Secure MISO Wiretap Channels With Multiantenna Passive Eavesdropper: Artificial Noise vs. Artificial Fast Fading

Article *in* IEEE Transactions on Wireless Communications · January 2015

DOI: 10.1109/TWC.2014.2332164

CITATIONS
75

READS
165

3 authors, including:

Tong-Xing Zheng
Xi'an Jiaotong University
62 PUBLICATIONS **716** CITATIONS

SEE PROFILE

Secure MISO Wiretap Channels With Multiantenna Passive Eavesdropper: Artificial Noise vs. Artificial Fast Fading

Hui-Ming Wang, *Member, IEEE*, Tongxing Zheng, and Xiang-Gen Xia, *Fellow, IEEE*

***Abstract*—The artificial noise (AN) scheme is an efficient strategy for enhancing the secrecy rate of a multiple-input–single-output channel in the presence of a passive eavesdropper, whose channel state information is unavailable. Recently, a randomized beamforming scheme has been proposed for deteriorating the eavesdropper's bit-error-rate performance via corrupting its receiving signal by time-varying multiplicative noise. However, the secrecy rate of such a scheme has not been well addressed yet. In this paper, we name it the *artificial fast fading* (AFF) scheme and provide a comprehensive secrecy rate analysis for it. We show that with this scheme, the eavesdropper will face a noncoherent Ricean fading single-input–multiple-output channel. Although the closed-form secrecy rate is difficult to obtain, we derive an exact expression for the single-antenna-eavesdropper case and a lower bound for the multiantenna-eavesdropper case, both of which can be numerically calculated conveniently. Furthermore, we compare the AFF scheme with the AN scheme and show that their respective superiorities to each other depend on the number of antennas that the transmitter and the eavesdropper possessed, i.e., when the eavesdropper has more antennas than the transmitter does, the AFF scheme achieves a larger secrecy rate; otherwise, the AN scheme outperforms. Motivated by this observation, we propose a hybrid AN-AFF scheme and investigate the power allocation problem, which achieves better secrecy performance further.**

***Index Terms*—Physical layer security, secrecy rate, multiple-input–single-output, artificial fast fading, artificial noise, noncoherent, power allocation.**

Manuscript received January 16, 2014; revised April 10, 2014; accepted June 11, 2014. Date of publication June 20, 2014; date of current version January 7, 2015. The work of H.-M. Wang and T. Zheng was supported in part by the NSFC under Grants 61102081 and 61221063, by the Specialized Research Fund for the Doctoral Program of Higher Education of China under Grant 20110201120013, by the New Century Excellent Talents Support Fund of China under Grant NCET-13-0458, by the Industrial Research Fund of Shaanxi Province under Grant 2012GY2-28, by the Fok Ying Tong Education Foundation under Grant 141063, and by the Fundamental Research Funds for the Central University under Grant 2013jdgz11. The work of X.-G. Xia was supported in part by the Air Force Office of Scientific Research (AFOSR) under Grant FA9550-12-1-0055 and by the National Science Foundation (NSF) under Grant CCF-0964500. The associate editor coordinating the review of this paper and approving it for publication was J. Wu.

H.-M. Wang and T. Zheng are with the School of Electronics and Information Engineering and the Ministry of Education Key Lab for Intelligent Networks and Network Security, Xi'an Jiaotong University, Xi'an 710049, China (e-mail: xjbswhm@gmail.com; txzheng@stu.xjtu.edu.cn).

X.-G. Xia is with the Institute of Electronics, Xidian University, Xi'an 710126, China, and also with the Department of Electrical and Computer Engineering, University of Delaware, Newark, DE 19716 USA (e-mail: xxia@ee.udel.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TWC.2014.2332164

I. Introduction

To guarantee transmission security at the *physical-layer* of wireless systems has attracted increasing attention recently [1]–[25]. The fundamental measure of the physical-layer security from the information-theoretic point of view is the notion of *secrecy capacity* established by Wyner for the degraded wiretap channel model in [2]. This conception was further developed to the Gaussian degraded wiretap channel by Cheong *et al.* in [3], and to the general non-degraded wiretap channel by Csiszár *et al.* in [4].

Multiple-antenna technique is an efficient way to enhance the physical layer secrecy [6]–[14]. Secure transmissions are investigated when the channel from the transmitter to the legitimate receiver is single-input multiple-output (SIMO) [6], multiple-input single-output (MISO) [7]–[9], and multiple-input multiple-output (MIMO) [10]–[14]. In [9], it is shown when the instantaneous channel state information (CSI) are fixed and known to all the transceivers, the optimal transmission scheme that achieves the secrecy capacity of a Gaussian MISO channel is *beamforming*. The secrecy capacity of a MIMO wiretap channel is established in [12], [13] under sum power constraints, and in [14] under power-covariance constraints. However, for sum power constraints, the secrecy capacity is still an open problem for general cases. Some very recent progresses can be found in [15], [16].

In a practical scenario the eavesdropper usually works in a passive way so that the transmitter can not get its instantaneous CSI. When only the statistical CSI of the eavesdropper is available, the secrecy capacity/rate of a MISO wiretap channel has been investigated in [8], [17], [18]. When the eavesdropper's CSI is completely absent, a so-called *artificial noise* (AN) scheme has been proposed in [19]–[21] for MISO and MIMO systems to improve the secrecy rate, and has been extended to the cooperative jamming schemes recently [22], [23]. The basic idea is to transmit a carefully designed jamming signal along with the information signal to deteriorate the receiving signal-to-interference-noise ratio (SINR) of the potential eavesdropper without impacting the intended receiver. Interestingly, it is shown in [9] that the AN scheme in a MISO wiretap channel is asymptotically near-optimal in the high SNR regime. However, when the number of eavesdropper's antenna is larger than that of the transmitter, the secrecy rate is greatly reduced. More worse, it is also shown in [9] that when the eavesdropper has nearly twice as many antennas as that of the transmitter, successful interception can be always guaranteed irrespective of

the amount of transmit power, which means that the AN scheme is completely failed.

All the aforementioned works have made the assumption that the eavesdropper has the full CSI of itself so that it can detect the intercepted signals coherently. This assumption is reasonable since in most of the practical wireless communication systems, there will be training signals transmitted by the source terminal for the legitimate receiver to estimate the channel coefficients, and to synchronize the sampling time and frequency. These training signals can also be received by the eavesdropper, making its CSI available. Another approach is that when the wireless fading is not so fast, the eavesdropper can exploit some blind channel estimation techniques such as those in [26], [27] to attain the channel coefficients without intercepting the training signals. In either case, with the CSI, the eavesdropper can *coherently* detect the intercepted signals. That is the reason why once the eavesdropper has sufficient antennas, it can always have a better equivalent channel than the legitimate receiver and drive the secrecy rate to 0 [9].

Then an interesting consideration is that what will happen when the eavesdropper does not have its CSI. In [28], [29], the authors proposed a randomized beamforming transmission scheme[1] to corrupt the received signal of the eavesdropper by a time varying multiplicative noise. It has been proved that with this scheme the eavesdropper's ability of blind deconvolution (by blind channel estimation techniques such as those in [26], [27]) can be forfeited. Simulations show the scheme is efficient in the sense that eavesdropper's bit error rate (BER) is nearly 0.5, but the secrecy rate analysis is absent. In [30], the authors do the secrecy rate analysis of the scheme when the eavesdropper has only a single antenna, and derive an achievable secrecy rate lower bound. However, this lower bound is very loose, and whether the scheme is robust to the multi-antenna eavesdropper has not been investigated. Finally, whether this scheme outperforms the AN scheme or not is unclear.

In this paper, we re-investigate the randomized beamforming transmission scheme in [28]–[30] under the general case where the eavesdropper is equipped with multiple antennas, and provide a comprehensive *secrecy rate analysis* for it. Since this scheme results in an equivalent fast fading channel for the eavesdropper, we call it *artificial fast fading* (AFF) scheme. Our work differs from the existing works [28]–[30] significantly in the following aspects:

1) We indicate that with the AFF scheme, the eavesdropper will face a *non-coherent Ricean* fading SIMO channel.[2] Although the closed-form secrecy rate is difficult to obtain, we derive an exact expression for the single-antenna eavesdropper case, and a lower bound for the multi-antenna eavesdropper case, both of which can be numerically calculated conveniently.

[1]The idea of randomized beamforming using multi-antennas has been proposed in multi-user diversity literatures [37], [38], where the technique is to increase the fluctuation and diversity of the slow fading channels so as to provide multi-user diversity gain.

[2]The channel capacity with non-coherent detection is studied in [31], [32] for SISO Rayleigh fading channels and in [33]–[35] for MIMO Rayleigh fading channels.

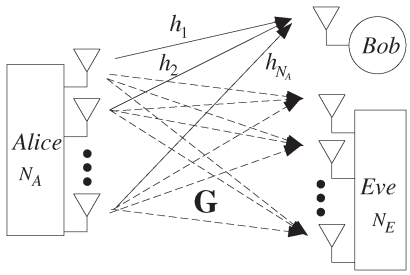


Fig. 1. System model of the secure transmission of a MISO system.

2) We also investigate the impact of the AFF period to the secrecy rate lower bound, and reveal that the efficiency of the AFF scheme depends heavily on how fast the artificial fading is, which has not been addressed in [28]–[30].
3) We compare the secrecy performance of the AN and AFF schemes and achieve an interesting and important observation: *When the eavesdropper has less antennas than that of the transmitter, the AN scheme outperforms the AFF scheme, otherwise, the AFF scheme achieves better secrecy at the high SNR regime*. When the number of the eavesdropper's antenna is twice of the transmitter's, the AFF scheme still works well while the AN scheme almost fails. This indicates that the AFF scheme is more robust to the multi-antenna eavesdropper. This conclusion has not been revealed by any other works yet.
4) Motivated by the above observation, we propose a hybrid AN-AFF scheme. By a proper power allocation, the achievable secrecy rate can be increased further.

The organization of the paper is as follows. In Section II, we describe the system model and the AN scheme. In Sections III and IV, we investigate the AFF scheme and analyze its secrecy rate. In Section V, we evaluate the impact of the AFF period and in Section VI, we propose the hybrid AN-AFF scheme. In Section VII, we present some simulation experiments to illustrate the performance of these schemes, and finally, Section VIII concludes the paper.

We use upper- and lowercase bold-faced letters to denote matrices and column vectors, respectively. Superscripts $(\cdot)^*$, $(\cdot)^T$, $(\cdot)^H$, and $(\cdot)^{-1}$ represent conjugate, transpose, Hermitian, and inverse, respectively. $\boldsymbol{I}$ is the identity matrix. $\mathrm{diag}(\cdot)$ is diagonal matrix with main diagonal $(\cdot)$. $\det(\cdot)$ is the determinant of a matrix. $|\cdot|$ and $\|\cdot\|$ are the absolute value of a complex scalar and Euclidean/Frobenius norm of a vector/matrix, respectively. $E(\cdot)$ is the mathematical expectation of a random variable. $\Re(\cdot)$ and $\Im(\cdot)$ are the real and image part of a complex, respectively.

II. System Model

We consider a secret communication between a transmitter (Alice) with N_A antennas and a single antenna legitimate receiver (Bob) in the presence of a passive eavesdropper (Eve) with N_E antennas,[3] as shown in Fig. 1. We assume the channels

[3]We have to emphasize that the scheme and the analysis in this paper can be generalized to the multiple eavesdroppers case by using the definition of the compound wire-tap channel [5]. They can also be generalized to the case when Bob has multiple-antennas.

are flat fading and block-invariant with block length T_B. Denote the channel vector between Alice and Bob as

$$\boldsymbol{h} = [h_1 \quad h_2 \quad \cdots \quad h_{N_A}], \tag{1}$$

and the channel matrix between Alice and Eve as

$$\boldsymbol{G} = \begin{bmatrix} \boldsymbol{g}_1 \\ \boldsymbol{g}_2 \\ \vdots \\ \boldsymbol{g}_{N_E} \end{bmatrix} = \begin{bmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,N_A} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,N_A} \\ \vdots & \vdots & \ddots & \vdots \\ g_{N_E,1} & g_{N_E,2} & \cdots & g_{N_E,N_A} \end{bmatrix}. \tag{2}$$

We assume all h_n, and $g_{n,m}$, $n = 1, 2, \ldots, N_A$, $m = 1, 2, \ldots, N_E$ are complex Gaussian random variables with zero means and unit variances. At time instant k, the transmitted signal vector from Alice is $\boldsymbol{x}(k) \triangleq [x_1(k), x_2(k), \ldots, x_{N_A}(k)]^T$, then the received signal by Bob and Eve are

$$y_B(k) = \boldsymbol{h}\boldsymbol{x}(k) + n_B(k), \tag{3}$$

$$\boldsymbol{y}_E(k) = \boldsymbol{G}\boldsymbol{x}(k) + \boldsymbol{n}_E(k), \tag{4}$$

respectively, where $n_B(k)$ and the elements of $\boldsymbol{n}_E(k)$ are additive white Gaussian complex noise (AWGN) with zero-mean and variance σ_n^2.

A. Channel State Information

Since Eve is a passive eavesdropper, it is reasonable to assume that Alice does not know Eve's instantaneous CSI $\boldsymbol{G}$. On the other hand, the reliable communication between Alice and Bob requires instantaneous CSI. If Alice sends the training signals, Eve can intercept them and get the instantaneous CSI $\boldsymbol{G}$ of himself, and thus do the coherent detection to eavesdrop the information. A method to prevent Eve getting $\boldsymbol{G}$ is to take advantage of the channel reciprocity in TDD mode, where Bob transmits training sequence and Alice estimates $\boldsymbol{h}$ so that Eve does not have the chance to obtain the estimation of $\boldsymbol{G}$. With $\boldsymbol{h}$ Alice does beamforming/precoding so that Bob can detect the information directly [28]. However, when the wireless fading is not so fast, Eve can exploit some blind channel estimation techniques to attain the equivalent channel estimation (The product of beamforming/precoding coefficients and the channel coefficients). Therefore, we assume that both Alice and Bob only know the instantaneous CSI $\boldsymbol{h}$, while Eve knows both $\boldsymbol{h}$ and $\boldsymbol{G}$ perfectly, which is a more rigorous scenario for the security.

B. Ergodic Secrecy Rate With Gaussian Random Codes

Different from [28], [29] where BERs are used to measure the secrecy, in this paper, due to the channel fading, we study the *ergodic achievable secrecy rate* with Gaussian random codes, which is defined in [2], [4] as

$$R_s \triangleq R_B - R_E, \tag{5}$$

where R_B is the maximum average rate of legitimate transmission to Bob, and R_E is the maximum average rate of information leakage to Eve, both with Gaussian random codes. The secrecy rate is a fundamental measure of the physical layer security because it uses the information theory concepts, which has been adopted by most of the existing literature.

C. Artificial Noise Scheme

For comparison convenience, we briefly describe the AN scheme here. With the CSI $\boldsymbol{h}$, the transmitted signal vector $\boldsymbol{x}(k)$ of the AN scheme can be written as

$$\boldsymbol{x}(k) = \frac{\boldsymbol{h}^H}{\|\boldsymbol{h}\|} s(k) + \boldsymbol{H}_\perp \boldsymbol{v}(k), \tag{6}$$

where $s(k)$ is the information symbol for Bob with $E[|s(k)|^2] = \sigma_s^2$, $\boldsymbol{v}(k) \triangleq [v_1(k), v_2(k), \ldots, v_{N_A-1}(k)]^T$ is any random vector, and $\boldsymbol{H}_\perp$ is the projection matrix onto the null space of vector $\boldsymbol{h}^H$, the columns of which constitute an orthogonal basis for the null space of $\boldsymbol{h}^H$, i.e. $\boldsymbol{h}\boldsymbol{H}_\perp = \boldsymbol{0}$. In this way, the AN $\boldsymbol{H}_\perp \boldsymbol{v}(k)$ is transmitted spatial isotropically but will not interfere with Bob. Generally, $v_n(k)$, $n = 1, 2, \ldots, N_A - 1$ are independent and identically distributed (i.i.d.) complex Gaussian random variables each with zero-mean and variance $E[v_n^2(k)] = \sigma_v^2$, and is also independent to $s(k)$. The average transmit power of Alice is

$$P_{\text{AN}} \triangleq E\left[\|\boldsymbol{x}(k)\|^2\right] = \sigma_s^2 + (N_A - 1)\sigma_v^2. \tag{7}$$

Substituting (6) into (3) and (4) yields

$$y_B^{\text{AN}}(k) = \|\boldsymbol{h}\| s(k) + n_B(k), \tag{8}$$

$$\boldsymbol{y}_E^{\text{AN}}(k) = \frac{\boldsymbol{G}\boldsymbol{h}^H}{\|\boldsymbol{h}\|} s(k) + \boldsymbol{G}\boldsymbol{H}_\perp \boldsymbol{v}(k) + \boldsymbol{n}_E(k). \tag{9}$$

We can see that in this scheme, Bob sees an equivalent flat fading channel $\|\boldsymbol{h}\|$ while Eve sees an equivalent flat fading channel $\boldsymbol{G}\boldsymbol{h}^H/\|\boldsymbol{h}\|$ corrupted by an additive interference $\boldsymbol{G}\boldsymbol{H}_\perp \boldsymbol{v}(k)$. With CSI $\boldsymbol{h}$ and $\boldsymbol{G}$, Eve can do the coherent detection of $s(k)$. Therefore, the secrecy rate improvement of the AN scheme comes from the basic idea to deteriorate the receive SINR of Eve using AN $\boldsymbol{G}\boldsymbol{H}_\perp \boldsymbol{v}(k)$ so as to reduce the information leakage R_E. However, when Eve has more antennas than Alice, i.e., $\boldsymbol{G}$ is a tall matrix, with the CSI Eve can do the null-space receive beamforming to eliminate the AN completely. This is the intuitive reason why the AN scheme completely fails when Eve has sufficient antennas, as shown in [9].

III. Artificial Fast Fading Scheme

In this section, we describe the signal model of the AFF scheme. Since we consider the multi-antenna eavesdropper case, the model has not been well addressed in [28]–[30]. Different from the AN scheme, the basic idea of the AFF scheme is to randomly weight the information symbol $s(k)$ at different transmit antennas in a special way so that the received signal at Bob is still the intended symbol $s(k)$ while that received at Eve is corrupted by an unknown multiplicative factor, which may vary symbol by symbol. So Eve will see

an equivalent AFF channel, which prevents the blind channel estimation. Mathematically, Alice transmits signal vector

$$\boldsymbol{x}(k) = \boldsymbol{\omega}^H(k)s(k) \tag{10}$$

at time k, where $\boldsymbol{\omega}(k) = [\omega_1(k), \omega_2(k), \ldots \omega_{N_A}(k)]$ is the weight coefficient vector. To generate AFF we let all $\omega_n(k)$'s be random variables with the only constraint $\boldsymbol{h}\boldsymbol{\omega}^H(k) = 1$. This can be easily done as follows. We first generate $N_A - 1$ elements $\omega_n(k)$, $n = 1, 2, \ldots, N_A - 1$, completely randomly, and then calculate the last element $\omega^*_{N_A}(k)$ by

$$\omega^*_{N_A}(k) = \frac{1 - \sum_{n=1}^{N_A-1} h_n\omega^*_n(k)}{h_{N_A}}. \tag{11}$$

Here, we assume $\omega_n(k)$, $n = 1, 2, \ldots, N_A - 1$, are i.i.d. complex Gaussian random variables with zero-mean and variance $E[|\omega_n(k)|^2] = \sigma^2_\omega$. In such a way, the signal received by Bob is

$$y^{\mathrm{AFF}}_B(k) = s(k) + n_B(k), \tag{12}$$

so that he can decode the received signal directly, without the channel coefficients $\boldsymbol{h}$, and the signal received by Eve is

$$\boldsymbol{y}^{\mathrm{AFF}}_E(k) = \boldsymbol{G}\boldsymbol{\omega}^H(k)s(k) + \boldsymbol{n}_E(k) = \boldsymbol{h}_e(k)s(k) + \boldsymbol{n}_E(k), \tag{13}$$

where $\boldsymbol{h}_e(k) \triangleq \boldsymbol{G}\boldsymbol{\omega}^H(k)$, $n_B(k)$ and $\boldsymbol{n}_E(k)$ are AWGN with zero-mean and the same variance σ^2_n. Denote $\bar{\boldsymbol{\omega}}(k) \triangleq [\omega_1(k), \omega_2(k), \ldots \omega_{N_A-1}(k)]$, then we have $\bar{\boldsymbol{\omega}}(k) \sim \mathcal{CN}(\boldsymbol{0}, \sigma^2_\omega \boldsymbol{I}_{N_A-1})$, and $\boldsymbol{\omega}^H(k) = \boldsymbol{A}\bar{\boldsymbol{\omega}}^H(k) + \boldsymbol{b}$ where

$$\boldsymbol{A} \triangleq \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & 1 \\ -\frac{h_1}{h_{N_A}} & -\frac{h_2}{h_{N_A}} & \cdots & \cdots & -\frac{h_{N_A-1}}{h_{N_A}} \end{bmatrix}_{N_A \times (N_A-1)},$$

and $\boldsymbol{b} \triangleq [0, \ldots, 0, (1/h_{N_A})]^T$.

Since we consider the block fading case, for any realization of $\boldsymbol{h}$ and $\boldsymbol{G}$, they keep invariant in each coherent fading block. $\bar{\boldsymbol{\omega}}(k)$ is controlled by Alice and varies in different time instant k in one coherent fading block. Therefore, for each $\boldsymbol{h}$, the average transmit power of Alice is

$$\begin{aligned} P_{\mathrm{AFF}} &= E\left(|s|^2 \sum_{n=1}^{N_A} |\omega_n|^2\right) \\ &= (N_A - 1)\sigma^2_\omega\sigma^2_s + \frac{\sigma^2_s + \sigma^2_s \sum_{n=1}^{N_A-1} |h_n|^2\sigma^2_\omega}{|h_{N_A}|^2}, \\ &= \sum_{n=1}^{N_A-1} \left(1 + \frac{|h_n|^2}{|h_{N_A}|^2}\right)\sigma^2_\omega\sigma^2_s + \frac{\sigma^2_s}{|h_{N_A}|^2}. \end{aligned} \tag{14}$$

With the power constraint P_{AFF}, σ^2_s can be expressed as

$$\sigma^2_s = \frac{P_{\mathrm{AFF}}}{\sigma^2_\omega \sum_{n=1}^{N_A-1} \left(1 + \frac{|h_n|^2}{|h_{N_A}|^2}\right) + \frac{1}{|h_{N_A}|^2}}. \tag{15}$$

On the other hand, $\boldsymbol{h}_e(k)$ is a complex Gaussian random vector with mean $\boldsymbol{a}_e$ and covariance matrix $\boldsymbol{C}_e$ as, respectively,

$$\boldsymbol{a}_e = \boldsymbol{G}\boldsymbol{b}, \qquad \boldsymbol{C}_e = \sigma^2_\omega \boldsymbol{G}\boldsymbol{A}\boldsymbol{A}^H\boldsymbol{G}^H, \tag{16}$$

i.e., $\boldsymbol{h}_e(k) \sim \mathcal{CN}(\boldsymbol{a}_e, \boldsymbol{C}_e)$. From (13) and (11), the m-th element of $\boldsymbol{h}_e(k)$ is

$$\begin{aligned} h_{e,m}(k) &= \sum_{n=1}^{N_A} g_{m,n}\omega^*_n(k) \\ &= \sum_{n=1}^{N_A-1} g_{m,n}\omega^*_n(k) + \frac{g_{m,N_A}}{h_{N_A}}\left(1 - \sum_{n=1}^{N_A-1} h_n\omega^*_n(k)\right) \\ &= \sum_{n=1}^{N_A-1} \left(g_{m,n} - \frac{g_{m,N_A}}{h_{N_A}}h_n\right)\omega^*_n(k) + \frac{g_{m,N_A}}{h_{N_A}}, \end{aligned} \tag{17}$$

for $m = 1, 2, \ldots, N_E$. Consequently, (13) and (17) show that under the AFF scheme, Eve will see an equivalent random SIMO fast fading channel $\boldsymbol{h}_e(k)$ artificially varying even symbol by symbol (The impact of fading period to the secrecy rate has been discussed in Section V.). It is interesting to see that the equivalent channel coefficient $h_{e,m}(k)$ is a complex Gaussian random variable satisfying

$$h_{e,m}(k) \sim \mathcal{CN}\left(\frac{g_{m,N_A}}{h_{N_A}}, \sum_{n=1}^{N_A-1} \left|g_{m,n} - \frac{g_{m,N_A}h_n}{h_{N_A}}\right|^2 \sigma^2_\omega\right). \tag{18}$$

Generally, the mean $(g_{m,N_A}/h_{N_A}) \neq 0$, thus the envelop of $h_{e,m}(k)$ obeys the *Ricean distribution*. The fast fading prevents Eve from getting the estimation of instantaneous $\boldsymbol{h}_e(k)$. Thus, Eve can only detect the information symbol non-coherently with only the statistical knowledge of the equivalent channel (17),[4] which greatly reduces the information leakage rate, as analyzed in the following sections.

Remark 1: The channel capacity with non-coherent detection is studied in [31], [32] for SISO Rayleigh fading channels and in [33]–[35] for MIMO Rayleigh fading channels. With Gaussian input, the achievable rate of non-coherent SISO and MIMO Rayleigh channels are investigated in [36], and closed-form expressions are found. Here, we have to calculate the rate of a non-coherent *Ricean fading SIMO channel* with Gaussian input, which has not been yet derived. In [30], an upper bound of the non-coherent capacity of a *SISO* channel has been derived, which is very loose since the Riciean distribution of the equivalent channel has not been taken into consideration.

IV. Secrecy Rate Analysis

A. Secrecy Rate Analysis of the AFF Scheme

Denote R^{AFF}_s as the ergodic secrecy rate of the AFF scheme. According to the definition in (5), we have $R^{\mathrm{AFF}}_s = R^{\mathrm{AFF}}_B - R^{\mathrm{AFF}}_E$. From (12) and (13), we can see that the AFF scheme

[4]Note that the statistical knowledge (18) of the equivalent wiretap channel is due to the special structure of the beamformer $\boldsymbol{h}\boldsymbol{\omega}^H(k) = 1$, which implies that Eve has already utilized this prior information of the special structure of the beamformer.

leads to an equivalent AWGN channel with $\text{SNR}_B = (\sigma_s^2/\sigma_n^2)$ for Bob and an equivalent fading channel for Eve. With a Gaussian input, the rate to Bob is

$$R_B^{\text{AFF}} = \log\left(1 + \frac{\sigma_s^2}{\sigma_n^2}\right). \tag{19}$$

To investigate the impact of AFF to the information leakage, we assume that the artificial fading fades much faster than the channels $\boldsymbol{h}$ and $\boldsymbol{G}$ do so that they are invariant during many artificial fading periods. We drop the subscript $_E$ and the time index k in (13) for notational convenience. The receiving model is now

$$\boldsymbol{y} = \boldsymbol{h}_e s + \boldsymbol{n}, \tag{20}$$

where we have $s \sim \mathcal{CN}(0, \sigma_s^2)$, $\boldsymbol{n} \sim \mathcal{CN}(\boldsymbol{0}, \sigma_n^2 \boldsymbol{I}_{N_E})$, and $\boldsymbol{h}_e \sim \mathcal{CN}(\boldsymbol{a}_e, \boldsymbol{C}_e)$. Due to the fast fading, Eve detects s non-coherently without the instantaneous CSI $\boldsymbol{h}_e$, and the average rate of information leakage to Eve is

$$\begin{aligned} R_E^{\text{AFF}} &= E_{\boldsymbol{h},\boldsymbol{G}}\left\{I(s;\boldsymbol{y}|\boldsymbol{h},\boldsymbol{G})\right\} \\ &= E_{\boldsymbol{h},\boldsymbol{G}}\left\{h(\boldsymbol{y}|\boldsymbol{h},\boldsymbol{G}) - h(\boldsymbol{y}|s,\boldsymbol{h},\boldsymbol{G})\right\}, \end{aligned} \tag{21}$$

where $I(\cdot;\cdot)$ denotes the mutual information, and $h(\cdot)$ is the differential entropy. Hereinafter we omit the condition on $\boldsymbol{h}$ and $\boldsymbol{G}$ just for brevity. We then have $h(\boldsymbol{y}) \triangleq -\int p(\boldsymbol{y}) \log p(\boldsymbol{y}) d\boldsymbol{y}$, and

$$\begin{aligned} h(\boldsymbol{y}|s) &\triangleq -\int\int p(s,\boldsymbol{y}) \log p(\boldsymbol{y}|s)\, ds\, d\boldsymbol{y} \\ &= -\int p(s) \int p(\boldsymbol{y}|s) \log p(\boldsymbol{y}|s)\, d\boldsymbol{y}\, ds. \end{aligned}$$

In the following parts, we will derive the expressions of $h(\boldsymbol{y})$ and $h(\boldsymbol{y}|s)$ to get $I(s;\boldsymbol{y})$.

First, conditioned on $\boldsymbol{h}_e$, we have $\boldsymbol{y}|\boldsymbol{h}_e \sim \mathcal{CN}(\boldsymbol{0}, \sigma_s^2 \boldsymbol{h}_e \boldsymbol{h}_e^H + \sigma_n^2 \boldsymbol{I}_{N_E})$, i.e., the probability density function (pdf) is

$$p_{\boldsymbol{y}}(\boldsymbol{y}|\boldsymbol{h}_e) = \frac{\exp\left[-\boldsymbol{y}^H \left(\sigma_s^2 \boldsymbol{h}_e \boldsymbol{h}_e^H + \sigma_n^2 \boldsymbol{I}_{N_E}\right)^{-1} \boldsymbol{y}\right]}{\pi^{N_E} \det\left(\sigma_s^2 \boldsymbol{h}_e \boldsymbol{h}_e^H + \sigma_n^2 \boldsymbol{I}_{N_E}\right)}. \tag{22}$$

Note that

$$\begin{aligned} \det\left(\sigma_s^2 \boldsymbol{h}_e \boldsymbol{h}_e^H + \sigma_n^2 \boldsymbol{I}_{N_E}\right) &= \sigma_n^{2N_E} \det\left(\frac{\sigma_s^2}{\sigma_n^2} \boldsymbol{h}_e \boldsymbol{h}_e^H + \boldsymbol{I}_{N_E}\right) \\ &= \sigma_n^{2N_E}\left(1 + \frac{\sigma_s^2}{\sigma_n^2}\|\boldsymbol{h}_e\|^2\right), \end{aligned}$$

where the last equation comes from the determinant identity $\det(\boldsymbol{I} + \boldsymbol{DB}) = \det(\boldsymbol{I} + \boldsymbol{BD})$. Meanwhile,

$$\begin{aligned} \left(\sigma_s^2 \boldsymbol{h}_e \boldsymbol{h}_e^H + \sigma_n^2 \boldsymbol{I}_{N_E}\right)^{-1} &= \frac{1}{\sigma_n^2}\left(\boldsymbol{I}_{N_E} + \frac{\sigma_s^2}{\sigma_n^2} \boldsymbol{h}_e \boldsymbol{h}_e^H\right)^{-1} \\ &= \frac{1}{\sigma_n^2}\left(\boldsymbol{I}_{N_E} - \frac{\frac{\sigma_s^2}{\sigma_n^2} \boldsymbol{h}_e \boldsymbol{h}_e^H}{1 + \frac{\sigma_s^2}{\sigma_n^2}\|\boldsymbol{h}_e\|^2}\right), \end{aligned}$$

where the last equation comes from the special case of the matrix inverse lemma $(\boldsymbol{B} + b\boldsymbol{u}\boldsymbol{v}^H)^{-1} = \boldsymbol{B}^{-1} - (b/(1 + b\boldsymbol{v}^H \boldsymbol{B}^{-1}\boldsymbol{u}))\boldsymbol{B}^{-1}\boldsymbol{u}\boldsymbol{v}^H \boldsymbol{B}^{-1}$. Now (22) can be rewritten as:

$$p_{\boldsymbol{y}}(\boldsymbol{y}|\boldsymbol{h}_e) = \frac{\exp\left[\frac{1}{\sigma_n^2}\left(\frac{\frac{\sigma_s^2}{\sigma_n^2}\|\boldsymbol{y}^H \boldsymbol{h}_e\|^2}{1 + \frac{\sigma_s^2}{\sigma_n^2}\|\boldsymbol{h}_e\|^2} - \|\boldsymbol{y}\|^2\right)\right]}{(\pi\sigma_n^2)^{N_E}\left(1 + \frac{\sigma_s^2}{\sigma_n^2}\|\boldsymbol{h}_e\|^2\right)}. \tag{23}$$

On the other hand, we have the pdf of $\boldsymbol{h}_e$ is

$$p_{\boldsymbol{h}_e}(\boldsymbol{h}_e) = \frac{1}{\pi^{N_E} \det(\boldsymbol{C}_e)} \exp\left(-(\boldsymbol{h}_e - \boldsymbol{a}_e)^H \boldsymbol{C}_e^{-1}(\boldsymbol{h}_e - \boldsymbol{a}_e)\right). \tag{24}$$

Then we can substitute (23) and (24) into $p_{\boldsymbol{y}}(\boldsymbol{y}) = \int p_{\boldsymbol{y}}(\boldsymbol{y}|\boldsymbol{h}_e) p_{\boldsymbol{h}_e}(\boldsymbol{h}_e)\, d\boldsymbol{h}_e$ to get $p_{\boldsymbol{y}}(\boldsymbol{y})$. However, we can not get a closed-form expression of $p_{\boldsymbol{y}}(\boldsymbol{y})$. Even the numerical calculation will be quickly prohibited as the dimension of $\boldsymbol{h}_e$ increases since a $2N_E$ dimensional real integral is required. The problem makes obtaining the exact evaluation of $I(s;\boldsymbol{y})$ in (21) very difficult.

To address this, we next will find an upper-bound of $I(s;\boldsymbol{y})$, which can be calculated more conveniently. Let us first consider the received signal at antenna 1 of Eve, i.e., $y_1 = h_{e,1} s + n_1$, and calculate $I(s;y_1) = h(y_1) - h(y_1|s)$. From (18), $h_{e,1} \sim \mathcal{CN}(a_{e,1}, \sigma_{h_{e,1}}^2)$, where $a_{e,1} \triangleq (g_{1,N_A}/h_{N_A})$, and $\sigma_{h_{e,1}}^2 \triangleq \sum_{n=1}^{N_A-1} |g_{1,n} - (g_{1,N_A} h_n/h_{N_A})|^2 \sigma_\omega^2$. Its pdf is $p_{h_{e,1}}(h_{e,1}) = (1/\pi\sigma_{h_{e,1}}^2)\exp[-(|h_{e,1} - a_{e,1}|^2/\sigma_{h_{e,1}}^2)]$. Let $r_{h_{e,1}} \triangleq |h_{e,1}|$, and $\theta \triangleq \arctan(\Im(h_{e,1})/\Re(h_{e,1}))$, then $r_{h_{e,1}}$ has a Ricean distribution and θ has an uniform distribution over $[0, 2\pi)$, i.e.,

$$\begin{aligned} &p_{h_{e,1}}\left(r_{h_{e,1}}, \theta\right) \\ &\quad = \frac{r_{h_{e,1}}}{\pi\sigma_{h_{e,1}}^2} \exp\left(-\frac{r_{h_{e,1}}^2 + r_{a_{e,1}}^2 - 2r_{h_{e,1}} r_{a_{e,1}} \cos(\theta - \phi)}{\sigma_{h_{e,1}}^2}\right). \end{aligned} \tag{25}$$

where $r_{a_{e,1}} \triangleq |a_{e,1}|$, and $\phi \triangleq \arctan(\Im(a_{e,1})/\Re(a_{e,1}))$. The conditional pdf of y_1 with fixed $h_{e,1}$ is $y_1|h_{e,1} \sim \mathcal{CN}(0, |h_{e,1}|^2\sigma_s^2 + \sigma_n^2)$, so

$$p_{y_1}(y_1|h_{e,1}) = \frac{1}{\pi\left(|h_{e,1}|^2\sigma_s^2 + \sigma_n^2\right)} \exp\left[-\frac{|y_1|^2}{|h_{e,1}|^2\sigma_s^2 + \sigma_n^2}\right]. \tag{26}$$

We then have the pdf of y_1 as (27), shown at the bottom of the next page, where $I_0(\cdot)$ is the zero order modified Bessel function of the first kind. In the second equation we change the orthogonal coordinates to the polar coordinates. In the third and last equation we just plug (25) and (26) in, respectively. Using (27), the differential entropy of y_1 can be calculated as

$$\begin{aligned} h(y_1) &= -\int \log p_{y_1}(y_1) p_{y_1}(y_1)\, dy_1 \\ &= -\int_{r_{y_1}}\int_{\varphi_{y_1}} \log\left(p_{y_1}(r_{y_1})\right) p_{y_1}(r_{y_1})\, r_{y_1}\, dr_{y_1}\, d\varphi_{y_1} \\ &= -2\pi \int_0^{+\infty} \log p_{y_1}(r_{y_1})\, p_{y_1}(r_{y_1})\, r_{y_1}\, dr_{y_1}, \end{aligned} \tag{28}$$

where $\varphi_{y_1} \triangleq \arctan(\Im(y_1)/\Re(y_1))$ has an uniform distribution over $[0, 2\pi)$.

To calculate $h(y_1|s) \triangleq -\int p_s(s) \int p(y_1|s) \log p(y_1|s)\, dy_1\, ds$, we first notice that conditioned on s, we have $y_1|s \sim \mathcal{CN}(a_{e,1}s, |s|^2\sigma^2_{h_{e,1}} + \sigma^2_n)$, and

$$q(s) \triangleq -\int p(y_1|s) \log p(y_1|s)\, dy_1 = \log \pi e \left(|s|^2\sigma^2_{h_{e,1}} + \sigma^2_n\right). \quad (29)$$

Denoting $r_s \triangleq |s|$, we can re-write $p_s(s)$ as $p_s(r_s) = (1/\pi\sigma^2_s)\exp(-(r^2_s/\sigma^2_s))$. Using the similar derivation as in (28), we have the following equations hold:

$$\begin{aligned} h(y_1|s) &= \int q(s)p_s(s)\, ds \\ &= 2\pi \int_{r_s} q(r_s)p_s(r_s)r_s\, dr_s = \log\left(\pi e\sigma^2_n\right) \\ &\quad + \frac{2}{\sigma^2_s}\int_{r_s} r_s \exp\left(-\frac{r^2_s}{\sigma^2_s}\right)\log\left(1 + \frac{\sigma^2_{h_{e,1}}}{\sigma^2_n}r^2_s\right) dr_s \\ &= \log\left(\pi e\sigma^2_n\right) + \int_0^{+\infty} \log(1+\beta_1 t)e^{-t}\, dt, \end{aligned} \quad (30)$$

where $\beta_1 \triangleq \sigma^2_{h_{e,1}}\sigma^2_s/\sigma^2_n$, and in the last equation we apply argument substitution $t \triangleq r^2_s/\sigma^2_s$, $t \in [0, +\infty)$. Using $h(y_1)$ obtained in (28) and $h(y_1|s)$ in (30), we can calculate the information leakage rate to antenna 1 of Eve $I(s; y_1)$. To calculate $h(y_1)$, a 2-dimensional real integral is required, and calculating $h(y_1|s)$ requires an 1-dimensional real integral. Although the integral upper bound is infinity, the integrands are negative exponential functions, which converge to zero very quickly and can be numerically calculated conveniently. Similarly, we can calculate the information leakage rate $I(s; y_n)$ to the antenna n of Eve numerically.

So far, we have derived the exact expression of the leakage rate to each single antenna. Next we will derive an upper bound of $I(s; \boldsymbol{y})$ of the multi-antenna case. We have the following lemma:

Lemma 1: The following inequality holds:

$$I(s; \boldsymbol{y}) < \sum_{n=1}^{N_E} I(s; y_n), \quad (31)$$

where y_n is the n-th element in $\boldsymbol{y}$.

Proof: See Appendix A. ■

Instead of the exact expression of $I(s; \boldsymbol{y})$, we find an upper bound that can be calculated numerically. The bound is intuitively correct since the information rate of an equivalent SIMO channel is definitely less than the sum of the information rate from the transmitter to each receive antenna.

Finally, with (19), (28)–(31), we get the lower bound of the secrecy rate $R_s^{\mathrm{AFF,L}}$ as

$$R_s^{\mathrm{AFF}} \geq R_s^{\mathrm{AFF,L}} \triangleq R_B^{\mathrm{AFF}} - R_E^{\mathrm{AFF,U}}. \quad (32)$$

where $R_E^{\mathrm{AFF,U}} \triangleq E_{\boldsymbol{h},\boldsymbol{G}}(\sum_{n=1}^{N_E} I(s; y_n))$. Note that (31) is calculated based on fixed $\boldsymbol{h}$ and $\boldsymbol{G}$. The ergodic secrecy rate can be obtained by averaging $\boldsymbol{h}$ and $\boldsymbol{G}$ according to their statistical distributions. Although we can not get an exact expression, in the simulations we will see that the lower bound is still larger than the exact secrecy rate of the AN scheme, when N_E is large.

Remark 2: In [25], the authors have investigated the achievable secrecy rate with Gaussian random codes when the main channel is an AWGN channel, while the eavesdropper's channel is Rayleigh fading with additive Gaussian noise. Adopting the AFF scheme in this paper, the equivalent channels may seem similar to the scenario considered in [25]. However, the differences lie in that: 1) The fading channel between Alice and Eve is Rayleigh distributed in [25] while in our paper it is an artificial channel with Ricean distribution, which is more general; 2) It is assumed that Eve can perfectly observe the instantaneous CSI of itself in [25] while in our case, instantaneous CSI can not be obtained by Eve due to the AFF.

$$\begin{aligned} p_{y_1}(y_1) &= \int p_{y_1}(y_1|h_{e,1})p_{h_{e,1}}(h_{e,1})\, dh_{e,1} \\ &= \int_{r_{h_{e,1}}=0}^{+\infty}\int_{\theta=0}^{2\pi} p_{y_1}\left(y_1|r_{h_{e,1}}, \theta\right) p_{h_{e,1}}\left(r_{h_{e,1}}, \theta\right)\, dr_{h_{e,1}}\, d\theta \\ &= \int_{r_{h_{e,1}}=0}^{+\infty} p_{y_1}\left(y_1|r_{h_{e,1}}\right)\frac{2r_{h_{e,1}}}{\sigma^2_{h_{e,1}}}\exp\left(-\frac{r^2_{h_{e,1}} + r^2_{a_{e,1}}}{\sigma^2_{h_{e,1}}}\right) I_0\left(\frac{2r_{h_{e,1}}r_{a_{e,1}}}{\sigma^2_{h_{e,1}}}\right) dr_{h_{e,1}} \\ &= \int_0^{+\infty} \frac{2r_{h_{e,1}}}{\pi\left(r^2_{h_{e,1}}\sigma^2_s + \sigma^2_n\right)\sigma^2_{h_{e,1}}} I_0\left(\frac{2r_{h_{e,1}}r_{a_{e,1}}}{\sigma^2_{h_{e,1}}}\right)\exp\left(-\frac{|y_1|^2}{r^2_{h_{e,1}}\sigma^2_s + \sigma^2_n} - \frac{r^2_{h_{e,1}} + r^2_{a_{e,1}}}{\sigma^2_{h_{e,1}}}\right) dr_{h_{e,1}} \end{aligned} \quad (27)$$

B. Transmit Power Analysis

As shown in Sec. III-A, in one coherent fading-block with fixed $\boldsymbol{h}$, the average transmit power of Alice is (14)

$$P_{\mathrm{AFF}} = \sum_{n=1}^{N_A-1}\left(1+\frac{|h_n|^2}{|h_{N_A}|^2}\right)\sigma_\omega^2\sigma_s^2+\frac{\sigma_s^2}{|h_{N_A}|^2}.$$

Note that since all $h_n \sim \mathcal{CN}(0,1),\ n=1,2,\ldots,N_A$, when $|h_{N_A}|^2$ is in deep fading, the transmit power of Alice could go extremely large. Indeed, we have

$$E\left(\frac{1}{|h_{N_A}|^2}\right)=\int_0^\infty \frac{1}{\gamma}e^{-\gamma}d\gamma > \int_0^\rho \frac{1}{\gamma}e^{-\gamma}d\gamma > e^{-\rho}\int_0^\rho \frac{1}{\gamma}d\gamma=\infty.$$

To avoid this, we choose $N_A \triangleq \arg\max_n\{|h_n|^2\}$, i.e., choose the antenna with the largest channel fading amplitude as the N_A-th antenna and set its weigh as (11). Then we have the pdf of $|h_{N_A}|^2$ as $p_{|h_{N_A}|^2}(\gamma)=N_A(1-e^{-\gamma})^{N_A-1}e^{-\gamma}$ and

$$\begin{aligned}E\left(\frac{1}{|h_{N_A}|^2}\right)&=N_A\int_0^\infty \frac{1}{\gamma}(1-e^{-\gamma})^{N_A-1}e^{-\gamma}d\gamma\\&=(-1)^{N_A}N_A\sum_{\nu=0}^{N_A-1}(-1)^\nu\binom{N_A-1}{\nu}\ln(N_A-\nu),\end{aligned} \tag{33}$$

where the second equation comes from [36, p.354]. In such a way, we eliminate the impact of deep fading to the transmit power.

It seems that the beamformer has an uneven transmission power at different antennas. However, according to the above antenna selection strategy, this can be avoided by selecting the N_A-th antenna in an alternating manner. Specially, since the channels of different antennas are i.i.d. distributed, each antenna has an identical probability to be $\arg\max_n\{|h_n|^2\}$. Therefore, *in the average sense*, the powers of all the antennas are even.

C. Artificial Noise

For comparison, we give the ergodic secrecy rate of the AN scheme. Recalling (8) and (9), the leakage rate is now

$$R_E^{\mathrm{AN}} = E_{\boldsymbol{h},\boldsymbol{G}}\left\{\log\det\left(\boldsymbol{I}_{N_E}+\frac{\boldsymbol{G}\boldsymbol{h}^H\boldsymbol{h}\boldsymbol{G}^H}{\|\boldsymbol{h}\|^2}\left(\sigma_n^2\boldsymbol{I}_{N_E}+\sigma_v^2\boldsymbol{G}\boldsymbol{H}_\perp\boldsymbol{H}_\perp^H\boldsymbol{G}^H\right)^{-1}\right)\right\}, \tag{34}$$

where $\sigma_v^2=(P_{\mathrm{AN}}-\sigma_s^2)/(N_A-1)$ according to (7). The exact ergodic secrecy rate of the AN scheme is

$$R_s^{\mathrm{AN}} = E_{\boldsymbol{h}}\left\{\log\left(1+\frac{\sigma_s^2\|\boldsymbol{h}\|^2}{\sigma_n^2}\right)\right\}-R_E^{\mathrm{AN}}. \tag{35}$$

Note that R_s^{AN} is a function of σ_s^2 and σ_v^2. Since $P_{\mathrm{AN}}=\sigma_s^2+(N_A-1)\sigma_v^2$, to maximize R_s^{AN} we have to solve the power allocation problem between σ_s^2 and σ_v^2. In [24], it has been found that when Eve only has a single antenna, the optimal power split between the information signal and the AN to maximize the ergodic secrecy rate is nearly half-half.[5] As N_E increases, more power should be allocated to the AN.

V. The Impact of the AFF Period

The above derivations consider the case when the random weight vector $\boldsymbol{\omega}(k)$ varies symbol by symbol. In this section, we derive the lower bound of the secrecy rate when $\boldsymbol{\omega}(k)$ varies every K symbols ($K \ll T_B$). In the simulations, we will show how the varying period K impacts the secrecy rate. Let us first focus on calculating the upper bound of leakage rate $R_{E,K}^{\mathrm{AFF}}$. Similarly, we first derive the information leakage to antenna 1 of Eve.

Since $\boldsymbol{\omega}(k)$ varies every K symbols and $\boldsymbol{G}$ is constant in the whole coherent block, we collect K successive received symbols at antenna 1 of Eve with the same $h_{e,1}$ into a vector $\bar{\boldsymbol{y}}_1=[y_1(1),y_1(2),\ldots,y_1(K)]^T$. We have

$$\bar{\boldsymbol{y}}_1 = h_{e,1}\boldsymbol{s}+\bar{\boldsymbol{n}}_1, \tag{36}$$

where $\boldsymbol{s}\triangleq[s(1),s(2),\ldots,s(K)]^T$ and $\bar{\boldsymbol{n}}_1\triangleq[n_1(1),n_1(2),\ldots,n_1(K)]^T$. In this case, the average rate of the information leakage to antenna 1 of Eve is

$$\frac{1}{K}I(\boldsymbol{s};\bar{\boldsymbol{y}}_1)=\frac{1}{K}\left[h(\bar{\boldsymbol{y}}_1)-h(\bar{\boldsymbol{y}}_1|\boldsymbol{s})\right]. \tag{37}$$

Conditioned on $h_{e,1}$, we have $\bar{\boldsymbol{y}}_1|h_{e,1}\sim\mathcal{CN}(\boldsymbol{0},\sigma_s^2|h_{e,1}|^2\boldsymbol{I}_K+\sigma_n^2\boldsymbol{I}_K)$. Similar to (27), we have

$$\begin{aligned}p_{\bar{\boldsymbol{y}}_1}(\bar{\boldsymbol{y}}_1)&=\int p_{\bar{\boldsymbol{y}}_1}(\bar{\boldsymbol{y}}_1|h_{e,1})p_{h_{e,1}}(h_{e,1})\,dh_{e,1}\\&=\int_0^{+\infty}\frac{2r_{h_{e,1}}}{\pi^K\left(r_{h_{e,1}}^2\sigma_s^2+\sigma_n^2\right)^K\sigma_{h_{e,1}}^2}I_0\left(\frac{2r_{h_{e,1}}r_{a_{e,1}}}{\sigma_{h_{e,1}}^2}\right)\\&\quad\times\exp\left(-\frac{\|\bar{\boldsymbol{y}}_1\|^2}{r_{h_{e,1}}^2\sigma_s^2+\sigma_n^2}-\frac{r_{h_{e,1}}^2+r_{a_{e,1}}^2}{\sigma_{h_{e,1}}^2}\right)dr_{h_{e,1}}.\end{aligned} \tag{38}$$

Using (38), the differential entropy of $\bar{\boldsymbol{y}}_1$ can be calculated as $h(\bar{\boldsymbol{y}}_1)=-\int p_{\bar{\boldsymbol{y}}_1}(\bar{\boldsymbol{y}}_1)\log p_{\bar{\boldsymbol{y}}_1}(\bar{\boldsymbol{y}}_1)\,d\bar{\boldsymbol{y}}_1$. However, similar to calculating $h(\boldsymbol{y})$ in Section IV, a $2K$-dimensional real integral is required, which is prohibited when K increases. In the following, we will derive a more compact form of $h(\bar{\boldsymbol{y}}_1)$. The basic idea is to transform the Cartesian coordinates to the hyperspherical coordinates $(r_{\bar{\boldsymbol{y}}_1},\boldsymbol{\varphi}_{\bar{\boldsymbol{y}}_1})$ where $r_{\bar{\boldsymbol{y}}_1}\triangleq\|\bar{\boldsymbol{y}}_1\|$, and $\boldsymbol{\varphi}_{\bar{\boldsymbol{y}}_1}\triangleq[\varphi_1,\varphi_2,\ldots\varphi_{2K-1}]$ is defined in Appendix B. Since $p_{\bar{\boldsymbol{y}}_1}(\bar{\boldsymbol{y}}_1)$ is only related to $r_{\bar{\boldsymbol{y}}_1}$, we thus re-denote $p_{\bar{\boldsymbol{y}}_1}(\bar{\boldsymbol{y}}_1)$ as $p_{\bar{\boldsymbol{y}}_1}(r_{\bar{\boldsymbol{y}}_1})$, by changing $\|\bar{\boldsymbol{y}}_1\|$ in (23) to $r_{\bar{\boldsymbol{y}}_1}$.

[5] Strictly speaking, the authors in [24] investigated the power allocation for a *lower bound* of the ergodic secrecy rate of the AN scheme, where the noise at Eve was omitted.

We have the following equations hold

$$\begin{aligned} h(\bar{\boldsymbol{y}}_1) &= -\int_{r_{\bar{\boldsymbol{y}}_1}}\int_{\boldsymbol{\varphi}_{\bar{\boldsymbol{y}}_1}} \log\left(p_{\bar{\boldsymbol{y}}_1}\left(r_{\bar{\boldsymbol{y}}_1}\right)\right) p_{\bar{\boldsymbol{y}}_1}\left(r_{\bar{\boldsymbol{y}}_1}\right) \\ &\quad \times \left|\det\left(\boldsymbol{J}(r_{\bar{\boldsymbol{y}}_1}, \boldsymbol{\varphi}_{\bar{\boldsymbol{y}}_1})\right)\right| dr_{\bar{\boldsymbol{y}}_1}\, d\boldsymbol{\varphi}_{\bar{\boldsymbol{y}}_1} \\ &= -\int_{r_{\bar{\boldsymbol{y}}_1}} \log p_{\bar{\boldsymbol{y}}_1}\left(r_{\bar{\boldsymbol{y}}_1}\right) p_{\bar{\boldsymbol{y}}_1}\left(r_{\bar{\boldsymbol{y}}_1}\right) dr_{\bar{\boldsymbol{y}}_1} \\ &\quad \times \int_{\boldsymbol{\varphi}_{\bar{\boldsymbol{y}}_1}} \left|\det\left(\boldsymbol{J}(r_{\bar{\boldsymbol{y}}_1}, \boldsymbol{\varphi}_{\bar{\boldsymbol{y}}_1})\right)\right| d\boldsymbol{\varphi}_{\bar{\boldsymbol{y}}_1} \\ &= -\int_0^{+\infty} \log p_{\bar{\boldsymbol{y}}_1}\left(r_{\bar{\boldsymbol{y}}_1}\right) p_{\bar{\boldsymbol{y}}_1}\left(r_{\bar{\boldsymbol{y}}_1}\right) r_{\bar{\boldsymbol{y}}_1}^{2K-1} \frac{2\pi^K}{\Gamma(K)}\, dr_{\bar{\boldsymbol{y}}_1}, \end{aligned} \tag{39}$$

where $\Gamma(K)$ is the gamma function, in the first equation, we change the Cartesian coordinates to the hyperspherical coordinates so $\boldsymbol{J}(r_{\bar{\boldsymbol{y}}_1}, \boldsymbol{\varphi}_{\bar{\boldsymbol{y}}_1})$ is the Jacobian matrix, and in the third equation, the integral of $\boldsymbol{\varphi}$ equals to the surface area of a $2K$-dimensional hypersphere. The detailed derivations are in Appendix B. We can see that now $h(\bar{\boldsymbol{y}}_1)$ can be calculated numerically by an one-dimensional real integral.

To calculate $h(\bar{\boldsymbol{y}}_1|\boldsymbol{s})$, we first notice that $\bar{\boldsymbol{y}}_1|\boldsymbol{s} \sim \mathcal{CN}(a_{e,1}\boldsymbol{s}, \sigma_{h_{e,1}}^2 \boldsymbol{s}\boldsymbol{s}^H + \sigma_n^2 \boldsymbol{I}_K)$. Similar to (29), we denote $q(\boldsymbol{s}) \triangleq -\int p(\bar{\boldsymbol{y}}_1|\boldsymbol{s}) \log p(\bar{\boldsymbol{y}}_1|\boldsymbol{s})\, d\bar{\boldsymbol{y}}_1$. Since the differential entropy of a complex Gaussian vector $\boldsymbol{c}$ with covariance matrix $\boldsymbol{Q}$ is $\log\det(\pi e \boldsymbol{Q})$, we then have

$$\begin{aligned} q(\boldsymbol{s}) &= \log\left[\left(\pi e \sigma_n^2\right)^K \det\left(\boldsymbol{I}_K + \frac{\sigma_{h_{e,1}}^2}{\sigma_n^2}\boldsymbol{s}\boldsymbol{s}^H\right)\right] \\ &= \log\left[\left(\pi e \sigma_n^2\right)^K \left(1 + \frac{\sigma_{h_{e,1}}^2}{\sigma_n^2} r_{\boldsymbol{s}}^2\right)\right], \end{aligned}$$

where $r_{\boldsymbol{s}} \triangleq \|\boldsymbol{s}\|$, and the second equation comes from the determinant identity $\det(\boldsymbol{I} + \boldsymbol{C}\boldsymbol{D}) = \det(\boldsymbol{I} + \boldsymbol{D}\boldsymbol{C})$. Similarly, we can rewrite $p_{\boldsymbol{s}}(\boldsymbol{s})$ as $p_{\boldsymbol{s}}(r_{\boldsymbol{s}}) = (1/\pi^K \sigma_s^{2K}) \exp(-(r_{\boldsymbol{s}}^2/\sigma_s^2))$. Using the similar derivation as in (39), we have the following equations hold:

$$\begin{aligned} h(\bar{\boldsymbol{y}}_1|\boldsymbol{s}) &= \int q(\boldsymbol{s}) p_{\boldsymbol{s}}(\boldsymbol{s})\, d\boldsymbol{s} \\ &= \int_{r_{\boldsymbol{s}}}\int_{\boldsymbol{\varphi}_{\boldsymbol{s}}} q(r_{\boldsymbol{s}}) p_{\boldsymbol{s}}(r_{\boldsymbol{s}}) \left|\det\left(\boldsymbol{J}(r_{\boldsymbol{s}}, \boldsymbol{\varphi}_{\boldsymbol{s}})\right)\right| dr_{\boldsymbol{s}}\, d\boldsymbol{\varphi}_{\boldsymbol{s}} \\ &= \frac{2\pi^K}{\Gamma(K)} \int_{r_{\boldsymbol{s}}} q(r_{\boldsymbol{s}}) p_{\boldsymbol{s}}(r_{\boldsymbol{s}}) r_{\boldsymbol{s}}^{2K-1}\, dr_{\boldsymbol{s}} \\ &= K \log\left(\pi e \sigma_n^2\right) + \frac{1}{\Gamma(K)} \int_0^{+\infty} \log(1+\beta_1 t) e^{-t} t^{K-1}\, dt, \end{aligned} \tag{40}$$

where $t \triangleq r_{\boldsymbol{s}}^2/\sigma_s^2$, $t \in [0, +\infty)$. By using the integral equation [35, p.572], we obtain the closed-form expression of $h(\bar{\boldsymbol{y}}_1|\boldsymbol{s})$ as (41), shown at the bottom of the page, where $\mathbf{Ei}(\alpha)$ is the exponential integral function $\mathbf{Ei}(\alpha) \triangleq -\int_{-\alpha}^{\infty} e^{-t}/t dt$, $\alpha < 0$.

Using (39) and (41) we obtain the information leakage rate (37) to antenna 1 of Eve, both of which only require a one-dimensional integral, respectively. Then we calculate the upper bound of the information leakage to Eve $\sum_{n=1}^{N_E} (1/K) I(\boldsymbol{s}; \bar{\boldsymbol{y}}_n)$. On the other hand, The average rate to Bob in (19) will not be changed. Therefore, we get the lower bound of the ergodic secrecy rate $R_{s,K}^{\mathrm{AFF,L}}$ as

$$R_{s,K}^{\mathrm{AFF}} \geq R_{s,K}^{\mathrm{AFF,L}} \triangleq R_B^{\mathrm{AFF}} - E_{\boldsymbol{h},\boldsymbol{G}}\left\{\frac{1}{K}\sum_{n=1}^{N_E} I(\boldsymbol{s}; \bar{\boldsymbol{y}}_n)\right\}. \tag{42}$$

In the simulations, we will show how the varying period K impacts this lower bound.

VI. Hybrid AN-AFF Scheme

The core idea of the AFF scheme is to eliminate the possibility of the coherent detection of Eve, while that of the AN scheme is to deteriorate the receiving SINR of Eve, both of which will reduce the information leakage rate. In the simulation, we find that when the eavesdropper has less antennas than the transmitter does, the AN scheme outperforms the AFF scheme, otherwise, the AFF scheme achieves better secrecy performance at the high SNR regime. To combine the advantages of these two schemes, in this section, we propose a hybrid AN-AFF scheme. The transmit signal of Alice is now

$$\boldsymbol{x}(k) = \boldsymbol{\omega}^H(k) s(k) + \boldsymbol{H}_{\perp} \boldsymbol{u}(k) \tag{43}$$

at time k, where $\boldsymbol{H}_{\perp}$ is the same as defined in (6), $\boldsymbol{u}(k) \triangleq [u_1(k), u_2(k), \ldots, u_{N_A-1}(k)]^T$ is a random AN vector with each element i.i.d. complex Gaussian random variable with zero-mean and variance $E[|u_n(k)|^2] = \sigma_u^2$, and $\boldsymbol{\omega}(k)$ is the same as (10). The average transmit power of Alice is

$$P_{\mathrm{Hybrid}} = \sum_{n=1}^{N_A-1}\left(1 + \frac{|h_n|^2}{|h_{N_A}|^2}\right)\sigma_\omega^2 \sigma_s^2 + \frac{\sigma_s^2}{|h_{N_A}|^2} + (N_A - 1)\sigma_u^2.$$

The AN is in the null-space of Bob so the signal received by Bob is the same as (12). The signal received by Eve is now

$$\boldsymbol{y}_E(k) = \boldsymbol{h}_e(k) s(k) + \boldsymbol{z}_E(k), \tag{44}$$

where $\boldsymbol{z}_E(k) \triangleq \boldsymbol{G}\boldsymbol{H}_{\perp}\boldsymbol{u}(k) + \boldsymbol{n}_E(k)$. Since $u_n(k)$, $n = 1, 2, \ldots, N_A - 1$ are i.i.d. Gaussian random variables independent to $\boldsymbol{n}_E(k)$, we have $\boldsymbol{z}_E(k) \sim \mathcal{CN}(\boldsymbol{0}, \boldsymbol{C}_z)$ where $\boldsymbol{C}_z \triangleq$

$$h(\bar{\boldsymbol{y}}_1|\boldsymbol{s}) = K\log\left(\pi e \sigma_n^2\right) + \frac{1}{\Gamma(K)} \sum_{i=0}^{K-1} \frac{(K-1)!}{(K-1-i)!}\left[\frac{(-1)^{K-i-2} e^{1/\beta_1}}{\beta_1^{K-1-i}} \mathbf{Ei}\left(-\frac{1}{\beta_1}\right) + \sum_{j=1}^{K-1-i} (j-1)! \left(\frac{-1}{\beta_1}\right)^{K-1-j-i}\right], \tag{41}$$

$\sigma_u^2 \boldsymbol{G}\boldsymbol{H}_\perp \boldsymbol{H}_\perp^H \boldsymbol{G}^H + \sigma_n^2 \boldsymbol{I}_{N_E}$. The equivalent noise power at the n-th antenna of Eve is

$$\begin{aligned}\sigma_{\boldsymbol{z},n}^2 &\triangleq E\left\{\left|\boldsymbol{g}_n \boldsymbol{H}_\perp \boldsymbol{u}(k) + n_E(k)\right|^2\right\} \\ &= \sigma_u^2 \boldsymbol{g}_n \left(\boldsymbol{I} - \frac{\boldsymbol{h}^H \boldsymbol{h}}{\|\boldsymbol{h}_e\|^2}\right) \boldsymbol{g}_n^H + \sigma_n^2 \\ &= \sigma_u^2 \|\boldsymbol{g}_n\|^2 - \sigma_u^2 \frac{\left|\boldsymbol{g}_n \boldsymbol{h}^H\right|^2}{\|\boldsymbol{h}_e\|^2} + \sigma_n^2. \end{aligned} \tag{45}$$

Let us normalize $\sigma_\omega^2 = 1$, then

$$P_{\text{Hybrid}} = \sum_{n=1}^{N_A-1} \left(1 + \frac{|h_n|^2}{|h_{N_A}|^2}\right) \sigma_s^2 + \frac{\sigma_s^2}{|h_{N_A}|^2} + (N_A - 1)\sigma_u^2.$$

With fixed σ_s^2 and σ_u^2, the lower bound of the ergodic secrecy rate can be calculated similarly as (28) and (30)–(32). However, when the total power P_{Hybrid} is fixed, there should be a balance between the powers of the signal and the AN. Indeed, if we increase σ_s^2, i.e., the power of the signal, R_B will be increased while the lower bound of R_E will also increase. Therefore, there is a power allocation problem between σ_s^2 and σ_u^2, i.e.,

$$\begin{aligned} R_s^{\text{Hybrid}} \geq R_s^{\text{Hybrid,L}} &\triangleq \max_{\sigma_u^2, \sigma_s^2} \quad R_B^{\text{AFF}}\left(\sigma_s^2\right) - R_E^{\text{AFF,U}}\left(\sigma_u^2, \sigma_s^2\right) \\ \text{s.t.} \quad & \sum_{n=1}^{N_A-1} \left(1 + \frac{|h_n|^2}{|h_{N_A}|^2}\right) \sigma_s^2 + \frac{\sigma_s^2}{|h_{N_A}|^2} + (N_A - 1)\sigma_u^2 \leq P_M, \end{aligned} \tag{46}$$

where P_M is the transmit power constrain. However, since we do not have a closed-form expression of $R_E^{\text{AFF,U}}$, we can not solve the problem analytically. In the simulations, we will search the optimum σ_u^2 and σ_s^2 numerically to find $R_s^{\text{Hybrid,L}}$. We will find that the hybrid scheme increases the secrecy rate further.

VII. Simulation Results

In this section, simulation results are presented to evaluate the performance of the AFF and hybrid AN-AFF schemes, and compared with that of the AN scheme. In the simulations the lower bounds of the secrecy rate of our proposed scheme are illustrated, as shown in (32), (42) and (46). The noise power σ_n^2 is normalized to be at 0 dBm. The secrecy rate is obtained by averaging 1000 Monte Carlo simulations, unless otherwise stated.

A. AFF Scheme

In Fig. 2 we illustrate the ergodic secrecy rates lower bounds of the AFF scheme (32) and compare them with the exact ergodic secrecy rates of AN scheme (35). We set $N_A = 4$ and $N_E = 2, 4, 6, 8$, respectively. For fair comparison we assign the same power to these two schemes, i.e., $P_{\text{AN}} = P_{\text{AFF}} = P_M$. To maximize R_s^{AN} in (35), we do one dimensional search over P and σ_u^2 under the constraint of $P_{\text{AN}} = \sigma_s^2 + (N-1)\sigma_v^2$. From Fig. 2 we can see that the increase of Eve's antenna number reduces the secrecy rates of both schemes. This is because more antennas increase Eve's capability of information interception.

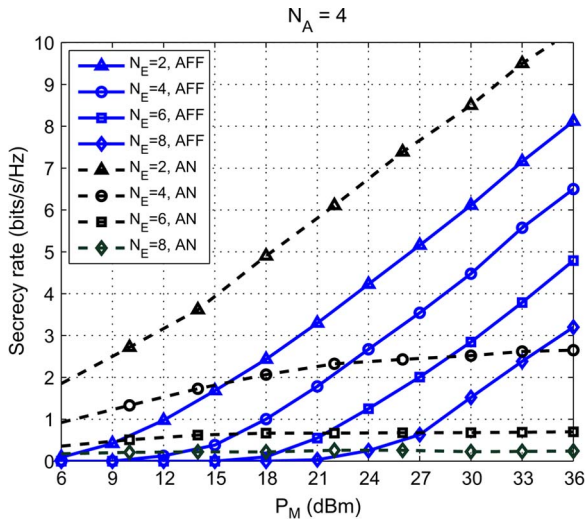


Fig. 2. Ergodic secrecy rate comparisons of the AN scheme and the lower bound of the AFF scheme.

However, the impact to these two schemes are different. For the AN scheme, when $N_E = 2$, the secrecy rate has a significant increase as the power increases. However, as the number of Eve's antenna increases, the secrecy rate enhancement becomes more and more insignificant as the power increases. This is because when Eve has sufficient antennas (degrees of freedom), with CSI, it can eliminate the spatial AN so that the increase of AN power will not increase the interference to Eve. On the contrary, it increases the information leakage rate R_E^{AN}. When $N_E = 8$, i.e., Eve has twice antennas as Alice does, the secrecy rate of the AN scheme stays near 0 in all power region. This phenomenon coincides with the theoretical analysis in [9]. For the AFF scheme, however, the slop of the secrecy rate increase will not be changed as N_E increases. When $N_E = 2$, this slop is the same as that of the AN scheme. In this case, the AFF scheme is always inferior to the AN scheme. However, as N_E increases, the secrecy rate lower bound of the AFF scheme increases very fast and will outperform the AN scheme greatly as the power increases. When $N_E = 8$, the AN scheme almost fails but with enough power (> 24 dBm), the AFF scheme still works well. Note that, since we only gives a secrecy rate lower bound of the AFF scheme, the actual value will be even better than this. The reason why AN outperforms AFF under the low power regime is that, the constraint $\mathbf{h}\mathbf{w}^H(k) = 1$ will impact the power efficiency of the AFF scheme. Specially, since each element of the channel vector $\mathbf{h}$ is Rayleigh fading, the amplitudes of some elements may be very small. To maintain $\mathbf{h}\mathbf{w}^H(k) = 1$, the power efficiency will be degraded.

To show the impact of the non-coherent detection to Eve more clearly, in Fig. 3 we demonstrate the upper bound of the leakage rate (31) as the transmission power increases. We set $N_A = 4$ and $N_E = 2, 4, 6, 8$, respectively. We can see that for any given N_E, the increase slop of the leakage rate decreases as the power increases. When $P_M > 18$ dBm, the slop becomes very small. The non-coherent detection brought in by the AFF scheme greatly reduces the leakage rate to Eve. That is why with enough power, the AFF scheme will always outperforms the AN scheme.

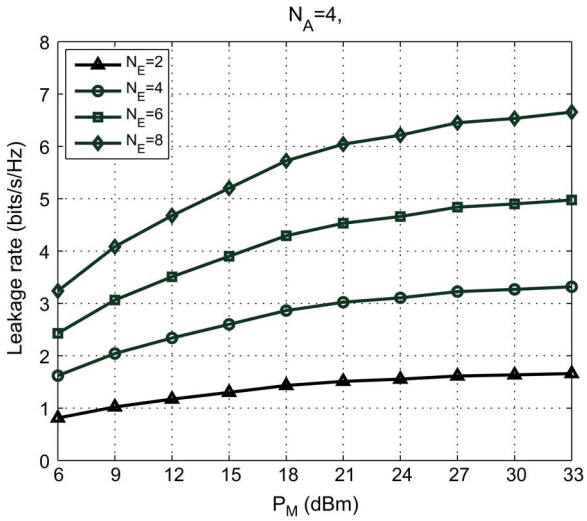


Fig. 3. Leakage rate upper bound to the eavesdroppers.

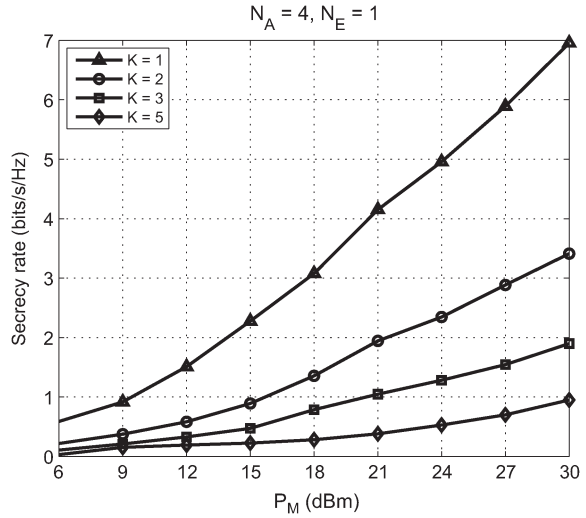


Fig. 4. Impact of K to the secrecy rate lower bound of the AFF scheme.

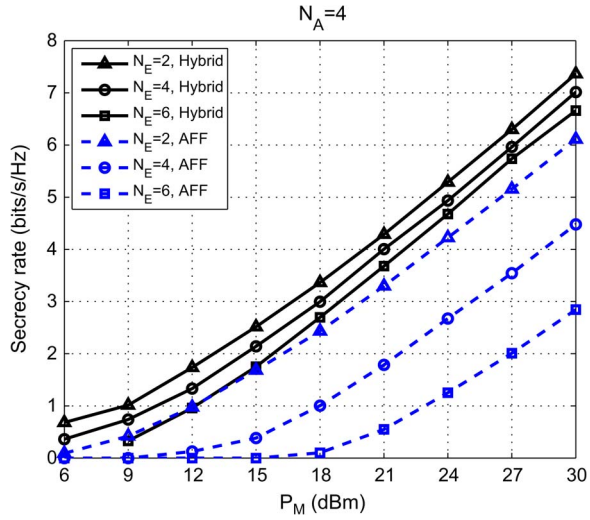


Fig. 5. Secrecy rate lower bound of the hybrid security scheme.

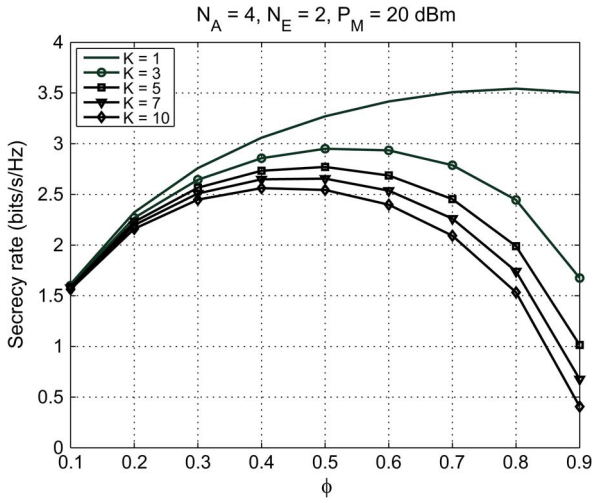


Fig. 6. A random trial of the power allocation of the hybrid scheme with $N_A = 4$, $N_E = 2$, and $P_M = 20$ dBm.

In Fig. 4 we demonstrate the lower bounds of the secrecy rate of the AFF (42) under different K, where K is the artificial fast fading period, when $N_A = 4$ and $N_E = 1$. We can see that as K increases, the slop of the secrecy rate to P_M is greatly declined. This implies that the efficiency of the AFF scheme depends heavily on how fast the artificial fading is. This is intuitively correct since when the artificial fading is not so fast, i.e., K is large, it is more likely that Eve can estimate the CSI to detect the information signal coherently, which invalidates the AFF scheme no matter how large the power is.

B. Hybrid AN-AFF Scheme

In Fig. 5 we show the lower bounds of the secrecy rate of the hybrid AN-AFF scheme (46) and compare them with those of the AFF scheme. To find $R_s^{\mathrm{Hybrid,L}}$ we search the optimum σ_s^2 and σ_u^2 numerically under the constraint of $\sum_{n=1}^{N_A-1}(1+(|h_n|^2/|h_{N_A}|^2))\sigma_s^2+(\sigma_s^2/|h_{N_A}|^2)+(N_A-1)\sigma_u^2=P_M$. We can see that compared with the AFF scheme, the hybrid scheme has larger secrecy rates. This enhancement is very significant over all P_M region, and becomes more significant as N_E increases.

In Fig. 6 and Fig. 7 we demonstrate two random examples of how the optimal power allocation is taken between the signal part and the AN part in the hybrid security scheme (46) under different varying period K. We fix $N_A = 4$, $P_N = 20$ dBm and set $N_E = 2, 6$, respectively, where the x-axis is the ratio of power allocated to the signal part, i.e., $\phi = (\sum_{n=1}^{N_A-1}(1+(|h_n|^2/|h_{N_A}|^2))\sigma_s^2+(\sigma_s^2/|h_{N_A}|^2))/P_M$. We can see in Fig. 6 that when $K = 1$, almost all the power is allocated to the signal part. However, as K increases, more power should be allocated to generate the AN. This is reasonable because when K increases, i.e., artificial fading becomes slower, Eve has more capability to estimate the CSI so the effect of the fast fading weakens and the impact of the AN becomes more significant. In Fig. 7, similar to the case in Fig. 6, more power should be allocated to the AN as K increases.

However, the optimal ϕ in these two cases are different when K is sufficiently large. As N_E increases, the optimal ϕ is smaller and smaller, i.e., more power should be allocated to the AN. This observation coincides with the theoretical analysis and simulation results in [24]. When K goes to very large, Eve can get the CSI and do the coherent detection, and it is shown

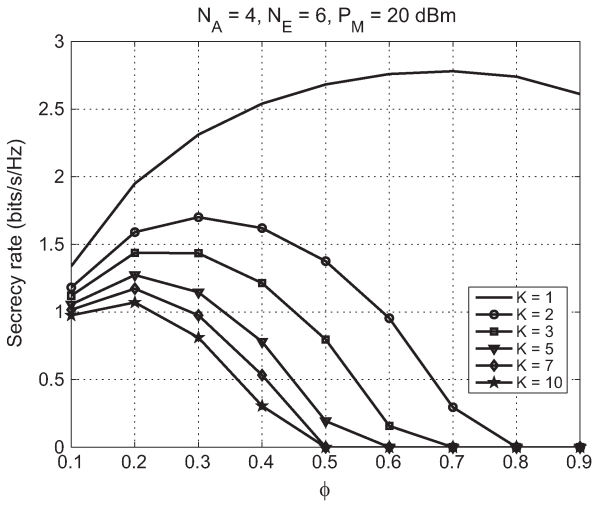


Fig. 7. A random trial of the power allocation of the hybrid scheme with $N_A = 4$, $N_E = 6$, and $P_M = 20$ dBm.

in [24] that, as N_E increases, the partial of power allocated to the AN should also increase.

VIII. Conclusion

In this paper, we investigate the security of a MISO channel in the presence of a multi-antenna passive eavesdropper. Under a more practical scenario that the CSI of the eavesdropper is unavailable, we analyze and compare two efficient secrecy schemes: AN scheme and AFF scheme. We provide a comprehensive secrecy rate analysis to the AFF scheme. We show that with this scheme, the eavesdropper will face a non-coherent Ricean fading SIMO channel. We derive an exact expression for the single-antenna eavesdropper case, and a lower bound for the multi-antenna eavesdropper case, both of which can be numerically calculated conveniently. We compare the AFF scheme with the AN scheme, and show that their respective superiorities depend on the number of antennas the transmitter and the eavesdropper possessed. Furthermore, we propose a hybrid AFF-AN scheme and investigate the power allocation problem, which achieves a better secrecy performance further.

Finally, we note that in all our analysis, large-scale fading, such as shadowing, has not been taken into consideration, which is the research direction of our future work [39].

Appendix A

It can be easily proved by contradiction. Assume we have a function sequence $f_i \triangleq I(s; y_i)$, $i = 1, 2, \ldots$. Obviously, we have $f_i > 0$. From the derivations (28), (30), we also have $f_i \nrightarrow 0$ as i increases, where $\nrightarrow$ means "will not converge to". For convenience, define $\phi'_n \triangleq I(s; \boldsymbol{y})$, and $\phi_n \triangleq \sum_{i=1}^{n} f_i$. We can see that ϕ_n is a monotonically increasing function of n.

Assume the contradiction of (31) holds, i.e., $\phi'_n \geq \phi_n$. Since $I(s; \boldsymbol{y}) = h(s) - h(s|\boldsymbol{y}) \leq h(s) = \log \pi e \sigma_s^2 \triangleq a$ where a is a constant, we have $\phi_n \leq \phi'_n \leq a$ for any $n > 0$. Combining the fact that ϕ_n is a monotonically increasing function of n, we conclude that ϕ_n will converge to a constant $b \leq a$, i.e., $\lim_n \phi_n = b$. This implies that for any small ε, we can find an N such that for any $n \geq N$, we have $0 \leq b - \phi_n \leq \varepsilon$, and $0 \leq b - \phi_{n+1} \leq \varepsilon$. Then we have $-\varepsilon \leq b - \phi_n - (b - \phi_{n+1}) \leq \varepsilon \Longleftrightarrow -\varepsilon \leq f_{n+1} \leq \varepsilon$. This means $f_{n+1} \to 0$, which contradicts to the fact that $f_i \nrightarrow 0$ as i increases.

Appendix B

In this appendix, we show the detailed derivation of (39). The basic idea is to change the $2K$-dimensional rectangular coordinates to the hyperspherical coordinates. The coordinates consist of a radial coordinate, $r_{\bar{\boldsymbol{y}}_1}$, and $2K-1$ angular coordinates $\boldsymbol{\varphi}_{\bar{\boldsymbol{y}}_1} \triangleq [\varphi_1, \varphi_2, \ldots \varphi_{2K-1}]$ where φ_{2K-1} ranges over $[0, 2\pi)$ and the other angles range over $[0, \pi)$. The relationship between $r_{\bar{\boldsymbol{y}}_1}$, $\boldsymbol{\varphi}_{\bar{\boldsymbol{y}}_1}$ and $\Re(y_1(1)), \Im(y_1(1)), \Re(y_1(2)), \Im(y_1(2)), \ldots, \Re(y_1(K)), \Im(y_1(K))$ are

$$
\begin{aligned}
z_1 &\triangleq \Re\left(y_1(1)\right) = r_{\bar{\boldsymbol{y}}_1} \cos(\varphi_1) \\
z_2 &\triangleq \Im\left(y_1(1)\right) = r_{\bar{\boldsymbol{y}}_1} \sin(\varphi_1) \cos(\varphi_2) \\
z_3 &\triangleq \Re\left(y_1(2)\right) = r_{\bar{\boldsymbol{y}}_1} \sin(\varphi_1) \sin(\varphi_2) \cos(\varphi_3) \\
z_4 &\triangleq \Im\left(y_1(2)\right) = r_{\bar{\boldsymbol{y}}_1} \sin(\varphi_1) \sin(\varphi_2) \sin(\varphi_3) \cos(\varphi_4) \\
&\vdots \\
z_{2K-1} &\triangleq \Re\left(y_1(K)\right) \\
&= r_{\bar{\boldsymbol{y}}_1} \sin(\varphi_1) \cdots \sin(\varphi_{2K-2}) \cos(\varphi_{2K-1}) \\
z_{2K} &\triangleq \Im\left(y_1(K)\right) \\
&= r_{\bar{\boldsymbol{y}}_1} \sin(\varphi_1) \cdots \sin(\varphi_{2K-2}) \sin(\varphi_{2K-1})
\end{aligned}
$$

The (i, j)-th element of the $2K \times 2K$ Jacobian matrix can be calculated as

$$
\left[\boldsymbol{J}\left(r_{\bar{\boldsymbol{y}}_1}, \boldsymbol{\varphi}_{\bar{\boldsymbol{y}}_1}\right)\right]_{i,j} = \begin{cases} \frac{\partial z_i}{\partial r_{\bar{\boldsymbol{y}}_1}}, & j = 1, \\ \frac{\partial z_i}{\partial \varphi_{j-1}}, & 2 \leq j \leq 2K. \end{cases}
$$

It is readily to obtain the determinant of the Jacobian matrix

$$
\left|\det \boldsymbol{J}\left(r_{\bar{\boldsymbol{y}}_1}, \boldsymbol{\varphi}_{\bar{\boldsymbol{y}}_1}\right)\right| = r_{\bar{\boldsymbol{y}}_1}^{2K-1} u\left(\bar{\boldsymbol{\varphi}}_{\bar{\boldsymbol{y}}_1}\right),
$$

where we let $\bar{\boldsymbol{\varphi}}_{\bar{\boldsymbol{y}}_1} \triangleq [\varphi_1, \varphi_2, \ldots \varphi_{2K-2}]$, and $u(\bar{\boldsymbol{\varphi}}_{\bar{\boldsymbol{y}}_1}) \triangleq \prod_{m=1}^{2K-2} \sin^{2K-1-m}(\varphi_m)$ for simplicity. We then have

$$
\begin{aligned}
&\int_{\boldsymbol{\varphi}_{\bar{\boldsymbol{y}}_1}} \left|\det \boldsymbol{J}\left(r_{\bar{\boldsymbol{y}}_1}, \boldsymbol{\varphi}_{\bar{\boldsymbol{y}}_1}\right)\right| d\boldsymbol{\varphi}_{\bar{\boldsymbol{y}}_1} \\
&= r_{\bar{\boldsymbol{y}}_1}^{2K-1} \int_{\varphi_1} \int_{\varphi_2} \cdots \int_{\varphi_{2K-1}} \sin^{2K-2}(\varphi_1) \sin^{2K-3}(\varphi_2) \\
&\qquad \cdots \sin(\varphi_{2K-2}) d\varphi_1 d\varphi_2 \cdots d\varphi_{2K-1} \\
&= r_{\bar{\boldsymbol{y}}_1}^{2K-1} \cdot 2 \cdot \left(2\pi \frac{1!!}{3!!}\right) \cdot \left(2\pi \frac{3!!}{5!!}\right) \cdots \\
&\qquad \cdot \left(2\pi \frac{(2K-5)!!}{(2K-3)!!}\right) \cdot \left(\pi \frac{(2K-3)!!}{(2K-2)!!}\right) \cdot 2\pi \\
&= \frac{(2\pi)^K}{(2K-2)!!} r_{\bar{\boldsymbol{y}}_1}^{2K-1} = \frac{2\pi^K}{(K-1)!} r_{\bar{\boldsymbol{y}}_1}^{2K-1},
\end{aligned}
$$

where in the second equation we use integral formulas [35, p.395]

$$
\int_0^{\pi} \sin^{2\mu} \varphi \, d\varphi = \frac{\pi \cdot (2\mu - 1)!!}{(2\mu)!!}, \tag{48}
$$

and

$$\int_0^{\pi} \sin^{2\mu-1}\varphi \, d\varphi = \frac{2\cdot(2(\mu-1))!!}{(2\mu-1)!!}. \tag{49}$$

for any positive integer μ.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell Sys. Tech. Journ.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[3] S. L. Y. Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.

[4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[5] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound wire-tap channels," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, pp. 142374-1–142374-12, Oct. 2009.

[6] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Adelaide, SA, Australia, Sep. 2005, pp. 2152–2155.

[7] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. 41st Conf. Information Sciences Systems*, Baltimore, MD, USA, Mar. 2007, pp. 905–910.

[8] S. Shafiee and S. Ulukus, "Achievable rates in Gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, Jun. 2007, pp. 2466–2470.

[9] A. Khisti and G. Wornell, "Secure transmission with multiple antennas—I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[10] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4033–4039, Sep. 2009.

[11] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *Proc. IEEE Int Symp. Inf. Theory*, Nice, France, Jun. 2007, pp. 2471–2475.

[12] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, ON, Canada, Jul. 2008, pp. 524–528.

[13] A. Khisti and G. Wornell, "Secure transmission with multiple antennas—II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[14] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 5, pp. 2547–2553, Jun. 2009.

[15] Q. Li *et al.*, "Transmit solutions for MIMO wiretap channels using alternating optimization," *IEEE. J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1714–1726, Sep. 2013.

[16] Y.-W. Hong, P.-C. Lan, and C.-C. Jay Kuo, "Enhancing physical-layer secrecy in multiantenna wireless system," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, Sep. 2013.

[17] J. Li and A. P. Petropulu, "On ergodic secrecy rate for Gaussian MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 2180–2189, Apr. 2011.

[18] J. Li and A. P. Petropulu, "Ergodic secrecy rate for multiple-antenna wiretap channels with Rician fading," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 861–867, Sep. 2011.

[19] R. Negi and S. Goel, "Secret communication using artificial noise," in *Proc. IEEE Veh. Technol. Conf.*, Dallas, TX, USA, Sep. 2005, vol. 3, pp. 1906–1910.

[20] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.

[21] A. L. Swindlehurst, "Fixed SINR solutions for the MIMO wiretap channel," in *Proc. IEEE ICASSP*, Taipei, Taiwan, Apr. 2009, pp. 2437–2440.

[22] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3532–3545, Jul. 2012.

[23] H.-M. Wang, M. Luo, X.-G. Xia, and Q. Yin, "Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI," *IEEE Signal Process. Lett.*, vol. 20, no. 2, pp. 39–42, Jan. 2013.

[24] 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.

[25] Z. Li, R. Yates, and W. Trappe, "Achieving secret communication for fast Rayleigh fading channels," *IEEE Trans. Wireless Commun.*, vol. 9, no. 9, pp. 2792–2798, Sep. 2010.

[26] G. B. Giannakis and J. M. Mendel, "Identification of nonminimum phase systems using higher-order statistics," *IEEE Trans. Acoust. Speech, Signal Process.*, vol. ASSP-37, no. 3, pp. 360–377, Mar. 1989.

[27] L. Tong, G. Xu, and T. Kailath, "Blind identification and equalization based on second-order statistics: A time domain approach," *IEEE Trans. Inf. Theory*, vol. 40, no. 2, pp. 340–349, Mar. 1994.

[28] X. Li and E. P. Ratazzi, "MIMO transmissions with information theoretic secrecy for secret-key agreement in wireless networks," in *Proc. IEEE MILCOM*, Atlantic City, NJ, USA, 2005.

[29] X. Li, J. Hwu, and E. Ratazzi, "Using antenna array redundancy and channel diversity for secure wireless transmissions," *J. Commun.*, vol. 2, no. 3, pp. 24–32, May 2007.

[30] Q. Li, H. Song, and K. Huang, "Achieving secure transmission with equivalent multiplicative noise in MISO wiretap channels," *IEEE Commun. Lett.*, vol. 17, no. 5, pp. 892–895, May 2013.

[31] I. C. A. Faycal, M. D. Trott, and S. Shamai (Shitz), "The capacity of discrete-time Rayleigh fading channels," in *Proc. Int. Symp. Inf. Theory*, Ulm, Germany, 1997, p. 473.

[32] I. C. A. Faycal, M. D. Trott, and S. Shamai (Shitz), "The capacity of discrete-time memoryless Rayleigh-fading channels," *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1290–1301, May 2001.

[33] T. Marzetta and B. Hochwald, "Capacity of mobile multiple-antenna communication link in a Rayleigh flat-fading environment," *IEEE Trans. Inf. Theory*, vol. 45, no. 1, pp. 139–157, Jan. 1999.

[34] B. Hochwald and T. Marzetta, "Unitary space–time modulation for multiple-antenna communications in Rayleigh flat fading," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 543–565, Mar. 2000.

[35] L. Zheng and D. N. C. Tse, "Communication on the Grassmann Manifold: A geometric approach to the noncoherent multiple-antenna channel," *IEEE Trans. Inf. Theory*, vol. 48, no. 2, pp. 359–383, Feb. 2002.

[36] R. R. Perera, T. S. Pollock, and T. D. Abhayapala, "Gaussian inputs: Performance limits over non-coherent SISO and MIMO channels," *Eur. Trans. Telecommun.*, vol. 18, no. 3, pp. 235–244, Apr. 2007.

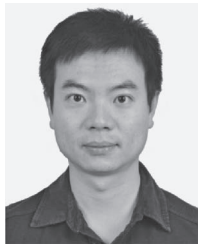
[37] P. Viswanath, D. N. C. Tse, and R. Laroia, "Opportunistic beamforming using dumb antennas," in *Proc. Int. Symp. Inf. Theory*, Lausanne, Switzerland, 2002, p. 449.

[38] P. Viswanath, D. N. C. Tse, and R. Laroia, "Opportunistic beamforming using dumb antennas," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1277–1294, Jun. 2002.

[39] M. Hanif and P. Smith, "On the statistics of cognitive radio capacity in shadowing and fast fading environments," *IEEE Trans. Wireless Commun.*, vol. 9, no. 2, pp. 844–852, Feb. 2010.

[40] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, Products*, A. Jeffrey and D. Zwillinger, Eds., 7th ed. New York, NY, USA: Academic, 2007.

[41] D. Tse and P. Viswanath, *Fundamentals of Wireless Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2005.



Hui-Ming Wang (S'07–M'10) received the B.S. and Ph.D. degrees in electrical engineering from Xi'an Jiaotong University, Xi'an, China, in 2004 and 2010, respectively.

He is currently an Associate Professor with the Department of Information and Communications Engineering, Xi'an Jiaotong University, where he is also with the Ministry of Education Key Lab for Intelligent Networks and Network Security. From May 2007 to April 2008 and from December 2009 to June 2010, he was a Visiting Scholar with the Department of Electrical and Computer Engineering, University of Delaware, DE, USA. His research interests include cooperative communication systems, physical-layer security of wireless communications, space–time coding, and signal processing for broadband wireless communications.

Dr. Wang received the National Excellent Doctoral Dissertation Award in China in 2012 and a Best Paper Award at the IEEE Wireless Communications and Signal Processing Conference in 2011.

Tongxing Zheng received the B.S. degree from the School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an, China, in 2010, where he is currently working toward the Ph.D. degree. His research interests include cooperative communications systems and physical-layer security of wireless communications.

Xiang-Gen Xia (M'97–S'00–F'09) received the B.S. degree in mathematics from Nanjing Normal University, Nanjing, China, in 1983; the M.S. degree in mathematics from Nankai University, Tianjin, China, in 1986; and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, CA, USA, in 1992. In 1996, he joined the Department of Electrical and Computer Engineering, University of Delaware, Newark, DE, USA, where he is the Charles Black Evans Professor. His current research interests include space–time coding, MIMO and OFDM systems, digital signal processing, and SAR and ISAR imaging. He has over 250 refereed journal articles published and accepted and seven U.S. patents awarded and is the author of one book.

Dr. Xia received several awards in the United States and China. He is currently an Associate Editor of the IEEE TRANSACTIONS ON SIGNAL PROCESSING, *Science China—Information Sciences, Signal Processing (China)*, and the *Journal of Communications and Networks (JCN)*. He is the Technical Program Chair of the Signal Processing Symposium, Globecom 2007 in Washington D.C. and the General Cochair of ICASSP 2005 in Philadelphia.