Research Article

Power Allocation for Reducing PAPR of Artificial-Noise-Aided Secure Communication System

Tao Hong and Geng-xin Zhang

College of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

Correspondence should be addressed to Tao Hong; hongt@njupt.edu.cn

Received 5 July 2019; Revised 2 June 2020; Accepted 9 June 2020; Published 18 July 2020

Academic Editor: Adrian Kliks

Copyright © 2020 Tao Hong and Geng-xin Zhang. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The research of improving the secrecy capacity (SC) of wireless communication system using artificial noise (AN) is one of the classic models in the field of physical layer security communication. In this paper, we consider the peak-to-average power ratio (PAPR) problem in this AN-aided model. A power allocation algorithm for AN subspaces is proposed to solve the nonconvex optimization problem of PAPR. This algorithm utilizes a series of convex optimization problems to relax the nonconvex optimization problem in a convex way based on fractional programming, difference of convex (DC) functions programming, and nonconvex quadratic equality constraint relaxation. Furthermore, we also derive the SC of the proposed signal under the condition of the AN-aided model with a finite alphabet and the nonlinear high-power amplifiers (HPAs). Simulation results show that the proposed algorithm reduces the PAPR value of transmit signal to improve the efficiency of HPA compared with benchmark AN-aided secure communication signals in the multiple-input single-output (MISO) model.

1. Introduction

With the rapid development of wireless communication technology, an ever-increasing amount of sensitive data (e.g., private information and commercially confidential data) is transmitted over wireless networks. However, the broadcasting nature of the wireless communication medium makes the information particularly vulnerable to malicious interception. Currently, encryption techniques are used to guarantee confidential information without considering the physical properties of the wireless communication medium. Due to the development of computing techniques (e.g., quantum computing and cloud computing), these classic security solutions are becoming ever more challenging. Considering the physical properties of the wireless communication medium, the recently developed physical layer security (PLS) techniques based on information theory can guarantee secure transmission regardless of the eavesdropper’s computational capability. As such, PLS techniques have drawn a lot of attention recently from information theory to security engineering by the research community [1–5].

The idea of PLS is to add structured redundancy in the transmit signal such that the legitimate user can correctly decode the confidential information, but the eavesdroppers cannot retrieve almost nothing from their observations [6–9]. To make PLS viable, we usually need the legitimate user’s channel condition to be better than the eavesdroppers’. However, this assumption may not be always possible in practice. A more active approach is to send artificially generated noise to interfere the eavesdroppers’ channel. This notion of using artificial noise (AN) to enhance PLS was first proposed by Negi and Goel in [10] and has received much attention in recent studies. In [11], Zhou derived a closed-form expression for the achievable secrecy rate with the Gaussian input, based on which the power allocation (PA) between the information signal and the AN was optimized. It was shown that equal power allocation is a near-optimal strategy in terms of maximizing the secrecy rate. Instead of transmitting AN isotropically, Li and Ma in [12] considered
joint optimization of the covariance matrices of the information signal and the AN for secrecy rate optimization. It was shown that transmit beamforming is optimal for secrecy rate maximization, which has been proved without using AN in [13]. Besides transmitting AN by Alice, a full-duplex Bob can also transmit AN in order to create interference to Eve, and this strategy is highly desirable in some specific practical scenarios (e.g., where Eve is close to Bob but far from Alice) [14]. To solve the problem of channel estimation, Yan in [15] proposed a new channel training (CT) scheme for this full-duplex AN-aided secure transmission in the receiver-side to prevent an eavesdropper from estimating the jamming channel from the receiver to the eavesdropper. Yang considered a practical transmission scheme (e.g., on-off transmission) with AN in [16] and optimized the system parameters to maximize the effective secrecy rate. In [17], Yan examined the secrecy performance of three typical artificial-noise-aided secure transmission schemes, namely, the partially adaptive, fully adaptive, and on-off schemes. A new analysis method was proposed to facilitate the optimization of the PA between the information signal and the AN. Liu in [18] developed an analytical framework to characterize the secrecy rate of the AN scheme as a function of the number of antennas in each terminal. In the aforementioned works about AN-aided secure transmission, it was mainly assumed that the multiple transmit antennas are independent. However, this assumption is not always held. In many practical scenarios, correlation exists among the multiple antennas at one transceiver due to limited separation between antenna elements or poor scattering conditions. In [19], Yan examined the impact of transmitter-side correlation on the AN-aided secure transmission and designed a correlation-based power allocation (CPA) for AN to optimize the minimum secrecy outage probability. In [20], a new design criterion based on the behavior of the eavesdropper’s bit error probability was proposed instead of the traditional design criterion secrecy capacity (SC). The result showed that the practical secrecy can be guaranteed by the randomly distributed AN with specified power even if the eavesdropper can afford more antennas than Alice. Unlike a single eavesdropper in AN model, Zheng considered a secure transmission model with randomly located eavesdroppers in [21]. An optimization algorithm for PA ratio was designed to minimize the secrecy outage probability. In [22], Liu focused on the location information of each terminal in AN-aided secure communication model. A new location-based secure transmission scheme for wiretap channels was proposed to outline how such an estimate of the eavesdropper’s location can still allow for quantitative assessment of key security metrics. Furthermore, Yan in [23] proposed a new optimal location-based beamforming scheme for the wiretap channel, where both the main channel and the eavesdropper’s channel are subject to Rician fading. The secrecy outage probability of the proposed scheme is derived in an easy-to-evaluate expression that is valid for arbitrary real values of the Rician k-factors.

Meanwhile, massive MIMO is emerging as a key technology enabler for future 5G wireless networks, and thus PLS in the context of massive MIMO is attracting increasing research interests. For example, in [24], the secure downlink transmission in a multicell massive MIMO system was examined, in which two AN shaping matrices were considered. The opportunities and challenges of PLS in the context of massive MIMO were discussed in [25], in which active pilot contamination attacks were revealed to be difficult to detect but of high harmfulness. In [26], Zhu investigated different precoding strategies of data and AN in secure massive MIMO system. This AN-aided scheme was also applied in many different communication systems to guarantee the security performance of private information at the physical layer, such as cognitive radio system [27–29], relay cooperative communication system [30–34], satellite communication system [35–37], information and power transfer system [38–40], and Internet of Things (IoT) network [41].

In [4], Hamamreh made a comprehensive survey for the PLS communication and pointed out the PAPR problem of AN-aided signal as a practical important issue in system design (in Section VI (G)). This problem is similar to the PAPR problem in the traditional OFDM system or high dynamic range ratio (DRR) problem in a pattern synthesis using a phased array [42, 43]. The large PAPR brings disadvantages like an increased complexity of the digital-to-analog (DA) and analog-to-digital (AD) converters and feed network, a reduced efficiency of the high-power amplifier (HPA), and signal distortion in the nonlinear region HPA. Especially in some power limited scenarios, these shortcomings are the key problem of system design, such as satellite communication system and wireless sensor network. In [44], the researchers showed that the famous AN-based technique proposed by Nagi and Goel [10] creates high PAPR in the antenna domain for a multiple-input single-output (MISO) model due to the accidental in-phase addition (superposition) of AN subspaces and the signal subspace compared with traditional OFDM signal in the time domain. To solve this problem, an angle rotation based technique was proposed to reduce the PAPR, while maintaining the SC performance as that of the original AN-aided method. In [45], Hamamreh proposed to either change the distribution of the added AN from Gaussian to uniform in flat fading environments or use an optimized AN that not only avoids PAPR increase but also helps reduce the PAPR of OFDM signal transmission in a single-input single-output (SISO) model.

Different from angle rotation based technique in [44], we utilize the system redundancy of the power allocation for the AN subspaces to reduce the PAPR value of AN-aided secure communication signal. An optimization problem is also formulated to reduce the PAPR value under the constraint of the total power of AN subspaces (maintaining the optimal SC performance with Gaussian input in [11] and finite-alphabet input in [46, 47]). Unfortunately, the formulated optimization problem is a nonconvex problem due to the objective function for PAPR with a fractional form and the constraint for total AN power with a quadratic equality form. To solve this optimization problem, we propose a triple-iterative algorithm to relax the nonconvex optimization problem into a series of convex optimization
problems based on fractional programming, difference of convex (DC) functions programming, and quadratic equality relaxing. Simulation results show that the proposed algorithm reduces the PAPR value of AN-aided signal to improve the efficiency of HPA compared with benchmark AN-aided secure communication signals in the multiple-input single-output (MISO) model.

The rest of this paper is organized as follows. Section 2 details the AN-aided secure transmission model and the optimization problem of PAPR. Section 3 presents the nonconvex relaxing algorithm for the optimization problem. Section 4 assesses the performance of the proposed signal. Section 5 provides numerical results to confirm our analysis and gives useful insights into the impact of PAPR problem. Section 6 draws concluding remarks.

Notations. Scalar variables are denoted by italic symbols. Vectors are denoted by lowercase boldface italic symbols. Matrices are denoted by uppercase boldface italic symbols. \( \mathbb{R} \) and \( \mathbb{C} \) represent the real and complex number fields, respectively. Given a complex number \( x \), \( |x| \), \( \text{Re}(x) \), and \( \text{Im}(x) \) denote the modulus, real part, and imaginary part of \( x \). Given a complex vector \( y \), \( \|y\| \) and \( \|y\|_\infty \) denote the Euclidean norm and infinite norm of \( y \), respectively. Given a matrix \( Z \), \( Z^T \) and \( Z^\dagger \) denote the transpose and conjugate transpose of \( Z \). The \( L \times L \) identity matrix is referred to as \( I_L \) and \( E_h[\cdot] \) denotes expectation of a random variable \( h \).

2. PAPR Problem of AN-Aided Secure Communication System

2.1. System Model. According to [10, 11, 44, 47], we consider the transmission from Alice to Bob in the presence of an eavesdropper Eve as shown in Figure 1. Alice is equipped with multiple transmit antennas \( N_A \) \( (N_A \geq 2) \), while each of Bob and Eve has one receive antenna. Thus, the channel from Alice to Bob or Eve is MISO model. We assume a nonline-of-sight rich scattering environment and, as such, model all channels as uncorrelated Rayleigh fading. It is also assumed that Bob can estimate his channel \( \mathbf{h}_{AB} \) \( \in \mathbb{C}^{N_A \times 1} \) accurately and use a perfect feedback link to inform Alice about his instantaneous CSI. Eve is considered as a passive eavesdropper; the instantaneous CSI \( \mathbf{g}_{AE} \) \( \in \mathbb{C}^{N_A \times 1} \) of Eve is thereby unavailable to Alice. The entries of \( \mathbf{h}_{AB} \) and \( \mathbf{g}_{AE} \) are assumed to be independent and identically distributed (i.i.d.) zero-mean complex Gaussian variables with unit variance.

The authors in [10] introduced the concept of generating artificial noise to guarantee secure transmission. The key idea is outlined as follows. Alice adopts multiple antennas to transmit the information bearing signal into Bob’s channel, at the same time generating the artificial noise into the null space of Bob’s channel. Thus, only Eve’s channel is degraded by the artificial noise. Generally, the null space of Bob’s channel is calculated based on the singular value decomposition (SVD) as \( \mathbf{h}_{AB} = \mathbf{Q}_S\mathbf{W} \), where the weighting matrix \( \mathbf{W} \in \mathbb{C}^{N_A \times N_A} \) for transmit signal is written as

\[
\mathbf{W}_{N_A \times N_A} = [ \mathbf{W}_1, \mathbf{W}_2 ] = [ \mathbf{w}_1 \mathbf{w}_2 \cdots \mathbf{w}_{N_A} ],
\]

where \( \mathbf{w}_n \in \mathbb{C}^{N_A \times 1} \) denote the \( n \)-th column vector of \( \mathbf{W} \), \( \mathbf{w}_1 \) is used for weighting information signal, and \( \mathbf{W}_2 \in \mathbb{C}^{N_A \times (N_A - 1)} \) is used for weighting AN. Thus, the transmit signal \( \mathbf{x} \in \mathbb{C}^{N_A \times 1} \) is expressed as

\[
\mathbf{x} = \begin{bmatrix} x_1, x_2, \ldots, x_{N_A} \end{bmatrix}^T = [ \mathbf{w}_1 \mathbf{w}_2 ] \begin{bmatrix} \sqrt{\alpha P} & 0 \\ 0 & \sqrt{(1 - \alpha) P / N_A - 1} \end{bmatrix} \begin{bmatrix} \mathbf{u} \\ \mathbf{v} \end{bmatrix} = \sqrt{\alpha P} \mathbf{w}_1 \mathbf{u} + \sqrt{(1 - \alpha) P / N_A - 1} \sum_{m=2}^{N_A} \mathbf{w}_m \mathbf{v}_m,
\]

Figure 1: System model of AN-aided secure communication.
where $x_u$ denotes the transmit signal in $u$th antenna, $u \in \{\pm 1\}$ denotes the BPSK modulation symbol, $v = [v_1, v_2, \ldots, v_{N_A-1}]^T \in \mathbb{C}^{(N_A-1)\times 1}$ denotes the AN vector, the entries of $v$ are assumed to be independent and identically distributed (i.i.d.) zero-mean complex Gaussian variables with unit variance, the total transmit power available at Alice is denoted by $P = aP + (1 - a)P$, the PA parameter $a$ is defined as the fraction of the information bearing signal power to the total transmit power, the variance $\sigma^2_v$ of $v$ is set to $aP$, the total variance $\sigma^2_v$ of $v$ is set to $(1-a)P$, and $\Omega = \text{diag}[\theta_1, \theta_2, \ldots, \theta_{N_A-1}] \in \mathbb{R}$ is a PA matrix for AN satisfying $\text{tr}(\Omega) = N_A - 1$. For the convenience of expression, $s_1 = [s_{1,1}, \ldots, s_{1,N_A}]^T \in \mathbb{C}^{N_A \times 1}$ and $s_n = [s_{n,1}, \ldots, s_{n,N_A}]^T \in \mathbb{C}^{N_A \times 1}, n = 2, \ldots, N_A$ denote the information subspace and the AN subspaces, respectively. It is noted that the index number of antenna appeared peak value is random for the $m$th transmit symbol because of random characteristics of AN vector. For the practical multiantenna system, the PA is the same for each antenna. Therefore, we focus on reducing the peak value of the transmit signal in AN-aided secure communication system. The most aforementioned papers about the PA were mainly focused on the PA parameter $\alpha$ to optimize the SC of this AN-aided method, such as [11] for Gaussian input and [47] for finite-alphabet input. Meanwhile, the PA matrix $\Omega$ for AN subspaces was equal distribution $\Omega = \mathbf{1}_{N_A \times 1}$, named EPA strategy, because of Alice without the a priori knowledge of eavesdropper’s channel $\mathbf{g}_A$. It is noted that the power allocation algorithm does not influence the independence of the $N_A - 1$ artificial-noise source. In this paper, we utilize the redundancy of PA matrix $\Omega$ of AN subspaces to optimize the PAPR value for relaxing the linear range requirement of amplifiers.

2.2. PAPR Definition and Optimization Problem Formulation

Following (2), the second term represents a series of summations of AN subspaces, whose value depends on the random AN vector $v$. Therefore, it is possible that peak value appears for the transmit signal $x$ when the AN subspaces $s_1$ and information subspace $s_2$ are added with the same phase. According to the definition in [44], the PAPR value of the transmit signal $x$ by multiple antennas is expressed as

$$
\text{PAPR} = \frac{\max_{n=1,2,\ldots,N_A} |x_n(\alpha, \Omega)|^2}{(1/N_A) \sum_{n=1}^{N_A} |x_n(\alpha, \Omega)|^2} = \frac{\|x(\alpha, \Omega)\|_\infty^2}{(1/N_A)\|x(\alpha, \Omega)\|_\infty^2}.
$$

From (3), it is clear that the PAPR value is associated with two PA parameters, $\alpha$ and $\Omega$. In [47], the authors proposed a gradient search algorithm to obtain the value of PA parameter $\alpha$ for approaching the optimal SC with a finite-alphabet input. Following these results, we focus on reducing the PAPR value of transmit signal to improve the efficiency of HPA by the system redundancy of the PA matrix $\Omega$ in the following optimization problem.

Compared with angle rotation based technique in [44], we formulate an optimization problem for PAPR by the PA matrix $\Omega$ as follows:

$$
\min_{\Omega \in \tau} \text{PAPR} = \max_{1 \leq n \leq N_A} |x_n(\Omega)|^2 = \frac{\|x(\Omega)\|_\infty^2}{(1/N_A)\|x(\Omega)\|_\infty^2},
$$

s.t. $\mathcal{C}_1$: $0 \leq \theta_n \leq \sqrt{(1-a)P}, \quad n = 1, 2, \ldots, N_A - 1$,

$$
\mathcal{C}_2: \sum_{n=1}^{N_A-1} \theta_n^2 = (1-a)P,
$$

where $\tau$ denotes the feasible region of the optimization problem. The physical meaning of the optimization problem (4) is to optimize PAPR value of the transmit vector signal $x = [x_1, x_2, \ldots, x_{N_A}]^T$ under the total power constraint of AN subspaces to approach the optimal SC with a finite-alphabet input. The objective function expressed by a nonconvex fractional form is used to reduce the peak value of the transmit vector signal $x$ from multiple transmit antennas for relaxing the linear range requirement of amplifiers. The convex constraint $\mathcal{C}_1$ denotes the linear range of PA matrix element $\theta_n$, which is used to optimize the PAPR value by allocating different power value to different AN subspace compared with the angle rotation based technique proposed in [44]. The nonconvex constraint $\mathcal{C}_2$ denotes the total power constraint for the AN subspaces to maintain the optimal SC performance. The value of PA parameter $\alpha$ has been addressed in many papers to obtain the optimal SC performance, such as [11] for Gaussian input and [47] for finite-alphabet input. It is noted that the PA parameter $\alpha$ in the constraint $\mathcal{C}_2$ as a constant in this paper is obtained by the gradient search algorithm proposed in [47]. In this paper, we focus on the PA matrix $\Omega$ to relax the linear range requirement of amplifiers. Thus, the formulated problem (4) is a nonconvex optimization problem.

3. Optimization Problem Solution

In this section, we use a series of convex optimization problems to relax the nonconvex optimization problem (4) in a convex way based on fractional programming, difference of convex (DC) functions programming, and non-convex quadratic equality constraint relaxation.

3.1. Fractional Programming

The fractional objective function in (4) can be classified as a nonlinear fractional programming [48]. Without loss of generality, we define the minimum PAPR value $p^*$ and corresponding PA matrix

$$
\Omega^* = \text{diag}[\theta_1^*, \theta_2^*, \ldots, \theta_{N_A-1}^*]
$$

as

$$
p^* = \frac{\|x(\Omega^*)\|_\infty^2}{(1/N_A)\|x(\Omega^*)\|_\infty^2} = \min_{\Omega \in \tau} \frac{\|x(\Omega)\|_\infty^2}{(1/N_A)\|x(\Omega)\|_\infty^2}.
$$

Following (5), we introduce Theorem 1.

**Theorem 1.** The optimal PA strategy $\Omega^* \in \tau$ achieves the minimum PAPR value $p^*$ if and only if
for $\|x(\Omega)\|_\infty > 0$, $(1/N_A)\|x(\Omega)\|^2 \geq 0$.

**Proof.** See Appendix. Theorem 1 reveals that, for an objective function in fractional form, there exists an equivalent objective function in subtractive form, for example, $\|x(\Omega)\|_\infty - p^*(1/N_A)\|x(\Omega)\|^2$ in the considered case. As a result, we can focus on the equivalent optimization problem as follows:

$$\min_{\Omega \in \mathcal{E}} \left\{ f(\Omega) = \|x(\Omega)\|_\infty^2 - p^* \frac{1}{N_A} \|x(\Omega)\|^2 \right\},$$

s.t. $\mathcal{E}_1, \mathcal{E}_2$.  

For solving the optimization problem (6), we employ an iterative algorithm (known as the Dinkelbach method [49]) via the equivalent optimization problem (7). The iterative algorithm is summarized in Algorithm 1 as follows.

In the following subsection, we will focus on the solution to the main loop problem (7) in Algorithm 1.

### 3.2. DC Programming

In the optimization problem (7), the objective function is expressed by a difference of two functions forms. According to DC programming [50], this nonconvex objective function can be replaced by its convex majorant form as shown in the following equation:

$$\min_{\Omega \in \mathcal{E}} \left\{ \tilde{f}(\rho', \Omega) = L_1(\Omega) - L_2(\rho', \Omega') - \langle \nabla L_2(\rho', \Omega'), \Omega - \Omega' \rangle \right\},$$

s.t. $\mathcal{E}_1, \mathcal{E}_2$,  

where $\Omega'$ denotes the $(j-1)$th solution in DC programming, $\nabla (1/N_A)\|x(\Omega')\|^2$ denotes the gradient function at the point $\Omega'$, and $\langle \cdot, \cdot \rangle$ denotes the inner product of vectors. Following (2) and (8), we can obtain

$$\nabla \frac{1}{N_A} \|x(\Omega')\|^2 = \left( \frac{\partial (1/N_A)\|x(\Omega')\|^2}{\partial \theta_1}, \ldots, \frac{\partial (1/N_A)\|x(\Omega')\|^2}{\partial \theta_{N_A-1}} \right),$$

where $\frac{\partial (1/N_A)\|x(\Omega')\|^2}{\partial \theta_n}, n = 1, 2, \ldots, N_A - 1$ is expressed as

$$\frac{\partial (1/N_A)\|x(\Omega')\|^2}{\partial \theta_n} = \frac{\partial}{\partial \theta_n} \left[ \Re (x(\Omega'))^2 + \Im (x(\Omega'))^2 \right]$$

$$= \Re \left( 2x(\Omega') + \sqrt{\frac{(1 - \alpha)P}{N_A - 1}} w_n v_n \right) + \Im \left( 2x(\Omega') + \sqrt{\frac{(1 - \alpha)P}{N_A - 1}} w_n v_n \right).$$

The iterative algorithm for solving the nonconvex optimization problem (7) is summarized in Algorithm 2 as follows.

This iterative algorithm relies on the fact that the term $-L_2(\rho', \Omega)$ in the objective function of (7) is replaced by its convex majorant $-L_2(\rho', \Omega') - \langle \nabla L_2(\rho', \Omega'), \Omega - \Omega' \rangle$ in (8). The objective function in (8) is solved iteratively to approach the optimal solution. It should be noted that there is no guarantee that Algorithm 2 will return a global optimum of a DC problem. However, there exist related branch-and-bound approaches based on outer approximations, which are indeed globally optimal [51]. The provable convergence to a global optimum of these methods is accompanied though with an increase in computational complexity.
the optimization problem (8) as

Following (4), the nonconvex constraint \( \zeta \) was solved by fractional programming in subsection 3.1 and DC programming in subsection 3.2. In this subsection, we will focus on the solution method for nonconvex constraint \( \mathcal{C}_2 \). Following (4), the nonconvex constraint \( \mathcal{C}_2 \) is transformed as

\[
\mathcal{C}_2: \sum_{n=1}^{N-1} \theta_n^2 - (1 - \alpha)P \leq \zeta, \tag{11}
\]

where \( \zeta \) denotes infinitely small quantity. To relax this nonconvex constraint, the classic approach in the field of array pattern synthesis [52] is to utilize a sequence of linear convex optimizations to approximate the original optimization problem. Inspired by this classic approach, we define an iteration variable \( u_n, n = 1, 2, \ldots, N - 1 \) to transform the optimization problem (8) as

\[
\min_{\Omega} \left\{ \tilde{f}(p', \Omega) = L_1(\Omega) - L_2(p', \Omega') - \left\langle \nabla L_2(p', \Omega), \Omega - \Omega' \right\rangle \right\}, \tag{12}
\]

where \( u_n \) denotes the iteration variable in the \( k \)th iterative process, \( \mathcal{C}_2 \) denotes the transform constraint, and \( \Omega \) denotes the transform feasible region. The iterative algorithm for solving the nonconvex constraint in (12) is summarized in Algorithm 3 as follows.

The core idea of the algorithm is described as follows: First, a reasonable starting point for Algorithm 3 is \( u_n^0 = \sqrt{(1 - \alpha)P/(N - 1)} \). Then, \( \Omega^k \) is computed by solving the optimization problem (12). The step to the \( (k + 1) \)th iteration variable \( u_n^{k+1} \) is an "averaging" or "smoothing" operation to ensure that asymptotically the difference between \( u_n^k \) and \( \theta_n^k \) vanishes. Indeed, at the first iteration \( u_n^{k+1} \) is set to \( 0.7\theta_n^k + 0.3u_n^k \), and along the iterations, this averaging is modified with \( \chi \) to approximate \( 0.5\theta_n^k + 0.5u_n^k \). Finally, the optimal PA strategy is obtained when the difference value between \( k \)th PAPR value and \((k+1)\)th PAPR value is less than the maximum tolerance \( \eta \). The convergence of Algorithm 3 is shown in [53].

3.3. Nonconvex Constraint Relaxing. The nonconvex objective function in the original optimization problem (4) is solved by fractional programming in subsection 3.1 and DC programming in subsection 3.2. In this subsection, we will focus on the solution method for nonconvex constraint \( \mathcal{C}_2 \). Following (4), the nonconvex constraint \( \mathcal{C}_2 \) is transformed as

\[
\mathcal{C}_2: \sum_{n=1}^{N-1} \theta_n^2 - (1 - \alpha)P \leq \zeta, \tag{11}
\]

where \( \zeta \) denotes a given convergence precision. The core idea of the algorithm is described as follows: First, a reasonable starting point for Algorithm 3 is \( u_n^0 = \sqrt{(1 - \alpha)P/(N - 1)} \). Then, \( \Omega^k \) is computed by solving the optimization problem (12). The step to the \( (k + 1) \)th iteration variable \( u_n^{k+1} \) is an "averaging" or "smoothing" operation to ensure that asymptotically the difference between \( u_n^k \) and \( \theta_n^k \) vanishes. Indeed, at the first iteration \( u_n^{k+1} \) is set to \( 0.7\theta_n^k + 0.3u_n^k \), and along the iterations, this averaging is modified with \( \chi \) to approximate \( 0.5\theta_n^k + 0.5u_n^k \). Finally, the optimal PA strategy is obtained when the difference value between \( k \)th PAPR value and \((k+1)\)th PAPR value is less than the maximum tolerance \( \eta \). The convergence of Algorithm 3 is shown in [53].

3.4. Summary of the Proposed Algorithm. We formulated a nonconvex optimization problem (4) to solve the PAPR problem of AN-aided secure communication signal. To solve this nonconvex optimization problem, we use a series of convex optimization problems to approximate the optimal solution. The triple-iterative algorithm is summarized in Algorithm 4.

The parameters transmission diagram of the proposed algorithm is shown in Figure 2. The complexity of the proposed algorithm depends on the solution method of the convex optimization problem (12). According to the fast gradient method in [54], the complexity of a convex problem is \( O(\min\{\sqrt{\psi/\rho} \ln(1/\gamma), \sqrt{\psi/\gamma}\}) \), where \( \psi \geq 0 \) is a Lipschitz constant to guarantee that the gradient of objective function satisfies the Lipschitz condition, \( \rho \) denotes the convexity parameter, and \( \gamma \) denotes a given convergence precision. The proposed algorithm in Algorithm 3 contains triple loops with the loop times \( N_p, N_\delta, \) and \( N_x \) for achieving the given convergence precisions \( \eta, \delta, \) and \( \epsilon \), respectively. Therefore, the proposed algorithm has a polynomial time complexity as follows:

\[
O\left( \min\left\{ \frac{\psi}{\rho} \ln\left( \frac{1}{\gamma} \right), \frac{\psi}{\gamma} \right\} \times N_p \times N_\delta \times N_x \right). \tag{13}
\]

4. Performance Assessment

To assess the performance of proposed signal, we establish two metrics: one is input back-off (IBO) of nonlinear HPA
(1) Initialize the iteration variable $u_k^0 = \sqrt{1 - \alpha} P_0 (N_A - 1), n = 1, \ldots, N_A - 1, \beta^0 = 0.2$, iteration step length $\chi = 0.02$, the maximum tolerance $\eta$, and the iteration index $k = 1$;

(2) **Repeat** [Main Loop]
   Solve the problem (12) for a given $\Omega^i$ to obtain $\Omega^i$, the PAPR value $p^*$, and the maximum tolerance $\varepsilon$ and the iteration index $i$;

(3) Update the iteration parameters:
   \[ u_k^{i-1} \leftarrow (0.5 + \beta^i-1) \theta^i_n + (0.5 - \beta^i-1) u_k^{i-1}; \]
   \[ \beta^i \leftarrow \beta^i - \chi, \text{ and } k \leftarrow k + 1; \]
   (5) **Until** $|f(p^i, \Omega^i) - f(p^*', \Omega^*)| \leq \eta$;

(6) **Return** $\Omega^i, \theta^i_n, n = 1, \ldots, N_A - 1$ (back to the step 3 in DC programming).

**Algorithm 3:** Iterative algorithm for nonconvex constraint.

Input: transmit antenna number $N_A$, legal channel $h_{AB}$, PA parameter $\alpha$ for different SNR values (according to reference [47]), modulation symbol $u$ with a finite alphabet, AN vector $v$; Output: PA matrix $\Omega^*$, optimized PAPR value $p^*$;

1. **Repeat** [Main Loop]
2. Initialize the PA matrix $\Omega^0$, and the iteration index $j$;

3. **Repeat** [Main Loop]
5. Initialize the iteration variable $u_0^i$, $\beta^0$, iteration step length $\chi$, and the iteration index $k$;

7. Solve the optimization problem (12) to obtain $\Omega^i$;

8. Update iteration parameters:
   \[ u_k^{i-1} \leftarrow (0.5 + \beta^i) \theta^i_n + (0.5 - \beta^i) u_k^{i-1}; \]
   \[ \beta^i \leftarrow \beta^i - \chi, \text{ and } k \leftarrow k + 1; \]
   (9) **Until** $|f(p^i, \Omega^i) - f(p^j, \Omega^j)| \leq \eta$;

10. Update the iteration parameters:
    \[ \Omega^i \leftarrow \theta^i_n, n = 1, \ldots, N_A - 1, \text{ and } j \leftarrow j + 1; \]
    (11) **Until** $|f(p^i, \Omega^j) - f(p^i, \Omega^j)| \leq \delta$;

12. Update the iteration parameters:
    \[ \Omega^{i+1} \leftarrow \Omega^i, p^i \leftarrow ||x(p^{i-1}, \Omega^i)||_2 / ||1/N_A||x(p^{i-1}, \Omega^i)||, \text{ and } i \leftarrow i + 1; \]
13. **Until** $||x(\Omega^i)||_2 - p^{i-1} (1/N_A)||x(\Omega^i)||_2 \leq \varepsilon$;
14. **Return** $\Omega^*, p^* = ||x(\Omega^i)||_2 / (1/N_A)||x(\Omega^i)||^2$.

**Algorithm 4:** The triple-iterative algorithm for the optimization problem (4).

**Figure 2:** Parameters transmission of the proposed algorithm.

and the other is SC performance with a finite alphabet. To compare the metrics with the proposed signal, we also consider two benchmark AN-aided signals: one is original signal with EPA strategy $x(\Omega = I_{N_A-1})$ proposed in [47] and the other is angle rotation based technique proposed in [44].

4.1. **Input Back-Off of Nonlinear High-Power Amplifier.** The modeling of nonlinear HPA is assumed as follows. For example, if the HPA input signal is $y(t) = \alpha(t) \exp[j\phi(t)]$, then

\[ y(t) = |y(t)| \exp[j\phi(t)]. \]
then the output signal is
\[ y_{out}(t) = G(\alpha(t))\exp[j\phi(y)t + \Phi(\alpha(t))], \]  
(15)
where \( G(\cdot) \) and \( \Phi(\cdot) \) are known as the AM/AM and AM/PM conversions, respectively. According to the Rapp model, we consider a solid-state power amplifier (SSPA) model as follows:
\[
G(\alpha) = \frac{\alpha_{sat}}{[1 + (\alpha_{sat}/\alpha)^{2q}]^{1/2q}},
\]
(16)
\[
\Phi(\alpha) = 0,
\]
where \( G(\alpha) \) denotes the normalized output signal amplitude, \( \alpha_{sat} \) is the input saturation level, and \( q \) determines the AM/AM sharpness of the saturation region. The AM/PM conversion is assumed to be negligibly small. In practical HPAs, output sharpness parameter is usually set at \( q = 2 \) or \( q = 3 \) [55], and we set \( q = 3 \) in this paper. We also consider the input saturation level \( \alpha_{sat} = \sqrt{1/N_{A}} \) to assess the performance for different transmit antenna number \( N_{A} \), where \( 1 \) denotes the normalized power of transmitter. It is noted that we use the total power with uniform distribution in each RF chain to evaluate PAPR characteristic of the transmit signal. For a given AN-aided signal, we need to adjust the average input power so that the peaks of the transmit signal rarely fall into the nonlinear range of HPA. The input back-off (IBO) is expressed as
\[
\text{IBO} = 10 \log_{10} \left( \frac{\alpha_{sat}^{2}}{E[|\mathbf{x}|^{2}]} \right) \text{ (dB)}.
\]
(17)

Figure 3 shows the normalized AM/AM conversion when \( N_{A} \) equals 8 and signal-to-noise ratio (SNR) equals 30 dB. It is shown that the dynamic amplitude range of the AN-aided signal with proposed strategy is more concentrated compared with both benchmark AN-aided signals. Under the constraint of the normalized transmit power, the IBO value equals 6.25 dB, 2.47 dB, and 0 dB, respectively. It is noted that high IBO value will cause low efficiency of the HPAs.

4.2. Secrecy Capacity Performance with a Finite Alphabet

According to the aforementioned SSPA model, the output signal \( \bar{x}_{n} \) in the \( n \)th transmit antenna can be written as
\[
\bar{x}_{n} = G\left( [x_{n}^{r} | x_{n}^{l}] \right) x_{n} = G\left( [x_{n}^{r} | x_{n}^{l}] \right) x_{n}^{r} + \sum_{n=2}^{N_{A}} G\left( [x_{n}^{r} | x_{n}^{l}] \right) x_{n}^{r} = A_{n}x_{n}^{r} + A_{n}x_{n}^{l}.
\]
(18)

After passing the HPAs, the information space \( \bar{s}_{1} \), the AN spaces \( \bar{n}_{1} \), and the transmit signal \( \bar{x} \) can be denoted by
\[
\bar{s}_{1} = [\bar{s}_{1,1}, \ldots, \bar{s}_{1,N_{A}}]^{T}, \quad \bar{n}_{1} = [\bar{n}_{2,1}, \ldots, \bar{n}_{2,N_{A}}]^{T}, \quad \bar{x} = [\bar{x}_{1}, \ldots, \bar{x}_{N_{A}}]^{T},
\]
respectively. We consider that the modulation symbol \( u \) belongs to a symbol set \( \Lambda \) with \( M \) modulation symbols. In [47], a gradient search algorithm was proposed to approximate the optimal value of PA parameter \( a \) in different SNR values. Following this conclusion, we will analyze the SC performance when the transmitter is equipped with the nonlinear HPAs in the following part. Based on (18), the transmit signal \( \bar{x} \) is affected by two factors: one is the orthogonal between the AN subspaces and the legal channel \( h_{AB} \) in the second term and the other is the capacity of the legal channel in the first term. For the transmit signal \( \bar{x} \), the receive signals of Bob and Eve can be written as follows:
\[
\tilde{y}_{\text{Bob}} = h_{AB}\bar{x} + v_{b} = h_{AB}\bar{s}_{1} + h_{AB}\left( \sum_{n=2}^{N_{A}} \bar{n}_{n} \right) + v_{b},
\]
\[
(19a)
\]
\[
\tilde{y}_{\text{Eve}} = g_{AE}\bar{x} + v_{e} = g_{AE}\bar{s}_{1} + g_{AE}\left( \sum_{n=2}^{N_{A}} \bar{n}_{n} \right) + v_{e},
\]
\[
(19b)
\]
where \( v_{b} \) and \( v_{e} \) are the AWGN at Bob and Eve satisfying \( E[v_{b}^{2}] = \sigma_{b}^{2} \) and \( E[v_{e}^{2}] = \sigma_{e}^{2} \), respectively, \( \mu_{\text{Bob}} = h_{AB}\left( \sum_{n=2}^{N_{A}} \bar{s}_{n} \right) \) and \( \mu_{\text{Eve}} = g_{AE}\left( \sum_{n=2}^{N_{A}} \bar{n}_{n} \right) \) denote the AN subspaces projecting into the legal channel and wiretap channel, respectively. Thus, the average SNR losses at Bob and Eve are given by
\[
\bar{\Delta}_{\text{Bob}} = E[\mu_{\text{Bob}}^{2}] / \sigma_{b}^{2} - \left( \tilde{y}_{\text{Bob}}^{2}/\sigma_{b}^{2} \right),
\]
\[
(20a)
\]
\[
\bar{\Delta}_{\text{Eve}} = E[\mu_{\text{Eve}}^{2}] / \sigma_{e}^{2} - \left( \tilde{y}_{\text{Eve}}^{2}/\sigma_{e}^{2} \right),
\]
\[
(20b)
\]
Motivated by the AN signal processing method in [56], the interference plus noise at Bob and Eve can be written as
\[
\tilde{y}_{\text{Bob}}^{r} = h_{AB}\left( \sum_{n=2}^{N_{A}} \bar{s}_{n} \right) + v_{b},
\]
\[
(21a)
\]
\[
\tilde{y}_{\text{Eve}}^{r} = g_{AE}\left( \sum_{n=2}^{N_{A}} \bar{s}_{n} \right) + v_{e},
\]
\[
(21b)
\]
which have zero mean and variance.
\[
R_{v_{b}} = h_{AB}\left( \sum_{n=2}^{N_{A}} \bar{s}_{n} \right) G^{\dagger} + \sigma_{b}^{2},
\]
\[
(22a)
\]
\[
R_{v_{e}} = g_{AE}\left( \sum_{n=2}^{N_{A}} \bar{s}_{n} \right) G^{\dagger} + \sigma_{e}^{2},
\]
\[
(22b)
\]
Thus, we can whiten the AN interference term as
\[
\tilde{y}_{\text{Bob}}^{w} = h_{AB}\bar{s}_{1} + v_{b}, \quad \tilde{y}_{\text{Eve}}^{w} = g_{AE}\bar{s}_{1} + v_{e},
\]
\[
(23)
\]
Without affecting the mutual information of the legal channel and wiretap channel, we apply a linear transformation
\[
K_{\text{Bob}} = \sigma_{v} R_{v_{b}}^{-1/2},
\]
\[
K_{\text{Eve}} = \sigma_{v} R_{v_{e}}^{-1/2},
\]
\[
(24)
\]
on \( \widetilde{y}_{\text{Bob}} \) and \( \tilde{y}_{\text{Eve}} \), respectively, to whiten the interference plus noise as follows:
where $\sigma^2_b$ and $\sigma^2_e$ have zero mean and variance $\sigma^2_b$ and $\sigma^2_e$, respectively. Following (24), the values of $K_{\text{Bob}}$ and $K_{\text{Eve}}$ are determined by two factors: one is the AN power projecting into the legal channel or wiretap channel and the other is noise variance of AWGN. Taking $K_{\text{Bob}}$ as example, when $\sigma^2_b$ is much larger than $|\mu_{\text{Bob}}|^2$, its value mainly depends on the noise variance and tends to $\sigma^2_b(\sigma^2_b)^{-1/2} = 1$ (ideal HPAs); when $\sigma^2_b$ has the same order of $|\mu_{\text{Bob}}|^2$, its value depends on these two factors and there appears inflection point of SC performance; when $\sigma^2_b$ is much less than $|\mu_{\text{Bob}}|^2$, its value mainly depends on the ratio of the noise variance to the AN power projecting into the legal channel and represents the decreasing gradient of SC performance.

According to the aforementioned processing method, the mutual information of the legal channel and wiretap channel is written as follows:

\[ \widetilde{y}_{\text{Bob}} = K_{\text{Bob}} h_{\text{AB}} \widetilde{x}_1 + K_{\text{Bob}} v_b = K_{\text{Bob}} h_{\text{AB}} \widetilde{x}_1 + \widetilde{v}_b, \quad (25a) \]
\[ \widetilde{y}_{\text{Eve}} = K_{\text{Eve}} g_{\text{AE}} \widetilde{x}_1 + K_{\text{Eve}} v_e = K_{\text{Eve}} g_{\text{AE}} \widetilde{x}_1 + \widetilde{v}_e, \quad (25b) \]

where $\widetilde{v}_b$ and $\widetilde{v}_e$ are the AN-aided signal with EPA strategy in [47]. (b) AN-aided signal with angle rotation based technique in [44]. (c) AN-aided signal with proposed PA strategy.

\begin{align*}
\text{IBO} & = 6.25\, \text{dB} \\
A_{\text{sat}} & = \sqrt{1/8} = 0.3536 \\
\text{Linear } L(A) & \\
\text{AM/AM } G(A) & \text{ with } q = 3
\end{align*}
Thus, the SC of AN-aided model with the nonlinear HPAs is written as follows:

$$C_{\text{HPA}} = E_{h_{\text{AB}},w} \left[ \max \{0, I(u_m, y_{\text{Bob}}) - I(u_m, y_{\text{Eve}}) \} \right]. \quad (27)$$

Following (21)–(27), the SC value is mainly determined by the parameters $K_{\text{Bob}}$, $K_{\text{Eve}}$, and noise variance $\sigma_b^2$. In Section 5, we will give useful insights into the impact of SC performance.

5. Simulation Results

In this section, we evaluate the system performance through simulations. The simulation conditions are supposed as follows. We consider that the modulation symbol $\alpha$ belongs to a BPSK symbol set with $A = \{ \pm 1 \}$. We focus on the PAPR problem of the transmitter. Thus, we suppose that Bob and Eve have the same noise variance $\sigma_b^2 = \sigma_e^2 = \sigma^2$. We use two HPA models in simulations: one is ideal HPA model with infinite linear range and the other is nonlinear HPA model. The total transmitter power $P$ is normalized as 1. The value of PA parameter $a$ is derived via gradient search algorithm in [47] as a constant value for different SNR values. Monte Carlo simulations with 100 repetitions are used to obtain the average SC performance by equation (27).

5.1. Peak-To-Average Power Ratio Performances. Figure 4 shows the PAPR performance of the AN-aided signal with proposed PA strategy by complementary cumulative distribution function (CCDF) compared with the AN-aided signal with EPA strategy proposed in [47] and AN-aided signal with angle rotation based technique proposed in [44]. The following are found: (1) For the proposed signal in [47], the PAPR performance degrades with the transmit antenna number increasing. When transmit antenna number $N_A$ equals 64, the PAPR value is greater than 10.5 dB with the probability of $10^{-4}$, which is similar to the performance of traditional OFDM signal with 64 subcarriers and BPSK modulation [57]. (2) For the proposed signal in [44], the PAPR value is decreased by 3.8 dB, 4 dB, and 4.2 dB when $N_A$ equals 8, 16, and 64, respectively. (3) For the AN-aided signal with proposed PA strategy, the PAPR value is decreased by 4 dB, 7 dB, and 8.5 dB when $N_A$ equals 8, 16, and 64, respectively. (4) For a fixed transmit antenna number, the PAPR curves for proposed signal in [44, 47] almost coincide for different SNR values. Meanwhile the PAPR reducing performance for the AN-aided signal with proposed PA strategy increases with SNR values because more power of the transmitter is used in AN subspaces to keep the optimal SC performance. The PAPR simulation results reveal that the effect of PAPR reducing by proposed PA strategy is better than the angle rotation based technique proposed in [44] to improve the efficiency of the HPAs because more AN subspaces and transmitter power can be used to adjust the PAPR value.

5.2. Signal-To-Noise Ratio Loss Performances. Figure 5 shows the average SNR loss of AN-aided signals at Bob and Eve. The following are found: (1) At Bob, the SNR loss increases with the transmit signal SNR and transmit antenna number both for EPA strategy in [47] and proposed PA strategy. The gradient of curves for the proposed PA strategy is much smaller than AN-aided signal with EPA strategy. We observe that the performance difference of these two AN-aided signals reaches about 6 dB for $N_A = 8$ and 11 dB for $N_A = 16$ when SNR equals 30 dB. (2) At Eve, the SNR loss almost equals 0 dB and coincides with different SNR values and transmit antennas because the nonlinear characteristic of HPA not only reduces the power of the information subspace but also degrades the interference effect of AN subspaces. This average SNR loss simulation results illustrate that the proposed PA strategy can improve the channel capacity performance with the transmit antenna number increasing. Furthermore, the SC performance is mainly determined by the capacity of legal channel.

5.3. Secrecy Capacity Performances. Figure 6 shows the SC performance of the AN-aided signals when $N_A$ equals 8 and 16, respectively. The key parameter $K_{\text{Bob}}$ is defined by the AN subspaces power projecting into the legal channel $\mu_{\text{Bob}}$. The relationship between $|\mu_{\text{Bob}}|^2$ and $\sigma^2$ determines the inflection point of the SC performance. If $|\mu_{\text{Bob}}|^2$ is much larger than $\sigma^2$, it means that the AN subspaces power projecting into the legal channel plays the main role in the value of $K_{\text{Bob}}$, which
will result in the SC performance degrading obviously. If $|\mu_{Bob}|^2$ is much smaller than $\sigma^2$ in $K_{Bob}$, it means less AN subspaces power projecting into the legal channel, which will result in the SC performance being similar to the AN-aided model with ideal HPA. From the subfigure in (a) and (b), the value of $|\mu_{Bob}|^2$ is reduced by the proposed PA strategy compared with proposed signal in [44, 47]. Therefore, the inflection point will appear later with the transmit signal SNR increasing.

Figure 4: CCDFs of AN-aided signal for different transmit antenna numbers and different SNR values. (a) CCDFs for different transmit antenna numbers when SNR equals 5 dB. (b) CCDFs for different SNR values when the transmit antenna number equals 8.

From Figures 6(a) and 6(b), the following are found: (1) For the AN-aided signal with EPA strategy in [47], the SC performance degrades with the transmit signal SNR increasing when the power of AN subspaces projecting into the legal channel plays the main role in $K_{Bob}$. Furthermore, the SC performance reduces with the transmit antennas increasing, for example, 0.55 bit/s/Hz for $N_A = 8$ and 0.45 bit/s/Hz for $N_A = 16$, almost half of the ideal HPAs scenario at $P/\sigma^2 = 30$ dB. (2) For the AN-aided signal with
Figure 6: The SC performances of AN-aided signals vary with the transmit signal SNR when transmit antenna number equals 8 and 16. (a) SC performance for $N_A = 8$. (b) SC performance for $N_A = 16$.

Our proposed angle rotation based technique in [44], the PAPR reducing algorithm improves the SC performance, for example, 0.86 bit/s/Hz for $N_A = 8$ and 0.90 bit/s/Hz for $N_A = 16$. (3) For the AN-aided signal with the proposed PA strategy, the degradation gradient of SC performance is smooth compared with proposed signal in [44, 47]. Furthermore, the SC performance is similar to the AN-aided model with ideal HPAs by the transmit antenna number increasing, for example, 0.92 bit/s/Hz for $N_A = 8$ and 0.99 bit/s/Hz for $N_A = 16$, almost coinciding with the ideal HPAs scenario at $P/\sigma^2 = 30$ dB. On the assumption of larger transmit antenna numbers, the nonlinear characteristic of HPA does not affect the SC performance of AN-aided signal by the proposed PA strategy because the amplitude of transmit signal is close to uniform distribution. Fortunately, this assumption is beneficial to the SC performance when eavesdropper equips multiple antennas [18].

### 6. Conclusion

In this paper, we have formulated the AN power allocation for PAPR problem of the AN-aided secure communication system as a mixed nonconvex optimization problem. By exploiting the properties of fractional programming, DC programming, and nonconvex constraint relaxing, the considered problem was transformed into an equivalent problem with a tractable solution. An efficient triple-iterative AN power allocation algorithm was derived for minimization of the PAPR value of transmit signal. Compared with the benchmark AN-aided signals, simulation results showed that the proposed algorithm can reduce the PAPR value of the transmit signal to improve the efficiency of HPAs in AN-aided secure communication model.

Interesting topics for future work include studying better algorithm for achieving the transmit signal with low PAPR characteristic, other system redundancy parameters to reduce PAPR value of transmit signal, and the complexity of PAPR reducing algorithm.

### Appendix

**Proof of Theorem 1.** First, we prove the forward implication of Theorem 1. Without loss of generality, we define $p^*$ and $\Omega^*$ as the optimal PAPR and the optimal power allocation strategy of the original objective function in (4), respectively. Then, the optimal PAPR can be expressed as

$$p^* = \frac{\|x(\Omega^*)\|_\infty}{(1/N_A)} \leq \frac{\|x(\Omega)\|_\infty}{(1/N_A)} \quad \forall \Omega \in \tau$$

$$\frac{\|x(\Omega^*)\|_\infty}{(1/N_A)} - p^* \frac{1}{N_A} \|x(\Omega^*)\|_\infty = 0$$

$$\|x(\Omega)\|_\infty - p^* \frac{1}{N_A} \|x(\Omega)\|_\infty \geq 0$$

(A.1)
Therefore, we conclude that $\|x(\Omega)\|_\infty^2 - p^* \left(1/N_A\right) \|x(\Omega)\|^2 = 0$ and it is achievable by power allocation strategy $\Omega^*$. This completes the forward implication.

Next, we prove the converse implication of Theorem 1. For any feasible power allocation strategy $\Omega \in \tau$, we can obtain the following inequality:

$$\|x(\Omega)\|_\infty^2 - p^* \left(1/N_A\right) \|x(\Omega)\|^2 \geq \|x(\Omega^*)\|_\infty^2 - p^* \left(1/N_A\right) \|x(\Omega^*)\|^2 = 0.$$  

(A.2)

The preceding inequality implies

$$\frac{\|x(\Omega)\|_\infty^2}{\left(1/N_A\right) \|x(\Omega)\|^2} \geq p^*, \quad \forall \Omega \in \tau,$$

(A.3)

In other words, the optimal power allocation strategy $\Omega^*$ for the equivalent objective function is also the optimal power allocation strategy for the original objective function. This completes the proof of the converse implication of Theorem 1. In summary, the optimization of the original objective function and the optimization of the equivalent objective function result in the same power allocation strategy.

**Data Availability**

Some or all data, models, and codes generated or used during the study are available in a repository or online in accordance with the funder data retention policies.

**Conflicts of Interest**

The authors declare that they have no conflicts of interest.

**Acknowledgments**

This work was supported in part by the National Natural Science Foundation of China under Grant 91738201, Grant 61971440 and Grant 61302102, and Special Program for Advanced Leading Research of the Jiangsu Province under Grant BK20192002.

**References**

[1] K. Zeng, “Physical layer key generation in wireless networks: challenges and opportunities,” *IEEE Communications Magazine*, vol. 53, no. 6, pp. 33–39, 2015.

[2] W. Mei, Z. Chen, J. Fang, and S. Li, “Physical layer service integration in 5G: potentials and challenges,” *IEEE Access*, vol. 6, pp. 16563–16575, 2018.

[3] N. Yang, L. Wang, G. Gercaci, 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, 2015.

[4] J. M. Hamamreh, H. M. Furqan, and H. Arslan, “Classifications and applications of physical layer security techniques for confidentiality: a comprehensive survey,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1773–1828, 2019.

[5] M. Bloch and J. Barros, *Physical-Layer Security: From Inf. Theory to Security Engineering*, Cambridge University Press, Cambridge, MA, USA, 2011.

[6] C. E. Shannon, “Communication theory of secrecy systems,” *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[7] A. D. Wyner, “The wire-tap channel,” *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[8] I. Caizsar and J. Körner, “Broadcast channels with confidential messages,” *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[9] Y.-B. Liang, H. V. Poor, and S. Shamai, “Secure communication over fading channels,” *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2470–2492, 2008.

[10] S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, 2008.

[11] X. Zhou and M. R. McKay, “Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation,” *IEEE Transactions on Vehicular Technology*, vol. 59, no. 8, pp. 3831–3842, 2010.

[12] Q. Li and W.-K. Ma, “Spatially selective artificial-noise-aided transmit optimization for MISO multi-eves secrecy rate maximization,” *IEEE Transactions on Signal Processing*, vol. 61, no. 10, pp. 2704–2717, 2013.

[13] A. Khisti and G. W. Wornell, “Secure transmission with multiple antennas I: the MISOME wiretap channel,” *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, 2010.

[14] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, “Improving physical layer secrecy using full-duplex jamming receivers,” *IEEE Transactions on Signal Processing*, vol. 61, no. 20, pp. 4962–4974, 2013.

[15] S. Yan, X. Zhou, N. Yang, T. D. Abhayapala, and A. L. Swindlehurst, “Secret channel training to enhance physical layer security with a full-duplex receiver,” *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2788–2800, 2018.

[16] N. Yang, S. Yan, J. Yuan, R. Malaney, R. Subramanian, and I. Land, “Artificial noise: transmission optimization in multi-input single-output wiretap channels,” *IEEE Transactions on Communications*, vol. 63, no. 5, pp. 1771–1783, 2015.

[17] S. Yan, N. Yang, I. Land, R. Malaney, and J. Yuan, “Three artificial-noise-aided secure transmission schemes in wiretap channels,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 4, pp. 3669–3673, 2018.

[18] S. Liu, Y. Hong, and E. Viterbo, “Artificial noise revisited,” *IEEE Transactions on Information Theory*, vol. 61, no. 7, pp. 3901–3911, 2015.

[19] S. Yan, X. Zhou, N. Yang, B. He, and T. D. Abhayapala, “Artificial-noise-aided secure transmission in wiretap channels with transmitter-side correlation,” *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 8286–8297, 2016.

[20] S.-Y. Liu, Y. Hong, and E. Viterbo, “Practical secrecy using artificial noise,” *IEEE Commun. Lett.*, vol. 17, no. 7, pp. 1483–1486, 2013.

[21] T.-X. Zheng, H.-M. Wang, J. Yuan, D. Towsley, and M. H. Lee, “Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers,” *IEEE Transactions on Information Theory*, vol. 63, no. 11, pp. 4347–4362, 2015.

[22] C. Liu, N. Yang, J. Yuan, and R. Malaney, “Location-based secure transmission for wiretap channels,” *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 7, pp. 1458–1470, 2015.
[23] S. Yan and R. Malaney, “Location-based beamforming for enhancing secrecy in wireless networks,” IEEE Transactions on Wireless Communications, vol. 15, no. 4, pp. 2780–2791, 2016.

[24] J. Zhu, R. Scholer, and V. K. Bhargava, “Secure transmission in multiecell massive MIMO systems,” IEEE Transactions on Wireless Communications, vol. 13, no. 9, pp. 4766–4781, 2014.

[25] 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, 2015.

[26] J. Zhu, R. Scholer, 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, 2016.

[27] F. Zhou, Z. Li, J. Cheng, Q. Li, and J. Si, “Robust AN-aided beamforming and power splitting design for secure MISO cognitive radio with SWIPT,” IEEE Transactions on Wireless Communications, vol. 16, no. 4, pp. 2450–2464, 2017.

[28] Y. Deng, L. Wang, S. A. R. Zaidi, J. Yuan, and M. Elkashlan, “Artificial-noise aided secure transmission in large scale spectrum sharing networks,” IEEE Transactions on Communications, vol. 64, no. 5, pp. 2116–2129, 2016.

[29] A. Al-nahari, G. Geraci, M. Al-jamali, M. H. Ahmed, and N. Yang, “Beamforming with artificial noise for secure MISOME cognitive radio transmissions,” IEEE Transactions on Information Forensics and Security, vol. 13, no. 8, pp. 1875–1889, 2018.

[30] X.-J. Ding, T.-C. Song, Y.-L. Zou, X.-S. Chen, and L. Hanzo, “Security-reliability tradeoff analysis of artificial noise aided two-way opportunistic relay selection,” IEEE Transactions on Vehicular Technology, vol. 66, no. 5, pp. 3930–3941, 2017.

[31] Q. Li, Y. Yang, W.-K. Ma, M. Lin, J. Ge, and J. Lin, “Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks,” IEEE Transactions on Signal Processing, vol. 63, no. 1, pp. 206–220, 2015.

[32] H. Guo, Z. Yang, L. Zhang, J. Zhu, and Y. Zou, “Joint cooperative beamforming and jamming for physical-layer security of decode-and-forward relay networks,” IEEE Access, vol. 5, pp. 19620–19630, 2017.

[33] R. Zhao, Y. Huang, W. Wang, and V. K. N. Lau, “Ergodic achievable secrecy rate of multiple-antenna relay systems with cooperative jamming,” IEEE Transactions on Wireless Communications, vol. 15, no. 4, pp. 2537–2551, 2016.

[34] X. Zhou, S. Yan, Q. Wu, J. Lin, and F. Shu, “Robust beamforming design for secure DM-based relay networks with self-sustained jammers,” IEEE Access, vol. 7, pp. 969–983, 2019.

[35] G. Zheng, P.-D. Arapoglou, and B. Ottersten, “Physical layer security in multibeam satellite systems,” IEEE Transactions on Wireless Communications, vol. 11, no. 2, pp. 852–863, 2012.

[36] J. Liu, J. Wang, W. Liu, Q. Wang, and M. Wang, “A novel cooperative physical layer security scheme for satellite downlinks,” Chinese Journal of Electronics, vol. 27, no. 4, pp. 860–865, 2018.

[37] J. Du, C. Jiang, H. Zhang, X. Wang, Y. Ren, and M. Debbah, “Secure satellite-terrestrial transmission over incumbent terrestrial networks via cooperative beamforming,” IEEE Journal on Selected Areas in Communications, vol. 36, no. 7, pp. 1367–1382, 2018.

[38] N. Zhao, Y. Cao, F. R. Yu, Y. Chen, M. Jin, and V. C. M. Leung, “Artificial noise assisted secure interference networks with wireless power transfer,” IEEE Transactions on Vehicular Technology, vol. 67, no. 2, pp. 1087–1098, 2018.

[39] M. Zhang, Y. Liu, and R. Zhang, “Artificial noise aided secrecy information and power transfer in OFDMA systems,” IEEE Transactions on Wireless Communications, vol. 15, no. 4, pp. 3085–3096, 2016.

[40] Y. Peng, Z. Yang, W.-P. Zhu, Q. Li, and B. Lv, “Robust cooperative secure beamforming for simultaneous wireless information and power transfer in amplify-and-forward relay networks,” IEEE Transactions on Vehicular Technology, vol. 66, no. 3, pp. 2354–2366, 2017.

[41] J. Hu, N. Yang, and Y. Cai, “Secure downlink transmission in the Internet of Things: how many antennas are needed?” IEEE Journal on Selected Areas in Communications, vol. 36, no. 7, pp. 1622–1634, 2018.

[42] Z. Xu, Y. Liu, M. Li, and Y. Li, “Linearly polarized shaped power pattern synthesis with dynamic range ratio control for arbitrary antenna arrays,” IEEE Access, vol. 7, pp. 53621–53628, 2019.

[43] X. Fan, J. Liang, Y. Zhang, H. C. So, and X. Zhao, “Shaped power pattern synthesis with minimization of dynamic range ratio,” IEEE Transactions on Antennas and Propagation, vol. 67, no. 5, pp. 3067–3078, 2019.

[44] T. Hong and Z.-P. Li, “Peak-to-average power ratio reduction for an artificial noise aided secure communication system,” in Proceedings of the 2016 3rd International Conference on Information Science and Control Engineering (ICISCE), pp. 1370–1374, Beijing, China, July 2016.

[45] J. M. Hamamreh and H. Arslan, “Joint PHY/MAC layer security design using ARQ with MRC and null-space independent PAPR-aware artificial noise in SISO systems,” IEEE Transactions on Wireless Communications, vol. 17, no. 9, pp. 6190–6204, 2018.

[46] S. R. Aghdam, A. Nooraiepour, and T. M. Duman, “An overview of physical layer security with finite-alphabet signaling,” IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1829–1850, 2019.

[47] X.-R. Liu, D.-T. Ma, J. Xiong, W. Li, and L.-W. Cheng, “Power allocation for AN-aided beamforming design in MISO wiretap channels with finite-alphabet signaling,” in Proce-edings of the 2016 IEEE 84th Vehicular Technology Conference, pp. 1–6, September 2016.

[48] W. Dinkelbach, “On nonlinear fractional programming,” Management Science, vol. 13, no. 7, pp. 492–498, 1967.

[49] S. Schaible, “Fractional programming. II, on Dinkelbach’s algorithm,” Management Science, vol. 22, no. 8, pp. 868–873, 1976.

[50] L. T. H. An and P. D. Tao, “The DC (difference of convex functions) programming and DCA revisited with DC models of real world nonconvex optimization problems,” Annals of Operations Research, vol. 133, no. 1–4, pp. 23–46, 2005.

[51] N. Vucic, S.-Y. Shi, and M. Schubert, “DC programming approach for resource allocation in wireless networks,” in Proceedings of the 8th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, pp. 380–386, May 2010.

[52] B. Fuchs, A. Skrivervik, and J. R. Mosig, “Shaped beam synthesis of arrays via sequential convex optimizations,” IEEE Antennas and Wireless Propagation Letters, vol. 12, pp. 1049–1052, 2013.

[53] J.-D. Wang, Q.-H. Zhang, and L. Ljung, “Revisiting the two-stage algorithm for Hammerstein system identification,” in Proceedings of the Joint 48th IEEE Conference Decision Control & 28th Chinese Control Conference, pp. 3620–3625, Shanghai, China, December 2009.

[54] S. Richter, C. N. Jones, and M. Morari, “Computational complexity certification for real-time MPC with input
constraints based on the fast gradient method," IEEE Transactions on Automatic Control, vol. 57, no. 6, pp. 1391-1403, 2012.

[55] A. J. Cann, “Improved nonlinearity model with variable Knee sharpness,” IEEE Transactions on Aerospace and Electronic Systems, vol. 48, no. 4, pp. 3637–3646, 2012.

[56] L. Wang, S. Bashar, Y. Wei, and R. Li, “Secrecy enhancement analysis against unknown eavesdropping in spatial modulation,” IEEE Communications Letters, vol. 19, no. 8, pp. 1351–1354, 2015.

[57] R. van Nee and R. Prasad, OFDM for Wireless Multimedia Communications, Artech House, Norwood, MA, USA, 1999.