Energy-Efficient Secure Transmission in Massive MIMO Systems with Pilot Attack

Bin Li, Lei Li, Dongxuan He, Jianqiang Chen, and Weilian Kong
School of Information and Electronics, Beijing Institute of Technology, Beijing 100081, China

***Abstract*—In this paper, we focus on the problem of energy-efficient power allocation for secure transmission in massive multiple-input multiple-output (MIMO) systems, where an active multi-antennas eavesdropper sends pilot signals as that of destination receiver to transmitter simultaneously in the uplink training phase. Our aim is to maximize the energy efficiency (EE) of the system by considering the power allocation strategy, while guaranteeing the secrecy rate and the transmit power constraints. We first analyze the impact of pilot attack on the secrecy rate and then prove that the secrecy EE is a concave function with respect to transmit power. The optimization problem formulated can be efficiently solved by using Lagrange multiplier method. Finally, numerical results are provided to validate the proposed energy-efficient scheme outperforms the fixed transmit power scheme.**

***Index Terms*—Secure communication, massive MIMO, energy-efficiency, pilot attack.**

I. Introduction

Physical layer security enhanced by multi-antenna techniques, such as precoding/beamforming and interference alignment, has gained substantial research attention in recent years [1]-[3], in which the multi-antenna nodes are capable of adjusting the directions of their transmitted signal to improve the security performance. On the other side, massive MIMO as a promising technique has been proposed to improve spectral efficiency by exploiting its large array gain [4], [5]. Therefore, introducing massive MIMO into physical layer security is identified as a powerful technique for significantly improving the secrecy performance of wireless communication systems [6], [7].

Recent efforts [8]-[13] have shown the significance of massive MIMO enabled physical layer security. Specifically, [8] designed the artificial noise (AN)-aided precoding for secure downlink transmission in a massive MIMO-aided multi-cell system with a multi-antenna eavesdropper. The authors of [8] further considered the secure downlink transmission in a massive MIMO-aided multi-cell with imperfect channel state information (CSI) of the eavesdropper in [9]. [10] analyzed the secrecy outage region and derived the secrecy outage probability of the massive MIMO Rician channels. In [11], authors studied the secure transmission in a two-tier heterogeneous networks (HetNets) using massive MIMO, where the locations of all nodes were modeled as independent Poisson point process. In addition, the secrecy problem in distributed massive MIMO systems [12] and in relay-assisted massive MIMO systems was also considered [13], respectively. However, all the aforementioned works assumed that the eavesdropper was passive and it did not attempt to impair the transmission between the transmitter and the destination receiver.

In practical communication systems, to improve eavesdropping performance, the eavesdropper may impersonate a destination receiver and actively transmit deterministic signals (pilot signals) to fool the channel estimation at the transmitter [14]-[16], which seriously interferes with uplink training phases. To be specific, [14] examined the detrimental effects of the pilot attack on the secrecy performance for multiple-input single-output (MISO) and MIMO broadcast channels, where a full-duplex eavesdropper was taken into account. The competitive interaction between the transmitter and the active eavesdropper was formulated as a one-shot zero-sum game in [15], in which the upper bound of the average secrecy rate was evaluated. To elaborate a little further, [16] showed that the effect of the active eavesdropper could be completely eliminated when the transmit correlation matrix of receivers placed at the null space of the active eavesdropper. In addition, there are some recent studies considering the active eavesdropping from a surveillance perspective, e.g., [17]-[19].

On the other hand, with the non-negligible carbon emissions imposed by the excessive power consumption of the information and communication infrastructures, energy efficiency (EE, bit per Joule) becomes a significant performance metric for evaluating 5G wireless networks. As a result, it necessitates to investigate the trade-off of the secrecy performance and the energy consumption in massive MIMO systems. [20] studied an energy-efficient power allocation scheme for secure amplify-and-forward (AF) massive MIMO relaying system in the presence of passive eavesdropper. For the pilot attack of active eavesdropper, the transmit power has a complicate effect on the secrecy performance, especially in massive MIMO systems. Therefore, it is desirable to optimize the transmit power at the transmitter.

Motivated by the aforementioned observation, in this paper, we focus on the problem of energy-efficient power allocation for a secure massive MIMO system, where the multi-antenna eavesdropper transmits pilot signals as that of destination receiver to enhance the eavesdropping performance. Our aim is to maximize the EE of the system by optimizing transmit power under the secrecy rate and the transmit power constraints. The contributions of this paper are two-fold:

1) We first derive the achieved secrecy rate of a massive MIMO system with pilot attack by using antenna selection at eavesdropper, and demonstrate the impact of pilot attack on

978-1-5090-2860-3/16/$31.00 ©2016 IEEE

the secrecy rate.

2) We prove that the secrecy EE is a concave function with respect to transmit power at the transmitter by means of the properties of fractional programming. Then, an optimal power iterative algorithm is proposed for the secrecy EE maximization.

Notations: Boldface lowercase and uppercase letters denote vectors and matrices, respectively. The transpose and conjugate transpose of matrix $\mathbf{A}$ are denoted as $\mathbf{A}^T$ and $\mathbf{A}^H$, respectively. $\mathbf{I}$ denotes an identity matrix. $\|\cdot\|$ denotes the Euclidean norm. $\mathbb{E}[\cdot]$ is the expectation operator.

II. System Model

We consider a typical three-node massive MIMO system as shown in Fig. 1, consisting of one transmitter (Alice) with $M \gg 1$ antennas, one single-antenna destination receiver (Bob) and one eavesdropper (Eve) with $N_e > 1$ antennas. In a TDD system, Bob sends pilot signal to Alice in the uplink training phase that Alice estimates the channel between them. Meanwhile, Eve sends the same pilot signal as Bob to actively attack[1]. Note that the number of transmit antennas at Alice is quite large in such massive MIMO system, i.e. the value of M is on the order of tens or even hundreds. As the system is operated in TDD mode, the channel reciprocity holds true.

Let $\sqrt{\beta_{AB}}\mathbf{h}_{AB} \in \mathbb{C}^{M\times 1}$ represent the channel coefficient from Alice to Bob and $\sqrt{\beta_{AE}}\mathbf{H}_{AE} \in \mathbb{C}^{M\times N_e}$ represent the channel matrix from Alice to Eve. β_{AB} and β_{AE} stand for the large-scale fading including path loss and shadowing, which are assumed to be known at Alice as they are varying slowly and can be estimated reliably. $\mathbf{h}_{AB}$ stand for the small-scale channel fading vector and $\mathbf{H}_{AE}$ is the small-scale channel fading matrix, the elements of $\mathbf{h}_{AB}$ and $\mathbf{h}_{AE_i}$ ($\mathbf{h}_{AE_i}$ is the i-th column of $\mathbf{H}_{AE}$, $i \in \{1, 2, \ldots, N_e\}$) are independent and identically distributed (i.i.d.) circularly symmetric complex Gaussian (CSCG) random variables with zero mean and unit variance, namely we consider Rayleigh fading.

In this paper, antenna selection is performed at Eve for decoding the received signal. When both Bob and Eve transmit the same pilot signal x_p to Alice in the uplink training phase, then the received signal at Alice is written as

$$\mathbf{y}_A = \left(\sqrt{p_B\beta_{BA}}\mathbf{h}_{BA} + \sqrt{p_E\beta_{EA}}\mathbf{h}_{E_iA}\right)x_p + \mathbf{n}_p \qquad (1)$$

where $\mathbf{h}_{BA}$ and $\mathbf{h}_{E_iA}$ denote the channel vectors from Bob to Alice and from the selected antenna of Eve to Alice, respectively. p_B and p_E denote the transmit power from Bob and Eve, respectively. $\mathbf{n}_p \sim \mathcal{CN}(\mathbf{0}, \sigma^2\mathbf{I})$ is the additive white Gaussian noise vector during the training phase. Without loss of generality, we assume that $\mathbb{E}[|x_p|^2] = 1$.

We assume that uplink and downlink channels are perfectly reciprocal, i.e., $\mathbf{h}_{AB} = \mathbf{h}_{BA}^T$. Using the least square channel estimation method, we obtain the uplink channel estimation $\hat{\mathbf{h}}_A$, it yields

$$\begin{aligned}\hat{\mathbf{h}}_A &= \left(\sqrt{p_B\beta_{BA}}\mathbf{h}_{BA} + \sqrt{p_E\beta_{EA}}\mathbf{h}_{E_iA} + \mathbf{n}_p\right)^T \\ &= \sqrt{p_B\beta_{BA}}\mathbf{h}_{AB} + \sqrt{p_E\beta_{EA}}\mathbf{h}_{AE_i} + \mathbf{n}_A \qquad (2)\end{aligned}$$

where $\mathbf{n}_A = \mathbf{n}_p^T$.

In the downlink transmission phase, Alice transmits data symbol x_d to Bob and performs maximum ratio transmission (MRT), namely designing the transmit beam $\mathbf{w} = \frac{\hat{\mathbf{h}}_A}{\|\hat{\mathbf{h}}_A\|}$. Therefore, the received signal at Bob, y_B, and the received signal at Eve using the selected antenna, y_{E_x}, which are expressed as

$$\begin{aligned}y_B &= \sqrt{p_A\beta_{AB}}\mathbf{h}_{AB}^H\mathbf{w}x_d + n_B \\ &= \sqrt{\frac{p_Ap_B\beta_{AB}\beta_{BA}}{a}}\mathbf{h}_{AB}^H\mathbf{h}_{AB}x_d + \sqrt{\frac{p_Ap_E\beta_{AB}\beta_{EA}}{a}}\mathbf{h}_{AB}^H\mathbf{h}_{AE_x}x_d \\ &+ \sqrt{\frac{p_A\beta_{AB}}{a}}\mathbf{h}_{AB}^H\mathbf{n}_Ax_d + n_B \qquad (3)\end{aligned}$$

$$\begin{aligned}y_{E_x} &= \sqrt{p_E\beta_{AE}}\mathbf{h}_{AE_x}^H\mathbf{w}x_d + n_E \\ &= \sqrt{\frac{p_Ap_B\beta_{AE}\beta_{BA}}{a}}\mathbf{h}_{AE_x}^H\mathbf{h}_{AB}x_d + \sqrt{\frac{p_Ap_E\beta_{AE}\beta_{EA}}{a}}\mathbf{h}_{AE_x}^H\mathbf{h}_{AE_x}x_d \\ &+ \sqrt{\frac{p_A\beta_{AE}}{a}}\mathbf{h}_{AE_x}^H\mathbf{n}_Ax_d + n_E \qquad (4)\end{aligned}$$

where $a \triangleq p_B\beta_{BA} + p_E\beta_{EA} + 1$. $\mathbf{h}_{AE_x}$ denotes the channel vector between Alice and Eve using the selected antenna such that $|\mathbf{h}_{AE_x}\mathbf{w}|^2 = \max_{i\in\{1,2,\ldots,N_e\}} |\mathbf{h}_{AE_i}^H\mathbf{w}|^2$. x_d is the normalized data symbol with unit variance, p_A is the transmit power at Alice, $n_B \sim \mathcal{CN}(0,1)$ and $n_E \sim \mathcal{CN}(0,1)$ denote the additive white Gaussian noises at Bob and Eve, respectively.

Accordingly, the instantaneous SNR at Bob, i.e., SNR_B, is given by

$$\begin{aligned}SNR_B &= p_A\beta_{AB}\left|\mathbf{h}_{AB}^H\frac{\hat{\mathbf{h}}_A}{\|\hat{\mathbf{h}}_A\|}\right|^2 \\ &= p_A\beta_{AB}\left|\frac{\sqrt{p_B\beta_{BA}}\mathbf{h}_{AB}^H\mathbf{h}_{AB} + \sqrt{p_E\beta_{AE}}\mathbf{h}_{AB}^H\mathbf{h}_{AE_x} + \mathbf{h}_{AB}^H\mathbf{n}}{\sqrt{a}}\right|^2 \\ &\overset{(a)}{\approx} p_A\beta_{AB}\left|\frac{\sqrt{p_B\beta_{BA}}\mathbf{h}_{AB}^H\mathbf{h}_{AB}}{\sqrt{a}}\right|^2 \\ &\overset{(b)}{\approx} \frac{Mp_Ap_B\beta_{AB}\beta_{BA}}{a} \qquad (5)\end{aligned}$$

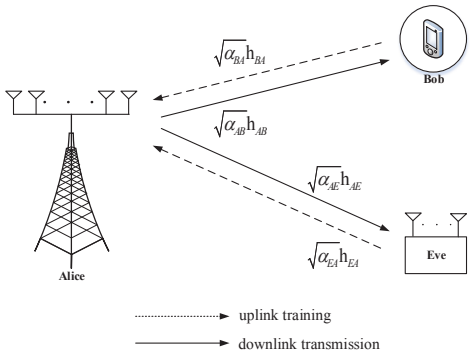

Fig. 1: System model.

[1]Note that Bob and Eve are assumed to be perfectly synchronization for transmitting pilots and data in the same frequency band, the details on when and how accurate synchronization is achievable are beyond the scope of this work.

where the step (a) can be easily recognized by noting the fact that, according to the law of large numbers [13], the effects of uncorrelated receive noise and fast fading vanish as $M \to \infty$. The step (b) follows the fact that $|\frac{\sqrt{p_B\beta_{BA}}\mathbf{h}_{AB}^H\mathbf{h}_{AB}}{\sqrt{a}}|^2$ scales with the order $\mathcal{O}(\frac{p_B\beta_{BA}M}{a})$.

Similarly, the instantaneous SNR at Eve, i.e., SNR_{E_x}, is given by

$$SNR_{E_x} = p_A\beta_{AE}\left|\mathbf{h}_{AE}^H\frac{\hat{\mathbf{h}}_A}{\|\hat{\mathbf{h}}_A\|}\right|^2 \approx \frac{Mp_Ap_E\beta_{AE}\beta_{EA}}{a} \quad (6)$$

It is worth mentioning that when Eve is passive in massive MIMO system, $SNR'_B \approx \frac{Mp_Ap_B\beta_{AB}\beta_{BA}}{p_B\beta_{BA}+1}$ and SNR'_{E_x} scales as the order $\mathcal{O}(1)$. By contrast, the active eavesdropper has a strong eavesdropping ability because existing pilot attack.

As a result, the achievable instantaneous secrecy rate is formulated as

$$\begin{aligned} R_s &= [\log_2(1+SNR_B) - \log_2(1+SNR_{E_x})]^+ \\ &= \left[\log_2\left(\frac{a+Mp_Ap_B\beta_{AB}\beta_{BA}}{a+Mp_Ap_E\beta_{AE}\beta_{EA}}\right)\right]^+ \end{aligned} \quad (7)$$

where the notation $[y]^+ = \max\{y, 0\}$ is used, since the secrecy rate is defined as a nonnegative quantity. We can observed from (7) that if Bob and Eve have the identical transmit power p_B and p_E, as well as they are located at symmetric position relative to Alice, i.e., $\beta_{AB}/\beta_{AE} = 1$, the achieved instantaneous secrecy rate $R_s = 0$. Furthermore, if Eve increases the transmit power p_E in the uplink training phase to make $p_E\beta_{AE}\beta_{EA} > p_B\beta_{AB}\beta_{BA}$, secure transmission cannot be achieved due to the pilot attack. From the above illustration, we can observe that the pilot attack affects the secrecy performance[2].

III. Energy-Efficient Power Allocation

Since the limitation of energy resource and the requirement of green communication, EE becomes an important performance metric in nature for evaluating 5G wireless networks. In this section, we only focus on the EE in the case of pilot attack, and we assume that Eve always exists. The power allocation scheme of Alice for maximizing the EE while guaranteeing the secrecy rate constraint and the transmit power requirement in a massive MIMO system is developed in the following.

To design a EE power allocation scheme, we first investigate the total power consumption in such a secure system. Following [20], [21], the total power consumption of the whole system, denoted as E_{tot}, is given by

$$E_{tot} = \frac{p_A + p_B + p_E}{\eta} + P_c \quad (8)$$

where P_c is circuit power consumption, which is a constant. $\eta \in (0, 1]$ represents the power amplifier efficiency, without loss of generality, we assume $\eta = 1$ for simplicity. The secrecy EE is defined as the ratio of the secrecy rate to the total power consumption (bits/Joule). Therefore, the optimization problem can be mathematically formulated as

$$\begin{aligned} \max_{p_A} \quad & \frac{R_s}{E_{tot}} \\ \text{s.t.} \quad & R_s \geq R_{\min}, \\ & p_A \leq P_{\max}, \end{aligned} \quad (9)$$

where $R_{\min}$ is the prescribed secrecy rate threshold and $P_{\max}$ is the maximum transmit power. Note that problem (9) is non-convex and difficult to solve directly, since the objective function is a fractional form.

Fortunately, using the fractional programming theory [24], problem (9) is equivalently transformed into a parameterized polynomial subtractive form. Here, we first define a parametric problem with respect to q as

$$F(q) = \max_{p_A} R_s - q^*E_{tot} \quad (10)$$

where q denotes the maximum secrecy EE, namely $q^* = \max_{p_A} \frac{R_s}{E_{tot}}$. $\mathbb{D} = \{p_A \mid R_s \geq R_{\min}, p_A \leq P_{\max}\}$ stands for the feasible set of problem (9). To proceed, we have the following two lemmas, the interested readers can refer to [22] for a detailed description.

Lemma 1: $F(q)$ is a strictly decreasing and continuous function with respect to q, and it has a unique zero solution.

Lemma 2: Assume that q^* is the unique zero solution to $F(q)$, then function $F(q^*)$ and problem (9) have the same optimal solution, as well as the optimal objective function value of problem (9) is q^*.

The preceding two lemmas enable us find the optimal q by seeking the unique zero solution of a function in a parameterized polynomial subtractive form. As a result, our strategy is to optimize (10) for a given q at first. For convenience, problem (9) is equivalently reformulated as

$$\max_{p_A} \quad R_s - q^*(p_A + p_B + p_E + P_c) \quad (11a)$$

$$\text{s.t.} \quad R_s \geq R_{\min}, \quad (11b)$$

$$p_A \leq P_{\max}. \quad (11c)$$

Proposition 1: $F(q^*)$ is a concave function with respect to transmit power p_A when $p_E\beta_{AE}\beta_{EA} \leq p_B\beta_{AB}\beta_{BA}$.

Proof: It can be easily observed that $F(q^*)$ has the same convexity or concavity as R_s since $q^*(p_A + p_B + p_E + P_c)$ is a affine. The first-order derivative of R_s with respect to p_A can be calculated as $\frac{\partial R_s}{\partial p_A} = \frac{aM(p_B\beta_{AB}\beta_{BA} - p_E\beta_{AE}\beta_{EA})}{\ln 2(a+Mp_Ap_B\beta_{AB}\beta_{BA})(a+Mp_Ap_E\beta_{AE}\beta_{EA})}$, and the second-order derivative of R_s with respect to p_A can be calculated as $\frac{\partial R_s^2}{\partial^2 p_A} = \frac{abM(p_E\beta_{AE}\beta_{EA} - p_B\beta_{AB}\beta_{BA})}{\ln 2[(a+Mp_Ap_B\beta_{AB}\beta_{BA})(a+Mp_Ap_E\beta_{AE}\beta_{EA})]^2}$, where $b = aM(p_B\beta_{AB}\beta_{BA} + p_E\beta_{AE}\beta_{EA}) + 2M^2(p_Ap_Bp_E\beta_{AB}\beta_{BA}\beta_{AE}\beta_{EA})$. If $p_E\beta_{AE}\beta_{EA} \leq p_B\beta_{AB}\beta_{BA}$, then $\frac{\partial R_s^2}{\partial^2 p_A} \leq 0$, thereby R_s is a concave function, which completes the proof.

By introducing the Lagrange multipliers $\lambda \geq 0$ and $\mu \geq 0$ associated with the constraints (11b) and (11c), the Lagrangian dual function of problem (9) is written as

[2]Note that the detection of the pilot attack is another interesting topic. The detail of this issue is beyond the scope of this paper and will be left as future studies.

$$\mathcal{L}(p_A,\lambda,\mu) = R_s - q^*(p_A + p_B + p_E + P_c) + \lambda(R_s - R_{\min}) + \mu(P_{\max} - p_A) \quad (12)$$

and the corresponding dual optimization problem of (10) is given by

$$\min_{\lambda,\mu} \max_{p_A} \mathcal{L}(p_A,\lambda,\mu) \quad (13)$$

For fixed λ and μ, the optimal power p_A^* can be derived by solving the following Karush-Kuhn-Tucker (KKT) condition [23], i.e.,

$$\frac{\partial \mathcal{L}(p_A,\lambda,\mu)}{\partial p_A} = (1+\lambda)\frac{\partial R_s}{\partial p_A} - q^* - \mu = 0 \quad (14)$$

Then we can obtain the optimal power solution

$$p_A = \left[\frac{\sqrt{M^2a^2c^2 - 4M^2d(a^2-l)} - Mac}{2M^2d}\right]^+ \quad (15)$$

where parameters $c \triangleq p_B\beta_{AB}\beta_{BA} + p_E\beta_{AE}\beta_{EA}$, $d = p_Bp_E\beta_{AB}\beta_{BA}\beta_{AE}\beta_{EA}$ and $l \triangleq \frac{(1+\lambda)aM(p_B\beta_{AB}\beta_{BA} - p_E\beta_{AE}\beta_{EA})}{\ln 2(q^*+\mu)}$.

At the same time, the Lagrange multipliers can be updated by the gradient method, which are given by

$$\lambda(t+1) = [\lambda(t) - \Delta_\lambda(R_s - R_{\min})]^+, \quad (16)$$

$$\mu(t+1) = [\mu(t) - \Delta_\mu(P_{\max} - p_A)]^+, \quad (17)$$

where $\Delta_\lambda > 0, \Delta_\mu > 0$ are step sizes, respectively. The symbol t is the iteration index.

To summarize, the procedure of energy-efficient power allocation algorithm is as follows:

Algorithm 1 Energy-Efficient Power Allocation Algorithm

1: **Initialization:**
Lagrange multipliers λ, μ, constants $\Delta_\lambda, \Delta_\mu \in (0,1)$, precision $\epsilon > 0$, and iteration number $t = 0$.
2: **Computing:**
Compute transmit power p_A according to (15).
3: **Updating:**
Update λ and μ according to (16) and (17).
4: **Until:**
If $R_s - q^*(p_A + p_B + p_E + P_c) > \epsilon$, then set $q^* = \frac{R_s}{p_A + p_B + p_E + P_c}$, and return to step 2.
Otherwise, p_A is the optimal transmit power.

IV. Numerical Results

In this section, we present numerical results to show the performance of the proposed power allocation scheme in the context of a massive MIMO secure system. All the channel coefficients are assumed to be i.i.d. complex-valued Gaussian random variables with zero mean and unit variance. Simulation parameters are set as follows: the number of transmit antennas at Eve $N_e = 2$, spectrum bandwidth B = 10KHz, maximum transmit power $P_{\max}$=15W, circuit power consumption P_c=5W, precision $\epsilon = 0.001$ and $R_{\min}$=20Kb/s.

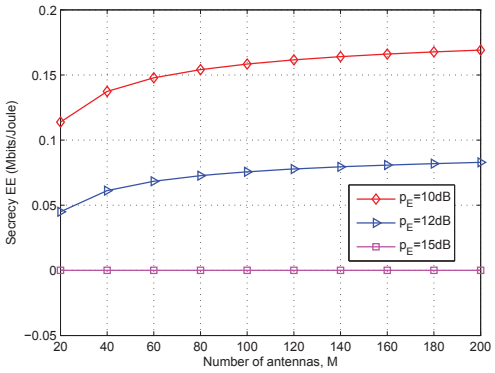

Fig. 2: Secrecy EE versus transmit antennas with $\beta_{AB} = \beta_{BA} = \beta_{AE} = \beta_{EA} = 1$ and $p_B = 15$dB.

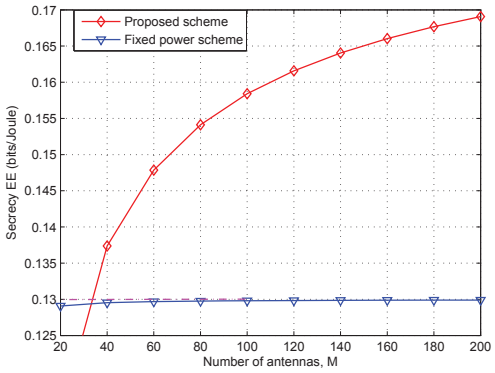

Fig. 3: Performance comparison of the fixed and proposed power allocation schemes. $\beta_{AB} = \beta_{BA} = \beta_{AE} = \beta_{EA} = 1$.

In Fig. 2, we show the effect of transmit antennas M on the secrecy EE for different Eve's power values p_E. It is observed that the secrecy EE decreases as p_E increases and the secrecy EE tends to zero when $p_E = p_B$, which is caused by the detrimental effect of active eavesdropping (pilot attack). In addition, we find that the proposed scheme converges within 15 iterations in the all simulation scenarios.

Fig. 3 compares the performance of secrecy EE for the proposed power allocation scheme and the fixed power allocation scheme with $p_B = 15$dB and $p_E = 10$dB. Intuitively, it is optimal to use P_{max} as the transmit power for the fixed power allocation scheme. It can be observed from Fig. 3 that the proposed power allocation scheme obviously outperforms the fixed one, especially when M is large. Therefore, the proposed scheme is more suitable for the future green and secure communications.

For more comprehensive investigating the performance of the proposed scheme, fig. 4 illustrates the secrecy EE versus the relative large-scale fading of the eavesdropper channel ρ_{AE} under $p_B = 15$dB and $p_E = 10$dB. As we expected, with the increase of ρ_{AE}, the secrecy EE with different transmit antennas become less. This is due to the fact that when relative

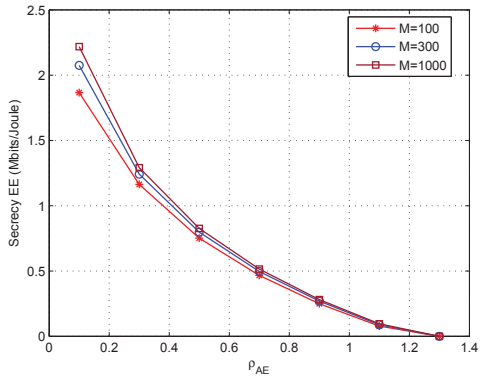

Fig. 4: Performance of the proposed power allocation scheme versus ρ_{AE} for different transmit antennas M, where $\rho_{AE} = \beta_{AE}/\beta_{AB}$ denotes the relative large-scale fading of the eavesdropper channel. $\beta_{AB} = \beta_{BA} = 1$.

large-scale fading ρ_{AE} increases, the link quality of Alice-Eve is lifted to a good level, thus the secrecy EE decreases. For example, if $\rho_{AE} > 1$, then it demonstrates Eve is closer to the Alice than Bob, thereby the Eve has a strong eavesdropping ability. For a given ρ_{AE}, it is also found that the secrecy EE increases accordingly as transmit antennas M increases, which confirms the main advantage of massive MIMO system by exploiting its large array gain.

V. Conclusions

In this paper, we investigated the problem of energy-efficient power allocation for secure transmission in a massive MIMO system, where an active multi-antenna eavesdropper by attacking the uplink training phase was considered. We aimed at maximizing the EE while guaranteeing the secrecy rate constraint and the transmit power requirement. Furthermore, we derived the optimal solution by exploiting the fractional-form structure of the problem. Our results provide useful guidelines on the energy-efficient power optimization for physical layer security with massive MIMO system. In our future work, the detection of pilot attack from eavesdroppers will be studied.

Acknowledgment

This work was supported by the National Natural Science Foundation of China (Grant No. 61371075 and 61421001) and 863 Project (Grant No. 2015AA01A708).

References

[1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[2] J. Ni, K.-K. Wong, Z. Fei, C. Xing, H. Chen, K.-F. Tong, and J. Kuang, "Secrecy-rate balancing for two-user MISO interference channels," *IEEE Wireless Commun. Lett.*, vol. 3, no, 1, pp. 6–9, Feb. 2014.

[3] B. Li and Z. Fei, "Robust beamforming and cooperative jamming for secure transmission in DF relay systems," *EURASIP Journal on Wireless Communications and Networking*, 2016. DOI:10.1186/s13638-016-0560-1.

[4] S. Jin, X. Wang, Z. Li, K.-K. Wong, Y. Huang, and X. Tang, "On massive MIMO zero-forcing transceiver using time-shifted pilots," *IEEE Trans. Veh. Technol.*, vol. 65, no, 1, pp. 59–74, Jan. 2016.

[5] Q. Zhang, S. Jin, M. McKay, D. Morales-Jimenez, and H. Zhu, "Power allocation schemes for multicell massive MIMO systems," *IEEE Trans. Wireless Commun.*, vol. 14, no, 11, pp. 5941–5955, Nov. 2015.

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

[7] D. Kapetanović and G. Zheng and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 31, no, 9, pp. 21–27, Jun. 2015.

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

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

[10] J. Wang, J. Lee, F. Wang, and T. Q. S. Quek, "Jamming-aided secure communication in massive MIMO rician channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 12, pp. 6854–6868, Dec. 2015.

[11] Y. Deng, L. Wang, K.-K. Wong, A. Nallanathan, M. Elkashlan, and S. Lambotharan, "Safeguarding massive MIMO aided HetNets using physical layer security," *Proc. IEEE Sixth International Conference on Wireless Communications and Signal Processing (WCSP)*, Nanjing, China, Oct. 2015.

[12] K. Guo, Y. Guo, and G. Ascheid, "Distributed antennas aided secure communication in MU-massive-MIMO with QoS guarantee," *Proc. IEEE 82nd Vehicular Technology Conference (VTC-Fall)*, Boston, USA, Sep. 2015.

[13] X. Chen, L. Lei, H. Zhang, and C. Yuen, "Large-scale MIMO relaying techniques for physical layer security: AF or DF?" *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 5135–5146, Sep. 2015.

[14] X. Zhou, B. Maham, and A. Hjørungnes, "Pilot contamination for active eavesdropping" *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 903–907, Mar. 2012.

[15] A. Chorti, S. M. Perlaza, Z. Han, and H. V. Poor, "On the resilience of wireless multiuser networks to passive and active eavesdroppers" *IEEE J. Sel. areas Commun.*, vol. 31, no. 9, pp. 1850–1863, Sep. 2013.

[16] Y. Wu, R. Schober, D. W. K. Ng, C. Xiao, and G. Caire, "Secure massive MIMO transmission with an active eavesdropper," *Proc. IEEE International Conference on Communications (ICC)*, London, UK, Jun. 2015.

[17] Y. Zeng and R. Zhang, "Wireless information surveillance via proactive eavesdropping with spoofing relay," *IEEE Journal of Selected Topics in Signal Processing, special issue on exploiting interference towards energy efficient and secure wireless communications*. (available on-line at arXiv:1606.03851)

[18] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via jamming for rate maximization over Rayleigh fading channels," *IEEE Commun. Lett.*, vol. 5, no. 1, pp. 80-83, February 2016.

[19] J. Xu, L. Duan, and R. Zhang, "Proactive eavesdropping via cognitive jamming in fading channels," *IEEE Trans. Wireless Commun.*. (available on-line at arXiv:1512.02754)

[20] J. Chen, X. Chen, T. Liu, and L. Lei, "Energy-efficient power allocation for secure communications in large-scale MIMO relaying systems," *Proc. IEEE/CIC International Conference on Communications in China (ICCC)*, Shanghai, China, Oct. 2014.

[21] X. Chen and L. Lei, "Energy-efficient optimization for physical layer security in multi-antenna downlink networks with QoS guarantee," *IEEE Commun. Lett.*, vol. 17, no. 4, pp. 637–640, Apr. 2013.

[22] J. Xu and L. Qiu, "Energy efficiency optimization for MIMO broadcast channels," *IEEE Trans. Wireless Commun.*, vol. 12, no. 2, pp. 690–701, Feb. 2013.

[23] S. Boyd and L. Vandenberghe, *Convex Optimization. Cambridge*, U.K.: Cambridge Univ. Press, 2004.

[24] S. Schaible, "Fractional programming," *Zeitschrift für Operations Research*, vol. 27, no. 1, pp. 39–54, 1983.