IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 28, 2019, accepted March 12, 2019, date of publication March 18, 2019, date of current version May 15, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2905764

The Secrecy Capacity Optimization Artificial Noise: A New Type of Artificial Noise for Secure Communication in MIMO System

YEBO GU, ZHILU WU, ZHENDONG YIN, AND XIAOJUN ZHANG
School of Electronics and Information Engineering, Harbin Institute of Technology, Harbin 150001, China
Corresponding author: Zhilu Wu (wuzhilu@hit.edu.cn)

ABSTRACT In multiple-input multiple-output wireless communication system, artificial noise (AN) is designed to be aligned into the null space of the legitimate channel so that it has no effect on the legitimate channel. Meanwhile, AN will reduce the secrecy capacity of the eavesdropping channel so that AN increase the secrecy capacity of the wireless communication system. Nevertheless, AN technology only pays attention to the CSI of the legitimate channel but does not pay attention to the CSI of the eavesdropping channel so that the secrecy capacity of the system can be further improved. In this paper, we analyze the performance of traditional AN. A secrecy capacity optimization artificial noise for the whole communication system to further improve the system's secrecy capacity is proposed. The secrecy capacity optimization artificial noise is considered as a kind of artificial noise which is disadvantageous to the legitimate receiver but more disadvantageous to the eavesdropper. Furthermore, we further analyzed the technical details of AN technology and found the key factor affecting the secrecy capacity. Meanwhile, the secrecy capacity optimization artificial noise is effectively designed by applying these conclusions and the key factors of secrecy capacity optimization artificial noise affecting the secrecy capacity of the wireless communication system are described. The analysis and simulation results in practical environments show that the proposed method has a good performance on improving the secrecy capacity.

INDEX TERMS MIMO, eavesdropping, physical layer security, secrecy capacity, artificial noise, secrecy capacity optimization artificial noise.

I. INTRODUCTION

In the past period of time, wireless communication technology has developed rapidly. Especially in the past two decades, the explosion of mobile phones and mobile internet has brought huge economic benefits which has promoted the rapid development of wireless communication technology. The rate of communication increases rapidly, especially after the explosion of MIMO technology, the rate of communication increases exponentially. However, the nature of wireless communication has natural defects. The information transmitted by wireless communication can be received by all receivers, so it is very easy to be eavesdropped. Therefore, the encryption technology of wireless communication is an important topic in the research of wireless communication technology. Wireless communication encryption technology is usually falled into two types: one is cryptography in the traditional sense, which encrypts the transmitted signal so that it is difficult for the eavesdropper to decipher, but if the eavesdropper has enough computing power, the encryption of the signal will be deciphered-no matter how perfect the encryption technique is. The second is to encrypt the signal from the point of view of physical layer and information theory, which is first proposed by Wyner [2]. Its core idea is that if the channel capacity of the legitimate communication channel is larger than that of the eavesdropper, then part of the information transmitted by the legitimate communication channel will not be received by the eavesdropper channel, that is to say, some information in the legitimate channel will not be received by the eavesdropping channel. The difference between the capacity of the legitimate communication channel and the eavesdropping channel is called the channel's secrecy capacity, which is called the physical layer security technology.

The associate editor coordinating the review of this manuscript and approving it for publication was Jie Tang.

Physical layer security technology is not applied well in single antenna communication system. So physical layer security technology has not been fully developed for a long time. Until MIMO technology begins to be widely used, physical layer security technology has been paid attention to gradually. Especially with the introduction of artificial noise (AN) technology, physical layer security technology has made significant progress [3]. It shows how physical security technology improve the security performance of the system effectively. The essence of AN technology is to add a noise orthogonal to the legitimate channel in MIMO system, so that the legitimate receiver will not be affected, and the channel's secrecy capacity of eavesdropper will be reduced due to the influence of AN, so that the secrecy capacity of wireless communication system will be improved.

In order to further expand the secrecy capacity of wireless communication systems, researchers have done a lot of research. A novel power allocation and AN precoding technology in MIMO-OFDM system are described in [4]. In [5] and [6], a creative technique based on interference alignment and AN is proposed, which greatly expands the application scope of AN technology. A three-level optimization procedure to increase the average secrecy rate of this wiretap channel by optimizing the transmit power allocation between the encrypted data symbols, unencrypted data symbols and the AN symbols is proposed in [7]. A joint optimization of AN signal and transmit filter for the information signals in order to achieve a target secrecy level is proposed in [8]. In [9], the optimal resource allocation for the weighted sum secrecy rate maximization for legitimate receivers by power and subcarrier allocation at the transmitter is proposed. In [10], In order to fully reveal the benefits of the legitimate receiver, we derive easy-to-evaluate expressions for the secrecy outage probability achieved by the legitimate receiver.

Researchers have made outstanding contributions in the field of physical layer security, but researchers design AN based on the hypothesis that the AN is orthogonal to the legitimate CSI. In other words, previous research on AN focus on the legitimate sender and ignore the eavesdropper, although AN have many advantages, such as we do not need to know the eavesdropper's CSI, signals of transmitter and legitimate receiver are not affected by any factors, etc.

But if we know all or part of the eavesdropper's CSI, or we know what distribution the eavesdropper's CSI obeys, even if we only know a little information of the eavesdropper's CSI, we can design AN for the whole wireless communication system (including eavesdropper and legitimate receiver) to further improve the system's secrecy capacity.

Meanwhile, in the design of AN, researchers only pay attention to the orthogonality of AN, but do not know what characteristics of AN affect the secrecy capacity.

Based on the above analysis, a secrecy capacity optimization artificial noise(SCO-AN) technology is proposed in this paper. SCO-AN includes AN and local artificial noise. The AN is orthogonal to the legitimate channel and the local artificial noise is not orthogonal to the leitimate channel. Traditional AN is used to reduce the impact of SCO-AN on the legitimate receiver. Local artificial noise is used to further increase the secrecy capacity of the system. Local artificial noise can transform the anti-noise ability of wireless communication system into secrecy capacity. Local artificial noise can be considered as the transformation of the anti-noise ability of the system which will be broadly applied in communication systems with high anti-noise capability or in environments with high confidentiality requirements such as battlefields.

For a wireless communication system, there may be an infinite number of artificial noises as long as they satisfy orthogonality. So, which kind of artificial noise is the best, what is the standard of evaluation, how to design artificial noise? we find that the component element of AN is the only factor affecting the secrecy capacity of AN.

At the end of this paper, the simulation results show that the SCO-AN makes the secrecy capacity of the system significantly improved.

The main contributions of this paper are summarized as follows :

- Following the AN method in [14]. we propose a SCO-AN theory to further improve the secrecy capacity of wireless communication systems by adding SCO-AN that is not orthogonal to the legitimate channel $\mathbf{H}$. The SCO-AN is a method to transform the anti-noise ability of wireless communication system into the secrecy capacity of the system. It is very useful in areas with high secrecy performance such as battlefield.
- The influence of SCO-AN on secrecy capacity is discussed. It is proved that there is no upper limit for adding SCO-AN in wireless communication system. Of course, SCO-AN can be considered as a kind of noise. Under certain SNR requirements, SCO-AN can't be added without limit.
- The theory of AN in [14] is supplemented. This paper considers that the variance of the component element of AN is the main factor affecting the secrecy capacity of AN. Therefore, besides the traditional schemes such as power enhancement, the concrete design of AN is put forward. When designing SCO-AN, the above conclusions are valid as well.

The rest of this paper is organized as follows. In Section II, we describe the system modeli and present the SCO-AN. Section III analyzes the secrecy performance of the SCO-AN and the key factors affecting the secrecy capacity of the system by AN are analyzed. Simulation results are shown in Section VI, and conclusions are drawn in Section V.

Notation: $\mathrm{A}^{\dagger}$ denotes the conjugate transpose of matrix A. $\mathbb{C}^{M\times N}$ represents the space of complex $M \times N$ matrices. $E(\cdot)$ represents the expectations.

II. PROBLEM STATEMENT

In this section, the system model of SCO-AN is first described and the AN theory is recalled and the SCO-AN is introduced.

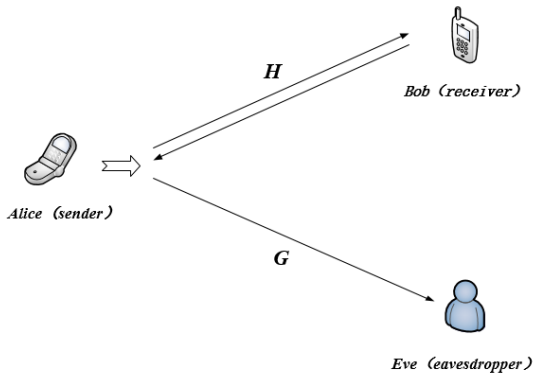

FIGURE 1. Framework of secure communication with wiretap channel.

A. SYSTEM MODEL

A wireless communication system model with eavesdroppers is shown in Figure 1. In this system, Alice is the transmitter of information, Bob is the legitimate receiver, and Eve is the eavesdropper. Alice is equipped with N_T antennas, Bob is equipped with N_R antennas and Eve is equipped with N_E antennas. It must be noted here that Eve equipped with N_E antennas may include two situations: a) a single eavesdropper has more than one antenna, b) multiple eavesdropper with single antenna collude. In contrast, worst case of secure communication is considered in this paper. $\mathbf{H}$ represents CSI between Alice and Bob and $\mathbf{G}$ represents CSI between Alice and Eve. $\mathbf{H}_k$ and $\mathbf{G}_k$ represent the channel between the transmitter to the legitimate receiver and the channel between transmitter to eavesdropper at time k, respectively. The elements $h_{i,j}(g_{i,j})$ in H(or G) represent the channel gain between the i_{th} transmitter antenna and the j_{th} receiver(eavesdropper) antenna. $\mathrm{x}_k \in \mathbb{C}^{N_\mathbf{R}}$ denotes the information transmitted by Alice at time k received by Bob and Eve, respectively,

$$\mathbf{z}_k = \mathbf{H}_k \mathbf{x}_k + \mathbf{n}_k, \tag{1}$$

$$\mathbf{y}_k = \mathbf{G}_k \mathbf{x}_k + \mathbf{e}_k, \tag{2}$$

where $\mathbf{n}_k$ and $\mathbf{e}_k$ are independent and identically distributed additive white Gaussian noise(AWGN) with variance of σ_n^2 and σ_e^2, In order to make the results of information theory applicable, We assume that block fading exists so that each element in $\mathbf{H}_k$ and $\mathbf{G}_k$, $\mathbf{H}_k \in \mathbb{C}^{\mathbf{N}_T \times \mathbf{N}_R}$, $\mathbf{G}_k \in \mathbb{C}^{\mathbf{N}_T \times \mathbf{N}_E}$. $h_{i,j}$ $g_{i,j}$ is constant and each element is independent. For each element in $\mathbf{H}_k$ and $\mathbf{G}_k$, the encoding and decoding of data are independent. $h_{i,j}$ and $g_{i,j}$ are assumed to be independent and unrelated complex number. For convenience of discussion, we assume that the channel estimation of $\mathbf{H}_k$ and $\mathbf{G}_k$ is perfect and error-free, and there is a channel (such as broadcast) for information transmission between the transmitter and the receiver so that the transmitter is able to get the CSI of $\mathbf{H}_k$ without error. It is generally considered that the CSI of $\mathbf{G}_k$ obeys Poisson distribution. But this assumption only complicates the discussion and does not help the discussion presented in the paper so we assume that the CSI of $\mathbf{G}_k$ is invariant and known in a certain time slot. The maximum transmitting power is assuming to be P_0, i.e, $E[\mathrm{x}_k^\dagger \mathrm{x}_k] \leq P_0$.

B. ARTIFICIAL NOISE

AN technology is first introduced by [14]. AN is designed to be in the null space of the legitimate receiver channel according to the CSI between the transmitter and the receiver. Therefore, the residual signal of AN at the legitimate receiver is zero. For the eavesdropper, the residual signal of AN will seriously affect the signal quality. The transmitter sends AN $\mathrm{w}_k \in \mathbb{C}^{N_\mathbf{R}}$ while sending the normal signal s_k so that

$$\mathbf{x}_k = \mathbf{w}_k + \mathbf{s}_k, \tag{3}$$

w_k is designed to lie in the null space of H_k so that $\mathrm{H}_k\, w_k = 0$. We assume that Z_k is an orthonormal basis for H_k so that $\mathbf{w}_k = \mathbf{Z}_k \mathbf{v}_k$ and $\mathrm{Z}_k^\dagger \mathrm{Z}_k = I$. So the signals received by the receiver and the eavesdropper are expressed as

$$\mathbf{z}_k = \mathbf{H}_k \mathbf{s}_k + \mathbf{n}_k, \tag{4}$$

$$\mathbf{y}_k = \mathbf{G}_k \mathbf{s}_k + \mathbf{G}_k \mathbf{w}_k + \mathbf{e}_k, \tag{5}$$

(4) and (5) shows that the AN has no effect on the legitimate channel because it lie sin the null space of the legitimate channel. For eavesdropper, AN will degrade the channel of the eavesdropper. In order to expand the influence of AN on eavesdroppers, the power of AN is very large, that is, $\|\mathbf{G}_k \mathbf{H}_k\|$ is very large. And v_k is designed to be i.i.d complex random variables with variance of σ_k^2.

In [14], the signal from the transmitter is designed to be $\mathbf{s}_k = \mathbf{p}_k \mathbf{u}_k$ where u_k is the information signal and p_k obeys the independent Gaussian distribution. p_k is designed to satisfy the following conditions a) $\mathbf{H}_k \mathbf{p}_k \neq 1$, b)$\|\mathbf{p}_k\| = 1$.

So the lower bound of secrecy capacity is

$$\begin{aligned} SecrecyCapacity_k &\geq C_{sec}^a = I(Z;U) - I(Y;U) \\ &= \log(1+\frac{|\mathbf{H}_k p_k|^2 \sigma_u^2}{\sigma_n^2}) - \log(1+\frac{|\mathbf{G}_k p_k|^2 \sigma_u^2}{E|\mathbf{G}_k w_k|^2 + \sigma_e^2}) \end{aligned} \tag{6}$$

C. THE SECRECY CAPACITY OPTIMIZATION ARTIFICIAL NOISE

Since the theory of AN is proposed, scholars have made many outstanding contributions in this field. AN theory is based on the basic framework of eavesdropping channel. The eavesdropping channel and legitimate channel are a pair of information countermeasure channels essentially.

Previous work could be regarded as a method in the framework which makes no effect on the legitimate channels while reducing the capacity of eavesdropping channels. The basic principle of AN is to design the AN based on the legitimate CSI so that the AN has no effect on the legitimate communication channel and has an impact on the eavesdropping channel so that the secrecy capacity is improved.

Because the impact of AN on legitimate channel is zero, the theory of AN is so simple and beautiful that it is impressive. In the subconscious of scholars, noise is considered harmful because of its randomness so that the noise can not be eliminated, and the null impact of noise is considered to be perfect. But AN is absolutely different from noise. AN is designed and controllable. The traditional design of AN only

pays attention to the legitimate communication channel, but does not pay attention to the whole secure communication system, which has certain limitations. For the limitation of AN, we propose SCO-AN in this paper. The SCO-AN is designed not only according to the legitimate receiver, but also according to the whole secrecy communication system. It should be noted that this paper only designs SCO-AN from the perspective of information theory, and does not consider the impact of SCO-AN on communication technology.

The goal of SCO-AN is to makes the secrecy capacity of communication system improved further on the basis of traditional AN. SCO-AN is a means of transforming the anti-noise ability of the system into the secrecy capacity so that SCO-AN may increase the secrecy capacity of the system and make the communication quality worse at the same time. The SCO-AN may be necessary in such environments as battle-field, where information is highly confidential, the security of communication is more important than the efficiency of communication. In this case, it is necessary to introduce SCO-AN. Of course, when we design the SCO-AN, the idea of AN is borrowed to minimize the damage of the SCO-AN to the communication quality of legitimate users.

The transmitter sends SCO-AN while sending the normal signal

$$\mathbf{x}_k = \mathbf{w}_g + \mathbf{s}_k, \tag{7}$$

where $\mathrm{w}_g \in \mathbb{C}^{N_\mathbf{R}}$ consists of SCO-AN and local artificial noise. s_k is the signal sent by the transmitter and $\mathrm{s}_k \in \mathbb{C}^{N_\mathbf{R}}$

$$\mathbf{w}_g = \mathbf{w}_k + \mathbf{w}_m, \tag{8}$$

$\mathrm{w}_m \in \mathbb{C}^{N_\mathbf{R}}$ is called local SCO-AN which enhance the secrecy capacity of the system and $\mathrm{w}_k \in \mathbb{C}^{N_\mathbf{R}}$ is the AN introduced in (3). We assume that Z_m is an orthonormal basis for w_m so that $\mathrm{w}_m = \mathrm{Z}_m \mathrm{v}_m$ and $\mathrm{Z}_m^\dagger \mathrm{Z}_m = I$ and v_m is designed to be i.i.d complex random variables with variance σ_m^2. So the signals received by the receiver and the eavesdropper are expressed as:

$$\mathbf{z}_k = \mathbf{H}_k \mathbf{s}_k + \mathbf{H}_k \mathbf{w}_g + \mathbf{n}_k, \tag{9}$$
$$\mathbf{y}_k = \mathbf{G}_k \mathbf{s}_k + \mathbf{G}_k \mathbf{w}_g + \mathbf{e}_k, \tag{10}$$

Because of $\mathbf{H}_k \mathbf{w}_k = 0$, so

$$\mathbf{z}_k = \mathbf{H}_k \mathbf{s}_k + \mathbf{H}_k \mathbf{w}_g + \mathbf{n}_k = \mathbf{H}_k \mathbf{s}_k + \mathbf{H}_k \mathbf{w}_k + \mathbf{H}_k \mathbf{w}_m + \mathbf{n}_k = \mathbf{H}_k \mathbf{s}_k + \mathbf{H}_k \mathbf{w}_m + \mathbf{n}_k \tag{11}$$

$$\mathbf{y}_k = \mathbf{G}_k \mathbf{s}_k + \mathbf{G}_k \mathbf{w}_g + \mathbf{e}_k \tag{12}$$

So the lower bound of secrecy capacity after adding SCO-AN is:

$$\begin{aligned} \sec recy_s &\geq C_{\sec}^a = I(Z;U) - I(Y;U) \\ &= \log(1 + \frac{|\mathbf{H}_k p_k|^2 \sigma_u^2}{\sigma_n^2 + E|\mathbf{H}_k w_m|^2}) - \log(1 + \frac{|\mathbf{G}_k \mathbf{p}_k|^2 \sigma_u^2}{E|\mathbf{G}_k \mathbf{w}_s|^2 + \sigma_e^2}), \end{aligned} \tag{13}$$

where $E|\mathbf{H}_k \mathbf{w}_m|^2 = (\mathbf{H}_k \mathbf{Z}_m \mathbf{Z}_m^\dagger \mathbf{H}_m^\dagger)\sigma_m^2$.

III. THE PROPERTIES OF SCO-AN AND THE FACTOR OF AN

A. APPLICABLE CONDITIONS OF SCO-AN

We need to find the proper $\mathbf{w}_m$ so that the secure capacity of the system increases after adding $\mathbf{w}_m$, that is to say, the system's secrecy capacity increases and the following formula should be satisfied:

$$\begin{aligned} &\sec recy_s - \sec recy_k \\ &= \log(1 + \frac{|\mathbf{H}_k \mathbf{p}_k|^2 \sigma_u^2}{\sigma_n^2 + E|\mathbf{H}_k \mathbf{w}_m|^2}) - \log(1 + \frac{|\mathbf{G}_k \mathbf{p}_k|^2 \sigma_u^2}{E|\mathbf{G}_k \mathbf{w}_g|^2 + \sigma_e^2}) \\ &- \{\log(1 + \frac{|\mathbf{H}_k \mathbf{p}_k|^2 \sigma_u^2}{\sigma_n^2}) - \log(1 + \frac{|\mathbf{G}_k \mathbf{p}_k|^2 \sigma_u^2}{E|\mathbf{G}_k \mathbf{w}_k|^2 + \sigma_e^2})\} \geq 0 \end{aligned} \tag{14}$$

where $E|\mathbf{H}_k \mathbf{w}_m|^2 = (\mathbf{H}_k \mathbf{Z}_m \mathbf{Z}_m^\dagger \mathbf{H}_k^\dagger)\sigma_m^2$, According to previous assumptions, only w_m and w_g are unknown in (14) that is, $E|\mathbf{H}_k \mathbf{w}_m|^2$ and $E|\mathbf{G}_k \mathbf{w}_g|^2$ are unknown. So the necessary and sufficient condition for (14) is given in (15), as shown at the bottom of this page.

It seems very complicated, but in (15), only $E|\mathbf{H}_k \mathbf{w}_m|^2$ and $E|\mathbf{G}_k \mathbf{w}_g|^2$ are variables, and the rest are constants. So (15) is considered to be a binary quadratic inequality. As long as $E|\mathbf{H}_k \mathbf{w}_m|^2$ and $E|\mathbf{G}_k \mathbf{w}_g|^2$ are properly designed to satisfy (15), the secrecy capacity of the system could be improved. To make a convenient for analysis, we assume

$$|\mathbf{H}_k \mathbf{p}_k|^2 \sigma_u^2 = A, \tag{16}$$
$$|\mathbf{G}_k \mathbf{p}_k|^2 \sigma_u^2 = B, \tag{17}$$

$$\left\{1 - \left(\frac{1 + |H_k p_k|^2 \sigma_u^2}{1 + \frac{|G_k p_k|^2 \sigma_u^2}{E|G_k w_k|^2 + \sigma_e^2}}\right)(|G_k p_k|^2 \sigma_u^2 + 1)\right\}(E|H_k w_m|^2) + \left(1 + |H_k p_k|^2 \sigma_u^2 - \frac{1 + |H_k p_k|^2 \sigma_u^2}{1 + \frac{|G_k p_k|^2 \sigma_u^2}{E|G_k w_k|^2 + \sigma_e^2}}\right)(E|G_k w_s|^2)$$
$$+ \left(1 - \frac{1 + |H_k p_k|^2 \sigma_u^2}{1 + \frac{|G_k p_k|^2 \sigma_u^2}{E|G_k w_k|^2 + \sigma_e^2}}\right)(E|H_k w_m|^2)(E|G_k w_s|^2) + \left\{1 - \left(\frac{1 + |H_k p_k|^2 \sigma_u^2}{1 + \frac{|G_k p_k|^2 \sigma_u^2}{E|G_k w_k|^2 + \sigma_e^2}}\right)(|G_k p_k|^2 \sigma_u^2) + 1) + |H_k p_k|^2 \sigma_u^2\right\} \geq 0, \tag{15}$$

$$\frac{1+|\mathbf{H}_k\mathbf{p}_k|^2\sigma_u^2}{1+\frac{|\mathbf{G}_k\mathbf{p}_k|^2\sigma_u^2}{E|\mathbf{G}_k\mathbf{w}_k|^2+\sigma_e^2}}=C, \tag{18}$$

$$E|\mathbf{H}_k\mathbf{w}_m|^2=X, \tag{19}$$

$$E|\mathbf{G}_k\mathbf{w}_g|^2=Y, \tag{20}$$

and all variances in (15) are set to 1. So (21) is obtained

$$K_a=(1-CB-C)X+(1+A-C)Y +(1-C)XY+(1+A-C-CB)\geq 0, \tag{21}$$

K_a is called the contribution degree of secrecy capacity. It expresses the effect of SCO-AN on system secrecy capacity. Because $\mathbf{w}_g=\mathbf{w}_k+\mathbf{w}_m$, so X and Y are only related to $\mathbf{w}_m$, and there is only one unknown variable $\mathbf{w}_m$ in (21). That is to say, we just need to design the proper $\mathbf{w}_m$ to satisfy (21).

B. THE PROPERTY OF KA

In this chapter, in order to determine the extreme value of Ka's influence on communication systems, we discuss the limit of Ka. Ka is a binary quadratic function about X and Y. (21) can be obtained by taking the first-order and second-order partial derivatives of the variable Ka with respect to independent variable X and Y respectively.

$$\frac{\partial K_a}{\partial X}=1-CB-C+(1-C)Y \tag{22}$$

$$\frac{\partial K_a}{\partial Y}=1+A-C+(1-C)X \tag{23}$$

So,

$$\frac{\partial^2 K_a}{\partial Y^2}=0 \tag{24}$$

$$\frac{\partial^2 K_a}{\partial X^2}=0, \tag{25}$$

$$\frac{\partial^2 K_a}{\partial XY}=(1-C), \tag{26}$$

According to convex optimization theory, there is no extremum point for Ka in space, that is to say, Ka is divergent in space, so we can only find the maximum value of Ka in a certain range. The fact that Ka has no extreme point means that Ka has no maximum or minimum value, and its value is all over the field. However, because excessive SCO-AN will seriously affect the communication efficiency of the system, the SCO-AN can't be added indefinitely in the communication system. We need to consider the requirement of different communication systems for noise level and the influence of SCO-AN on system BER, which will be discussed in the future. As shown in Figure 1, Ka is divergent, and the intersection of Ka in the xoy plane is a plane rather than a curve or a point, so (21) is the simplest way to solve Ka.

From the above analysis, we can see that SCO-AN can be added to the secure communication system without restriction, which can increase the system's secrecy capacity without restriction. But in the actual system, the SCO-AN is also noise in essence. Adding noise will increase the bit error rate of the communication system and worsen the communication quality. Therefore, it is not recommended to use SCO-AN in daily communication systems or systems requiring high bit error rates. In communication systems with high security requirements, such as battlefield communications, SCO-AN will be excellent.

C. THE KEY FACTORS OF ARTIFICIAL NOISE AFFECTING SECRECY CAPACITY

In this chapter, we will continue to disscuss the relationship between X, Y and K_a in (19), (20). In order to make X and Y easier to be understood and discussed, we assume that

$$\mathbf{w}_m=\mathbf{Z}_k\mathbf{V}_m, \tag{27}$$

where $\mathbf{V}_m$ is a vector obeying Gaussian distribution and the mean value of a is 0 and the variance of $\mathbf{V}_m$ is σ_m^2. So

$$E|\mathbf{H}_k\mathbf{w}_m|^2=(\mathbf{H}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{H}_k^\dagger)\sigma_m^2, \tag{28}$$

A difference from [14], $\mathbf{Z}_k$ is a standard orthogonal basis of $\mathbf{H}_k$. According to the properties of standard orthogonal basis, so that

$$\mathbf{Z}_k\mathbf{Z}_k^\dagger=\mathbf{Z}_k^\dagger\mathbf{Z}_k=\mathbf{I}, \tag{29}$$

So(28) could be written as

$$E|\mathbf{H}_k\mathbf{w}_m|^2=(\mathbf{H}_k\mathbf{H}_k^\dagger)\sigma_m^2, \tag{30}$$

From (30), we know that the power of $\mathbf{H}_k\mathbf{w}_m$ is related to the variance of $\mathbf{V}_m$. This is a very important conclusion. When designing $\mathbf{w}_m$, we can control X by controlling the variance of $\mathbf{w}_m$ while guaranteeing that $\mathbf{w}_m$ obeys the Gaussian distribution.

Since the artificial noise only needs to be orthogonal to H, there are numerous cases of artificial noise. Different artificial noise has different enhancement to the system's secrecy capacity, so which kind of artificial noise has the best effect and what is the design criterion?The above research provides a solution to this problem. When designing artificial noise, the following steps should be taken:

(a) The standard orthogonal basis $\mathbf{Z}_K$ of $\mathbf{H}_k$ is obtained by calculation.

(b) By using the $\mathbf{Z}_K$ in (a) and the formula $\mathbf{H}_k\mathbf{Z}_k\mathbf{v}_k=0$, the $\mathbf{v}_k$ can be obtained.

(c) $\mathbf{v}_k$ is a set of general solutions, we can control the system secrecy capacity by controlling the variance of $\mathbf{v}_k$.

This conclusion is also valid in [6] and [6] could change to

$$SecrecyCapacity_k\geq C_{sec}^a=I(Z;U)-I(Y;U) =\log(1+\frac{|\mathbf{H}_k p_k|^2\sigma_u^2}{\sigma_n^2})-\log(1+\frac{|\mathbf{G}_k p_k|^2\sigma_u^2}{E\left|\mathbf{G}_k\mathbf{G}_k^\dagger\right|\sigma_k^2+\sigma_e^2}, \tag{31}$$

From (31), we konw that if we want to change the secrecy capacity, we only need to change the variance of $\mathbf{v}_k$. Of course, when we design $\mathbf{v}_k$, we need to satisfy $\mathbf{w}_k=\mathbf{Z}_k\mathbf{v}_k$.

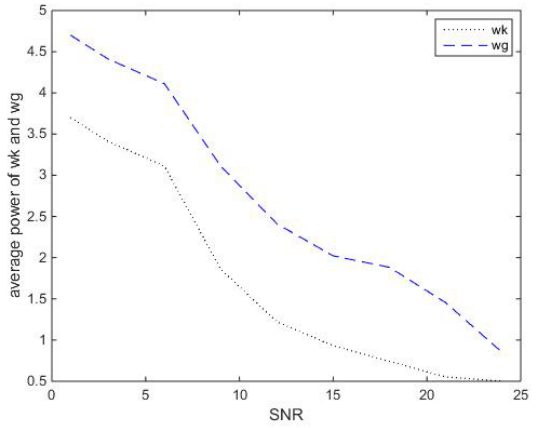

FIGURE 2. The average power of artificial noise.

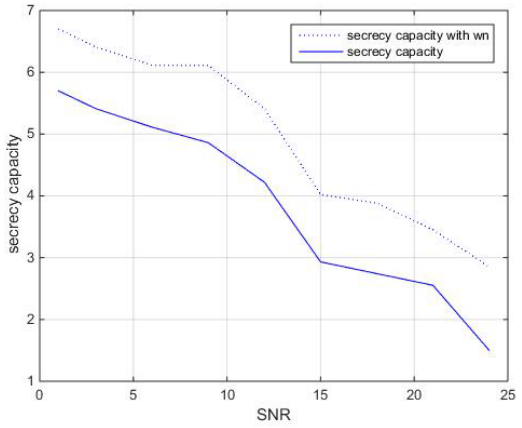

FIGURE 3. Comparison of the secrecy capacity of SCO-AN and AN6.

The above conclusions are also applicable to Y. (32) could be obtained from (8) and (27).

$$\begin{aligned}\mathbf{w}_g &= \mathbf{w}_m + \mathbf{w}_k \\ &= \mathbf{Z}_k\mathbf{v}_m + \mathbf{Z}_k\mathbf{v}_k \\ &= \mathbf{Z}_k(\mathbf{v}_m + \mathbf{v}_k),\end{aligned} \tag{32}$$

$\mathbf{V}_n$ and $\mathbf{V}_k$ are both Gaussian vectors. We assume that

$$\mathbf{v}_g = \mathbf{v}_k + \mathbf{v}_m, \tag{33}$$

Based on the properties of Gaussian vectors, we konw that $\mathbf{v}_g$ is a Gaussian vector with a mean of 0 and a variance of $(\sigma_k^2 + \sigma_m^2)$.

$$\begin{aligned}E\left|\mathbf{G}_k\mathbf{w}_g\right|^2 &= \left|\mathbf{G}_k\mathbf{Z}_k(\mathbf{v}_m + \mathbf{v}_k)(\mathbf{v}_m + \mathbf{v}_k)^\dagger\mathbf{Z}_k^\dagger\mathbf{G}_k^\dagger\right| \\ &= \left|\mathbf{G}_k\mathbf{Z}_k\mathbf{v}_g\mathbf{v}_g^\dagger\mathbf{Z}_k^\dagger\mathbf{G}_k^\dagger\right| \\ &= \left|\mathbf{G}_k\mathbf{Z}_k\mathbf{Z}_k^\dagger\mathbf{G}_k^\dagger\right|(\sigma_k^2 + \sigma_m^2) \\ &= \left|\mathbf{G}_k\mathbf{G}_k^\dagger\right|(\sigma_k^2 + \sigma_m^2)\end{aligned} \tag{34}$$

From (34), we konw that if we want to enhance or reduce secrecy capacity of the wireless communication system, we only need to change the variance of $\mathbf{v}_k + \mathbf{v}_m$. Of course, when we design $\mathbf{v}_g$, we need to satisfy $\mathbf{w}_m = \mathbf{Z}_k\mathbf{v}_m$.

IV. SIMULATION RESULTS AND DISCUSSIONS

In this section, extensive simulation results are presented to analyze the performance of the SCO-AN. In the simulations the number of the antennas are set to be $N_T = N_R = N_E = 2$ so that the channel H and G are matrices of 2×2. All channels are Rayleigh fading channels. When calculating the bit error rate, the signal is transmitted by QPSK modulation and demodulation. The signal is not coded to increase anti-noise ability. In Figures 4 and 5, secrecyN represents the secrecy capacity using SCO-AN, and secrecy represents the secrecy capacity using AN, the unit of SNR is dB.

In Figure 2, we simulate the average signal power of $\mathbf{w}_g$ and $\mathbf{w}_k$ respectively. It can be seen that under different SNR conditions, the energy of $\mathbf{w}_g$ is always greater than that of $\mathbf{w}_k$.

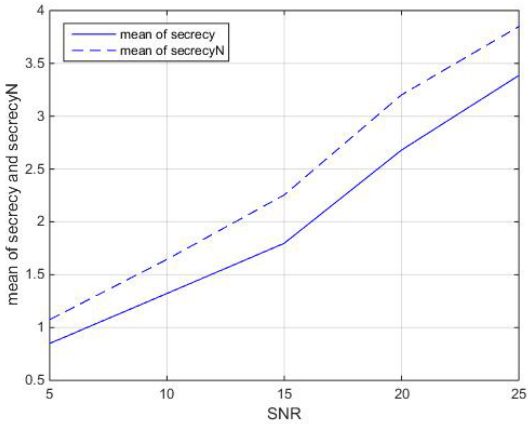

FIGURE 4. The average of secrecy capacity with and without SCO-AN.

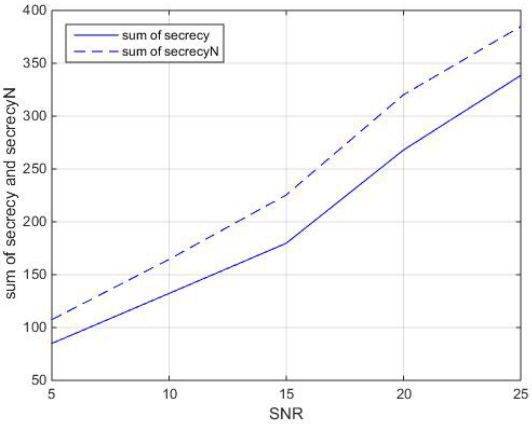

FIGURE 5. The sum of secrecy capacity with and without SCO-AN.

In (8) we know that $\mathbf{w}_g$ is composed of $\mathbf{w}_k$ and $\mathbf{w}_m$, so it is obvious that the average signal power of $\mathbf{w}_g$ is greater than $\mathbf{w}_k$.

In Figure 3, we simulate the secrecy capacity of adding SCO-AN and traditional AN respectively. It can be known that after adding the SCO-AN, the secrecy capacity of the system has been improved.

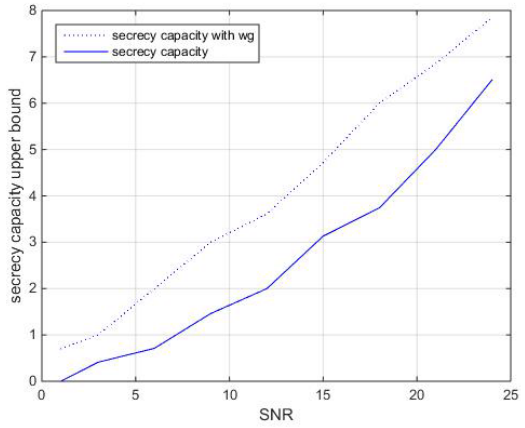

FIGURE 6. The performance of $\mathbf{w}_g$ on upper bound of secrecy capacity.

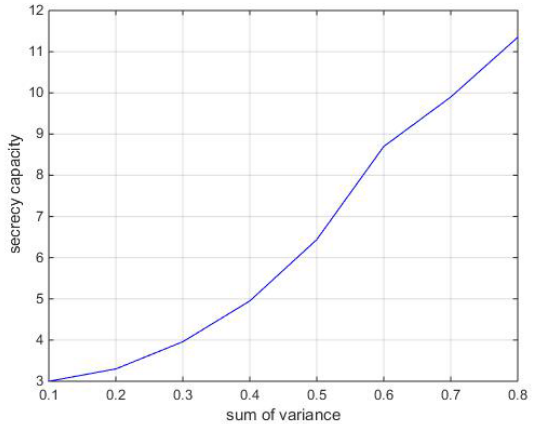

FIGURE 7. The influence of $\sigma_k^2 + \sigma_m^2$ on the secrecy capacity.

According to the preceding conditions, we conduct 100 experiments for data statistics. Fig. 4 and Fig. 5 show the changes of secure communication capacity when adding SCO-AN and not adding SCO-AN. Fig. 4 shows the change of the average value of the secure communication capacity. Fig. 5 shows the change of the sum of the secure communication capacity. Fig. 4 and Fig. 5 show that the secrecy capacity of the communication system has been further improved than that of the traditional AN system by adding the traditional AN to Fig. 4 and Fig. 5 and the secrecy capacity of the system will increase with the increase of SNR.

From Figure 7, we quote the upper limit of secrecy capacity proposed by [12]. It can be seen that after adding SCO-AN $\mathbf{w}_g$ to the system, the secrecy capacity of the system breaks through the upper bound of the traditional AN secrecy capacity, which greatly increases the secrecy capacity. This also proves that SCO-AN has a great role in improving the secrecy capacity of the system.

The results in (34) are simulated and verified. In the process of simulation, the parameters of channel H and G remain unchanged. As can be seen clearly in Figure 8, with the increase of $\sigma_k^2 + \sigma_m^2$, the channel's secrecy capacity increases. It also proves that the component element $\mathbf{v}_m$ of SCO-AN is the only factor affecting the system secrecy capacity.

V. CONCLUSION

In this article, we propose the theoretical framework of SCO-AN, and verify that the SCO-AN has a greater improvement on the system's secrecy capacity than AN. At the same time, it is verified that the variance of the component of AN is the key factor affecting the system's secrecy capacity and this conclusion is also true for SCO-AN.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.
[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
[3] M. F. Marzban, A. E. Shafie, R. Chabaan, and N. Al-Dhahir, "Securing OFDM-based wireless links using temporal artificial-noise injection," in *Proc. IEEE Consum. Commun. Netw. Conf.*, Jan. 2018, pp. 1–6.
[4] N. Zhao, F. R. Yu, M. Li, and V. C. Leung, "Anti-eavesdropping schemes for interference alignment (IA)-based wireless networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5719–5732, Aug. 2016.
[5] Y. Cao, N. Zhao, F. R. Yu, Y. Chen, X. Liu, and V. C. M. Leung, "An anti-eavesdropping interference alignment scheme with wireless power transfer," in *Proc. IEEE Int. Conf. Commun. Syst.*, Dec. 2017, pp. 1–5.
[6] A. El Shafie, M. F. Marzban, R. Chabaan, and N. Al-Dhahir, "A hybrid artificial-noise and secret-key scheme for securing OFDM transmissions in V2G networks," in *Proc. 15th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, Jan. 2018, pp. 1–6.
[7] M. Zhang *et al.*, "Artificial noise aided secrecy information and power transfer in OFDMA systems," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 3085–3096, Apr. 2016.
[8] 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 Trans. Wireless Commun.*, vol. 15, no. 2, pp. 8286–8297, Dec. 2016.
[9] J. Ji, L. Jin, and K.-Z. Huang, "Secrecy capacity analysis of MISO system with artificial noise," *J. Commun.*, vol. 33, pp. 138–142, Oct. 2012.
[10] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
[11] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
[12] N. Shlezinger, D. Zahavi, Y. Murin, and R. Dabora, "The secrecy capacity of Gaussian MIMO channels with finite memory," *IEEE Trans. Inf. Theory*, vol. 63, no. 3, pp. 1874–1897, Mar. 2017.
[13] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.
[14] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE Veh. Technol. Conf.*, Sep. 2005, pp. 1–5.
[15] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Process. Lett.*, vol. 19, no. 2, pp. 71–74, Feb. 2012.
[16] N. Romero-Zurita, D. McLernon, M. Ghogho, and A. Swami, "PHY layer security based on protected zone and artificial noise," *IEEE Signal Process. Lett.*, vol. 20, no. 5, pp. 487–490, May 2013.
[17] X. Zhou and M. R. Mckay, "Physical layer security with artificial noise: Secrecy capacity and optimal power allocation," in *Proc. Int. Conf. Signal Process. Commun. Syst.*, Sep. 2009, pp. 1–5. [Online]. Available: http://www.bookref.com
[18] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1628–1631, Oct. 2012.
[19] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.
[20] P.-H. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1728–1740, Sep. 2013.

[21] W. Li, B. Chen, J. B. Wei, C. L. Xiong, and X. Y. Zhang, "Secure communications via sending artificial noise by the receiver: Ergodic secure region analysis," *Signal Process.*, vol. 28, no. 9, pp. 1314–1320, 2012.
[22] 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 Trans. Commun.*, vol. 63, no. 11, pp. 4347–4362, Nov. 2015.
[23] 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 Trans. Signal Process.*, vol. 63, no. 1, pp. 206–220, Jan. 2015.
[24] H. Qin *et al.*, "Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2717–2729, Jun. 2013.
[25] A. Khisti and D. Zhang, "Artificial-noise alignment for secure multicast using multiple antennas," *IEEE Commun. Lett.*, vol. 17, no. 8, pp. 1568–1571, Aug. 2013.
[26] S. H. Chae, W. Choi, J. H. Lee, and T. Q. S. Quek, "Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 10, pp. 1617–1628, Oct. 2014.
[27] S.-H. Tsai and H. Poor, "Power allocation for artificial-noise secure MIMO precoding systems," *IEEE Trans. Signal Process.*, vol. 62, no. 13, pp. 3479–3493, Jul. 2014.

YEBO GU was born in Harbin, China, in 1987. He received the B.S. degree from Heilongjiang University, in 2010 and the M.S. degree from the Harbin Institute of Technology, China, in 2012, where he is currently pursuing the Ph.D. degree with the School of Electronics and Information Engineering, Harbin Institute of Technology. His current research interests include physical layer security and wireless cooperative communications.

ZHILU WU is currently a Professor with the School of Electronics Information Engineering, Harbin Institute of Technology. His research interests include space information acquisition and processing, formation flying satellite control, cognitive radio, and software radio.

ZHENDONG YIN received the Ph.D. degree from the Harbin Institute of Technology, in 2008, where he is currently an Associate Professor with the School of Electronics Information Engineering. His current research interests include UWB wireless communications, formation flying satellites communications, and relay communication systems.

XIAOJUN ZHANG was born in Shijiazhuang, China, in 1984. He received the bachelor's degree in communications from the School of Electronic and Information Engineering, Harbin University of Technology, where he is currently pursuing the master's degree in information and communication engineering. His research interests include machine learning, signal processing, and radio communication.