_e}\right)$ are additive white Gaussian noise, the first terms in (4) and (5) are the desired signals, and the other terms respectively correspond to the effective interference plus noise component which are represented by z_k and $\mathbf{z}_e$, $\mathbf{v}_e \in \mathbb{C}^{1\times N_e}$ denotes the receive filter of Eve. Considering a pessimistic case, Eve is able to acquire knowledge of the effective channel that affects its desired signal [11]. Thus, Eve can design its receive filter by performing maximum-ratio combining, i.e., $\mathbf{v}_e = \frac{\mathbf{w}_k^*\mathbf{G}_e^H}{\left\|\mathbf{w}_k^*\mathbf{G}_e^H\right\|}$.

III. Secrecy performance analysis

For the sake of clarity, the ergodic secrecy rate is used to measure the secrecy performance of considered massive MIMO network, which can be given by

$$R_k^{\text{sec}} = [R_k - R_e]^+, \tag{6}$$

where $[x]^+ = \max\{0, x\}$, $R_k\,(R_e)$ denotes the achievable ergodic rate of kth user (Eve). According to [11] and [18], we can derive the lower bound of R_k as $R_k = \log_2(1+\gamma_k)$, where the signal-to-interference-plus-noise ratio (SINR) γ_k can be given by (7) on the top of the next page.

Next, we analyze the achievable ergodic eavesdropping rate at Eve. With the worst-case assumption that Eve perfectly knows effective channel, we can achieve an upper bound of the eavesdropping rate, i.e. $R_e = \log_2(1+\gamma_e)$, where the SINR at Eve can be represented as (8) at the top of the next page. Combining the above lower bound and upper bound for target user's information rate and Eve's eavesdropping rate, consequently, we obtain a tight and tractable lower bound on the secrecy rate in (6). Furthermore, we can have the following theorem.

Theorem 1: Using specular component-based beamformer at BS and maximum ratio combining at Eve, when M is

$$\gamma_k = \frac{\left|\sqrt{p\beta_k\bar{\kappa}}\bar{\mathbf{h}}_k\mathbf{w}_k^T s_k\right|^2}{\mathbb{E}\left\{\left|\sqrt{p\beta_k\tilde{\kappa}}\tilde{\mathbf{h}}_k\mathbf{w}_k^T s_k\right|^2\right\} + \mathbb{E}\left\{\left|\sqrt{p}\sum_{i\neq k}^{K}\mathbf{g}_k\mathbf{w}_i^T s_i\right|^2\right\} + \mathbb{E}\left\{\left|\sqrt{q}\sum_{i=1}^{M-K}\mathbf{g}_k\mathbf{v}_i z_i\right|^2\right\} + \delta^2}, \tag{7}$$

$$\gamma_e = \frac{\mathbb{E}\left\{\left|\sqrt{p}\mathbf{r}_e\mathbf{G}_e\mathbf{w}_k^T s_k\right|^2\right\}}{\mathbb{E}\left\{\left|\sqrt{p}\sum_{i\neq k}^{K}\mathbf{r}_e\mathbf{G}_e\mathbf{w}_i^T s_i\right|^2\right\} + \mathbb{E}\left\{\left|\sqrt{q}\sum_{i=1}^{M-K}\mathbf{r}_e\mathbf{G}_e\mathbf{v}_i^T z_i\right|^2\right\} + \mathbb{E}\left\{\left|\mathbf{r}_e\mathbf{n}_e^T\right|^2\right\}}, \tag{8}$$

$$\bar{R}_k^{\text{sec}} = \left[\log_2\left(\frac{\left(\phi P\beta_k\bar{\kappa}\frac{1}{\eta} + P\beta_k\tilde{\kappa} + \delta^2\right)\left(-\phi P\beta_e\bar{\kappa} + P\beta_e + \delta_e^2\right)}{\left(P\beta_k\tilde{\kappa} + \delta^2\right)\left(\phi P\beta_e\left(\frac{\tilde{\kappa}\lambda}{\eta} - \bar{\kappa}\right) + P\beta_e + \delta_e^2\right)}\right)\right]^+. \tag{12}$$

large enough, the deterministic equivalents of SINRs can be approximated by

$$\gamma_k = \frac{p\beta_k\bar{\kappa}M}{P\beta_k\tilde{\kappa} + \delta^2}, \tag{9}$$

$$\gamma_e = \frac{p\beta_e\tilde{\kappa}N_e}{(K-1)\,p\beta_e\tilde{\kappa} + (M-K)\,q\beta_e + \delta_e^2}. \tag{10}$$

Proof: See Appendix A.

Note that the SINR of the target user is monotonically increasing while that of Eve monotonically decreasing with K_a. Thus, the ergodic secrecy rate is a strictly increasing function of K_a. Furthermore, the considered secure massive MIMO system can achieve a positive secrecy rate (i.e., $\gamma_k > \gamma_e$) when the number of Eve's antennas is not exceeding the threshold, namely

$$\frac{N_e}{M} < \lambda_0 = \frac{\beta_k\bar{\kappa}\left((K-1)\,p\beta_e\tilde{\kappa} + (1-\phi)\,P\beta_e + \delta_e^2\right)}{\beta_e\tilde{\kappa}\left(P\beta_k\tilde{\kappa} + \delta^2\right)}. \tag{11}$$

Proposition 1: Let P be fixed. As $M \to \infty$, with $\eta = \frac{K}{M}$ and $\lambda = \frac{N_e}{M}$ be finite, a fixed level of security can be guaranteed, which can be rewritten as (12), shown at the top of the next page. Through derivative calculation of (12), the optimal values of ϕ can be obtained as

$$\phi_{opt} = \begin{cases} -c + \sqrt{c^2 + c\,(b-a) - ab}, & \lambda/\eta \geq K_a \\ -c - \sqrt{c^2 + c\,(b-a) - ab}, & \lambda/\eta < K_a \end{cases}. \tag{13}$$

where $a = \frac{\eta\left(P\beta_k\tilde{\kappa}+\delta^2\right)}{P\beta_k\bar{\kappa}}$, $b = \frac{P\beta_e+\delta_e^2}{P\beta_e\bar{\kappa}}$ and $c = \frac{\eta\left(P\beta_e+\delta_e^2\right)}{P\beta_e(\tilde{\kappa}\lambda-\eta\bar{\kappa})}$.

Proof: See Appendix B.

The above proposition gives a closed-form approximation for the secrecy rate when $M \to \infty$. Note that the AN leakage has a great influence on system's secrecy rate, which needs to be jointly considered for secure transmission design.

IV. Numerical Results

Simulations are conducted to evaluate the secrecy performance of the considered system. Without loss of generality, we set that $\beta_k = \beta_E = 1$ and $\delta^2 = \delta_e^2 = 0.1$ throughout the simulations. Fig. 2 shows the achievable ergodic secrecy rates versus M and K_a for different values of K and N_e

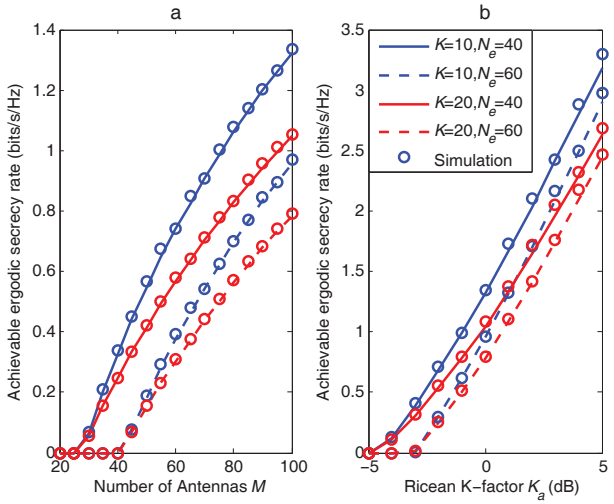

Fig. 2: The achievable ergodic secrecy rate versus M and K_a

with $p = 10$W, which illustrates that the derived analytical values can match the numerical simulations with satisfied accuracy. The ergodic secrecy rates versus M are shown in Fig. 2(a) with $K_a = 1$. As expected, increasing M can improve the achievable ergodic secrecy rate which is consistent with existing works [11], [16]. Also, the achievable secrecy rates decrease with the increase of K or N_e due to the increased inter-user interference or improved Eve's eavesdropping capability. For $K = 10, 20$, the thresholds can be computed as $\lambda_0 = 1.441, 1.466$. Moreover, we note that a non-negative secrecy rate can be achieved only when M exceeds the computed thresholds. Fig. 2(b) illustrates the ergodic secrecy rates with respect to K_a with $M = 100$. It can be seen that the ergodic secrecy rates increase when a larger K_a is employed.

Moreover, we verify the asymptotic properties of the considered secure massive MIMO networks and depict the simulation results in Fig. 3. It is observed that the ergodic secrecy rates improve with the increase of M but gradually converge to deterministic constants, just as predicted in Proposition 1. Moreover, Fig. 3 further proves that the ergodic secrecy rate

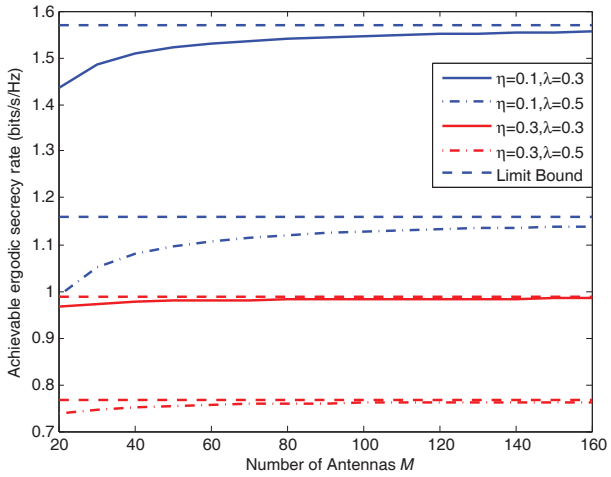

Fig. 3: The ergodic secrecy rate versus M and limits with $P = 10$ and $K_a = 1$

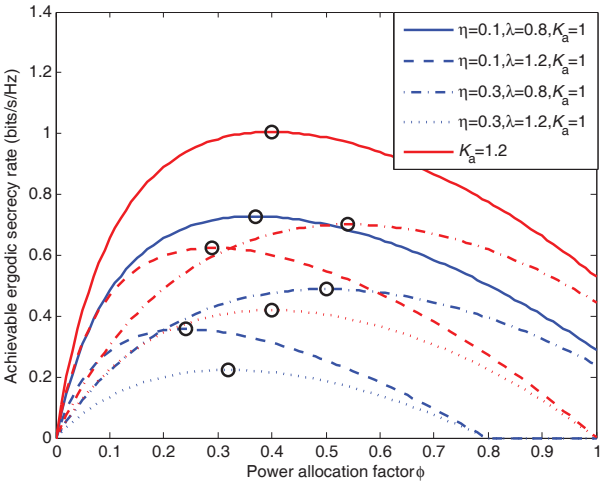

Fig. 4: The ergodic secrecy rate versus ϕ and limits with $P = 10$ and $M = 100$

is reduced if K or N_e increases. In Fig. 4, we demonstrate the ergodic secrecy rate as a function of the power allocation factor ϕ for different values of K_a, η and λ. The black circles in Fig. 4 denote the optimal power allocation factor ϕ_{opt} which is calculated from (13). The analytical optimal values are consistent with the maximum of the simulated curves. Fig. 4 also reveals that the system should allocate more power to AN if the eavesdropper has more antennas, or the ergodic secrecy rates reduce to zero. As demonstrated in Fig. 2, it is observed from Fig. 4 that the ergodic secrecy rate rapidly increases with increasing K_a. This indicates that the specular component-based beamforming scheme is more suitable for Ricean fading propagation channels with strong specular component.

V. Conclusion

In this paper, we investigated the secure transmission in a multi-user massive MIMO systems over Ricean fading channels in the presence of a multi-antenna eavesdropper. To reduce the overhead of channel estimation and provide additional secrecy enhancement, the specular component-based beamforming and AN were employed at the BS. Specifically, a tight closed-form lower bound on the achievable ergodic secrecy rate was derived. Furthermore, optimal power allocation was presented based on the asymptotic analysis. Numerical results were conducted to validate the analytical results.

Appendix

A. Proof of Theorem 1

Firstly, we focus on the term $\sqrt{p\beta_k\bar{\kappa}}\bar{\mathbf{h}}_k\mathbf{w}_k^T$. Since vector $\bar{\mathbf{h}}_k$ and $\mathbf{w}_k$ are both deterministic, we can derive the deterministic equivalent as

$$\left|\sqrt{p\beta_k\bar{\kappa}}\bar{\mathbf{h}}_k\mathbf{w}_k^T\right|^2 = p\beta_k\bar{\kappa}M. \tag{14}$$

Note that $\|\mathbf{w}_k\|^2 = 1$, it is straightforward to derive that $\tilde{\mathbf{h}}_k\mathbf{w}_k^T \sim \mathcal{CN}(0,1)$, which results in

$$\mathbb{E}\left\{\left|\sqrt{p\beta_k\tilde{\kappa}}\tilde{\mathbf{h}}_k\mathbf{w}_k^T\right|^2\right\} = p\beta_k\tilde{\kappa}. \tag{15}$$

Similarly, we have that $\tilde{\mathbf{h}}_k\mathbf{w}_i^T \sim \mathcal{CN}(0,1), i \neq k$. Note that s_i and $s_j\,(j \neq i)$ are zero-mean and pairwisely independent, we can derive that

$$\begin{aligned}
&\mathbb{E}\left\{\left|\sum_{i\neq k}^{K}\mathbf{g}_k\mathbf{w}_i^T s_i\right|^2\right\} \\
&= \beta_k\sum_{i\neq k}^{K}\mathbb{E}\left\{\left|\sqrt{\bar{\kappa}}\bar{\mathbf{h}}_k\mathbf{w}_i^T + \sqrt{\tilde{\kappa}}\tilde{\mathbf{h}}_k\mathbf{w}_i^T\right|^2\right\} \\
&= \beta_k\sum_{i\neq k}^{K}\left(\bar{\kappa}\mathbb{E}\left\{\left|\bar{\mathbf{h}}_k\mathbf{w}_i^T\right|^2\right\} + \tilde{\kappa}\mathbb{E}\left\{\left|\tilde{\mathbf{h}}_k\mathbf{w}_i^T\right|^2\right\}\right).
\end{aligned} \tag{16}$$

Note that the first term of above formula is deterministic [14]. It is not difficult to get that

$$\left|\bar{\mathbf{h}}_k\mathbf{w}_i^T\right|^2 = \frac{\sin^2\left(M\pi d_t\left(\sin\theta_k - \sin\theta_i\right)\right)}{M\sin^2\left(\pi d_t\left(\sin\theta_k - \sin\theta_i\right)\right)}. \tag{17}$$

If $\sin\theta_k \neq \sin\theta_i$ (different users), we can derive that

$$\left|\bar{\mathbf{h}}_k\mathbf{w}_i^T\right|^2 \to 0, \quad as \quad M \to \infty. \tag{18}$$

Hence, we can get that

$$\mathbb{E}\left\{\left|\sqrt{p}\sum_{i\neq k}^{K}\mathbf{g}_k\mathbf{w}_i^T s_i\right|^2\right\} = (K-1)\,p\beta_k\tilde{\kappa}. \tag{19}$$

Similarly, the AN interference is calculated as

$$\mathbb{E}\left\{\left|\sqrt{q}\sum_{i=1}^{M-K}\mathbf{g}_k\mathbf{v}_i^T z_i\right|^2\right\} = (M-K)\,q\beta_k\tilde{\kappa}. \tag{20}$$

Then, we focus on the SINR at Eve γ_e. It is straightforward to derive that

$$\begin{aligned}
\mathbf{G}_e\mathbf{w}_k^T &= \sqrt{\beta_e\bar{\kappa}}\mathbf{r}_e^T\mathbf{t}_{\theta_e}\mathbf{w}_k^T + \sqrt{\beta_e\tilde{\kappa}}\tilde{\mathbf{H}}_e\mathbf{w}_k^T \\
&= \sqrt{\beta_e\tilde{\kappa}}\tilde{\mathbf{H}}_e\mathbf{w}_k^T.
\end{aligned} \tag{21}$$

Moreover, it is noted that $\mathbf{t}_{\theta_e}\mathbf{w}_k^T = 0$ when $M \to \infty$, $\theta_k \neq \theta_e$, the receive filter at Eve can be rewritten as $\mathbf{v}_e = \frac{\mathbf{w}_k^* \tilde{\mathbf{H}}_e^H}{\left\| \mathbf{w}_k^* \tilde{\mathbf{H}}_e^H \right\|}$.

Note that $\|\mathbf{v}_e\|^2 = 1$. Using the mutual independence of transmitting information symbols and similar derivations as shown above, we can derive the following results:

$$\mathbb{E}\left\{ \left| \sqrt{p}\mathbf{r}_e \mathbf{G}_e \mathbf{w}_k^T \right|^2 \right\} = p\beta_e \tilde{\kappa} N_e, \tag{22}$$

$$\mathbb{E}\left\{ \left| \sqrt{p} \sum_{i \neq k}^{K} \mathbf{r}_e \mathbf{G}_e \mathbf{w}_i^T s_i \right|^2 \right\} = (K-1)\, p\beta_e \tilde{\kappa}, \tag{23}$$

$$\mathbb{E}\left\{ \left| \sqrt{q} \sum_{i=1}^{M-K} \mathbf{r}_e \mathbf{G}_e \mathbf{w}_i^T s_i \right|^2 \right\} = (M-K)\, q\beta_e, \tag{24}$$

$$\mathbb{E}\left\{ \left| \mathbf{r}_e \mathbf{n}_e^T \right|^2 \right\} = \delta_e^2. \tag{25}$$

Substituting these expressions into (7) and (8), we can get the final result as (9) and (10). This concludes the proof.

B. Proof of Proposition 1

Based on the derived deterministic equivalents in Theorem 1, we further have the following results when $Mp = E$ and $M \to \infty$ as

$$\bar{\gamma}_k = \lim_{M \to \infty} \gamma_k = \frac{\phi P \beta_k \bar{\kappa}}{\eta \left(P\beta_k \tilde{\kappa} + \delta^2 \right)}, \tag{26}$$

$$\bar{\gamma}_e = \lim_{M \to \infty} \gamma_e = \frac{\phi P \beta_e \tilde{\kappa} \lambda}{\eta \left(P\beta_e - \phi P \beta_e \bar{\kappa} + \delta_e^2 \right)}. \tag{27}$$

Plugging these two limit values into (6), we can derive the result as (12). Furthermore, since R_k^{sec} and $f(\phi) = \frac{1+\lambda_k}{1+\lambda_e}$ have the same monotonicity, the optimal power allocation can be calculated by solving equation $f'(\phi) = 0$, $\phi \in [0, 1]$. Then, it is not difficult to obtain the optimal power allocation factor ϕ_{opt} as (13).This concludes the proof.

REFERENCES

[1] F. Rusek, D. Persson, B. K. Lau, E. G. Larsson, T. L. Marzetta, O. Edfors, and F. Tufvesson, "Scaling Up MIMO: Opportunities and Challenges with Very Large Arrays", *IEEE Signal Processing Magazine*, vol. 30, no. 1, pp. 40-60, Jan. 2013.

[2] H. Q. Ngo, E. G. Larsson, and T. L. Marzetta, "Energy and Spectral Efficiency of Very Large Multiuser MIMO Systems", *IEEE Transactions on Communications*, vol. 61, no. 4, pp. 1436-1449, Apr. 2013.

[3] T. L. Marzetta, "Massive MIMO: An introduction", *Bell Labs Technical Journal*, vol. 20, pp. 11-22, Mar. 2015.

[4] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure Massive MIMO Transmission With an Active Eavesdropper", *IEEE Transactions on Information Theory*, vol. 62, no. 7, pp. 3880-3900, Jul. 2016.

[5] T. E. Bogale and L. B. Le, "Massive MIMO and mmWave for 5G Wireless HetNet: Potential Benefits and Challenges", *IEEE Vehicular Technology Magazine*, vol. 11, no. 1, pp. 64-75, Mar. 2016.

[6] J. Zhu, R. Schober, and V. K. Bhargava, "Secure Transmission in Multicell Massive MIMO Systems", *IEEE Transactions on Wireless Communications*, vol. 13, no. 9, pp. 4766-4781, Sept. 2014.

[7] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G Wireless Communication Networks Using Physical Layer Security", *IEEE Communications Magazine*, vol. 53, no. 4, pp. 20-27, Apr. 2015.

[8] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, "A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead", *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 679-695, Apr. 2018.

[9] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical Layer Security for Massive MIMO: An Overview on Passive Eavesdropping and Active Attacks", *IEEE Communications Magazine*, vol. 53, no. 6, pp. 21-27, Jun. 2015.

[10] 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, May 2019.

[11] J. Zhu, R. Schober, and V. K. Bhargava, "Linear Precoding of Data and Artificial Noise in Secure Massive MIMO Systems", *IEEE Transactions on Wireless Communications*, vol. 15, no. 3, pp. 2245-2261, Mar. 2016.

[12] X. Zhang, D. Guo, K. An and B. Zhang, "Secure Communications Over Cell-Free Massive MIMO Networks With Hardware Impairments," *IEEE Systems Journal*, doi.10.1109/JSYST.2019.2919584, 2019.

[13] X. Sun, K. Xu, and Y. Xu, "Performance analysis of multi-pair two-way amplify-and-forward relaying with imperfect CSI over Ricean fading channels", *IET Communications*, vol. 12, no. 3, pp. 261-270, Mar. 2018.

[14] 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 Journal of Selected Topics in Signal Processing*, vol. 8, no. 5, pp. 966-981, Oct. 2014.

[15] H. Yang and T. L. Marzetta, "Massive MIMO With Max-Min Power Control in Line-of-Sight Propagation Environment", *IEEE Transactions on Communications*, vol. 65, no. 11, pp. 4685-4693, Nov. 2017.

[16] X. Zhang, D. Guo, and K. An, "Secure communication in multigroup multicasting cell-free massive MIMO networks with active spoofing", *Electronics Letters*, vol. 55, no. 2, pp. 96-98, Jan. 2019.

[17] D. Yue, "Specular component-based beamforming for broadband massive MIMO systems with doubly-ended correlation", *Electronics Letters*, vol. 52, no. 12, pp. 1082-1084, Jun. 2016.

[18] D. Yue, Y. Zhang, and Y. Jia, "Beamforming Based on Specular Component for Massive MIMO Systems in Ricean Fading", *IEEE Wireless Communications Letters*, vol. 4, no. 2, pp. 197-200, Apr. 2015.