Optimal Power Allocation for Artificial Noise under Imperfect CSI against Spatially Random Eavesdroppers

Tong-Xing Zheng, *Student Member, IEEE*, and Hui-Ming Wang, *Member, IEEE*

***Abstract*—In this correspondence, we study the secure multi-antenna transmission with artificial noise (AN) under imperfect channel state information in the presence of spatially randomly distributed eavesdroppers. We derive the optimal solutions of the power allocation between the information signal and the AN for minimizing the secrecy outage probability (SOP) under a target secrecy rate and for maximizing the secrecy rate under a SOP constraint, respectively. Moreover, we provide an interesting insight that channel estimation error affects the optimal power allocation strategy in opposite ways for the above two objectives. When the estimation error increases, more power should be allocated to the information signal if we aim to decrease the rate-constrained SOP, whereas more power should be allocated to the AN if we aim to increase the SOP-constrained secrecy rate.**

***Index Terms*—Physical layer security, artificial noise, multi-antenna, secrecy outage, power allocation, imperfect CSI.**

I. Introduction

Physical layer security (PLS), which achieves secure transmissions by exploiting the randomness of wireless channels, has drawn considerable attention recently [1], [2]. It has been shown that we are able to greatly improve PLS using multi-antenna techniques with global channel state information (CSI). However, to acquire the CSI of an eavesdropper is very difficult in real wiretap scenarios, since the eavesdropper is usually passive. Without the eavesdropper's CSI, Goel *et al.* [3] proposed a so-called artificial noise (AN) aided multi-antenna transmission strategy, in which the transmitter masked the information-bearing signal by injecting isotropic AN into the null space of the main channel (from the transmitter to a legitimate receiver), thus creating non-decodable interference to potential eavesdroppers while without impairing the legitimate receiver. This seminal work has unleashed a wave of innovation [4]-[9], and the AN scheme has become a promising approach to safeguarding wireless communications.

In practice, the CSI of the main channel is acquired by training, channel estimation and feedback, which inevitably result in CSI imperfection. Some endeavors have studied the AN scheme allowing for imperfect CSI. For example, robust beamforming schemes have been proposed in [5] for MIMO systems and in [6] for cooperative relay systems. The effects of channel quantized feedback to the AN scheme are discussed in [7] and [8], while in [9], training and feedback have been jointly investigated and optimized.

However, all the aforementioned works ignored the uncertainty of eavesdroppers' spatial positions. Generally, eavesdroppers are geographically distributed randomly, especially in large-scale wireless networks. Analyzing secrecy performance in such random wiretap scenarios is fundamentally different from that with deterministic eavesdroppers's locations.

Recently, stochastic geometry theory has provided a powerful tool to analyze network performance by modeling nodes' positions according to some spatial distributions such as a Poisson point process (PPP) [10]; it facilitates the study of the AN scheme against random eavesdroppers [11]-[13]. However, the impact of imperfect CSI on designing the AN is still an open problem. Particularly, it is yet unknown what the optimal power allocation strategy is, and how a channel estimation error influences power allocation and secrecy performance. Due to the complicated/implicit forms of the objective functions caursed by location randomness and CSI imperfection, previous works can only obtain the optimal power allocation either by exhaustive search or by numerical calculation instead of providing a tractable expression. This makes it challenging to reveal an explicit analytical relationship between the optimal power allocation and the channel estimation error. Our research are motivated by the above observations and challenges.

In this correspondence, we study an AN-aided multi-input single-output (MISO) secure transmission against randomly located eavesdroppers under imperfect channel estimation. We investigate two important performance metrics, namely, secrecy outage probability (SOP) and secrecy rate, respectively. The SOP reflects the quality difference between the main and wiretap channels; the secrecy rate measures the rate efficiency of secure transmission. We provide the optimal power allocation strategies for the following optimization problems:

1) Minimizing the SOP subject to a secrecy rate constraint;
2) Maximizing the secrecy rate subject to a SOP constraint.

Furthermore, we draw an interesting conclusion that channel estimation error influences the optimal power allocation in *opposite ways* for the above two objectives. *When the estimation error increases, more power should be allocated to the information signal if we aim to decrease the rate-constrained SOP, whereas more power should be given to the AN if we aim to increase the SOP-constrained secrecy rate.*

To the best of our knowledge, we are the first to reveal an explicit analytical relationship between the optimal power

This work was partially supported by the Foundation for the Author of National Excellent Doctoral Dissertation of China under Grant 201340, the National High-Tech Research and Development Program of China under Grant No. 2015AA011306, the New Century Excellent Talents Support Fund of China under Grant NCET-13-0458, the Fok Ying Tong Education Foundation under Grant 141063, the Fundamental Research Funds for the Central University under Grant No. 2013jdgz11, and the Young Talent Support Fund of Science and Technology of Shaanxi Province under Grant 2015KJXX-01. The review of this paper was coordinated by Prof. G. Mao.

The authors are with the School of Electronics and Information Engineering, and also with the MOE Key Lab for Intelligent Networks and Network Security, Xian Jiaotong University, Xi'an, 710049, Shaanxi, China (e-mail: txzheng@stu.xjtu.edu.cn; xjbswhm@gmail.com). H.-M. Wang is the corresponding author.

allocation and channel estimation error through strict mathematical proofs. Although existing works have also shown that AN should be exploited to increase the secrecy rate under imperfect CSI in point-to-point transmissions, their conclusions are just extracted from simulations under specific parameter settings, which may not apply to more general cases.

Notations: $(\cdot)^\dagger$, $(\cdot)^{\mathrm{T}}$, $|\cdot|$, $\|\cdot\|$ denote conjugate, transpose, absolute value, and Euclidean norm, respectively. $\mathcal{CN}$ denotes the circularly symmetric complex Gaussian distribution with zero mean and unit variance. $\mathbb{C}^{m\times n}$ denotes the $m\times n$ complex number domain.

II. System Model and Problem Description

Consider a secure transmission from a transmitter (Alice) to a legitimate receiver (Bob) overheard by randomly located eavesdroppers (Eves)[1]. Alice has N antennas, Bob and Eves each has a single antenna. Without loss of generality, we place Alice at the origin and Bob at a deterministic position with a distance r_B from Alice. The locations of Eves are modeled as a homogeneous PPP Φ_E of density λ_E on a 2-D plane with the k-th Eve a distance r_k from Alice.

All wireless channels are assume to undergo flat Rayleigh fading together with a large-scale path loss governed by the exponent $\alpha > 2$. The channel vector of a node with a distance r from Alice is characterized as $\boldsymbol{h}r^{-\frac{\alpha}{2}}$, where $\boldsymbol{h} \in \mathbb{C}^{N\times 1}$ denotes the small-scale fading vector, with independent and identically distributed (i.i.d.) entries $h_i \sim \mathcal{CN}$.

We focus on a *frequency-division duplex* (FDD) system in which the channel reciprocity no longer holds. We assume Bob estimates the main channel with estimation errors, and sends the estimated channel to Alice via an ideal feedback link (e.g., a high-quality link with negligible quantization error). In this case, the exact main channel $\boldsymbol{h}_b$ can be modeled as

$$\boldsymbol{h}_b = \sqrt{1-\tau^2}\hat{\boldsymbol{h}}_b + \tau\tilde{\boldsymbol{h}}_b, \tag{1}$$

where $\hat{\boldsymbol{h}}_b$ and $\tilde{\boldsymbol{h}}_b$ denote the estimated channel and estimation error with i.i.d. entries $\hat{h}_{b,i}, \tilde{h}_{b,i} \sim \mathcal{CN}(0,1)$. This assumption arises from employing the minimum mean square error (MMSE) estimation[2] [5], [14]. Here, $\tau \in [0,1]$ denotes the error coefficient; $\tau = 0$ corresponds to a perfect channel estimation, and $\tau = 1$ means no CSI is acquired at all. For each eavesdropper, although its CSI is unknown, we assume its channel statistics information is available, which is a general assumption when dealing with PLS [4]-[13].

Recalling the AN scheme in [3], the transmitted signal vector $\boldsymbol{x}$ at Alice is designed in the form of

$$\boldsymbol{x} = \sqrt{\xi P}\boldsymbol{w}s + \sqrt{(1-\xi)P/(N-1)}\boldsymbol{G}\boldsymbol{v}, \tag{2}$$

where s is the information signal with $\mathbb{E}[|s|^2] = 1$, $\boldsymbol{v} \in \mathbb{C}^{(N-1)\times 1}$ is an AN vector with i.i.d. entries $v_i \sim \mathcal{CN}$, and ξ is the power allocation ratio (PAR) of the desired signal power to the total power P. $\boldsymbol{w} \triangleq \hat{\boldsymbol{h}}_b^\dagger/\|\hat{\boldsymbol{h}}_b\|$ is the beamforming vector for the information signal, $\boldsymbol{G} \in \mathbb{C}^{N\times(N-1)}$ is a weighting matrix for the AN. The columns of $\boldsymbol{W} \triangleq [\boldsymbol{w}\ \boldsymbol{G}]$ constitute an orthogonal basis. Let $\boldsymbol{s} \triangleq \left[s\ \boldsymbol{v}^{\mathrm{T}}\right]$, and the received signals at Bob and the k-th Eve are given from (2)

$$y_B = \sqrt{1-\tau^2}\|\hat{\boldsymbol{h}}_b\|^2 r_B^{-\frac{\alpha}{2}} s + \underbrace{\tau\tilde{\boldsymbol{h}}_b\boldsymbol{W}\boldsymbol{s}^{\mathrm{T}} r_B^{-\frac{\alpha}{2}} + n_B}_{n_B^o}, \tag{3}$$

$$y_k = \boldsymbol{h}_{e,k}\boldsymbol{w}r_k^{-\frac{\alpha}{2}}s + \boldsymbol{h}_{e,k}\boldsymbol{G}\boldsymbol{v}r_k^{-\frac{\alpha}{2}} + n_k,\ \forall k \in \Phi_E, \tag{4}$$

where $\boldsymbol{h}_{e,k}$ denotes the channel from Alice to the k-th Eve, and n_B^o combines the residual channel estimation error and thermal noise. Without loss of generality, we assume $n_B, n_{k\in\Phi_E} \sim \mathcal{CN}$. The exact capacity expression of the main channel under imperfect receiver CSI is still unavailable. A commonly used approach is to examine a capacity lower bound by treating n_B^o as the worst-case Gaussian noise[3]. By doing so, the SINRs of Bob and the k-th Eve are respectively given by

$$\gamma_B = \xi\kappa(\tau), \tag{5}$$

$$\gamma_k = \frac{\xi P|\boldsymbol{h}_{e,k}^{\mathrm{T}}\boldsymbol{w}|^2 r_k^{-\alpha}}{(1-\xi)P\|\boldsymbol{h}_{e,k}^{\mathrm{T}}\boldsymbol{G}\|^2 r_k^{-\alpha}/(N-1)+1}, \tag{6}$$

where $\kappa(\tau) = \frac{(1-\tau^2)P\gamma}{\tau^2 P + r_B^\alpha}$ with $\gamma \triangleq \|\hat{\boldsymbol{h}}_b\|^2$. Eq. (6) holds for the pessimistic assumption that the k-th Eve has perfect knowledge of both $\hat{\boldsymbol{h}}_b$ and $\tilde{\boldsymbol{h}}_b$. Given that $\tau \in [0,1]$, $\kappa(\tau)$ is a monotonically decreasing function of τ; it reflects the accuracy of channel estimation. Specifically, a small value of $\kappa(\tau)$ corresponds to a low estimation accuracy and vice versa. Hereafter, we omit τ from $\kappa(\tau)$ for notational brevity.

We consider the wiretap scenario in which each Eve individually decodes a secret message. This corresponds to a *compound* wiretap channel model [17], and the capacities of the main channel and the equivalent wiretap channel are $C_B = \log_2(1+\gamma_B)$ and $C_E = \log_2(1+\gamma_E)$ with $\gamma_E \triangleq \max_{k\in\Phi_E}\gamma_k$. Note that the capacity of Eves is determined by the maximum capacity among all links connecting Alice with Eves. As done in [4] and [13], after encoding secret information, Alice transmits the codewords and embedded secret messages at rates C_B and R_S, respectively. If *at least one Eve decodes the secret messages*, i.e., C_E exceeds the *rate* $C_B - R_S$ *of redundant information* (to protect from eavesdropping), perfect secrecy is compromised and a secrecy outage occurs; the corresponding SOP is defined as

$$\mathcal{O} \triangleq \mathbb{P}\{C_E > C_B - R_S\},\ \forall\ C_B > R_S. \tag{7}$$

In the following, we will optimize the PAR to minimize the SOP under a target secrecy rate, and to maximize the secrecy rate under a SOP constraint $\mathcal{O} \le \epsilon \in (0,1)$, respectively. We emphasize that different from existing research with deterministic Eves' positions, the analysis and design here is much more complicated due to the extra spatial randomness.

III. Secrecy Outage Probability Minimization

In this section, we optimize the PAR that minimizes the SOP under a target secrecy rate. Recalling (7), Alice transmits only

[1]This may correspond to such a scenario that a multi-antenna transmitter Alice provides specific service to a specified subscriber Bob, while the service should be kept secret to eavesdroppers (also named unauthorized users).

[2] The Gaussian error model is a stochastic uncertainty model. Another widely used model is the deterministic bounded error model, which is more convenient for analyzing the quantized CSI [8].

[3] The tightness of this capacity lower bound was verified for Gaussian inputs with MMSE channel estimation in [15], [16].

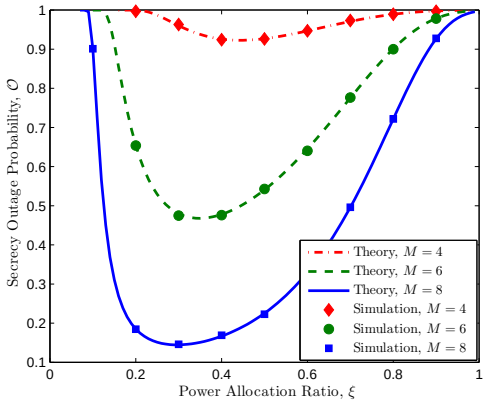

Fig. 1. SOP $\mathcal{O}$ vs. ξ for different values of M, with $P = 10$dBm, $R_S = 2$, $\tau = 0.3$, and $\lambda_E = 2$. Unless otherwise specified, we set $\alpha = 4$, $r_B = 1$ (unit distance), and the unit of R_S is bits/s/Hz.

when $C_B = \log_2(1+\xi\kappa) > R_S$, i.e., $\xi > \frac{2^{R_S}-1}{\kappa}$ should hold to guarantee a reliable connection between Alice and Bob. For ease of notation, throughout the paper we define $T \triangleq 2^{R_S}$, $\omega \triangleq \frac{T-1}{\kappa}$, $\delta \triangleq \frac{2}{\alpha}$, $\beta \triangleq \pi\Gamma(1+\delta)$, $\theta \triangleq \frac{T-1}{T}$, and $\varphi \triangleq \frac{\xi^{-1}-1}{N-1}$.

The problem of minimizing $\mathcal{O}$ in (7) is formulated as

$$\min_{\xi} \ \mathcal{O}, \qquad \text{s.t.} \quad \omega < \xi \leq 1. \tag{8}$$

Before proceeding to this optimization problem, we provide a closed-form expression of $\mathcal{O}$ over the PPP network.

Lemma 1: If $\xi > \omega$, the SOP defined in (7) *is given by*

$$\mathcal{O} = 1 - \exp\left(-\beta\lambda_E \left(P\theta^{-1}\right)^{\delta} \mathcal{J}(\xi)\right), \tag{9}$$

where $\mathcal{J}(\xi) = \left(\omega^{-1}-\xi^{-1}\right)^{-\delta}\left(1+\left(\xi\omega^{-1}-1\right)\theta\varphi\right)^{1-N}$.

Proof: Substitute C_B and C_E along with (5) and (6) into (7), and after some algebraic manipulations, we obtain $\mathcal{O} = 1 - \mathcal{F}_{\gamma_E}(x)$ with $x \triangleq \frac{1+\kappa\xi}{T} - 1$, where $\mathcal{F}_{\gamma_E}(x)$ is the cumulative distribution function (CDF) of γ_E, which is

$$\begin{aligned}
\mathcal{F}_{\gamma_E}(x) &= \mathbb{P}\left\{\max_{k\in\Phi_E} \gamma_k < x\right\} = \mathbb{E}_{\Phi_E}\left[\prod_{k\in\Phi_E} \mathbb{P}\{\gamma_k < x\}\right] \\
&\overset{(a)}{=} \mathbb{E}_{\Phi_E}\left[\prod_{k\in\Phi_E}\left(1 - e^{-\frac{r_k^{\alpha} x}{P\xi}}(1+\varphi x)^{1-N}\right)\right] \\
&\overset{(b)}{=} \exp\left(-2\pi\lambda_E(1+\varphi x)^{1-N}\int_0^{\infty} e^{-\frac{r^{\alpha}x}{P\xi}} r dr\right) \\
&= \exp\left(-\beta\lambda_E(P\xi)^{\delta}x^{-\delta}(1+\varphi x)^{1-N}\right),
\end{aligned} \tag{10}$$

where (a) holds for the CDF of γ_k [4], and (b) holds for the probability generating functional (PGFL) over a PPP [19]. Substituting (10) into $\mathcal{O}$ completes the proof. ■

The theoretical values of $\mathcal{O}$ are well verified by Monte-Carlo simulations, as shown in Fig. 1. We see that adding transmit antennas is beneficial for decreasing the SOP. We also observe that as ξ increases, $\mathcal{O}$ first decreases and then increases; there exists a unique ξ that minimizes $\mathcal{O}$. In the following we are going to calculate the value of this unique ξ. From (9), it is apparent that minimizing $\mathcal{O}$ is equivalent to minimizing $\mathcal{J}(\xi)$.

The first-order derivative of $\mathcal{J}(\xi)$ on ξ is given by

$$\frac{d\mathcal{J}(\xi)}{d\xi} = \frac{\theta\mathcal{J}(\xi)(\xi^3 + a\xi^2 + b\xi + c)}{\xi^2(\xi-\omega)(\omega+(\xi-\omega)\theta\varphi)}, \tag{11}$$

where $a \triangleq -l_1\omega$, $b \triangleq -\frac{\delta}{\theta}\omega^2 - l_0\omega^2 - l_2\omega$, and $c \triangleq l_2\omega^2$, with $l_0 \triangleq \frac{\delta}{N-1}$, $l_1 \triangleq 1 - l_0$, and $l_2 \triangleq 1 + l_0$. Let $\mathcal{K}(\xi) = \xi^3 + a\xi^2 + b\xi + c$. Since $\xi > \omega$, the sign of $\frac{d\mathcal{J}(\xi)}{d\xi}$ follows that of $\mathcal{K}(\xi)$. In other words, to investigate the monotonicity of $\mathcal{J}(\xi)$ on ξ, we need to just examine the sign of $\mathcal{K}(\xi)$. In the following theorem, we provide the solution to problem (8).

Theorem 1: The optimal PAR that minimizes $\mathcal{O}$ in (8) *is*

$$\xi^* = \begin{cases} \varnothing, & 0 < \kappa \leq T-1 \\ 1, & T-1 < \kappa \leq (T-1)\left(1+\sqrt{\delta/\theta}\right) \\ \xi_o, & \textit{otherwise} \end{cases} \tag{12}$$

where $\xi_o = \sqrt[3]{q+p} + \sqrt[3]{q-p} - \frac{a}{3}$ *with* $p \triangleq \sqrt{\left(\frac{b}{3} - \frac{a^2}{9}\right)^3 + q^2}$ *and* $q \triangleq \frac{ab}{6} - \frac{c}{2} - \frac{2a^3}{54}$, *and a, b, c have been defined in* (11). *$\xi^* = \varnothing$ means that transmission is suspended.*

Proof: We know that Alice transmits only when $\xi > \omega$. 1) If $\omega \geq 1$, i.e., $\kappa \leq T-1$, no feasible $\xi \in [0,1]$ satisfies $\xi > \omega$, and transmission is suspended. 2) If $\omega < 1$, Alice transmits in the range of $\xi \in (\omega, 1]$. Next, we derive the optimal value of ξ that minimizes $\mathcal{J}(\xi)$.

We first prove the convexity of $\mathcal{K}(\xi)$ on $\xi \in (\omega, 1]$. From the expression of $\mathcal{K}(\xi)$, we have $\frac{d^2\mathcal{K}(\xi)}{d\xi^2} = 6\xi - 2l_1\omega > 0$, i.e., $\mathcal{K}(\xi)$ is a *convex* function of ξ. Then we determine the sign of $\mathcal{K}(\xi)$. The values of $\mathcal{K}(\xi)$ at boundaries $\xi = \omega$ and $\xi = 1$ are $\mathcal{K}(\omega) = -\frac{\delta}{\theta}\omega^3$ and $\mathcal{K}(1) = (1-\omega)^2 - \frac{\delta}{\theta}\omega^2$, respectively. Obviously, $\mathcal{K}(\omega) < 0$ always holds. Next, we discuss the optimal value of ξ for the following two cases.

Case 1: $\mathcal{K}(1) \leq 0$. Since $\mathcal{K}(\xi)$ is convex on $\xi \in (\omega, 1]$, $\mathcal{K}(\xi)$ or $\frac{d\mathcal{J}(\xi)}{d\xi}$ is always negative. Hence $\mathcal{J}(\xi)$ monotonically decreases with ξ, and the minimum $\mathcal{J}(\xi)$ is achieved at $\xi = 1$, with the corresponding condition obtained from $\mathcal{K}(1) \leq 0$, which is $\frac{1}{1+\sqrt{\delta/\theta}} \leq \omega < 1$.

Case 2: $\mathcal{K}(1) > 0$. It means $\mathcal{K}(\xi)$ or $\frac{d\mathcal{J}(\xi)}{d\xi}$ becomes first negative and then positive as ξ increases from ω to 1, i.e., $\mathcal{J}(\xi)$ first decreases and then increases with ξ, and the optimal value of ξ is the unique root of the cubic equation $\mathcal{K}(\xi) = 0$. Solving this equation using Cardano's formula yields ξ_o.

Combining *Case 1* and *Case 2* completes the proof. ■

Theorem 1 indicates that when the value of κ is small which corresponds to a poor link quality or a large channel estimation error, Alice either suspends the transmission or transmits with full power. When the value of κ becomes large enough, it is wise to create AN to decrease the SOP. The resulting minimum SOP, denoted as $\mathcal{O}^*$, is obtained by substituting ξ^* into (9).

Next, we investigate the influence of channel estimation error on the optimal PAR. Although we obtain a closed-form expression of ξ_o in (12), it is complicated to reveal the explicit connection between ξ_o and κ. Nevertheless, by leveraging the equation $\mathcal{K}(\xi_o) = 0$, we develop some insights into the behavior of ξ_o with respect to κ in the following proposition.

Proposition 1: ξ_o monotonically decreases with κ.

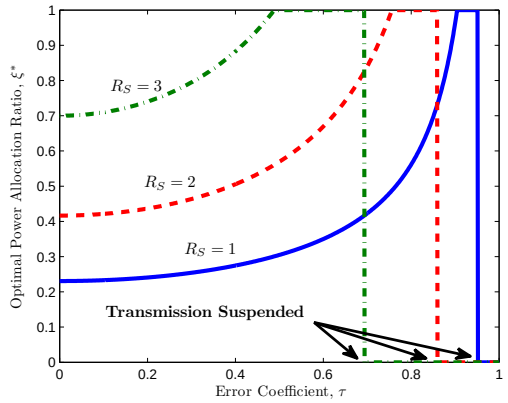

Fig. 2. Optimal PAR ξ^* vs. error coefficient τ for different values of R_S, with $P = 0$dBm, $N = \gamma = 20$, and $\lambda_E = 2$.

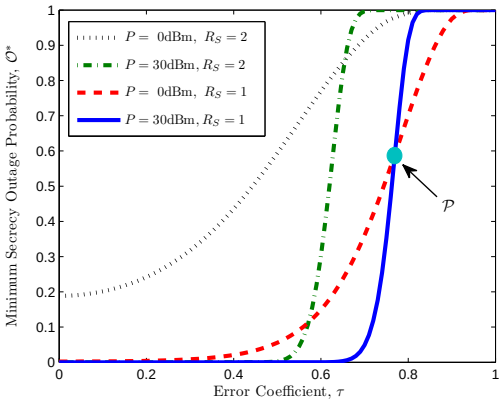

Fig. 3. Minimum SOP $\mathcal{O}^*$ vs. τ for different values of P and R_S, with $N = \gamma = 20$, and $\lambda_E = 2$.

Proof: Since $\omega = \frac{T-1}{\kappa}$, to complete the proof, we need to just prove the monotonicity of ξ_o on ω. Utilizing the derivative rule for implicit functions [18] with $\mathcal{K}(\xi_o) = 0$, we obtain

$$\frac{d\xi_o}{d\omega} = \frac{-\partial\mathcal{K}/\partial\omega}{\partial\mathcal{K}/\partial\xi_o} = \frac{l_1\xi_o^2 + 2\frac{\delta}{\theta}\omega\xi_o + 2l_0\omega\xi_o + l_2\xi_o - 2l_2\omega}{3\xi_o^2 - 2l_1\omega\xi_o - \frac{\delta}{\theta}\omega^2 - l_2\omega - l_0\omega^2}. \tag{13}$$

Substituting a, b and c defined in (11) into $\mathcal{K}(\xi_o) = 0$ yields

$$\frac{\delta}{\theta} = \frac{(\xi_o^2 + l_0\omega\xi_o - l_2\omega)(\xi_o - \omega)}{\omega^2\xi_o}. \tag{14}$$

Since $\xi_o > \omega$ and $\frac{\delta}{\theta} > 0$, the term $\xi_o^2 + l_0\omega\xi_o - l_2\omega$ in (14) satisfies the following inequality

$$0 < \xi_o^2 + l_0\omega\xi_o - l_2\omega < \xi_o^2 + l_0\xi_o^2 - l_2\omega < l_2(\xi_0^2 - \omega) \Rightarrow \xi_o > \sqrt{\omega}.$$

Substituting $\frac{\delta}{\theta}$ in (14) into (13) yields the numerator $-\frac{\partial\mathcal{K}}{\partial\omega} = \frac{\xi_o}{\omega}[l_1\xi_o(\xi_o - \omega) + l_2(\xi_o^2 - \omega)] > 0$ and denominator $\frac{\partial\mathcal{K}}{\partial\xi_o} = l_1\xi_o(\xi_o - \omega) + \frac{l_2}{\xi_o}(\xi_o^3 - \omega^2) > 0$, hence we have $\frac{d\xi_o}{d\omega} > 0$. Combined with $\omega = \frac{T-1}{\kappa}$, we directly obtain $\frac{d\xi_o}{d\kappa} = \frac{d\xi_o}{d\omega}\frac{d\omega}{d\kappa} < 0$, which completes the proof. ■

Proposition 1 shows that, *when the channel estimation error gets larger, if we aim to decrease the SOP under a target secrecy rate, we should increase the information signal power*, which is validated in Fig. 2. It is because that, in order to minimize the SOP, we should first guarantee the link quality of the main channel to support the target secrecy rate. Hence, we should increase the information signal power to balance the deterioration caused by the channel estimation error. When τ exceeds a certain value, transmission is suspended, which is just as analyzed previously. We also find from Fig. 2 that the value of ξ^* increases as R_S increases, which can be easily confirmed by the fact $\frac{d\xi_o}{dT} = \frac{d\xi_o}{d\omega}\frac{d\omega}{dT} > 0$.

Fig. 3 shows that the minimum SOP $\mathcal{O}^*$ increases with τ. For a given P, $\mathcal{O}^*$ increases with R_S. For a given R_S, the two curves with different values of P cross as τ increases (see the intersection $\mathcal{P}$). Specifically, before τ exceeds $\mathcal{P}$, increasing P decreases $\mathcal{O}^*$, and after that the opposite happens. This transition occurs because for too large an estimation error, increasing transmit power does not significantly improve Bob's capacity, whereas it is of great benefit to Eves. This result implies that using full power is not always advantageous, particularly when the estimation error is large.

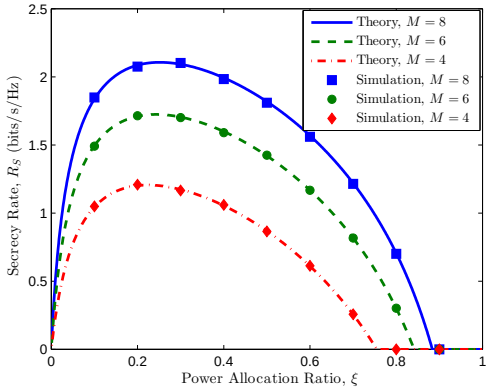

Fig. 4. Secrecy rate R_S versus ξ for different values of M, with $\epsilon = 0.01$, $\tau = 0.2$, and $\lambda_E = 5$.

IV. Secrecy Rate Maximization

In this section, we optimize the PAR that maximizes the secrecy rate subject to a SOP constraint. We first transform the SOP constraint $\mathcal{O} \le \epsilon$ into the following equivalent form

$$1 - \mathcal{F}_{\gamma_E}\left(\frac{1+\kappa\xi}{2^{R_S}} - 1\right) \overset{(c)}{\le} \epsilon \Rightarrow \frac{1+\kappa\xi}{2^{R_S}} - 1 \ge \mathcal{F}_{\gamma_E}^{-1}(1-\epsilon)$$
$$\Rightarrow R_S \le \log_2\frac{1+\kappa\xi}{1+\varrho(\xi)\xi}, \tag{15}$$

where (c) holds due to the monotonically increasing feature of the CDF $\mathcal{F}_{\gamma_E}(x)$ on x. $\varrho(\xi) \triangleq \frac{\mathcal{F}_{\gamma_E}^{-1}(1-\epsilon)}{\xi}$ with $\mathcal{F}_{\gamma_E}^{-1}(\cdot)$ the inverse function of $\mathcal{F}_{\gamma_E}(\cdot)$. Clearly, a positive value of R_S that satisfies the SOP constraint (15) exits only when $\varrho(\xi) < \kappa$. The problem of maximizing R_S can be formulated as

$$\max_{\xi} R_S = \log_2\frac{1+\kappa\xi}{1+\varrho(\xi)\xi} \quad \text{s.t. } \varrho(\xi) < \kappa,\ 0 \le \xi \le 1. \tag{16}$$

An illustration on the relationship between the secrecy rate and the PAR is shown in Fig. 4. It is intuitive that increasing the number of antennas helps to improve the secrecy rate. We

observe that, R_S first increases with ξ, then decreases with it, and even reduces to zero for too large a ξ. This implies we should carefully choose the PAR to achieve a high secrecy rate.

From (16), we see that the value of R_S is bottlenecked by $\varrho(\xi)$, which implicitly reflects the influence of the density of PPP Eves λ_E and the SOP threshold ϵ. For example, a larger λ_E or a smaller ϵ increases $\varrho(\xi)$ (see (9) and the definition of $\varrho(\xi)$), and then decreases R_S (see (16)). Therefore, $\varrho(\xi)$ plays a critical role in maximizing R_S. Although it is intractable to obtain an analytical expression of $\varrho(\xi)$ due to the transcendental equation $1-\mathcal{F}_{\gamma_E}(\xi\varrho(\xi))=\epsilon$ (see (10)), we provide an explicit connection between $\varrho(\xi)$ and ξ in the following lemma, which is very critical for the subsequent optimization.

Lemma 2: $\varrho(\xi)$ is a monotonically increasing and convex function of $\xi\in[0,1]$.

Proof: For notational brevity, we omit ξ from $\varrho(\xi)$. Plugging $x=\xi\varrho$ into $1-\mathcal{F}_{\gamma_E}(x)=\epsilon$ yields

$$\mathcal{Z}(\xi,\varrho)-L=0, \tag{17}$$

where $\mathcal{Z}(\xi,\varrho)=\varrho^{\delta}\left(1+\varrho\frac{1-\xi}{N-1}\right)^{N-1}$, and $L\triangleq\frac{\beta\lambda_E P^{\delta}}{-\ln(1-\epsilon)}$. Using the derivative rule for implicit functions with (17), the first- and second-order derivatives of ϱ on ξ are given by

$$\frac{d\varrho}{d\xi}=-\frac{\partial\mathcal{Z}/\partial\xi}{\partial\mathcal{Z}/\partial\varrho}=\frac{\varrho^2}{\delta+l_2(1-\xi)\varrho}, \tag{18}$$

$$\frac{d^2\varrho}{d\xi^2}=\frac{2}{\varrho}\left(\frac{d\varrho}{d\xi}\right)^2+\frac{l_2\varrho^2\left(\varrho-(1-\xi)\frac{d\varrho}{d\xi}\right)}{\left(\delta+l_2(1-\xi)\varrho\right)^2}. \tag{19}$$

Clearly, $\frac{d\varrho}{d\xi}>0$ always holds. With (18), we have $\varrho-(1-\xi)\frac{d\varrho}{d\xi}=\frac{\delta\varrho+l_0(1-\xi)\varrho^2}{\delta+l_2(1-\xi)\varrho}>0$ in (19). Removing the second term from the right-hand side of (19) yields $\frac{d^2\varrho}{d\xi^2}>\frac{2}{\varrho}\left(\frac{d\varrho}{d\xi}\right)^2>0$. With $\frac{d\varrho}{d\xi}>0$ and $\frac{d^2\varrho}{d\xi^2}>0$, we complete the proof. ∎

Lemma 2 indicates the maximum value of $\varrho(\xi)$ is achieved at $\xi=1$, which is $\varrho_{max}=\varrho(1)=L^{1/\delta}$ from (17). Besides, it is clearly that $\mathcal{Z}(\xi,\varrho)-L$ monotonically increases with ϱ for a given ξ. Generally, we can calculate the unique value of $\varrho(\xi)$ that satisfies (17) using the bisection method in the range $[0,\varrho_{max}]$. For the special case of large antennas, i.e., $N\to\infty$, we provide an approximate value of $\varrho(\xi)$, denoted as $\varrho^o(\xi)$. Simulation results show that, when $N\geq 20$, the maximum value of R_S calculated based on $\varrho^o(\xi)$ is quite close to that based on the exact $\varrho(\xi)$, i.e., $\varrho^o(\xi)$ can be a computationally convenient alternative to $\varrho(\xi)$ when N is large.

Corollary 1: As $N\to\infty$, $\varrho(\xi)$ in (17) *approximates to*

$$\varrho^o(\xi)=\begin{cases}L^{1/\delta}, & \xi=1\\ \frac{\delta}{1-\xi}\ln\left(\frac{\delta^{-1}(1-\xi)L^{1/\delta}}{\mathcal{W}\left(\delta^{-1}(1-\xi)L^{1/\delta}\right)}\right), & \textit{otherwise}\end{cases} \tag{20}$$

where $\mathcal{W}(\cdot)$ is the Lambert-W function.

Proof: Since $\lim_{N\to\infty}\left(1+\frac{x}{N}\right)^{-N}=e^{-x}$, we have $\mathcal{Z}(\xi,\varrho^o)=(\varrho^o)^{\delta}e^{(1-\xi)\varrho^o}$ where $\varrho^o\triangleq\lim_{N\to\infty}\varrho$, and (17) transforms to $L=(\varrho^o)^{\delta}e^{(1-\xi)\varrho^o}$. 1) When $\xi=1$, we easily obtain $\varrho^o=L^{\frac{1}{\delta}}$. 2) When $\xi\neq 1$, we find that $\frac{1-\xi}{\delta}L^{\frac{1}{\delta}}=\frac{(1-\xi)\varrho^o}{\delta}e^{\frac{(1-\xi)\varrho^o}{\delta}}$. Let $\mu\triangleq\frac{1-\xi}{\delta}\varrho^o$, and we obtain $\frac{1-\xi}{\delta}L^{\frac{1}{\delta}}=\mu e^{\mu}\Rightarrow e^{\frac{1-\xi}{\delta}L^{\frac{1}{\delta}}}=e^{\mu e^{\mu}}$. We further let $\nu\triangleq e^{\mu}$ and $t\triangleq e^{\frac{1-\xi}{\delta}L^{\frac{1}{\delta}}}$, such that $\nu^{\nu}=t\Rightarrow\nu=\frac{\ln t}{\mathcal{W}(\ln t)}$. The solution ϱ^o can be given by $\varrho^o=\frac{1-\xi}{\delta}\mu=\frac{1-\xi}{\delta}\ln\nu$, with yields the final expression in (20) by substituting in ν along with t. ∎

Due to the implicit function of $\varrho(\xi)$ on ξ, we can hardly derive an explicit expression of R_S. Nevertheless, we still reveal the concavity of R_S on ξ, and provide the solution to problem (16) in the following theorem.

Theorem 2: R_S in (16) *is a concave function of ξ. The optimal ξ that maximizes R_S is given by*

$$\xi^*=\begin{cases}\varnothing, & \kappa\leq\varrho_{min}\\ 1, & \kappa>\frac{\delta L^{\alpha/2}+L^{\alpha}}{\delta-L^{\alpha}}\ \textit{and}\ L<\sqrt[\alpha]{\delta}\\ \xi_r, & \textit{otherwise}\end{cases} \tag{21}$$

where $\varrho_{min}\triangleq\varrho(0)$ denotes the minimum value of $\varrho(\xi)$. ξ_r is the unique root of $\frac{dR_S}{d\xi}=0$, where

$$\frac{dR_S}{d\xi}=\frac{1}{\ln 2}\left[\frac{\kappa}{1+\kappa\xi}-\frac{\varrho(\xi)+\frac{\xi d\varrho(\xi)}{d\xi}}{1+\xi\varrho(\xi)}\right]. \tag{22}$$

Proof: Alice transmits only when $\varrho<\kappa$. Obviously, if $\kappa\leq\varrho_{min}$, then $\varrho<\kappa$ never holds for an arbitrary ϱ since $\varrho_{min}\leq\varrho$, such that transmission is suspended. If $\kappa>\varrho_{min}$, Alice transmits for a ξ that satisfies $\varrho<\kappa$. To maximize R_S, we first give the second-order derivative of R_S on ξ from (16)

$$\frac{d^2R_S}{d\xi^2}=\frac{1}{\ln 2}\left[\frac{-\kappa^2}{(1+\kappa\xi)^2}-\frac{2\frac{d\varrho}{d\xi}+\xi\frac{d^2\varrho}{d\xi^2}}{(1+\varrho\xi)}+\frac{\left(\varrho+\xi\frac{d\varrho}{d\xi}\right)^2}{(1+\varrho\xi)^2}\right],$$

with $\frac{d\varrho}{d\xi}$ and $\frac{d^2\varrho}{d\xi^2}$ given in Lemma 2. Substituting $\frac{d^2\varrho}{d\xi^2}>\frac{2}{\varrho}\left(\frac{d\varrho}{d\xi}\right)^2>0$ (see Lemma 2) into the above equation yields

$$\frac{d^2R_S}{d\xi^2}<-\frac{1}{\ln 2}\left(\frac{\kappa^2}{(1+\kappa\xi)^2}-\frac{\varrho^2}{(1+\varrho\xi)^2}\right). \tag{23}$$

Since $\varrho<\kappa$, we have $\frac{\kappa^2}{(1+\kappa\xi)^2}-\frac{\varrho^2}{(1+\varrho\xi)^2}>0\Rightarrow\frac{d^2R_S}{d\xi^2}<0$, i.e., R_S is a *concave* function of ξ.

Due to the concavity of R_S on ξ, the maximum value of R_S is achieved either at boundaries or at stationary points. From (22), the boundary values are $\frac{dR_S}{d\xi}|_{\xi=0}=\frac{\kappa-\varrho_{min}}{\ln 2}$ and $\frac{dR_S}{d\xi}|_{\xi=1}=\frac{1}{\ln 2}\left(\frac{\kappa}{1+\kappa}-\frac{L^{\alpha/2}+\frac{\alpha}{2}L^{\alpha}}{1+L^{\alpha/2}}\right)$. Obviously, $\frac{dR_S}{d\xi}|_{\xi=0}>0$. 1) If $\frac{dR_S}{d\xi}|_{\xi=1}>0$, R_S monotonically increases with ξ, and the optimal value of ξ is 1, with the corresponding condition directly obtained from $\frac{dR_S}{d\xi}|_{\xi=1}>0$. 2) If $\frac{dR_S}{d\xi}|_{\xi=1}\leq 0$, R_S first increases and then decreases with ξ, and the optimal value of ξ is the unique root of $\frac{dR_S}{d\xi}=0$. ∎

Theorem 2 shows only for a large κ (small estimation error) and a small L (a sparse-eavesdropper scenario or a moderate SOP constraint), allocating full power to the information signal provides a higher secrecy rate than the AN scheme does, otherwise generating AN is advantageous. Since R_S is a concave function of ξ, we can efficiently calculate the unique root ξ_r of $\frac{dR_S}{d\xi_r}=0$ in (22) using the bisection method. Substituting ξ^* and $\varrho(\xi^*)$ into (16) yields R_S^*.

Although ξ_r can only be calculated numerically, we show how ξ_r is affected by κ in the following.

Proposition 2: ξ_r in (21) *monotonically increases with κ.*

Proof: From (22), $\frac{dR_S}{d\xi_r}=0$ transforms to $\mathcal{A}(\xi_r)=0$, and

$$\mathcal{A}(\xi_r)=(\kappa\xi_r^2-l_0\xi_r+l_2)\varrho_r^2+(l_2\kappa\xi_r-l_2\kappa+\delta)\,\varrho_r-\delta\kappa, \quad (24)$$

with $\varrho_r \triangleq \varrho(\xi_r)$. Using the derivative rule for implicit functions with the equation $\mathcal{A}(\xi_r)=0$ yields

$$\frac{d\xi_r}{d\kappa}=-\frac{\partial\mathcal{A}/\partial\kappa}{\partial\mathcal{A}/\partial\xi_r}=-\frac{\varrho_r^2\xi_r^2-(\delta+l_2(1-\xi_r)\varrho_r)}{\psi_1(\xi_r)+\psi_2(\xi_r)\frac{d\varrho_r}{d\xi_r}}, \quad (25)$$

where $\psi_1(\xi_r)=(1+2\kappa\xi_r)\varrho_r^2+l_2(\kappa-\varrho_r)\varrho_r$ and $\psi_2(\xi_r)=2\left(\kappa\xi_r^2+l_2\right)\varrho_r+(l_2\kappa\xi_r+\delta)-2l_0\xi_r\varrho_r-l_2\kappa$. Obviously, $\kappa>\varrho_r\Rightarrow\psi_1(\xi_r)>0$ and $\frac{d\varrho_r}{d\xi_r}>0$ (see Lemma 2). $\mathcal{A}(\xi_r)=0$ can be further reformed as $\left(\kappa\xi_r^2+l_2\right)\varrho_r+(l_2\kappa\xi_r+\delta)=l_0\xi_r\varrho_r+l_2\kappa+\frac{\delta\kappa}{\varrho_r}$, substituting which into $\psi_2(\xi_r)$ directly yields $\psi_2(\xi_r)>0$. Hence we have $\frac{\partial\mathcal{A}}{\partial\xi_r}>0$. Leveraging (22), $\frac{dR_S}{d\xi_r}=0$ can be reformed by $\xi_r^2\frac{d\varrho_r}{d\xi_r}=1-\frac{1+\varrho_r\xi_r}{1+\kappa\xi_r}<1$. Substituting $\frac{d\varrho_r}{d\xi_r}$ in (18) into this inequality yields $\varrho_r^2\xi_r^2<(\delta+l_2(1-\xi_r)\varrho_r)$, i.e., $\frac{\partial\mathcal{A}}{\partial\kappa}<0$. With $\frac{\partial\mathcal{A}}{\partial\xi_r}>0$ and $\frac{\partial\mathcal{A}}{\partial\kappa}<0$, we see from (25) that $\frac{d\xi_r}{d\kappa}>0$, which completes the proof. ■

Proposition 2 indicates that, *when channel estimation error becomes larger, if we aim to increase the secrecy rate under a SOP constraint, we should increase the AN power*, just as shown in Fig. 5. The reason is: channel estimation error heavily degrades the main channel while has no effect on the wiretap channels. For a large estimation error, although increasing the information signal power improves Bob's capacity, the improvement is not significant. On the contrary, increasing AN power always greatly deteriorates the wiretap channels regardless of CSI imperfection. Therefore, when estimation error becomes larger, increasing AN power is more beneficial to the secrecy rate than increasing signal power. Nevertheless, transmission is suspended if τ exceeds a certain value, which corresponds to the case $\kappa\leq\varrho_{min}$ as indicated in Theorem 2. We can also prove $\frac{d\xi_r}{d\lambda_E}<0$ and $\frac{d\xi_r}{d\epsilon}>0$ in a similar way as the proof of Proposition 2. Due to space limit, we omit the relevant proofs, and the results are verified in Fig. 5. We see that the optimal PAR ξ^* decreases for a larger λ_E or a smaller ϵ. It means that, when transmission is more vulnerable to wiretapping, we should increase AN power.

Fig. 6 depicts the maximum secrecy rate R_S^* versus τ. The approximated value of R_S^* is quite close to the exact one. We observe that R_S^* monotonically decreases with τ. Interestingly, R_S^* increases with P at the small τ region, whereas decreases with it at the large τ region. The underlying reason is just similar to the explanation for the intersection in Fig. 3.

V. Conclusions

In this correspondence, we investigate the AN-aided multi-antenna transmission under imperfect CSI against PPP Eves. We provide explicit solutions of the optimal PARs with channel estimation errors for minimizing the SOP under a secrecy rate constraint and for maximizing the secrecy rate subject to a SOP constraint, respectively. We strictly prove that, when the channel estimation error becomes larger, we should increase the information signal power if we aim to decrease the SOP, whereas we should increase the AN power if we aim to increase the secrecy rate.

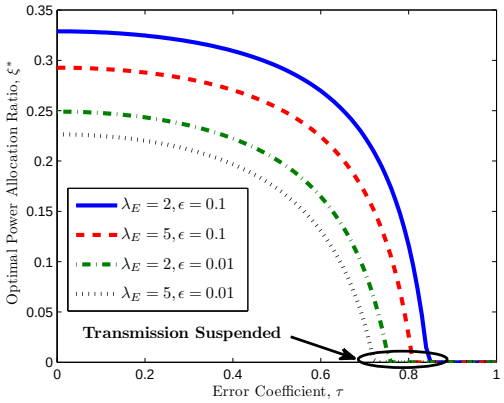

Fig. 5. Optimal PAR ξ^* versus τ for different values of λ_E and ϵ, with $P=0$dBm, and $N=\gamma=20$.

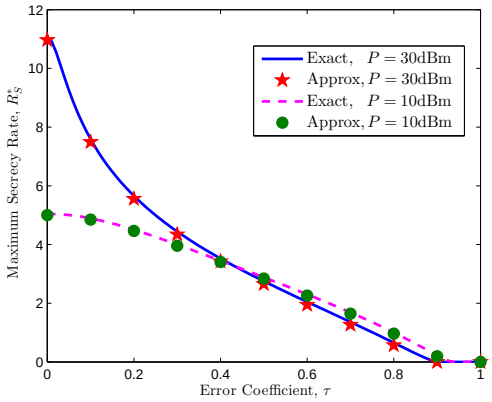

Fig. 6. Maximum secrecy rate R_S^* versus τ for different values of P, with $N=\gamma=20$, $\lambda_E=2$, and $\epsilon=0.01$. "Approx" corresponds to the value of $\varrho^o(\xi)$ in (20) as opposed to the exact value of $\varrho(\xi)$ obtained from (17).

References

[1] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20-27, Apr. 2015.

[2] H.-M. Wang and X.-G. Xia, "Enhancing wireless secrecy via cooperation: signal design and optimization," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 47-53, Dec. 2015.

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

[4] X. Zhang, X. Zhou and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2170-2181, Jun. 2013.

[5] A. Mukherjee, and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351-361, Jan. 2011.

[6] C. Wang and H.-M. Wang, "Robust joint beamforming and jamming for secure AF networks: low complexity design," *IEEE Trans. Veh. Tech.*, vol. 64, no. 5, pp. 2192 - 2198, May 2015.

[7] S.-C. Lin, T.-H. Chang, Y.-L. Liang, Y.-W. P. Hong, and C.-Y. Chi, "On the impact of quantized channel feedback in guaranteeing secrecy with artificial noise: The noise leakage problem," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 901-915, Mar. 2013.

[8] X. Zhang, M. R. McKay, X. Zhou, and R. W. Heath, Jr. “Artificial-noise-aided secure multi-antenna transmission with limited feedback,” *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2742-2754, May, 2015.

[9] H.-M. Wang, C. Wang, and D. W. K. Ng, “Artificial noise assisted secure transmission under training and feedback”, *IEEE Trans. on Signal Process.*, vol. 63, no. 23, pp. 6285 - 6298, Dec. 2015.

[10] M. Haenggi, J. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, “Stochastic geometry and random graphs for the analysis and design of wireless networks,” *IEEE J. Select. Areas Commun.*, vol. 27, no. 7, pp. 1029-1046, Sep. 2009.

[11] M. Ghogho and A. Swami, “Physical-layer secrecy of MIMO communications in the presence of a Poisson random field of eavesdroppers,” in *Proc. IEEE ICC Workshops*, Jun. 2011, pp. 1-5.

[12] T. Zheng, H.-M. Wang, and Q. Yin, “On transmission secrecy outage of multi-antenna system with randomly located eavesdroppers,” *IEEE Commun. Letters*, vol. 18, no. 8, pp. 1299-1302, Aug. 2014.

[13] 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. on Commun.*, vol. 63, no. 11, pp. 4347-4362, Nov. 2015.

[14] G. Geraci, H. S. Dhillon, J. G. Amdrews, J. Yuan, and I. B. Collings, “Physical layer security in downlink multi-antenna cellular networks,” *IEEE Trans. Commun.*, vol. 62, no. 6, pp. 2006-2021, June 2014.

[15] B. Hassibi and B. M. Hochwald, “How much training is needed in multiple-antenna wireless links?” *IEEE Trans. Inform. Theory*, vol. 49, no. 4, pp. 951-963, Apr. 2003.

[16] X. Zhou, P. Sadeghi, T. A. Lamahewa, and S. Durrani, “Design guidelines for training-based MIMO systems with feedback,” *IEEE Trans. Signal Process.*, vol. 57, no. 10, pp. 4014-4026, Oct. 2009.

[17] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, “Compound wiretap channels,” *EURASIP J. Wireless Commun. Network.*, 2009.

[18] K. Jittorntrum, “An implicit function theorem,” *J. of Optimization Theory and Applications*, vol. 25, no. 4, pp. 575-577, 1978.

[19] D. Stoyan, W. Kendall, and J. Mecke, *Stochastic Geometry and its Applications, 2nd ed*. John Wiley and Sons, 1996.