Secure Energy-Efficient Resource Allocation Algorithm of Massive MIMO System with SWIPT

Xiaoxia Yang ¹, Zhengqiang Wang ¹,*†, Xiaoyu Wan ² and Zifu Fan ²

¹ School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China; S170101175@stu.cqupt.edu.cn
² Institute of Next Generation Network, Chongqing University of Posts and Telecommunications, Chongqing 400065, China; wanxy@cqupt.edu.cn (X.W.); fanzf@cqupt.edu.cn (Z.F.)
* Correspondence: wangzq@cqupt.edu.cn; Tel.: +86-151-2300-9069
† Current address: No. 2 Chongwen Road, Nan’an district, Chongqing 400064, China

Received: 24 October 2019; Accepted: 22 December 2019; Published: 25 December 2019

Abstract: In this paper, we consider the resource allocation problem to maximize the minimum (max–min) user’s secure energy efficiency (SEE) in downlink massive multiple-input multiple-output (MIMO) systems with simultaneous wireless information and power transfer (SWIPT). First, transmission power and power splitting ratio are designed to achieve the max–min user’s SEE subject to harvested energy threshold, the constraints of transmission power, and power splitting ratio. Secondly, the optimization problem is non-convex and very difficult to tackle. In order to solve the optimization problem, we converted to a series of parameter optimization subproblems by fractional programming. Then, we employ the first-order Taylor expansion and successive convex approximation (SCA) method to solve parameter optimization problems. Next, a secure energy-efficient resource allocation (SERA) algorithm with the bisection method is proposed to find the max–min SEE of the system. Finally, simulation results show the effectiveness and superiority of the SERA algorithm.

Keywords: massive MIMO; max-min; SEE; SWIPT

1. Introduction

With the rapid development of mobile internet technology, the broadcast characteristics of wireless information have led to severe information leakage problems. Physical layer security has increasingly attracted research interests in 5th-Generation (5G) mobile communication because it can ensure safe protection from information theory even when eavesdroppers have a powerful computing ability [1]. Massive multiple-input multiple-output (MIMO) is a promising technology in 5G which can be used to improve the spectrum efficiency and security of wireless communication. Moreover, massive MIMO can be used to enhance the security and power transfer efficiency of a simultaneous wireless information and power transfer (SWIPT) system because it can beamform the energy and information more accurately with large array gain [2,3].

Secure problems in massive MIMO systems have been investigated in References [4–11]. The authors in Reference [4] studied the impact of residual hardware impairment (HWI) on massive MIMO secure communication and showed the HWI has a negative impact on information security. In Reference [5], S. Timilsina et al. studied the effect of active eavesdropping on physical layer security and revealed that active eavesdroppers had a stronger ability to eavesdrop confidential information with higher pilot power. In Reference [6], Z. Chu et al. studied a MIMO secrecy channel with SWIPT. The minimum harvested energy is maximized under the secrecy rate requirements. In Reference [7], H. D. Tuan et al. considered the problem of power allocation to maximize the worst links’ secrecy...
throughput or the network’s secure energy efficiency (SEE) under various scenarios of available channel state information. In Reference [8], C. Du et al. studied massive MIMO relay-assisted secure communication systems, which considered the channel reciprocity in time division duplexing (TDD) mode and the energy harvesting at the relay. An energy efficiency power allocation (EEPA) scheme is proposed to maximize SEE. In Reference [9], J. He et al. studied the effect of channel aging on full-duplex massive MIMO spectral efficiency (SE) and energy efficiency (EE) and proposed four power allocation schemes. In Reference [10], S. Timilsina et al. studied relay-assisted massive MIMO downlink secure transmission with the random and zero-space degrees of freedom of artificial noise (AN) matrix vectors. In Reference [11], J. Zhu et al. studied the influence of phase noise on the downlink of secure massive MIMO with a SWIPT system. The closed-form lower bound on the worst-case secrecy rate is derived. However, most of the above works focus on security rate optimization. Energy efficiency has been one of the key performance indexes for 5G because green communication has become the developing trend and direction of the future society [12]. Therefore, it is important to optimize SEE for massive MIMO with SWIPT.

In this paper, we consider secure transmission in massive MIMO systems with SWIPT. A secure energy-efficiency resource allocation (SERA) algorithm for massive MIMO systems with SWIPT is proposed. The users utilize the harvesting energy in the previous time slot to transmit pilot information, and the active eavesdropper transmits the same pilot information as a user to achieve the purpose of eavesdropping. To reduce the eavesdropping ability of the active eavesdropper, the base station (BS) uses AN auxiliary communication. At the BS, the power splitting ratio is used to reasonably allocate the information transmission power and the AN transmission power. The AN matrix-vector at the BS adopts the null space beamforming [13], which is simplified by the properties of the Wishart matrix. By adopting a variable substitution method, the non-convex SEE maximization problem is converted into a series of parameter optimization subproblems by fractional programming. A joint power splitting ratio and the BS transmitted power allocation algorithm are proposed to maximize the minimum (max–min) SEE of the user. Simulation results are also compared with the users’ system SEE maximization in Reference [14,15] and the secure rate maximization in Reference [16] to confirm the effectiveness and superiority of the SERA algorithm.

Note: Bold letters denote matrices or vectors, $(\cdot)^{H}$ denotes conjugate transposes of matrices or vectors, $(\cdot)^{T}$ denotes transpose of matrices or vectors, $Tr(\cdot)$ denotes trace of matrices, $E(\cdot)$ denotes mathematical expectation, $\otimes$ are the Kronecker product, and $[x]^{+}=\max\{0,x\}$.

2. System Model

As shown in Figure 1, a single-cell downlink massive MIMO system with SWIPT consists of one BS connected with $K$ users and one eavesdropper [17–19]. The number of transmitting antennas at BS is $N$, which satisfies $N \gg K$. Each user and the eavesdropper are equipped with a single antenna. The BS simultaneously serves $K$ users in the same time-frequency resource block [20]. Especially, it is assumed that the active eavesdropper perfectly knows the pilot sequence transmitted by the $m$th user node [21], where $m \in \{1, ..., K\}$. Without loss of generally, we suppose that each time slot has a unit length. Each time slot has two parts. In the first time slot $\tau$, users use the energy harvested by the previous time block to transmit pilot information to the BS. The active eavesdropper also transmits pilot information to the BS. In the $1-\tau$ time slot, BS transmits information or energy to users and the eavesdropper. The user’s terminal receiver decodes the signal into two parts; one part is used for information decoding, and the other is used for energy harvesting. The eavesdropper mainly is used for information decoding [15].
The BS-to-user and BS-to-eavesdropper channels are denoted by \( G, h \), which is given by

\[
G = \sqrt{D} G, h = \sqrt{\vartheta} h
\]  

where \( G \sim CN_{K \times N}(0, I_K \otimes I_N) \) and \( h \sim CN_{1 \times N}(0, I_{1 \times N}) \) are the small scale Rayleigh fading and where \( D_{m,m} = \beta_m, m = \{1, \ldots, K\} \) and \( \vartheta \) are the path loss from BS-to-user and BS-to-eavesdropper channels, respectively. The path loss is modeled as \( \beta_m = l_m^{-r} \) and \( \vartheta = d^{-r} \), where \( r \) is the path loss exponent factor, \( l_m \) is the distance between the BS and user \( m \), and \( d \) is the distance between the BS and eavesdropper [5].

In TDD massive MIMO, the users-to-BS and eavesdropper-to-BS channels are estimated at the BS via uplink pilots transmitted. The BS stores the channel state information (CSI) through channel reciprocity. The superimposed pilot signal received at BS is

\[
y_{BS} = \sqrt{\tau} p_u G^T s + \sqrt{\tau} p_e h^T s_m + n
\]

where \( p_u \) and \( p_e \) express the average transmit powers from the users and the eavesdropper; \( s = \{s_1, \ldots, s_m, \ldots, s_K\}^T \), where \( s_m^H = 1 \) and \( s_m s_m^H = 0 \) for \( m \neq m' \) and \( m, m' \in \{1, \ldots, K\} \). \( n \) is the noise with independent and identically distributed (i.i.d.) \( \sim CN(0, 1) \) distribution for each element. Assuming that BS uses the minimum mean squared error (MMSE) estimation, the BS-to-user channel is obtained as follows [5,19]:

\[
G = \hat{G} + E
\]

\[
\hat{g}_m = (\sqrt{\tau} p_u g_m + \sqrt{\tau} p_e h + n)(\tau p_u \beta_m + I_{i,m} \tau p_e \vartheta + 1)^{-1} \sqrt{\tau} p_u \beta_m
\]

where \( \hat{G} = \{\hat{g}_1, \hat{g}_2, \ldots, \hat{g}_K\}, i, m \in \{1, \ldots, K\}, \begin{cases} I_{i,m} = 1, \quad m = i \\ I_{i,m} = 0, \quad m \neq i \end{cases} \hat{\beta}_m = \frac{\tau p_u \beta_m^2}{\tau p_u \beta_m + I_{i,m} \tau p_e \vartheta + 1} \), \( E \) is the estimation error matrix.

To prevent the eavesdropper from stealing confidential information, the BS introduces AN subsidiary communications [13]. The BS uses the power splitting ratio to information power and AN transmission power [5,19]; the transmission information at BS is given as follows:

\[
X = \hat{W} \sqrt{p_i q x} + V \sqrt{\frac{(1-q) p_i}{N-K}} z
\]
where $P_t$ represents the transmit power; $\phi = \text{diag}(\phi_1, \phi_2, \ldots, \phi_K)$, where $\phi_m$ is the power splitting ratio coefficient of the BS for user $m$ ($m = 1, \ldots, K$); channel matrices $\hat{W} \in \mathbb{C}^{N \times K}$ and $V \in \mathbb{C}^{N \times K}$ denote the precoding matrix for the data and AN [13,22]; $\hat{W} = \alpha \hat{G}^H (\hat{G} \hat{G}^H)^{-1}; \alpha = \sqrt{\frac{N-K}{Tr(D^{-1})}}; V = (I - \hat{G}^H (\hat{G} \hat{G}^H)^{-1} \hat{G})$; $x = \{x_1, x_2, \ldots, x_K\}^T$ is the signal vector transmitted to $K$ users satisfying $E[xx^H] = I_K$; and $z \sim \mathcal{CN}(0_K, \sigma_z^2 I_K)$ is an AN sequence.

The users utilize the power splitting ratio to decode information from BS simultaneously, where one part is used to harvest energy and the other part is decoded into useful information, and the eavesdropper mainly wiretaps useful information from BS [23]. Therefore, the $m$th user and the eavesdropper receiving useful information is given as follows [5,19,20]:

$$y_m = \sqrt{P_t \varphi_m (1 - \rho_m)} g_m \hat{W}_m x_m + \sqrt{P_t \varphi_m (1 - \rho_m)} (g_m \hat{W}_m - E[g_m \hat{W}_m]) x_m + \sum_{m \neq i}^{K} \sqrt{P_t \varphi_m (1 - \rho_m)} g_m \hat{W}_m x_i + \sqrt{P_t (1 - \varphi_m) (1 - \rho_m)} \frac{(N-K)}{g_m} V z + n_m$$

$$y_{e,m} = \sqrt{P_t \varphi_m} h \hat{W}_m x_m + \sqrt{P_t (1 - \varphi_m)} \frac{(N-K)}{h} V z + n_e$$

where $\rho = \{\rho_1, \ldots, \rho_m, \ldots, \rho_K\}$ express the power splitting receiver from users. The first item denotes the desired signal, the second term is the beamforming gain uncertainty, the third term is the inter-user interference, and the remaining terms are AN leaked to legitimate users and the additive white Gaussian noise (AWGN) at the $m$th user node. The $m$th user harvest energy is given by

$$E_m(P_t, \varphi_m, \rho_m) = \eta_m (1 - \tau) \rho_m (P_t \varphi_m g_m \hat{W}_m)^2 + \frac{(1 - \varphi_m) P_t \sigma_z^2 |g_m V|^2}{N - K}$$

where $\eta_m (0 < \eta_m \leq 1)$ is the energy conversion efficiency for user $m$, which transfers the harvested energy into electric energy stored by the users and eavesdropper.

Provided that the worst-case uncorrelated additive noise distributed as independent Gaussian noise has the same variance [5], the achievable rate of the $m$th user can be lower by the following expression

$$R_m^l(P_t, \varphi_m, \rho_m) = (1 - \tau) \ln(1 + E(\gamma_m))$$

where $\gamma_m$ is given by

$$\gamma_m = \frac{(1 - \rho_m) P_t \varphi_m |g_m \hat{W}_m|^2}{(1 - \rho_m) P_t \varphi_m |g_m \hat{W}_m - E[g_m \hat{W}_m]|^2 + \gamma_{m,o}}$$

where $\gamma_{m,o}$ is the effective noise which is defined as follows:

$$\gamma_{m,o} = (1 - \rho_m) P_t \varphi_m \sum_{m \neq i}^{K} |g_m \hat{W}_i|^2 + \frac{P_t (1 - \varphi_m) (1 - \rho_m) \sigma_z^2 |g_m V|^2}{(N-K)} + \sigma_m^2$$

Provided that the eavesdropper eliminates the other users interference terms [5,19], the upper bounded achievable rate of the $m$th user signal leaked into eavesdropper can be written as

$$R_m^u(P_t, \varphi_m) = (1 - \tau) \ln(1 + E(\gamma_{e,m}))$$
where \(y_{e,m}\) is expressed as
\[
\gamma_{e,m} = \frac{P_z q_m |h_w|^2}{(1-q_m)N^{-1}K + \sigma_e^2}
\] (13)

Hence, the \(m\)th user achievable secure rate is as follows [5,19]:
\[
R_{sec,m}(P_t, q_m, \rho_m) \geq R_{sec,m}^e(P_t, q_m, \rho_m) = \max\{0, R_{m}^l(P_t, q_m, \rho_m) - R_{e,m}^u(P_t, q_m)\}
\] (14)

Using wishart matrix to simplify Equations (8)–(14) as in References [5,19], the harvesting energy by user \(m\) can be written as follows:
\[
E_m(P_t, q_m, \rho_m) = P_t \eta_m (1-\tau) \rho_m (q_m k^2 + \frac{(1-q_m)\sigma_e^2 (\beta_m - \hat{\beta}_m)}{N}}
\] (15)

The achievable secure rate of user \(m\) is given by [5,19]
\[
R_{m}^l(P_t, q_m, \rho_m) = (1-\tau) \ln(1 + (E[\gamma_m^{-1}]^{-1} = (1-\tau) \ln(1 + \frac{q_m k^2 (1-\rho_m) P_t}{(\rho_m A_m + (1-\rho_m) B_m) (1-\rho_m) P_t + \sigma_e^2})}
\] (16)

The achievable rate of the \(m\)th user signal leaked into eavesdropper is simplified as follows [5,19]:
\[
R_{e,m}^u(P_t, q_m) = (1-\tau) \ln(1 + (E[\gamma_m^{-1}]^{-1} = (1-\tau) \ln(1 + \frac{q_m K P_t}{(1-\rho_m) D_m + \sigma_e^2})}
\] (17)

where \(A_m = \frac{\sigma_e^2 (\rho_m - \hat{\rho}_m) (\hat{\beta}_m - 1)}{N-K} \sum_{i \neq m} \hat{\beta}_i^{-1} > 0, B_m = \frac{\sigma_e^2 (\rho_m - \hat{\rho}_m)}{N-K} > 0, C_m = a^2 \sigma_e^2 \beta_m - 2 \rho_m > 0,\) and \(D_m = \sigma_e^2 \phi > 0.\)

3. Problem Formulation and Energy-Efficient Algorithm

With the above analysis for achievable rate and energy for user and eavesdropper, the max–min SEE optimization problem of the system can be expressed as
\[
P_1: \max_{P_t, q_m, \rho_m 1 \leq m \leq K} \min_{\varepsilon \leq K} \frac{R_{sec,m}(P_t, q_m, \rho_m)}{P_t (1-\tau) + P_u \tau}
\]
subject to
\[
C_1: \sum_{m=1}^{K} P_t \rho_m \leq P_{max}, m = 1, ..., K,
\]
\[
C_2: E_0 \leq E_m(P_t, q_m, \rho_m), m = 1, ..., K,
\]
\[
C_3: 0 < P_t, 0 < q_m, m = 1, ..., K,
\]
\[
C_4: 0 < \rho_m < 1, m = 1, ..., K
\] (18)

In \(P_1\), the objective is to maximize and minimize SEE of the system. \(C_1\) and \(C_3\) are the transmit power constraints, and \(C_2\) is the energy harvested constraint for user \(m\). \(\varepsilon (P_t q_m (1-\tau) + P_u \tau)\) and \(P_{c,m}\) denote the power consumption of the \(m\)th user and circuit consumption, and \(\epsilon\) denotes the power consumption coefficient.

The optimal solution to Equation (18) can be solved by fractional programming [24] to find zero roots of the following parameter optimization problem \(F(\lambda)\) [25]:
\[
F(\lambda) = \max_{P_t, q_m, \rho_m 1 \leq m \leq K} \min_{\lambda \leq K} \{R_{m}^l(P_t, q_m, \rho_m) - R_{e,m}^u(P_t, q_m) - \lambda (\varepsilon (P_t q_m (1-\tau) + P_u \tau) + P_{c,m})\}
\] (19)
According to the conclusions in References [24,25], the optimal solution to Equation (19) is $\lambda^*$ such that $F(\lambda^*) = 0$ is held. We define $\Gamma_m$ as

$$
\Gamma_m(\lambda, P_t, \varphi_m, \rho_m) = R_m^l(P_t, \varphi_m, \rho_m) - R_m^u(P_t, \varphi_m) - \lambda(\epsilon(P_t \varphi_m(1 - \tau) + p_u \tau) + P_c,m)
$$

(20)

Due to the non-smoothness of the objective function, we introduce a new variable $t$ to transform the equivalent non-smooth optimization problem in Equation (20) into a smooth optimization problem. Equation (18) can be equivalently reformulated as

$$
P_2 : \max_{P_t, \varphi_m, \rho_m, t} t
$$

s.t. $C_1 : \sum_{m=1}^{K} P_t \varphi_m \leq P_{\text{max}}, \forall m$

$$
C_2 : E_0 \leq \eta_m(1 - \tau)\rho_m(P_t \varphi_m \alpha^2 + \frac{(1 - \varphi_m)P_t \sigma^2_m(\hat{\beta}_m - \beta_m)}{N - K}), \forall m
$$

$$
C_3 : 0 < P_t, 0 < \varphi_m, \forall m
$$

$$
C_4 : 0 < \rho_m < 1, \forall m
$$

$$
C_5 : t \leq \Gamma_m(P_t, \varphi_m, \rho_m), \forall m
$$

$P_2$ has four optimization variables. First, fix BS’ power splitting ratio coefficient $\varphi_m$ and the transmit power $P_t$ are used to obtain a $\rho_m$ suboptimal solution. Then, use the suboptimal solution of $\rho_m$ iterative optimization power splitting ratio coefficient $\varphi_m$ and the BS transmit power $P_t$. Finally, update variable $t$.

Firstly, optimize $\rho_m$. Because $\rho_m$ is only associated with $R_m^l(P_t, \varphi_m, \rho_m)$ from Equations (16) and (20), which is monotonic decreasing function about $\rho_m$, $\rho_m$ depends on constraint $C_2$.

$$
\rho_m = (\frac{E_0}{\eta_m(1 - \tau)P_t(\varphi_m \alpha^2 + \frac{(1 - \varphi_m)\sigma^2_m(\hat{\beta}_m - \beta_m)}{N - K})}), \forall m
$$

(22)

Then, optimize $\varphi_m$, and $P_t$ is a hard problem. In Equation (21), the difference of two convex functions is non-convex. Therefore, we need to replace the non-convex part in Equation (21) by linear approximation and we rewrite constraint $C_5$; let

$$
f_m(P_t, \varphi_m) = (1 - \tau)\ln(1 + \frac{\alpha^2(1 - \rho_m)P_t \varphi_m}{(P_t \varphi_m A_m + (1 - \varphi_m)P_t B_m)(1 - \rho_m) + \sigma^2_m})
$$

$$
-\lambda(\epsilon(P_t \varphi_m(1 - \tau) + p_u \tau) + P_c,m), \forall m
$$

(23)

$$
h_m(P_t, \varphi_m) = (1 - \tau)\ln(1 + \frac{C_m P_t \varphi_m}{(1 - \varphi_m)D_m P_t + \sigma^2_m}), \forall m
$$

(24)

Finally, we use the difference of convex functions algorithm (DCA) from References [14,26]. $P_3$ is as follows:

$$
P_3 : \max_{P_t, \varphi_m, t} t
$$

s.t. $C_1, C_2, C_3, C_4$

$$
C_5 : t \leq f_m(P_t, \varphi_m) - h_m(P_t, \varphi_m), \forall m
$$

(25)
In Equation (25), $C_5$ is the difference between two concave functions, which can be effectively solved by sequential convex programming. At step $n$, we get an iterative power allocation. We use first-order Taylor expansion $h_m(P_t, \varphi_m)$

$$h_m(P_t, \varphi_m) = h_m(P_t^n, \varphi_m^n) + \frac{\partial h_m(P_t^n, \varphi_m^n)}{\partial P_t^n}(P_t - P_t^n) + \frac{\partial h_m(P_t^n, \varphi_m^n)}{\partial \varphi_m^n}(\varphi_m - \varphi_m^n), \forall m$$

(26)

We further transform $P_3$ into

$$P_4: \max_{P_t, \varphi_m} t$$

s.t. $C_1, C_2, C_3, C_4$

$$C_5: t \leq f_m(P_t, \varphi_m) - (h_m(P_t^n, \varphi_m^n) + \frac{\partial h_m(P_t^n, \varphi_m^n)}{\partial P_t^n}(P_t - P_t^n) + \frac{\partial h_m(P_t^n, \varphi_m^n)}{\partial \varphi_m^n}(\varphi_m - \varphi_m^n)), \forall m$$

(27)

$P_4$ now is a smooth and standard convex optimization problem, and thus, it can be efficiently solved by successive convex approximation (SCA) method [15].

Up till now, the convex programming $P_4$ is capable of successively approximating the solution of the original SEE optimization problem. We will employ the bisection method in one-dimension to update $\lambda$

$$F(\lambda) = R_m^e(P_t^e, \varphi_m^e, \rho_m^e) - R_{c,m}^e(P_t^e, \varphi_m^e) - \lambda(\varepsilon(P_t^e, \varphi_m^e(1 - \tau) + p_u \tau) + P_{c,m})$$

(28)

where $\rho_m^e$ is the optimal values of $\rho_m$ in Equation (22) and where $P_t^e$ and $\varphi_m^e$ are the optimal values of $P_t$ and $\varphi_m$ from Algorithm 1.

**Algorithm 1** SCA algorithm for solving Equation (26)

**Initialization**

Set $n = 0$ and the tolerance $0 < \zeta < 1$.

Set $\varphi_m^n = 0, P_t^n$, calculate $F^0 = \min_m [f_m(\varphi_m^n, P_t^n) - h_m(\varphi_m^n, P_t^n)]$

**repeat**

Solve (27) to obtain $P_t^n$ and $\varphi_m^n$

Set $n = n + 1$, and $P_t^n = P_t^e$ and $\varphi_m^n = \varphi_m^e$

Calculate $F^n = \min_m [f_m(\varphi_m^n, P_t^n) - h_m(\varphi_m^n, P_t^n)]$

**until**

$F^n - F^{n-1} < \zeta$

Based on the above discussion, we propose a SERA algorithm for the max–min SEE in massive MIMO systems by Algorithm 2.

Then, we characterize the computational complexity of the proposed algorithm to get a better insight into the computational complexity of the SERA algorithm. The SCA method complexity is $O(I K^3 \log \frac{1}{\varepsilon})$ [27]; $\varepsilon$ is the convergence precision, and $I$ denotes the value of iterations. Therefore, the total computational complexity of the SERA algorithm is about $O(I K^3 \log \frac{1}{\varepsilon})$, and $I$ is the length of the value.
Algorithm 2 SERA algorithm for the min user’ SEE maximization.

Initialization \( N, K, \tau, \epsilon, \eta, \sigma^2, P_{\text{max}}, \varphi^0_m, \) for \( m = 1, \ldots, K. \) SEE initial value \( \lambda_{\text{min}}, \lambda_{\text{max}}, \) tolerance \( 0 < \zeta \ll 1, P^0_m, \varphi^0_m, \) iteration index \( i = 0, \) the maximum iteration number \( T_{\text{max}}. \)

repeat
Set \( \lambda^i = \frac{\lambda_{\text{max}} + \lambda_{\text{min}}}{2} \)
\( F_{\text{min}}^i, F_{\text{max}}^i = \frac{1}{2} \)
Solve (28) for given \( \lambda^i \) and obtain the \( P^i_t \) and \( \varphi^i_m \) using SCA method.
if \( (|F(\lambda^i)| = \min_m (\mathcal{R}_m(P^i_t, \varphi^i_m) - \mathcal{R}_e_m(P^i_t, \varphi^i_m) - \lambda^i (\epsilon (P^i_t \varphi^i_m (1 - \tau) + p_u \tau) + P_{\text{c},m})]) < \zeta \) then
\( \varphi^* = \varphi^i_m, P^*_t = P^i_t, \lambda^* = \min_m \mathcal{R}_m(P^*_t, \varphi^*_m) - \mathcal{R}_e_m(P^*_t, \varphi^*_m) \)
else if \( F(\lambda^i) < 0 \) then
\( \lambda_{\text{max}} = \lambda^i \)
else
\( \lambda_{\text{min}} = \lambda^i \)
end
\( i = i + 1 \)
until \( i > T_{\text{max}} \)

4. Simulation Results

In this part, simulation results are presented to show the effectiveness of the proposed algorithm. The simulation parameters are given as follows. The number of users is \( K = 4. \) The coordinates of BS are \((40, 0)\) m; the users are randomly distributed in the rectangular area \([-20, 20] \times [-20, 20]\) m. The path loss model is adopted with path loss exponent \( r = 3.3. \) The background noise is \( \sigma^2_m = \sigma^2_e = \sigma^2_z = -90 \) dBm [14], and the user fixed circuit power loss is \( P_{\text{c},m} = 5 \) dBm.

Figure 2 compares the minimum SEE of each algorithm for different \( P_{\text{max}}. \) When the transmit power \( P_{\text{max}} \) of the BS increases, the minimum SEE obtained by the min user’ SEE maximization and users’ system SEE maximization gradually increases to remain unchanged; this is because the increase of the BS transmit power resistant against eavesdroppers achieves a balance in the information rates leaked into the eavesdropper. Moreover, as can be seen from the secure rate maximization algorithm, with the increase of power, the ultimate SEE decreases. Therefore, it shows the stability of the SERA algorithm.

![Figure 2. Minimum SEE for different BS transmit power.](image-url)
Figure 3 shows the minimum SEE of the three algorithms for the different number of BS antennas. The minimum SEE is monotone increasing with the antenna number of BS for three algorithms. This is because of the array gain due to the multi-antenna diversity. As the number of BS antennas increases, the secure rate of three algorithms increases faster than the power consumption. In addition, it can be observed that the minimum SEE performance of the SERA algorithm is better than the other two algorithms.

![Figure 3. Minimum SEE under a different number of BS antennas.](image)

In Figure 4, we show the convergence performance of the different $P_{\text{max}}$. It can be seen that the SERA algorithm can quickly converge. In the three cases under consideration, the number of iterations that the algorithm converges to the optimal value is within four times. When the number of BS antennas is $N = 100$, the numerical results reveal that the performance of the $P_{\text{max}} = 30$ dBm has increased about 20.1% and 41.5% more than $P_{\text{max}} = 25$ dBm and $P_{\text{max}} = 15$ dBm.

![Figure 4. The convergence performance of the different BS transmit powers.](image)
In Figure 5, we show the minimum SEE versus the eavesdropper transmit power under different algorithms. When the number of BS antennas is $N = 100$ and BS transmit power $P_{\text{max}} = 30$ dBm, as the eavesdropper transmit power increases, the minimum SEE gradually decreases. From Equation (4), increasing the eavesdropper transmit power impacts the channel estimation. This leads to a decrease in the SEE and an increase in the information rates leaked into the eavesdropper.

![Figure 5](image)

**Figure 5.** The minimum SEE versus the eavesdropper transmit power.

Figure 6 shows the minimum SEE of the three algorithms for a different number of users. The minimum SEE is monotone decreasing with the number of users. The minimum SEE obtained by SERA algorithms is about 3% and 62.2% compared with the users’ system SEE maximization and secure rate maximization algorithm when the number of users $K$ is 4 and BS maximum transmit power is $P_{\text{max}} = 30$ dBm. In addition, it can be observed that the minimum SEE performance of the SERA algorithm is better than the other two algorithms.

![Figure 6](image)

**Figure 6.** Minimum SEE under a different number of users.
5. Conclusions

In this paper, we consider downlink massive MIMO systems employing AN auxiliary communication for the physical layer. The users use the energy harvested by the previous time block for channel estimation. At the BS, the power splitting ratio is used to reasonably allocate the information transmission power and the AN transmission power; the eavesdropper’s eavesdropping ability is reduced while ensuring the integrity of the secret information transmission. The non-convex SEE maximization problem is first converted into a series of parameter optimization subproblems, which is then solved by the SCA method. A SERA algorithm with joint power splitting ratio and BS transmitted power allocation is proposed to max–min SEE of the systems. Simulation results show that the proposed algorithm can provide higher SEE compared with other benchmark algorithms.

Author Contributions: Z.W. conceived and designed the system model; X.W. analyzed the data; Z.F. contributed the formal analysis; X.Y. performed the simulation and wrote the paper. All authors have read and agreed to the published version of the manuscript.

Acknowledgments: This work was partially supported by the National Natural Science Foundation of China (No.61701064), Chongqing Natural Science Foundation (No.cstc2019jcyj-msxmX0264), and Scientific and Technological Research Program of Chongqing Municipal Education Commission (No.KJ1600424).

Conflicts of Interest: The authors declare no conflict of interest.

References
1. Wu, Y.; Khisti, A.; Xiao, C.; Caire, G.; Wong, K.; Gao, X. A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead. *IEEE J. Sel. Areas Commun.* 2018, 36, 679–695.
2. Chen, X.; Ng, D.W.K.; Chen, H. Secrecy wireless information and power transfer: Challenges and opportunities. *IEEE Wirel. Commun.* 2016, 23, 54–61.
3. Wu, Q.; Li, G.Y.; Chen, W.; Ng, D.W.K.; Schober, R. An Overview of Sustainable Green 5G Networks. *IEEE Wirel. Commun.* 2017, 24, 72–80.
4. Zhu, J.; Ng, D.W.K.; Wang, N.; Schober, R.; Bhargava, V.K. Analysis and Design of Secure Massive MIMO Systems in the Presence of Hardware Impairments. *IEEE Trans. Wirel. Commun.* 2017, 16, 2001–2016.
5. Timilsina, S.; Baduge, G.A.A.; Schaefer, R.F. Secure Communication in Spectrum-Sharing Massive MIMO Systems with Active Eavesdropping. *IEEE Trans. Commun.* 2018, 4, 390–405.
6. Zhu, Z.; Chu, Z.; Zhou, F.; Niu, H.; Wang, Z.; Lee, I. Secure Beamforming Designs for Secrecy MIMO SWIPT Systems. *IEEE Wirel. Commun. Lett.* 2018, 7, 424–427.
7. Sheng, Z.; Tuan, H.D.; Nasir, A.A.; Duong, T.Q.; Poor, H.V. Power Allocation for Energy Efficiency and Secrecy of Wireless Interference Networks. *IEEE Trans. Wirel. Commun.* 2018, 17, 3737–3751.
8. Du, C.; Chen, X.; Lei, L. Energy-efficient optimisation for secrecy wireless information and power transfer in massive MIMO relaying systems. *IET Commun.* 2018, 11, 10–16.
9. He, J.; Li, L.; Zhang, H.; Chen, W.; Yang, L.; Han, Z. Multi-Pair Bidirectional Relaying with Full-Duplex Massive MIMO Experiencing Channel Aging. In Proceedings of the IEEE GLOBECOM, Singapore, 4–8 December 2017; pp. 1–6.
10. Timilsina, S.; Amarasuriya, G. Secure Communication in Relay-Assisted Massive MIMO Downlink. In Proceedings of the IEEE GLOBECOM, Singapore, 4–8 December 2017; pp. 1–7.
11. Zhu, J.; Li, Y.; Wang, N.; Xu, W. Wireless Information and Power Transfer in Secure Massive MIMO Downlink with Phase Noise. *IEEE Wirel. Commun. Lett.* 2017, 6, 298–301.
12. Wu, Q.; Zhang, G.; Ng, D.W.K.; Chen, W.; Schober, R. Generalized Wireless-Powered Communications: When to Activate Wireless Power Transfer? *IEEE Trans. Veh. Technol.* 2019, 68, 8243–8248.
13. Song, H.; Wen, H.; Hu, L.; Chen, Y.; Liao, R. Optimal Power Allocation for Secrecy Rate Maximization in Broadcast Wiretap Channels. *IEEE Wirel. Commun. Lett.* 2018, 7, 514–517.
14. Chen, Y.; Wang, L.; Ma, M.; Jiao, B. Power Allocation for Full-Duplex Relay Networks: Secure Energy Efficiency Optimization. In Proceedings of the IEEE GLOBECOM, Washington, DC, USA, 4–8 December 2016; pp. 1–6.
15. Zhou, X.; Cai, W.; Chen, R. Secrecy energy efficiency optimization for MISO SWIPT systems. *Phys Commun.* 2018, 28, 19–27.
16. Alageli, M.; Ikhlef, A.; Chambers, J. SWIPT massive mimo systems with active eavesdropping. *IEEE J. Sel. Areas Commun.* 2019, 37, 233–247.

17. Chakravarty, J.; Johnson, O.; Piechocki, R. A Convex Scheme for the Secrecy Capacity of a MIMOWiretap Channel with a Single Antenna Eavesdropper. In Proceedings of the IEEE ICC, Shanghai, China, 20–24 May 2019; pp. 1–5.

18. Xu, S.; Han, S.; Du, Y.; Meng, W.; He, L.; Zhang, C. AN-Aided Secure Beamforming Design for MISO Wiretap Channels. *IEEE Commun. Lett.* 2019, 4, 628–631.

19. Schaefer, R.F.; Amarasuriya, G.; Poor, H.V. Physical layer security in massive MIMO systems. In Proceedings of the Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, USA, 29 October–1 November 2017; pp. 3–8.

20. Tan, F.; Lv, T.; Huang, P. Global Energy Efficiency Optimization for Wireless-Powered Massive MIMO Aided Multiway AF Relay Networks. *IEEE Trans. Signal Process.* 2018, 9, 2384–2398.

21. Li, B.; Li, L.; He, D.; Chen, J.; Kong, W. Energy-efficient secure transmission in massive MIMO systems with pilot attack. In Proceedings of the IC-WCSP, Yangzhou, China, 13–15 October 2016; pp. 1–5.

22. Zhu, J.; Schober, R.; Bhargava, V.K. Linear Precoding of Data and Artificial Noise in Secure Massive MIMO Systems. *IEEE Trans. Wirel. Commun.* 2016, 15, 2245–2261.

23. Khan, T.A.; Yazdan, A.; Heath, R.W. Optimization of Power Transfer Efficiency and Energy Efficiency for Wireless-Powered Systems with Massive MIMO. *IEEE Trans. Wirel. Commun.* 2018, 17, 7159–7172.

24. Zappone, A.; Jorswieck, E. Energy efficiency in wireless networks via fractional programming theory. *Found. Trends Commun. Inf. Theory* 2015, 11, 185–396.

25. Li, Y.; Sheng, M.; Wang, X.; Zhang, Y.; Wen, J. Max Min Energy Efficient Power Allocation in Interference Limited Wireless Networks. *IEEE Trans. Veh. Technol.* 2015, 64, 4321–4326.

26. Tran, T.T.; Thi, H.A.L.; Dinh, T.P. DC Programming and DCA for Enhancing Physical Layer Security via Cooperative Jamming. *Comput. Oper. Res.* 2016, 87, 235–244.

27. Nesterov, Y.; Nemirovskii, A. *Interior-Point Polynomial Algorithms in Convex Programming*; Studies in Applied Mathematics; Siam: Philadelphia, PA, USA, 1994.

© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).