Artificial Noise: Transmission Optimization in Multi-Input Single-Output Wiretap Channels

Nan Yang, *Member, IEEE,* Shihao Yan, *Student Member, IEEE,* Jinhong Yuan, *Senior Member, IEEE,* Robert Malaney, *Member, IEEE,* Ramanan Subramanian, *Member, IEEE,* and Ingmar Land, *Senior Member, IEEE*

***Abstract*—We analyze and optimize the secrecy performance of artificial noise (AN) in multi-input single-output wiretap channels with multiple antennas at the transmitter and a single antenna at the receiver and the eavesdropper. We consider two transmission schemes: 1) an on-off transmission scheme with a constant secrecy rate for all transmission periods, and 2) an adaptive transmission scheme with a varying secrecy rate during each transmission period. For the on-off transmission scheme, an easy-to-compute expression is derived for the hybrid outage probability, which allows us to evaluate the transmission outage probability and the secrecy outage probability. For the adaptive transmission scheme where transmission outage does not occur, we derive a closed-form expression for the secrecy outage probability. Using these expressions, we determine the optimal power allocation between the information signal and the AN signal and also determine the optimal secrecy rate such that the effective secrecy throughput is maximized for both transmission schemes. We show that the maximum effective secrecy throughput requires more power to be allocated to the AN signal when the quality of the transmitter-receiver channel or the transmitter-eavesdropper channel improves. We also show that both transmission schemes achieve a higher maximum effective secrecy throughput while incurring a lower secrecy outage probability than existing schemes.**

***Index Terms*—Artificial noise, multi-input single-output wiretap channels, optimization, physical-layer security.**

Manuscript received June 5, 2014; revised November 11, 2014 and February 28, 2015; accepted March 15, 2015. The work of J. Yuan and R. Malaney was supported by the Australian Research Council Discovery Project (DP120102607). The work of N. Yang was supported by the Australian Research Council Discovery Projects (DP120102607 and DP150103905). The material in this paper was presented in part at the IEEE International Conference on Communications, Sydney, Australia, June 2014. The associate editor coordinating the review of this paper and approving it for publication was A. Khisti.

N. Yang was with the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, NSW 2052, Australia. He is now with the Research School of Engineering, Australian National University, Canberra, ACT 0200, Australia (email: nan.yang@anu.edu.au).

S. Yan, J. Yuan, and R. Malaney are with the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, NSW 2052, Australia (email: shihao.yan@student.unsw.edu.au; j.yuan@unsw.edu.au; r.malaney@unsw.edu.au).

R. Subramanian is with the Institute for Telecommunications Research, University of South Australia, Adelaide, SA 5001, Australia (email: ramanan.subramanian,@unisa.edu.au).

I. Land was with the Institute for Telecommunications Research, University of South Australia, Adelaide, SA 5001, Australia. He is now with the Mathematical and Algorithmic Sciences Lab, France Research Center, Huawei Technologies Co. Ltd., 92100 Boulogne-Billancourt, France. (email: ingmar.land@ieee.org).

Digital Object Identifier 10.1109/TCOMM.2015.2419634

I. Introduction

RAPID and continuous growth of wireless mobile services has opened up an emerging and promising research focus in the design of wireless transmission strategies, in the form of protecting the confidentiality and security of the transmitted information. The need for this research focus arises from the broadcast nature of the wireless medium that makes wireless transmission vulnerable to potential eavesdropping. To address this research focus, recent efforts have been devoted to physical-layer security [1, 2], the core principle of which is to exploit the characteristics of wireless channels in order to guarantee secure communication between legitimate parties [3–5]. By adding structured redundancy and randomness in transmit signals, physical-layer security allows the legitimate user to correctly decode confidential messages, but prevents the eavesdroppers from successfully retrieving the messages. Motivated by the benefits of physical-layer security, [6–9] analyzed the secrecy performance of wiretap channels with a single antenna at the transmitter, receiver, and eavesdropper(s).

The deployment of co-located multiple antennas at the transmitter and/or the legitimate receiver has recently been recognized as an effective means to enhance physical-layer security. The effectiveness of multiple antennas lies in exploiting spatial degrees of freedom and thus increasing the channel reliability between the transmitter and the receiver while degrading the reception quality at the eavesdropper(s). In early studies, e.g., [10–14], the secrecy capacity was analyzed to realize the benefits of multiple antennas from an information-theoretic perspective. An important assumption in these theoretical studies is that the eavesdropper's channel state information (CSI) is available at the transmitter. Such a strong assumption was relaxed in other recent papers which concentrated on the design of signal processing algorithms in multi-antenna wiretap channels. For example, [15] used transmit beamforming (BF) in the direction of the legitimate receiver to perform secure transmission. In order to reduce the feedback and computational overheads caused by transmit BF, [16–20] proposed transmit antenna selection and examined its secrecy performance.

It is critical to note that transmit BF and transmit antenna selection focus on enhancing the quality of the main channel between the transmitter and the receiver only. In contrast to those, [21] proposed a transmission scheme which transmits artificial noise (AN) together with information signals to deliberately interfere with the eavesdropper's received signal. Considering fast fading channels where the channel coherence time is smaller than the codeword period, [22–26] examined the ergodic secrecy rate of the AN transmission scheme and investigated the optimal power allocation for the maximization of the secrecy rate. Considering slow fading channels where the channel coherence time is larger than the codeword period, [27–29] examined the secrecy outage probability of the AN transmission scheme. More recently, [30, 31] investigated not only the secrecy outage probability but the throughput of the AN transmission scheme. Given a secrecy outage constraint, [30] optimized the wiretap code rate in order to maximize the average throughput of non-adaptive encoding (NAE) and adaptive encoding (AE) schemes under the assumption of zero noise at the eavesdropper. Different from [30], we considered non-zero noise at the eavesdropper in [31] and determined the optimal secrecy rate that maximizes the secrecy throughput.

In this paper, we analyze and optimize the effective secrecy throughput (EST) of AN transmission schemes in multi-input single-output (MISO) wiretap channels where the transmitter is equipped with multiple antennas whereas the receiver is equipped with a single antenna. We assume that a single-antenna eavesdropper overhears the communication from the transmitter to the receiver. In this work, we consider slow fading and the scenario where the eavesdropper's instantaneous CSI is not known at the transmitter. In this scenario, the transmitter only uses the receiver's instantaneous CSI to design AN signals. We determine the optimal values of two parameters: a) the power allocation between information signals and AN signals, and b) the secrecy rate of wiretap codes. These optimal parameters are determined so as to maximize the EST of two AN transmission schemes: 1) an on-off transmission scheme where the optimal power allocation and the optimal secrecy rate are chosen independent of the main channel realization across all transmission periods and 2) an adaptive transmission scheme where the optimal power allocation and the optimal secrecy rate are chosen based on the main channel realization for each transmission period. Here, the EST[1] is defined as the product of the secrecy rate and the secure transmission probability [33]. Thus, the analysis and optimization of the EST are practically significant since they characterize the maximum average secrecy data rate in secure communications. Notably, the optimization of EST does not involve an *a prior* secrecy constraint that was applied for all transmission blocks in [30]. In this work we remove this constraint and quantify the maximum secrecy data rate by allowing for different secrecy outage probabilities for distinct transmission blocks. As such, our results are useful for scenarios where a strict requirement on the secrecy outage probability is not necessary.

In order to determine the optimal parameters of the two AN transmission schemes, we derive an easy-to-compute expression for the hybrid outage probability given a secrecy rate for the on-off transmission scheme. This expression characterizes the probability that either transmission outage or secrecy outage occurs. We also derive a closed-form expression for the secrecy outage probability given a main channel realization and a secrecy rate for the adaptive transmission scheme. Based on our newly derived expressions, we obtain the EST in closed form and determine the joint optimal power allocation and secrecy rate that maximizes the EST of both transmission schemes. Notably, our optimal solutions are valid for general operating scenarios with an arbitrary number of antennas at the transmitter, an arbitrary average SNR at the receiver, and an arbitrary average SNR at the eavesdropper. As such, our results apply to the scenario where the eavesdropper is a regular user and its average SNR is known at the transmitter. This is different from [30], the results of which apply to the scenario where the average SNR at the eavesdropper is unknown.

We offer valuable insights into the design of AN transmission built upon our analysis. For both schemes, we demonstrate that the transmitter is required to allocate more power to the AN signal to achieve the maximum EST when the number of antennas at the transmitter increases, the average SNR of the main channel increases, or the average SNR of the eavesdropper's channel increases. Moreover, we demonstrate that the adaptive transmission scheme offers a higher EST than the on-off transmission scheme, at the cost of increasing signal processing complexity. Furthermore, we compare the on-off and adaptive transmission schemes with the transmit BF schemes [15] and the NAE and AE schemes [30]. We also demonstrate that the on-off and adaptive transmission schemes achieve a higher maximum EST than the NAE and AE schemes [30] while maintaining a lower secrecy outage probability[2].

[1]The EST is different from the throughput in [30, 32] which was defined as the product of the secrecy rate and the transmission probability and thus examined the average rate at which the messages are transmitted.

[2]The higher maximum EST achieved by our schemes over the schemes in [30] is due to the fact that we consider a different assumption from [30]. Due to the different assumption on the knowledge of the eavesdropper's noise level, no fair and direct comparison can be truly made between our results and those of [30]. Rather, our work should be viewed as complimentary to the work of [30].

II. Artificial Noise in MISO Wiretap Channels

A. MISO wiretap channels

We consider a MISO wiretap channel, as depicted in Fig. 1, where the data transmission from an N-antenna transmitter (Alice) to a single antenna legitimate receiver (Bob) is overheard by a single antenna eavesdropper (Eve). We denote the main channel between Alice and Bob by an $1 \times N$ vector $\mathbf{h}$ and denote the eavesdropper's channel between Alice and Eve by an $1 \times N$ vector $\mathbf{g}$. We assume that the entries of $\mathbf{h}$ are independent and identically distributed (i.i.d.) zero-mean circularly symmetric complex Gaussian random variables with unit variance, and the entries of $\mathbf{g}$ are i.i.d. zero-mean circularly symmetric complex Gaussian random variables with unit variance. We also assume that the noise components at Bob and Eve are independent zero-mean circularly symmetric complex Gaussian random variables that have unequal variances. As such, the average SNRs of the main channel and eavesdropper's channel may be different. We further assume that the main channel and the eavesdropper's channel are subject to slow block fading where the fading coefficients keep invariant during the channel coherence time, and the channel coherence time is larger than the codeword period.

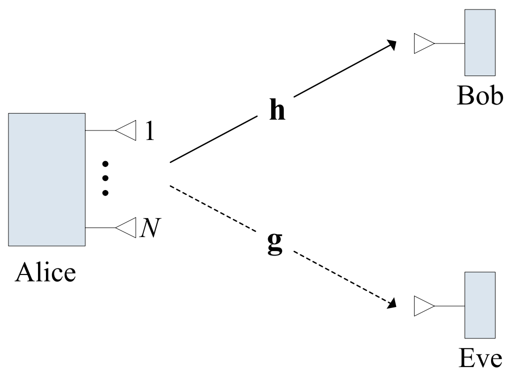


Fig. 1. Illustration of a multi-input single-output wiretap channel where Alice is equipped with N antennas while Bob and Eve are equipped with a single antenna each.

In this work, we consider the realistic scenario where instantaneous information about $\mathbf{g}$ is not available to Alice. We assume that Bob precisely estimates $\mathbf{h}$ and feeds it back to Alice. Since the feedback from Bob to Alice is not secure, we further assume that $\mathbf{h}$ is perfectly known at Eve. In order to perform secure transmission, Alice encodes her messages and transmits the resulting codewords to Bob. Eve passively overhears the information conveyed from Alice to Bob without causing any interference to the main channel.

In the MISO wiretap channel, the achievable secrecy rate C_s is expressed as [14]

$$C_s = \begin{cases} C_b - C_e \quad , & \gamma_b > \gamma_e \\ 0 \quad , & \gamma_b \leq \gamma_e, \end{cases} \tag{1}$$

where $C_b = \log_2(1+\gamma_b)$ is the instantaneous capacity of the main channel and $C_e = \log_2(1+\gamma_e)$ is the instantaneous capacity of the eavesdropper's channel. Here, γ_b denotes the instantaneous received SNR at Bob and γ_e denotes the instantaneous received SNR at Eve. Wiretap codes are adopted at Alice in order to perform secure transmission to Bob such that Alice needs to choose two rates of wiretap codes, namely, the overall codeword rate, R_b, and the secrecy rate, R_s. The difference between R_b and R_s, i.e., $R_b - R_s$, is the rate redundancy that provides secrecy against eavesdropping. Since we consider the passive eavesdropping scenario where the instantaneous CSI of the eavesdropper's channel is not known at Alice, Alice assumes the capacity of the eavesdropper's channel as C'_e and designs the wiretap codes as $R_b = C_b$ and $R_s = C_b - C'_e$. We note that perfect secrecy cannot be always guaranteed in the passive eavesdropping scenario since there exists a probability that some messages transmitted by Alice are leaked to Eve.

B. Artificial noise

The signal transmitted by Alice is constructed in such a manner that it contains both the information signal and the AN signal, in order to secure the information signal from the eavesdropper. We denote the transmitted signal vector by $\mathbf{t}$, the information signal by t_{IS}, and the $(N-1)\times 1$ AN vector by $\mathbf{t}_{\text{AN}}$. In order to perform this transmission, the $N \times N$ BF matrix is designed as [22]

$$\mathbf{W} = [\mathbf{w}_{\text{IS}} \ \mathbf{W}_{\text{AN}}], \tag{2}$$

where $\mathbf{w}_{\text{IS}}$ is used to transmit t_{IS} and $\mathbf{W}_{\text{AN}}$ is used to transmit $\mathbf{t}_{\text{AN}}$. Notably, the aim of $\mathbf{W}$ is to degrade the quality of the received signals at Eve by transmitting AN in all directions except towards Bob. As such, we choose $\mathbf{w}_{\text{IS}}$ as the principal eigenvector corresponding to the largest eigenvalue of $\mathbf{h}^H\mathbf{h}$ [21], where $\mathbf{h}^H$ denotes the complex conjugate transpose of $\mathbf{h}$. Here, $\mathbf{w}_{\text{IS}}$ is normalized such that $\|\mathbf{w}_{\text{IS}}\|^2 = 1$. We then choose $\mathbf{W}_{\text{AN}}$ such that $\mathbf{W}_{\text{AN}}$ is comprised of the remaining $N-1$ eigenvectors of $\mathbf{h}^H\mathbf{h}$. As such, the columns $\mathbf{W}_{\text{AN}}$ form an orthonormal basis of the nullspace of $\mathbf{h}$, i.e., $\mathbf{h}\mathbf{W}_{\text{AN}} = \mathbf{0}$. Note that $\mathbf{W}$ is a unitary matrix. Using $\mathbf{W}$, the $N \times 1$ transmitted signal vector at Alice is given by

$$\mathbf{t} = \mathbf{W}\begin{bmatrix} t_{\text{IS}} \\ \mathbf{t}_{\text{AN}} \end{bmatrix} = \mathbf{w}_{\text{IS}}t_{\text{IS}} + \mathbf{W}_{\text{AN}}\mathbf{t}_{\text{AN}}. \tag{3}$$

Therefore, the received signal at Bob is given by

$$\begin{aligned} y &= \mathbf{h}\mathbf{t} + n_b = \mathbf{h}\mathbf{w}_{\text{IS}}t_{\text{IS}} + \mathbf{h}\mathbf{W}_{\text{AN}}\mathbf{t}_{\text{AN}} + n_b \\ &= \mathbf{h}\mathbf{w}_{\text{IS}}t_{\text{IS}} + n_b, \end{aligned} \tag{4}$$

where n_b is additive white Gaussian noise (AWGN) at Bob satisfying $\mathbb{E}\left[n_b n_b^H\right] = \sigma_b^2$; $\mathbb{E}[\cdot]$ denotes the expectation.

During data transmission, we assume that the total transmit power adopted at Alice is constrained by P_{T}. We define the overall transmit SNR of the main channel as $\overline{\gamma}_b = P_{\text{T}}/\sigma_b^2$. We also define the received SNR without AN at Bob as $\tilde{\gamma}_b = \overline{\gamma}_b\|\mathbf{h}\|^2$, where $\|\cdot\|$ denotes the Euclidean norm. The value of $\tilde{\gamma}_b$ can be obtained based on the feedback of $\|\mathbf{h}\|^2$ from Bob. We further define σ_{IS}^2 as the variance of t_{IS} and σ_{AN}^2 as the variance of each entry of $\mathbf{t}_{\text{AN}}$. Let the power allocation ratio α, $0 < \alpha \leq 1$, represent the fraction of the power allocated to t_{IS}. As such, we have $\sigma_{\text{IS}}^2 = \alpha P_{\text{T}}$. Since Alice has no knowledge about $\mathbf{g}$, she equally distributes the transmit power to each entry of $\mathbf{t}_{\text{AN}}$ such that $\sigma_{\text{AN}}^2 = (1-\alpha)P_{\text{T}}/(N-1)$. We note that the case of $\alpha = 1$ is equivalent to transmit BF [15] where Alice does not transmit AN but transmits information signals using MRT with P_{T}. Based on (4), we write the received SNR with AN at Bob as

$$\gamma_b = \frac{\alpha P_{\text{T}}}{\sigma_b^2}\|\mathbf{h}\|^2 = \alpha\tilde{\gamma}_b. \tag{5}$$

Given the transmitted signal vector in (3), the received signal at Eve is given by

$$z = \mathbf{g}\mathbf{t} + n_e = \mathbf{g}\mathbf{w}_{\text{IS}}t_{\text{IS}} + \mathbf{g}\mathbf{W}_{\text{AN}}\mathbf{t}_{\text{AN}} + n_e, \tag{6}$$

where n_e is AWGN at Eve satisfying $\mathbb{E}\left[n_e n_e^H\right] = \sigma_e^2$. The overall transmit SNR of the eavesdropper's channel is defined as $\overline{\gamma}_e = P_{\text{T}}/\sigma_e^2$. We assume that $\overline{\gamma}_b$ and $\overline{\gamma}_e$ are publicly known at Alice. This assumption that $\overline{\gamma}_e$ is known at Alice applies to the scenario where Eve is a regular user served by Alice in previous time slots. That is, we assume Eve is part of a multiuser system which in alternate time slots she becomes an active legitimate participant in the system, and as such will feedback to the transmitter her CSI and the estimated thermal noise level for the time slot in which she is being served. From this information, and under the assumption the eavesdropper is static (or moving slowly) the average SNR of Eve in the time slots she is not being served can be derived. We note that the assumption of available knowledge about $\overline{\gamma}_e$ is adopted in other physical-layer security studies, e.g., [8, 15, 17, 24, 28, 29]. It is important to point out that although Eve knows the instantaneous knowledge of $\mathbf{h}$, $\mathbf{W}$, and $\mathbf{g}$, she cannot completely eliminate the interference caused by $\mathbf{W}_{\rm AN}\mathbf{t}_{\rm AN}$. As such, the instantaneous received signal-to-interference-plus-noise ratio (SINR) at Eve is written as

$$\gamma_e = \frac{\alpha P_{\rm T}\|\mathbf{g}\mathbf{w}_{\rm IS}\|^2}{\frac{1-\alpha}{N-1}P_{\rm T}\|\mathbf{g}\mathbf{W}_{\rm AN}\|^2+\sigma_e^2} = \frac{\alpha\|\mathbf{g}\mathbf{w}_{\rm IS}\|^2}{\frac{1-\alpha}{N-1}\|\mathbf{g}\mathbf{W}_{\rm AN}\|^2+\frac{1}{\overline{\gamma}_e}}. \quad (7)$$

C. Statistics of γ_b and γ_e

We next derive the statistics of γ_b and γ_e in order to facilitate our subsequent analysis. We find from (5) that γ_b follows a chi-squared distribution since $\|\mathbf{h}\|^2$ is a sum of the squares of N independent Gaussian random variables. As such, we obtain the cumulative distribution function (CDF) of γ_b as

$$F_{\gamma_b}(\gamma) = 1 - \frac{\Gamma\left(N, \frac{\gamma}{\alpha\overline{\gamma}_b}\right)}{\Gamma(N)} = 1 - e^{-\frac{\gamma}{\alpha\overline{\gamma}_b}}\sum_{n=0}^{N-1}\frac{1}{n!}\left(\frac{\gamma}{\alpha\overline{\gamma}_b}\right)^n, \quad (8)$$

where $\Gamma(\cdot,\cdot)$ is the upper incomplete gamma function [35, Eq. (8.350.2)] and $\Gamma(\cdot)$ is the gamma function [35, Eq. (8.310.1)]. In (8), the second equation holds by applying [35, Eq. (8.351.2)] to expand $\Gamma\left(N, \frac{\gamma}{\alpha\overline{\gamma}_b}\right)$.

We now derive the CDF of γ_e. We note that the entries of $\mathbf{g}$ are i.i.d. zero-mean complex Gaussian random variables and $\mathbf{W}$ is a unitary matrix. Since the generation of $\mathbf{W}$ is completely determined by the realization of $\mathbf{h}$, as stated in Section II-B, we conclude that $\mathbf{W}$ and $\mathbf{g}$ are mutually independent. This leads to the outcome that $\mathbf{g}\mathbf{W}$ has the same distribution as $\mathbf{g}$, i.e., the entries of $\mathbf{g}\mathbf{W}$ are i.i.d. zero-mean complex Gaussian random variables. The CDF of γ_e is derived as

$$F_{\gamma_e}(\gamma) = 1 - \left(1+\frac{(1-\alpha)\gamma}{\alpha(N-1)}\right)^{-(N-1)} e^{-\frac{\gamma}{\alpha\overline{\gamma}_e}}. \quad (9)$$

The detailed derivation of (9) can be found in [28, Appendix A]. We highlight that (9) is valid for arbitrary values of $\overline{\gamma}_e$. When $\overline{\gamma}_e \to \infty$, we find that (9) simplifies to [30, Eq. (5)].

III. On-Off Transmission

In this section, we focus on the on-off transmission scheme and examine its secrecy performance in the MISO wiretap channel. We first introduce the principle of the general on-off transmission scheme. We next derive closed-form expressions for the transmission outage probability, the secrecy outage probability, and the secure transmission probability. Based on these expressions, we obtain the expressions for the EST, the probability of non-zero secrecy rate, and the ε-outage secrecy rate. Utilizing these closed-form expressions, we first determine the optimal power allocation ratio α^* that minimizes the hybrid outage probability for a given R_s, and then determine the joint optimal pair $(\alpha^{*\circ}, R_s^{*\circ})$ that maximizes the EST.

A. Principle of On-Off Transmission

In the general on-off transmission scheme, Alice selects a predetermined power allocation ratio α and a predetermined constant secrecy rate R_s for transmission. In this scheme, Alice sets $R_b = C_b$ and $R_s = C_b - C_e'$ and determines the values of α and R_s based on $\overline{\gamma}_b$ and $\overline{\gamma}_e$. As such, the values of α and R_s are fixed for all transmission periods and independent of channel realizations. The optimal values of α and R_s will be discussed in Section III-C. We next define three mutually exclusive events which partition the entire event space of this scheme.

Event 1: Transmission outage
This event occurs when $C_b \leq R_s$. In this case, we find that wiretap codes cannot be constructed since $C_e' = C_b - R_s$ conflicts with $C_e' > 0$. As such, R_s is not supported by the main channel and Alice does not transmit.

Event 2: Secrecy outage
This event occurs when $C_s < R_s$ and $C_b > R_s$. In this case, we find that the assumed capacity of the eavesdropper's channel is lower than its actual instantaneous value, i.e., $C_e' < C_e$. As such, Alice transmits but secrecy is compromised.

Event 3: Secure transmission
This event occurs when $C_s \geq R_s$. In this case, we find that the assumed capacity of the eavesdropper's channel is better than the capacity of the eavesdropper's channel, i.e., $C_e' \geq C_e$. As such, Alice transmits and the wiretap code guarantees perfect secrecy.

For these events, we examine four probabilities: i) the *transmission outage probability* which is defined as the probability of **Event 1**, ii) the *secrecy outage probability* which is defined as the probability of **Event 2**, iii) the *hybrid outage probability* which is defined as the summation of the transmission outage probability and the secrecy outage probability, and iv) the *secure transmission probability* which is defined as the probability of **Event 3**. We clarify that our on-off transmission scheme is different from the NAE scheme of [30]. In the NAE scheme the value of R_b is fixed, whereas in our scheme the value of R_b is chosen dynamically as $R_b = C_b$. We quantify later (Section V) the improvement in secrecy performance achieved by dynamically setting $R_b = C_b$. We also clarify that the secrecy outage probability we investigate in this work is different from the conditional secrecy outage probability in [30, Eq. (9)] which evaluates the probability of secrecy outage conditioned on transmission.

B. Secrecy Performance of On-Off Transmission

1) Transmission outage probability: The transmission outage probability is defined as

$$\begin{aligned} P_{\rm to}(\alpha, R_s) &= \Pr(C_b \leq R_s) \\ &= \Pr(\log_2(1+\gamma_b) \leq R_s). \end{aligned} \quad (10)$$

Based on the properties of γ_b, we express the transmission outage probability in terms of the CDF of γ_b as

$$P_{\rm to}(\alpha, R_s) = F_{\gamma_b}\left(2^{R_s}-1\right). \quad (11)$$

Substituting (8) into (11), we obtain $P_{\text{to}}(\alpha, R_s)$ as

$$P_{\text{to}}(\alpha, R_s) = 1 - e^{-\frac{2^{R_s}-1}{\alpha\overline{\gamma}_b}} \sum_{n=0}^{N-1} \frac{1}{n!}\left(\frac{2^{R_s}-1}{\alpha\overline{\gamma}_b}\right)^n. \quad (12)$$

2) Secrecy outage probability: The secrecy outage probability is defined as

$$\begin{aligned} P_{\text{so}}(\alpha, R_s) &= \Pr(C_s < R_s, C_b > R_s) \\ &= \Pr(R_s < C_b < C_e + R_s) \\ &= \Pr(R_s < \log_2(1+\gamma_b) < \log_2(1+\gamma_e) + R_s). \quad (13) \end{aligned}$$

We next present our new result for the secrecy outage probability in the following theorem.

Theorem 1: The secrecy outage probability for the on-off transmission scheme is given by

$$P_{\text{so}}(\alpha, R_s) = \begin{cases} -P_{\text{s}}^{(1)}(\alpha, R_s) + P_{\text{t}}(\alpha, R_s) &, \quad 0 < \alpha < 1 \\ -P_{\text{s}}^{(2)}(R_s) + P_{\text{t}}(\alpha, R_s) &, \quad \alpha = 1, \end{cases} \quad (14)$$

where

$$\begin{aligned} P_{\text{s}}^{(1)}(\alpha, R_s) =& \frac{1}{\alpha\overline{\gamma}_e} e^{-\frac{2^{R_S}-1}{\alpha\overline{\gamma}_b}} \sum_{n=0}^{N-1} \frac{1}{n!(\alpha\overline{\gamma}_b)^n} \sum_{m=0}^{n} \binom{n}{m} \\ &\times 2^{mR_S}\left(2^{R_S}-1\right)^{n-m} \kappa^{m+1}\Gamma(m+1) \\ &\times [\mathbb{U}(m+1, -N+m+3, \lambda) \\ &\quad + (1-\alpha)\overline{\gamma}_e \mathbb{U}(m+1, -N+m+2, \lambda)], \quad (15) \end{aligned}$$

$$\begin{aligned} P_{\text{s}}^{(2)}(R_s) =& \frac{1}{\overline{\gamma}_e} e^{-\frac{2^{R_S}-1}{\overline{\gamma}_b}} \sum_{n=0}^{N-1} \frac{1}{n!\overline{\gamma}_b^n} \sum_{m=0}^{n} \binom{n}{m} \\ &\times 2^{mR_S}\left(2^{R_S}-1\right)^{n-m} \frac{\Gamma(m+1)}{\left(\frac{2^{R_S}}{\overline{\gamma}_b} + \frac{1}{\overline{\gamma}_e}\right)^{m+1}}, \quad (16) \end{aligned}$$

and $P_{\text{t}}(\alpha, R_s) = 1 - P_{\text{to}}(\alpha, R_s)$. In (15), we use

$$\kappa = \frac{\alpha(N-1)}{1-\alpha}, \quad \lambda = \left(\frac{2^{R_S}}{\overline{\gamma}_b} + \frac{1}{\overline{\gamma}_e}\right)\frac{N-1}{1-\alpha},$$

and denote $\mathbb{U}(\cdot,\cdot,\cdot)$ as the Tricomi confluent hypergeometric function [35, Eq. (9.211.4)].

Proof: The proof is presented in Appendix A. ■

3) Hybrid outage probability and secure transmission probability: The hybrid outage probability is defined as

$$P_{\text{ho}}(\alpha, R_s) = P_{\text{to}}(\alpha, R_s) + P_{\text{so}}(\alpha, R_s). \quad (17)$$

Substituting (12) and (14) into (17), we obtain $P_{\text{ho}}(\alpha, R_s)$ as

$$P_{\text{ho}}(\alpha, R_s) = \begin{cases} 1 - P_{\text{s}}^{(1)}(\alpha, R_s) &, \quad 0 < \alpha < 1 \\ 1 - P_{\text{s}}^{(2)}(R_s) &, \quad \alpha = 1. \end{cases} \quad (18)$$

The secure transmission probability is equal to the complementary probability of $P_{\text{ho}}(\alpha, R_s)$. Therefore, it is defined as

$$P_{\text{st}}(\alpha, R_s) = 1 - P_{\text{ho}}(\alpha, R_s). \quad (19)$$

Using (18), the secure transmission probability is obtained as

$$P_{\text{st}}(\alpha, R_s) = \begin{cases} P_{\text{s}}^{(1)}(\alpha, R_s) &, \quad 0 < \alpha < 1 \\ P_{\text{s}}^{(2)}(R_s) &, \quad \alpha = 1. \end{cases} \quad (20)$$

We highlight that our new expressions in (18) and (20) are easy to compute since they involve power functions, exponential functions, and hypergeometric functions only. We highlight that the values of these functions, including the hypergeometric function, can be easily computed. Thus, the optimal parameter and the optimal performance presented in Section III-C can be easily obtained. Notably, the derived results in (18) and (20) are valid for an arbitrary number of transmit antennas and arbitrary average SNRs.

4) Effective secrecy throughput: We define the *EST* (in bps/Hz) as the product of the secrecy rate, R_s, and the secure transmission probability, $P_{\text{st}}(\alpha, R_s)$. Mathematically, it is expressed as

$$T(\alpha, R_s) = R_s P_{\text{st}}(\alpha, R_s). \quad (21)$$

As explained in Section I, such a performance metric evaluates the average secrecy rate at which the messages are securely transmitted from Alice to Bob without being eavesdropped on by Eve [33]. Of course, it is impossible for Bob to identify which messages are securely transmitted and which messages are leaked in the passive eavesdropping scenario. However, this performance metric is still meaningful since it quantifies the average amount of the securely transmitted messages.

We note that $P_{\text{st}}(\alpha, R_s)$ is a function of α, N, $\overline{\gamma}_b$, and $\overline{\gamma}_e$. As such, it is indicated from (21) that $T(\alpha, R_s)$ is jointly determined by α and R_s for given N, $\overline{\gamma}_b$, and $\overline{\gamma}_e$.

5) Other performance metrics: First, we focus on the *probability of non-zero secrecy rate* which is defined as the probability of $\gamma_b > \gamma_e$ [8]. We formulate the probability of non-zero secrecy rate as

$$\begin{aligned} P_{\text{nz}} &= \Pr(C_s > 0) = \Pr(\gamma_b > \gamma_e) \\ &= 1 - \int_0^\infty \int_0^{\gamma_e} f_{\gamma_b}(\gamma_b) f_{\gamma_e}(\gamma_e)\, d\gamma_b d\gamma_e \\ &= 1 - \int_0^\infty f_{\gamma_e}(\gamma_e) F_{\gamma_b}(\gamma_e)\, d\gamma_e. \quad (22) \end{aligned}$$

Comparing (22) with ℓ_1 in (43) in Appendix A, we observe that P_{nz} can be obtained via $P_{\text{nz}} = 1 - P_{\text{ho}}(\alpha, R_s)|_{R_s=0}$. Specifically, we obtain the probability of non-zero secrecy rate as

$$P_{\text{nz}} = \begin{cases} P_{\text{nz}}^{(1)}(\alpha) &, \quad 0 < \alpha < 1 \\ P_{\text{nz}}^{(2)} &, \quad \alpha = 1, \end{cases} \quad (23)$$

where

$$\begin{aligned} P_{\text{nz}}^{(1)}(\alpha) &= P_{\text{s}}^{(1)}(\alpha, 0) \\ &= \frac{1}{\alpha\overline{\gamma}_e} \sum_{n=0}^{N-1} \omega \mathbb{U}(n+1, -N+n+3, \lambda) \\ &\quad + \frac{1-\alpha}{\alpha} \sum_{n=0}^{N-1} \omega \mathbb{U}(n+1, -N+n+2, \lambda) \quad (24) \end{aligned}$$

with $\omega = \frac{\Gamma(n+1)\kappa^{n+1}}{n!(\alpha\overline{\gamma}_b)^n}$ and

$$\begin{aligned} P_{\text{nz}}^{(2)} &= P_{\text{s}}^{(2)}(0) \\ &= \frac{1}{\overline{\gamma}_e} \sum_{n=0}^{N-1} \frac{\Gamma(n+1)}{n!\overline{\gamma}_b^n} \left(\frac{1}{\overline{\gamma}_b} + \frac{1}{\overline{\gamma}_e}\right)^{-(n+1)}. \quad (25) \end{aligned}$$

Second, we examine the *ε-outage secrecy rate* which is defined as the highest secrecy rate $R_{s,\max}$ when the hybrid outage probability is less than ε [36]. We formulate the ε-outage secrecy rate as

$$C(\alpha, \varepsilon) = \max_{R_s : P_{\text{ho}}(\alpha, R_s) \leq \varepsilon} R_s. \quad (26)$$

Substituting (18) into (26), the ε-outage secrecy rate can be obtained via numerical root-finding.

C. Performance Optimization of On-Off Transmission

In this subsection, we determine the joint optimal power allocation ratio and secrecy rate pair $(\alpha^{*\circ}, R_s^{*\circ})$ that maximizes the EST of the on-off transmission scheme. Mathematically, $(\alpha^{*\circ}, R_s^{*\circ})$, is determined by

$$(\alpha^{*\circ}, R_s^{*\circ}) = \underset{R_s,\ 0<\alpha^* \leq 1}{\operatorname{argmax}}\ T(\alpha^*, R_s), \quad (27)$$

where α^* denotes the optimal power allocation ratio that minimizes the hybrid outage probability $P_{\text{ho}}(\alpha, R_s)$ in (18) (or equivalently, maximizes the secure transmission probability $P_{\text{st}}(\alpha, R_s)$ in (20)) for a given R_s. Mathematically, α^* is determined by

$$\alpha^* = \underset{0<\alpha \leq 1}{\operatorname{argmin}}\ P_{\text{ho}}(\alpha, R_s). \quad (28)$$

We note that α^* is a function of R_s. By numerically taking the second derivative of $P_{\text{ho}}(\alpha, R_s)$ with respect to α for a given R_s, we find that $\partial^2 P_{\text{ho}}(\alpha, R_s)/\partial^2 \alpha > 0$ when $0 < \alpha \leq 1$. This indicates that the optimal value of α that minimizes $P_{\text{ho}}(\alpha, R_s)$ is unique. We note that a closed-form solution for α^* is mathematically intractable, due to the complexity of (18). As such, we resort to exhaustive search in order to find the local optimal α between 0 and 1 and denote it as α^*. Using α^*, we define the optimal hybrid outage probability and the optimal secure transmission probability for a given R_s as $P_{\text{ho}}^*(\alpha^*, R_s)$ and $P_{\text{st}}^*(\alpha^*, R_s)$, respectively. Accordingly, we obtain the EST achieved by α^* is written as $T(\alpha^*, R_s) = R_s P_{\text{st}}^*(\alpha^*, R_s)$.

Due to the fact that $P_{\text{st}}^*(\alpha^*, R_s)$ is maximized by α^*, we find that $T(\alpha^*, R_s)$ is maximized by α^* since $T(\alpha^*, R_s)$ is a product of R_s and $P_{\text{st}}^*(\alpha^*, R_s)$. We then take the first derivative of $T(\alpha^*, R_s)$ with respect to R_s for a given α^* and find that $\partial T(\alpha^*, R_s)/\partial R_s$ is first positive then negative with increasing R_s. This implies that the optimal value of R_s maximizing $T(\alpha^*, R_s)$ is unique. The uniqueness of the optimal R_s is not surprising since $P_{\text{st}}^*(\alpha^*, R_s)$ decreases as R_s increases. Therefore, there is absolutely an optimal R_s maximizing $T(\alpha^*, R_s)$. Substituting $T(\alpha^*, R_s) = R_s P_{\text{st}}^*(\alpha^*, R_s)$ into (27), we are able to solve the optimization problem in (27) numerically. Specifically, we numerically find the value of R_s maximizing $T(\alpha^*, R_s)$ and define it as $R_s^{*\circ}$. The value of α^* for $R_s^{*\circ}$ is chosen as $\alpha^{*\circ}$. We define the maximum EST achieved by $R_s^{*\circ}$ and $\alpha^{*\circ}$ as $T^{*\circ} \triangleq T(\alpha^{*\circ}, R_s^{*\circ})$.

IV. Adaptive Transmission

In this section, we focus on the adaptive transmission scheme and examine its secrecy performance in the MISO wiretap channel. First, we introduce the principle of the general adaptive scheme. Second, we derive closed-form expressions for the secrecy outage probability which is distinct from (14) and the secure transmission probability which is distinct from (20). Using these expressions, the EST, the probability of non-zero secrecy capacity, and the ε-outage secrecy capacity are obtained. In order to optimize the secrecy performance, we first determine the optimal power allocation ratio $\alpha^\dagger$ that minimizes the secrecy outage probability. Then we determine the joint optimal pair $\left(\alpha^{\dagger\circ}, R_s^{\dagger\circ}\right)$ that maximizes the EST.

A. Principle of Adaptive Transmission

In the general adaptive transmission scheme, Alice selects a flexible power allocation ratio α and a flexible code rate R_s for each transmission period. In this scheme, Alice sets $R_b = C_b$ and $R_s = C_b - C'_e$ and determines the values of α and R_s based on $\tilde{\gamma}_b$ and $\overline{\gamma}_e$. The range of R_s is $0 < R_s < \tilde{C}_b$, where $\tilde{C}_b = \log_2(1 + \alpha\tilde{\gamma}_b)$, and the range of α is $\left(2^{R_s} - 1\right)/\tilde{\gamma}_b < \alpha \leq 1$. We note that transmission outage occurs in the on-off transmission scheme but does not occur in the adaptive transmission scheme, since the value of R_s is chosen to be lower than C_b. As such, wiretap codes can always be constructed based on C_b and R_s and Alice always transmits. We also note that the values of α and R_s depend upon the realization of the main channel. It follows that once the main channel realization changes, the values of α and R_s change accordingly. The optimal values of α and R_s will be discussed in Section IV-C. We next define two mutually exclusive events which partition the entire event space of this scheme.

Event 1: Secrecy outage
This event occurs when $C_s < R_s$. In this case, the assumed capacity of the eavesdropper's channel is lower than the actual capacity of the eavesdropper's channel, i.e., $C'_e < C_e$. Therefore, secrecy is compromised.

Event 2: Secure transmission
This event occurs when $C_s \geq R_s$. In this case, the assumed capacity of the eavesdropper's channel is better than the actual capacity of the eavesdropper's channel, i.e., $C'_e \geq C_e$. Therefore, the code guarantees perfect secrecy.

We clarify that in the adaptive transmission scheme, Alice always transmits, which is due to two reasons. First, the wiretap codes can be constructed using C_b and R_s. Second, it is improbable that the instantaneous capacity of the main channel is zero. This fact indicates that the transmission outage probability is zero. Therefore, we examine two probabilities: i) the *secrecy outage probability* which is defined as the probability of **Event 1** and ii) the *secure transmission probability* which is defined as the probability of **Event 2**. Note that these two probabilities are conditional probabilities for a given $\tilde{\gamma}_b$.

B. Secrecy Performance of Adaptive Transmission

1) Secrecy outage probability: The secrecy outage probability is defined as

$$\begin{aligned} P_{\text{so}}\left(\alpha, R_s|\tilde{\gamma}_b\right) &= \Pr\left(C_e > C_b - R_s|\tilde{\gamma}_b\right) \\ &= \Pr\left(\log_2\left(1+\gamma_e\right) > \log_2\left(1+\gamma_b\right) - R_s|\tilde{\gamma}_b\right). \end{aligned} \quad (29)$$

Using (9), we derive the secrecy outage probability as

$$\begin{aligned} P_{\text{so}}\left(\alpha, R_s|\tilde{\gamma}_b\right) &= 1 - F_{\gamma_e}\left(2^{\log_2(1+\alpha\tilde{\gamma}_b)-R_s} - 1\right) \\ &= \left(1 + \frac{(1-\alpha)\,\zeta(\alpha)}{\alpha(N-1)}\right)^{-(N-1)} e^{-\frac{\zeta(\alpha)}{\alpha\overline{\gamma}_e}}, \end{aligned} \quad (30)$$

where $\zeta(\alpha) = 2^{-R_s}\left(1+\alpha\tilde{\gamma}_b\right) - 1$.

2) Secure transmission probability: We note that the hybrid outage probability of the adaptive transmission scheme is equal to the secrecy outage probability in (30) since the transmission outage probability is zero. Therefore, the secure transmission probability is obtained as

$$P_{\text{st}}\left(\alpha, R_s|\tilde{\gamma}_b\right) = 1 - P_{\text{so}}\left(\alpha, R_s|\tilde{\gamma}_b\right). \quad (31)$$

We highlight that (30) and (31) are valid for $\left(2^{R_s}-1\right)/\tilde{\gamma}_b < \alpha \leq 1$. Moreover, we clarify that (30) is different from [30, Eq. (8)] since [30, Eq. (8)] considered zero noise at Eve while (30) considers an arbitrary noise power at Eve.

3) Effective secrecy throughput: We now examine the EST. Utilizing (31), the EST is formulated as

$$T\left(\alpha, R_s|\tilde{\gamma}_b\right) = R_s P_{\text{st}}\left(\alpha, R_s|\tilde{\gamma}_b\right). \quad (32)$$

Since $P_{\text{st}}\left(\alpha, R_s|\tilde{\gamma}_b\right)$ is a function of α, N, $\tilde{\gamma}_b$, and $\overline{\gamma}_e$, (32) indicates that $T\left(\alpha, R_s|\tilde{\gamma}_b\right)$ is jointly determined by α and R_s for given N, $\tilde{\gamma}_b$, and $\overline{\gamma}_e$.

4) Other performance metrics: First, we derive the *probability of non-zero secrecy rate* as

$$\begin{aligned} P_{\text{nz}}\left(\alpha|\tilde{\gamma}_b\right) =& 1 - P_{\text{so}}\left(\alpha, R_s|\tilde{\gamma}_b\right)|_{R_s=0} \\ =& 1 - \left(1 + \frac{(1-\alpha)\,\tilde{\gamma}_b}{N-1}\right)^{-(N-1)} e^{-\frac{\tilde{\gamma}_b}{\overline{\gamma}_e}}. \end{aligned} \quad (33)$$

Second, we obtain the *ε-outage secrecy rate* as

$$C\left(\alpha, \varepsilon|\tilde{\gamma}_b\right) = \max_{R_s: P_{\text{so}}(\alpha, R_s|\tilde{\gamma}_b) \leq \varepsilon} R_s. \quad (34)$$

Substituting (30) into (34), the ε-outage secrecy rate can be obtained via numerical root-finding.

C. Performance Optimization of Adaptive Transmission

In this subsection, we determine the joint optimal power allocation ratio and secrecy rate pair $\left(\alpha^{\dagger\circ}, R_s^{\dagger\circ}\right)$ in order to maximize the EST of the adaptive scheme for a given $\tilde{\gamma}_b$. Such an optimization problem is formulated as

$$\left(\alpha^{\dagger\circ}, R_s^{\dagger\circ}\right) = \underset{0<R_s<C_b,\ \frac{2^{R_s}-1}{\tilde{\gamma}_b}<\alpha^\dagger\leq 1}{\operatorname{argmax}} T\left(\alpha^\dagger, R_s|\tilde{\gamma}_b\right), \quad (35)$$

where $\alpha^\dagger$ denotes the optimal power allocation ratio that minimizes the secrecy outage probability $P_{\text{so}}\left(\alpha, R_s|\tilde{\gamma}_b\right)$ in (30) (or equivalently, maximizes the secure transmission probability $P_{\text{st}}\left(\alpha, R_s|\tilde{\gamma}_b\right)$ in (31)) for given $\tilde{\gamma}_b$ and R_s.

In order to solve (35), we first find $\alpha^\dagger$ for a given R_s via

$$\alpha^\dagger = \underset{\frac{2^{R_s}-1}{\tilde{\gamma}_b}<\alpha\leq 1}{\operatorname{argmin}} P_{\text{so}}\left(\alpha, R_s|\tilde{\gamma}_b\right). \quad (36)$$

We numerically confirm the uniqueness of the optimal α that minimizes $P_{\text{so}}\left(\alpha, R_s|\tilde{\gamma}_b\right)$ by finding that $\partial^2 P_{\text{so}}\left(\alpha, R_s|\tilde{\gamma}_b\right)/\partial^2\alpha > 0$ for $\left(2^{R_s}-1\right)/\tilde{\gamma}_b < \alpha \leq 1$. Setting the first order derivative of $P_{\text{so}}\left(\alpha, R_s|\tilde{\gamma}_b\right)$ to zero and performing mathematical operations, we obtain a cubic equation given by

$$\theta_1\alpha^3 + \theta_2\alpha^2 + \theta_3\alpha + \theta_4 = 0, \quad (37)$$

where $\theta_1 = 2^{R_s}(N-1)\,\tilde{\gamma}_b\overline{\gamma}_e$, $\theta_2 = \left(2^{R_s}-1\right)\tilde{\gamma}_b$, $\theta_3 = -\left(2^{R_s}-1\right)\left[\tilde{\gamma}_b - 1 - 2^{R_s}\overline{\gamma}_e + 2^{R_s}N\left(\overline{\gamma}_e+1\right)\right]$, and $\theta_4 = \left(2^{R_s}-1\right)^2$. With the aid of the Cardano's formula [29], we find the root of (37) as

$$\alpha_i = -\frac{1}{3\theta_1}\left(\theta_2 + \tau_i\Theta + \frac{\Delta_0}{\tau_i\Theta}\right), \quad (38)$$

where $i \in \{1,2,3\}$, τ_i are the three cube roots of unity given by $\tau_1 = 1$, $\tau_2 = \frac{1}{2}\left(-1+\sqrt{-3}\right)$, and $\tau_3 = \frac{1}{2}\left(-1-\sqrt{-3}\right)$, and Θ is given by

$$\Theta = \left(\frac{1}{2}\left(\Delta_1 + \sqrt{\Delta_1^2 - 4\Delta_0^3}\right)\right)^{\frac{1}{3}}, \quad (39)$$

with $\Delta_0 = \theta_2^2 - 3\theta_1\theta_3$ and $\Delta_1 = 2\theta_2^3 - 9\theta_1\theta_2\theta_3 + 27\theta_1^2\theta_4$. In order to compute $\alpha^\dagger$ in the desired range $(\frac{2^{R_s}-1}{\tilde{\gamma}_b}, 1]$ that minimizes $P_{\text{so}}\left(\alpha, R_s|\tilde{\gamma}_b\right)$, we compare the values of the cost function $P_{\text{so}}\left(\alpha, R_s|\tilde{\gamma}_b\right)$ at the extreme point[3] $\alpha = 1$ and at $\alpha = \alpha_i$ for $i \in \{1,2,3\}$ if $\alpha_i \in (\frac{2^{R_s}-1}{\tilde{\gamma}_b}, 1]$. The value of α that achieves the minimum $P_{\text{so}}\left(\alpha, R_s|\tilde{\gamma}_b\right)$ is chosen as $\alpha^\dagger$. Accordingly, we define the optimal secrecy outage probability and the optimal secure transmission probability with $\alpha^\dagger$ for given $\tilde{\gamma}_b$ and R_s as $P_{\text{so}}^\dagger\left(\alpha^\dagger, R_s|\tilde{\gamma}_b\right)$ and $P_{\text{st}}^\dagger\left(\alpha^\dagger, R_s|\tilde{\gamma}_b\right)$, respectively. We further define the EST achieved by $\alpha^\dagger$ as $T\left(\alpha^\dagger, R_s|\tilde{\gamma}_b\right) = R_s P_{\text{st}}^\dagger\left(\alpha^\dagger, R_s|\tilde{\gamma}_b\right)$.

We confirm that the optimal value of α maximizing $T\left(\alpha^\dagger, R_s|\tilde{\gamma}_b\right)$ is unique, based on the definition of $T\left(\alpha^\dagger, R_s|\tilde{\gamma}_b\right)$. We then confirm that the optimal value of R_s maximizing $T\left(\alpha^\dagger, R_s|\tilde{\gamma}_b\right)$ is unique by finding that $\partial T\left(\alpha^\dagger, R_s|\tilde{\gamma}_b\right)/\partial R_s$ is first positive then negative as R_s increases. After obtaining $T\left(\alpha^\dagger, R_s|\tilde{\gamma}_b\right)$, we can numerically find the value of R_s maximizing $T^\dagger\left(\alpha^\dagger, R_s|\tilde{\gamma}_b\right)$, which is defined as $R_s^{\dagger\circ}$. Accordingly, the value of $\alpha^\dagger$ for $R_s^{\dagger\circ}$ is chosen as $\alpha^{\dagger\circ}$. The maximum EST achieved by $R_s^{\dagger\circ}$ and $\alpha^{\dagger\circ}$ is defined as $T^{\dagger\circ}\left(\tilde{\gamma}_b\right) \triangleq T\left(\alpha^{\dagger\circ}, R_s^{\dagger\circ}|\tilde{\gamma}_b\right)$. Finally, we obtain the maximum average EST of the adaptive transmission scheme as

$$T^{\dagger\circ} = \mathbb{E}_{\tilde{\gamma}_b}\left[T^{\dagger\circ}\left(\tilde{\gamma}_b\right)\right], \quad (40)$$

which takes expectation of $T^{\dagger\circ}\left(\tilde{\gamma}_b\right)$ over $\tilde{\gamma}_b$.

[3]Here, we do not examine $\alpha = \frac{2^{R_s}-1}{\tilde{\gamma}_b}$. This is due to the fact that when $\alpha = \frac{2^{R_s}-1}{\tilde{\gamma}_b}$, we find that $C_b = R_s$ and thus $P_{\text{so}}\left(\alpha, R_s|\tilde{\gamma}_b\right) = \Pr\left(C_e > 0|\tilde{\gamma}_b\right) = 1$.

V. NUMERICAL RESULTS

In this section, we present numerical results to examine the impact of the number of transmit antennas, N, and the SNRs of the main channel and the eavesdropper's channel on the secrecy performance. We also compare the performance of the AN transmission schemes with the following schemes: 1) the transmit BF schemes [15] where maximal ratio transmission [34] is adopted at Alice and 2) the NAE and AE schemes [30].

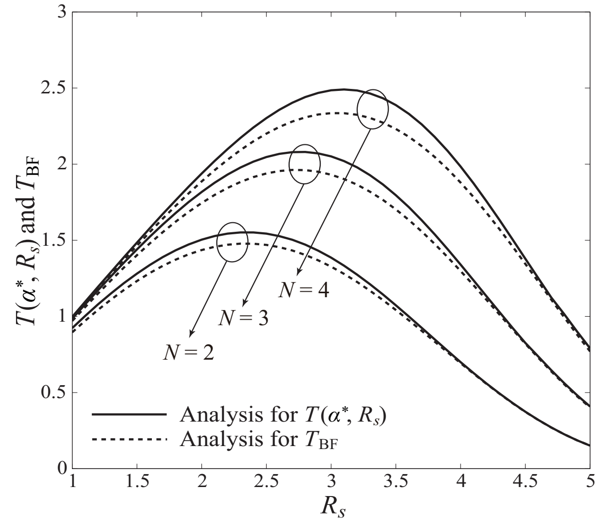
A. On-Off Transmission

In this subsection, we examine the performance of the on-off AN transmission scheme. We first examine the impact of N, $\overline{\gamma}_b$, and $\overline{\gamma}_e$ on the EST of the on-off transmission scheme. In Figs. 2(a), 2(b), and 2(c), we compare the EST achieved by the on-off AN transmission scheme with α^* to that achieved by the on-off transmit BF scheme versus R_s. In these figures, the EST achieved by the on-off transmit BF scheme is obtained as $T_{\text{BF}} = R_s P_{\text{s}}^{(2)}(R_s)$. We find from these figures that the maximum EST achieved by the on-off AN transmission scheme with α^* is higher than that achieved by the on-off transmit BF scheme.

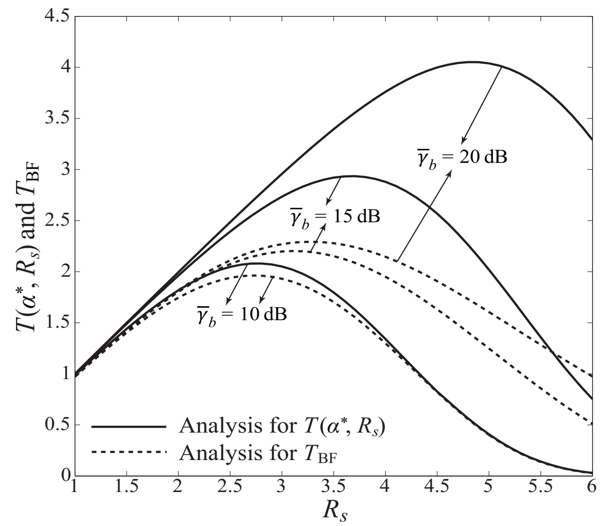
1) Impact of N and $\overline{\gamma}_b$: We first examine the impact of the network parameters that can be controlled at Alice, namely N and $\overline{\gamma}_b$, on the EST. Fig. 2(a) examines the impact of N and Fig. 2(b) examines the impact of $\overline{\gamma}_b$. In these figures, we first see that the EST increases when N or $\overline{\gamma}_b$ increases. We also see that the value of $R_s^{*\circ}$ that maximizes the EST shifts to the right when N or $\overline{\gamma}_b$ increases. This reveals that Alice is able to use a higher secure transmission rate if she possesses a larger number of antennas or she uses a higher transmit power. We further confirm that the value of $\alpha^{*\circ}$ that maximizes the EST decreases when N or $\overline{\gamma}_b$ increases. For example, $\alpha^{*\circ}$ decreases from 0.79 to 0.72 when N increases from 2 to 4, and $\alpha^{*\circ}$ decreases from 0.75 to 0.47 when $\overline{\gamma}_b$ increases from 10 dB to 20 dB. This reveals that Alice allocates more power to the AN signal to achieve the maximum EST for larger N and higher $\overline{\gamma}_b$ in the on-off transmission scheme.

2) Impact of $\overline{\gamma}_e$: Fig. 2(c) examines the impact of the network parameter that cannot be controlled at Alice, $\overline{\gamma}_e$, on the EST. In this figure, we consider a fixed $\overline{\gamma}_b = 20$ dB such that $\overline{\gamma}_e$ increases when $\overline{\gamma}_b/\overline{\gamma}_e$ decreases. We first see that the EST decreases when $\overline{\gamma}_e$ increases. We also see that $R_s^{*\circ}$ shifts to the left when $\overline{\gamma}_e$ increases. This reveals that Alice can only use a lower secure transmission rate if the quality of the eavesdropper's channel becomes higher. Furthermore, it is confirmed that the value of $\alpha^{*\circ}$ that maximizes the EST decreases when $\overline{\gamma}_e$ increases. For example, $\alpha^{*\circ}$ decreases from 0.54 to 0.47 when $\overline{\gamma}_e$ increases from $\overline{\gamma}_b/15$ to $\overline{\gamma}_b/5$. This reveals that Alice allocates more power to the AN signal to achieve the maximum EST for higher $\overline{\gamma}_e$ in the on-off transmission scheme.

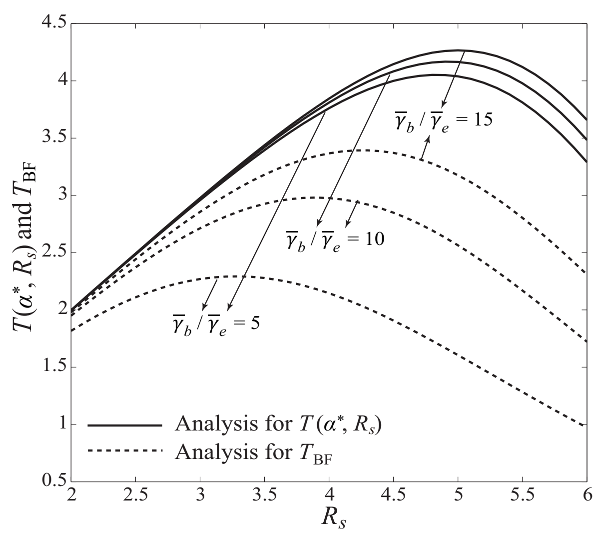
We now compare the maximum EST of the on-off transmission scheme, $T^{*\circ}$, with the EST of the NAE scheme, T^*_{NAE}, versus $\overline{\gamma}_b$ in Fig. 3. Here, we define T^*_{NAE} as $T^*_{\text{NAE}} = (1-\epsilon)\eta^*_{\text{NAE}}$, where η^*_{NAE} is the maximum throughput given by [30, Eq. (18)] and ϵ is the conditional secrecy outage probability. Here, we consider $\epsilon = 0.1$ and $\epsilon = 0.01$. We observe that



(a) EST comparison for $\overline{\gamma}_b = 10$ dB, $\overline{\gamma}_b/\overline{\gamma}_e = 5$, and different values of N.



(b) EST comparison for $N = 3$, $\overline{\gamma}_b/\overline{\gamma}_e = 5$, and different values of $\overline{\gamma}_b$.



(c) EST comparison for $N = 3$, $\overline{\gamma}_b = 20$ dB, and different values of $\overline{\gamma}_b/\overline{\gamma}_e$.

Fig. 2. EST comparison of the on-off transmission scheme: Artificial noise with α^* versus BF.

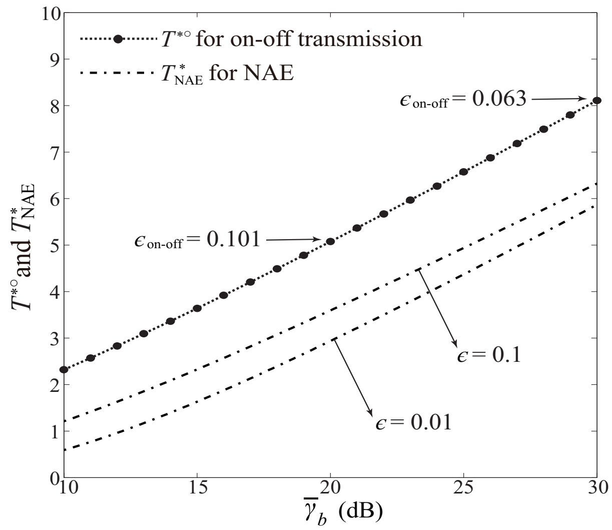


Fig. 3. Maximum EST comparison between the on-off transmission scheme and the NAE scheme for $N = 4$ and $\overline{\gamma}_e = 5$ dB.

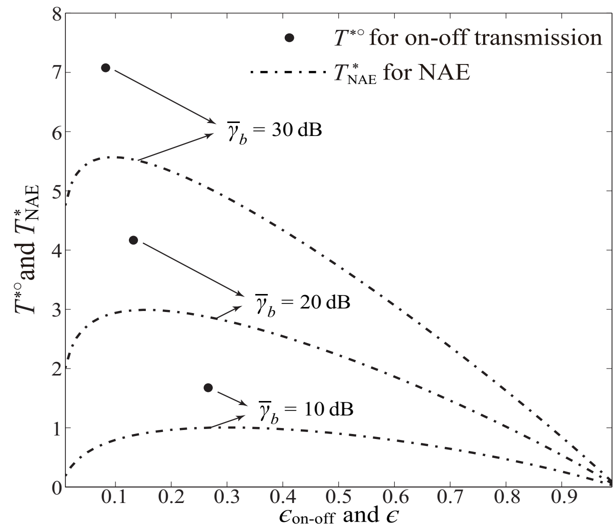


Fig. 4. Maximum EST comparison between the on-off transmission scheme and the NAE scheme for $N = 3$ and $\overline{\gamma}_e = 10$ dB.

the on-off transmission scheme provides a higher EST than the NAE scheme across the whole range of $\overline{\gamma}_b$. In particular, the EST advantage of the on-off transmission scheme over the NAE scheme becomes higher when ϵ becomes lower. For the sake of a fair comparison, we examine the conditional secrecy outage probability of the on-off transmission scheme when the maximum EST is achieved, which is defined as

$$\epsilon_{\text{on-off}} \triangleq P_{\text{so}}\left(\alpha^{*\circ}, R_s^{*\circ} | C_b \geq R_s^{*\circ}\right) = \frac{P_{\text{so}}\left(\alpha^{*\circ}, R_s^{*\circ}\right)}{P_{\text{t}}\left(\alpha^{*\circ}, R_s^{*\circ}\right)}. \quad (41)$$

We find that $\epsilon_{\text{on-off}}$ decreases when $\overline{\gamma}_b$ increases. For example, we find that $\epsilon_{\text{on-off}} = 0.101$ when $\overline{\gamma}_b = 20$ dB and $\epsilon_{\text{on-off}} = 0.063$ when $\overline{\gamma}_b = 30$ dB. This fact implies that the on-off transmission scheme offers a higher EST, while incurring a lower conditional secrecy outage probability than the NAE scheme with $\epsilon = 0.1$ in the high SNR regime, e.g., $\overline{\gamma}_b > 20$ dB. In the low SNR regime, the on-off transmission scheme offers a higher EST at the cost of incurring a higher conditional secrecy outage probability than the NAE scheme. As such, the on-off transmission scheme trades off the secrecy outage with a higher EST.

We now plot $T^{*\circ}$ versus $\epsilon_{\text{on-off}}$ and plot T^{*}_{NAE} versus ϵ in Fig. 4. In this figure, we clarify that $T^{*\circ}$ and $\epsilon_{\text{on-off}}$ do not change for given N, $\overline{\gamma}_b$, and $\overline{\gamma}_e$. We first see that $T^{*\circ}$ is higher than T^{*}_{NAE} achieved at $\epsilon = \epsilon_{\text{on-off}}$. For example, when $\overline{\gamma}_b = 20$ dB, we find that $T^{*\circ} - T^{*}_{\mathrm{NAE}} = 1.19$ bps/Hz at $\epsilon = \epsilon_{\text{on-off}} = 0.132$. Second, we see that there exists a unique ϵ that maximizes T^{*}_{NAE}, which is denoted as $\epsilon^{*}_{\mathrm{NAE}}$. We find that $T^{*\circ}$ is higher than the maximum T^{*}_{NAE}. Notably, we also see that $\epsilon_{\text{on-off}}$ is slightly smaller than $\epsilon^{*}_{\mathrm{NAE}}$. For example, we find that $\epsilon_{\text{on-off}} = 0.132$ and $\epsilon^{*}_{\mathrm{NAE}} = 0.154$ when $\overline{\gamma}_b = 20$ dB. This fact demonstrates that the on-off transmission scheme provides a higher EST while maintaining a lower conditional secrecy outage probability than the NAE scheme. Therefore, the on-off transmission scheme is more promising than the NAE scheme for practical applications from the EST perspective.

TABLE I
THE VALUES OF $\alpha^{\dagger\circ}$ AND $R_s^{\dagger\circ}$ FOR $T^{\dagger\circ}(\tilde{\gamma}_b)$ WHEN $N = 3$

	$\overline{\gamma}_e = 5$ dB		$\overline{\gamma}_e = 10$ dB	
$\tilde{\gamma}_b$ (dB)	$\alpha^{\dagger\circ}$	$R_s^{\dagger\circ}$	$\alpha^{\dagger\circ}$	$R_s^{\dagger\circ}$
0	0.608	0.35	0.516	0.31
5	0.583	0.83	0.489	0.74
10	0.564	1.68	0.465	1.52
15	0.548	2.86	0.442	2.63
20	0.531	4.24	0.421	3.96

B. Adaptive Transmission

In this subsection, we examine the performance of the adaptive AN transmission scheme. In Fig. 5, we compare the maximum EST achieved by the adaptive AN transmission scheme to that achieved by the adaptive transmit BF scheme versus $\tilde{\gamma}_b$. In this figure, the maximum EST achieved by the adaptive transmit BF scheme is obtained as $T^{\dagger\circ}_{\mathrm{BF}} = \max_{R_s} T_{\mathrm{BF}}\left(R_s|\tilde{\gamma}_b\right)$, where $T_{\mathrm{BF}}\left(R_s|\tilde{\gamma}_b\right)$ denotes the EST achieved by the adaptive transmit BF scheme, given by

$$T_{\mathrm{BF}}\left(R_s|\tilde{\gamma}_b\right) = R_s\left(1 - e^{-\frac{2^{-R_s}(1+\tilde{\gamma}_b)-1}{\overline{\gamma}_e}}\right). \quad (42)$$

We see that the maximum EST increases when $\tilde{\gamma}_b$ increases but decreases when $\overline{\gamma}_e$ increases. We also see that the maximum EST achieved by the adaptive AN transmission scheme is higher than that achieved by the adaptive transmit BF scheme. Notably, the maximum EST advantage of AN over BF increases with $\tilde{\gamma}_b$ for a given $\overline{\gamma}_e$. Furthermore, the maximum EST advantage of AN over BF increases with $\overline{\gamma}_e$ for a given $\tilde{\gamma}_b$. These observations indicate that the adaptive AN transmission scheme brings a more profound throughput gain relative to the adaptive transmit BF scheme when either $\tilde{\gamma}_b$ or $\overline{\gamma}_e$ increases.

We next examine the impact of $\tilde{\gamma}_b$ and $\overline{\gamma}_e$ on the values of $\alpha^{\dagger\circ}$ and $R_s^{\dagger\circ}$ to offer practical insights into system design. Table I lists the values of $\alpha^{\dagger\circ}$ and $R_s^{\dagger\circ}$ that achieve $T^{\dagger\circ}(\tilde{\gamma}_b)$.

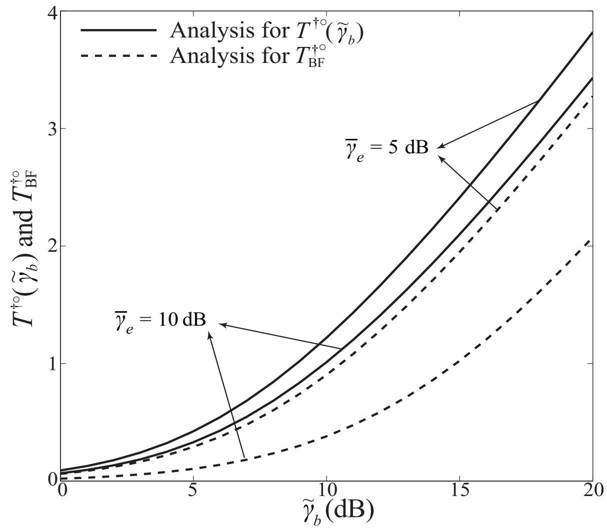


Fig. 5. Maximum EST comparison of the adaptive transmission scheme: Artificial noise with $\alpha^{\dagger\circ}$ and $R_s^{\dagger\circ}$ versus BF for $N = 3$.

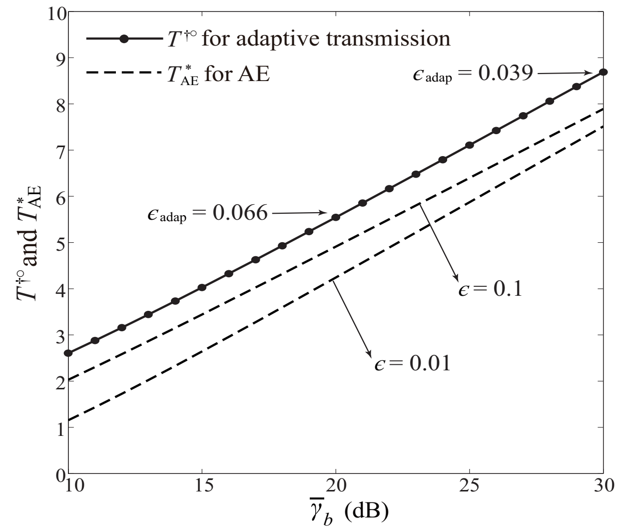


Fig. 6. Maximum average EST comparison between the adaptive transmission scheme and the AE scheme for $N = 4$ and $\overline{\gamma}_e = 5$ dB.

In this table we see that the value of $\alpha^{\dagger\circ}$ decreases as $\tilde{\gamma}_b$ increases, which indicates that Alice allocates more power to the AN signal to achieve the maximum EST for higher $\tilde{\gamma}_b$ in the adaptive transmission scheme. This observation is due to the fact that when the quality of the main channel becomes higher, e.g., Bob is located closer to Alice, Alice does not need as much power to transmit information signals. As such, Alice allocates more power to AN signals so as to confuse Eve. Intuitively, allocating more power to AN signals decreases the SINR at Eve, and thus potentially improves the EST. We also see that the value of $\alpha^{\dagger\circ}$ decreases as $\overline{\gamma}_e$ increases, which indicates that Alice allocates more power to the AN signal to achieve the maximum EST for higher $\overline{\gamma}_e$ in the adaptive transmission scheme. This observation is due to the fact that when the quality of the eavesdropper's channel becomes higher, e.g., Eve is located closer to Alice, Alice needs to use a larger amount of power to confuse Eve. We further see that the value of $R_s^{\dagger\circ}$ increases as $\tilde{\gamma}_b$ increases. Additionally, we see that the value of $R_s^{\dagger\circ}$ decreases as $\overline{\gamma}_e$ increases. These observations indicate that Alice supports a larger optimal secrecy rate for higher $\tilde{\gamma}_b$ but a smaller optimal secrecy rate for higher $\overline{\gamma}_e$ in the adaptive transmission scheme.

We now compare the maximum average EST of the adaptive transmission scheme, $T^{\dagger\circ}$, with the average EST of the AE scheme, T_{AE}^{*}, versus $\overline{\gamma}_b$ in Fig. 6. Here, T_{AE}^{*} is defined as $T_{\mathrm{AE}}^{*} = (1-\epsilon)\eta_{\mathrm{AE}}^{*}$, where η_{AE}^{*} is the maximum average throughput given by [30, Eq. (33)]. Two values of ϵ are considered in this figure, namely $\epsilon = 0.1$ and $\epsilon = 0.01$. It is evident that the adaptive transmission scheme offers a higher average EST than the AE scheme, regardless of the value of ϵ. For a smaller ϵ, a larger EST advantage of the adaptive transmission scheme over the AE scheme is achieved. Similar to Fig. 3, we examine the secrecy outage probability of the adaptive transmission scheme associated with the maximum average EST, defined as $\epsilon_{\mathrm{adap}} \triangleq \mathbb{E}_{\tilde{\gamma}_b}\left[P_{\mathrm{so}}\left(\alpha^{\dagger\circ}, R_s^{\dagger\circ}|\tilde{\gamma}_b\right)\right]$. It is found that ϵ_{adap} decreases as $\overline{\gamma}_b$ increases. For example, we find that $\epsilon_{\mathrm{adap}} = 0.066$ when $\overline{\gamma}_b = 20$ dB and $\epsilon_{\mathrm{adap}} = 0.039$ when $\overline{\gamma}_b = 30$ dB. Compared to the AE scheme with $\epsilon = 0.01$, the adaptive transmission scheme trades off the secrecy outage with a higher EST.

In Fig. 7, we plot $T^{\dagger\circ}$ versus ϵ_{adap} and plot T_{AE}^{*} versus ϵ. We first see that $T^{\dagger\circ}$ is higher than T_{AE}^{*} at $\epsilon = \epsilon_{\mathrm{adap}}$. We also see that $T^{\dagger\circ}$ is higher than the maximum T_{AE}^{*}. We further see that ϵ_{adap} is slightly smaller than $\epsilon_{\mathrm{AE}}^{*}$. These two observations indicate that the adaptive transmission scheme offers a higher EST while incurring a lower conditional secrecy outage probability than the AE scheme. As such, the adaptive transmission scheme is more suitable to be applied than the AE scheme if the EST maximization is the design target.

C. On-Off Transmission versus Adaptive Transmission

We finally compare the throughput performance between the on-off transmission scheme and the adaptive transmission scheme. In Fig. 8, we plot the maximum EST of the on-off transmission scheme and the maximum average EST of the adaptive transmission scheme versus $\overline{\gamma}_b$. We see that the adaptive transmission scheme achieves a higher EST than the on-off transmission scheme. This observation is due to the fact that the adaptive transmission scheme optimizes α and R_s during each transmission period while the on-off transmission scheme optimizes α and R_s only once and uses the optimized α and R_s for all the transmission periods. Of course, we note that the EST advantage of the adaptive transmission scheme over the on-off transmission scheme is not pronounced. Moreover, we see that $T^{*\circ}$ and $T^{\dagger\circ}$ increase as $\overline{\gamma}_b$ increases and N increases. Furthermore, we see that $T^{*\circ}$ and $T^{\dagger\circ}$ decrease as $\overline{\gamma}_e$ increases. These observations are consistent with the expectation.

VI. Conclusions

We proposed two transmission schemes using AN that maximize the EST in MISO wiretap channels with a passive

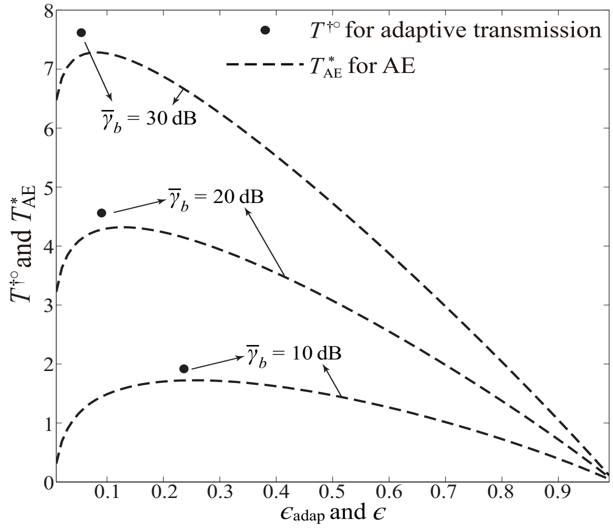


Fig. 7. Maximum average EST comparison between the adaptive transmission scheme and the AE scheme for $N = 3$ and $\overline{\gamma}_e = 10$ dB.

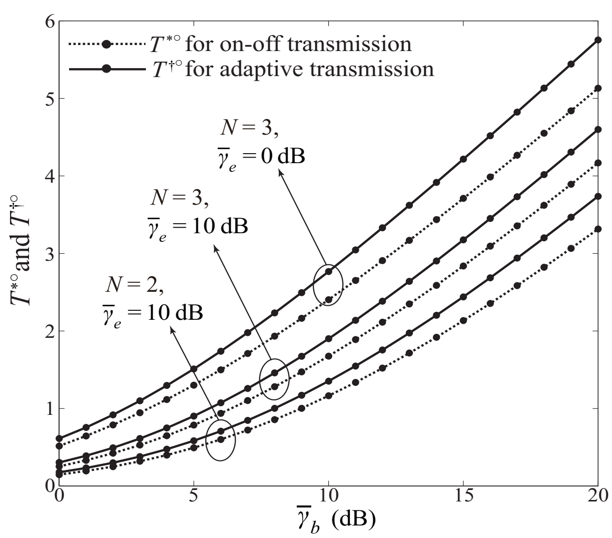


Fig. 8. Maximum EST comparison: On-off transmission $T^{*\circ}(R_s^{*\circ})$ versus adaptive transmission $T^{\dagger\circ}(R_s^{\dagger\circ})$.

eavesdropper. For the on-off transmission scheme, the optimal solutions were constructed based on our easy-to-compute and channel-independent expression for the hybrid outage probability. For the adaptive transmission scheme, the optimal solutions were constructed based on our new closed-form expression for the secrecy outage probability. Based on these expressions, we determined the joint optimal power allocation ratio and secrecy rate in order to achieve the maximum EST. Numerical results were presented to characterize the impact of N and SNRs on the secrecy performance, the optimal power allocation, and the optimal secrecy rate.

Appendix A
Proof of Theorem 1

Based on the properties of the statistics of γ_b and γ_e, we first express (13) as

$$\begin{aligned} P_{\text{so}}(\alpha, R_s) &= \int_0^\infty \int_{2^{R_s}-1}^{2^{R_s}(1+\gamma_e)-1} f_{\gamma_b}(\gamma_b) f_{\gamma_e}(\gamma_e)\, d\gamma_b d\gamma_e \\ &= \underbrace{\int_0^\infty f_{\gamma_e}(\gamma_e) F_{\gamma_b}\left(2^{R_s}(1+\gamma_e)-1\right) d\gamma_e}_{\ell_1} \\ &\quad - \underbrace{\int_0^\infty f_{\gamma_e}(\gamma_e) F_{\gamma_b}\left(2^{R_s}-1\right) d\gamma_e}_{\ell_2}. \end{aligned} \tag{43}$$

Differentiating $F_{\gamma_e}(\gamma)$ with respect to γ, we obtain the probability density function of γ_e, $f_{\gamma_e}(\gamma)$. Substituting $f_{\gamma_e}(\gamma)$ and (8) into (43), we derive ℓ_1 as

$$\begin{aligned} \ell_1 =& 1 - e^{-\frac{2^{R_S}-1}{\alpha\overline{\gamma}_b}} \sum_{n=0}^{N-1} \frac{\left(2^{R_S}-1\right)^n}{n!\left(\alpha\overline{\gamma}_b\right)^n} \sum_{m=0}^{n} \binom{n}{m} \left(\frac{2^{R_S}}{2^{R_S}-1}\right)^m \\ &\times \left(\frac{1}{\alpha\overline{\gamma}_e}\hbar_1 + \frac{1-\alpha}{\alpha}\hbar_2\right), \end{aligned} \tag{44}$$

where

$$\hbar_1 = \int_0^\infty e^{-\left(\frac{2^{R_S}}{\overline{\gamma}_b}+\frac{1}{\overline{\gamma}_e}\right)\frac{\gamma_e}{\alpha}} \gamma_e^m \left(1+\frac{(1-\alpha)\gamma_e}{\alpha(N-1)}\right)^{-(N-1)} d\gamma_e \tag{45}$$

and

$$\hbar_2 = \int_0^\infty e^{-\left(\frac{2^{R_S}}{\overline{\gamma}_b}+\frac{1}{\overline{\gamma}_e}\right)\frac{\gamma_e}{\alpha}} \gamma_e^m \left(1+\frac{(1-\alpha)\gamma_e}{\alpha(N-1)}\right)^{-N} d\gamma_e. \tag{46}$$

When $0 < \alpha < 1$, we use [35, Eq. (9.211.4)] to solve the integrals $\hbar_1$ and $\hbar_2$ in closed form. Specifically, we change the variable $t = \frac{(1-\alpha)\gamma_e}{\alpha(N-1)}$ in $\hbar_1$ and derive it as

$$\begin{aligned} \hbar_1 &= \kappa^{m+1} \int_0^\infty e^{-\lambda t} \frac{t^m}{(1+t)^{N-1}} dt \\ &= \kappa^{m+1} \Gamma(m+1)\, \mathbb{U}(m+1, -N+m+3, \lambda). \end{aligned} \tag{47}$$

where κ and λ are defined in (15). We then derive $\hbar_2$ as

$$\begin{aligned} \hbar_2 &= \kappa^{m+1} \int_0^\infty e^{-\lambda t} \frac{t^m}{(1+t)^{N}} dt \\ &= \kappa^{m+1} \Gamma(m+1)\, \mathbb{U}(m+1, -N+m+2, \lambda). \end{aligned} \tag{48}$$

When $\alpha = 1$, we simplify $\hbar_1$ and $\hbar_2$ as $\hbar_1 = \hbar_2 = \hbar_3$ and derive $\hbar_3$ using [35, Eq. (3.381.4)] as

$$\begin{aligned} \hbar_3 &= \int_0^\infty e^{-\left(\frac{2^{R_S}}{\overline{\gamma}_b}+\frac{1}{\overline{\gamma}_e}\right)\gamma_e} \gamma_e^m d\gamma_e \\ &= \Gamma(m+1)\left(\frac{2^{R_S}}{\overline{\gamma}_b}+\frac{1}{\overline{\gamma}_e}\right)^{-(m+1)}. \end{aligned} \tag{49}$$

We further derive ℓ_2 in (43) as

$$\begin{aligned} \ell_2 &= 1 - F_{\gamma_b}\left(2^{R_s}-1\right) \\ &= 1 - e^{-\frac{2^{R_s}-1}{\alpha\overline{\gamma}_b}} \sum_{n=0}^{N-1} \frac{1}{n!} \left(\frac{2^{R_s}-1}{\alpha\overline{\gamma}_b}\right)^n. \end{aligned} \tag{50}$$

Therefore, the secrecy outage probability for $0 < \alpha < 1$ in (15) is obtained by substituting $\hbar_1$, $\hbar_2$, and ℓ_2 into (43). Moreover, the secrecy outage probability for $\alpha = 1$ in (16) is obtained by substituting $\hbar_3$ and ℓ_2 into (43). This completes the proof.

References

[1] R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. R. Bloch, S. Ulukus, and A. Yener, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Commun. Mag.*, vol. 30, no. 5, pp. 16–28, Aug. 2013.

[2] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Commun. Mag.*, vol. 30, no. 5, pp. 29–40, Aug. 2013.

[3] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

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

[5] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[6] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–2492, Jun. 2008.

[7] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[8] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[9] M. Z. I. Sarkar, T. Ratnarajah, and M. Sellathurai, "Secrecy capacity of Nakagami-m fading wireless channels in the presence of multiple eavesdroppers," in *Proc. ACSSC 2009*, Pacific Grove, CA, Nov. 2009, pp. 829–833.

[10] T. Liu and S. Shamai (Shitz), "A note on the secrecy capacity of the multiple-antenna wiretap channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[11] 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.

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

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

[14] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[15] S. Bashar, Z. Ding, and G. Y. Li, "On secrecy of codebook-based transmission beamforming under receiver limited feedback," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1212–1223, Apr. 2011.

[16] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 372–375, Jun. 2012.

[17] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, no. 1, pp. 144–154, Jan. 2013.

[18] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical layer security of TAS/MRC with antenna correlation," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 1, pp. 254–259, Jan. 2013.

[19] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and J. Yuan, "MIMO wiretap channels: A secure transmission using transmit antenna selection and receive generalized selection combining," *IEEE Commun. Lett.*, vol. 17, no. 9, pp. 1754–1757, Sep. 2013.

[20] S. Yan, N. Yang, R. Malaney, and J. Yuan, "Transmit antenna selection with Alamouti coding and power allocation in MIMO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1656–1667, Mar. 2014.

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

[22] 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.

[23] 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. 2011.

[24] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704–2717, May 2013.

[25] P.-H. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE J. Select. Areas Commun.*, vol. 31, no. 9, pp. 1728–1740, Sept. 2013.

[26] Y. Zhu, Y. Zhou, S. Patel, X. Chen, L. Pang, and Z. Xue, "Artificial noise generated in MIMO scenario: Optimal power design," *IEEE Signal Process. Lett.*, vol. 20, no. 10, pp. 964–967, Oct. 2013.

[27] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy outage in MISO systems with partial channel information," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 704–716, Apr. 2012.

[28] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Process. Lett.*, vol. 19, no. 2, pp. 71–74, Feb. 2012.

[29] J. Xiong, K.-K. Wong, D. Ma, and J. Wei, "A closed-form power allocation for minimizing secrecy outage probability for MISO wiretap channels via masked beamforming," *IEEE Commun. Lett.*, vol. 16, no. 9, pp. 1496–1499, Sept. 2012.

[30] 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.

[31] N. Yang, J. Yuan, R. Malaney, R. Subramanian, and I. Land, "Artificial noise with optimal power allocation in multi-input single-output wiretap channels," in *Proc. IEEE ICC 2014*, Sydney, Australia, June 2014, pp. 2184–2190.

[32] Y. Abdallah, M. A. Latif, M. Youssef, A. Sultan, and H. El Gamal, "Keys through ARQ: Theory and practice," *IEEE Trans. Inf. Forensics Security.* vol. 6, no. 3, pp. 737–751, Sept. 2011.

[33] S. Yan, G. Geraci, N. Yang, R. Malaney, and J. Yuan, "On the target secrecy rate for SISOME wiretap channels," in *Proc. IEEE ICC 2014*, Sydney, Australia, Jun. 2014, pp. 987–992.

[34] T. K. Y. Lo, "Maximum ratio transmission," *IEEE Trans. Commun.*, vol. 47, no. 10, pp. 1458–1461, Oct. 1999.

[35] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, 7th ed., Academic, San Diego, C.A., 2007.

[36] V. U. Prabhu and M. R. D. Rodrigues, "On wireless channels with M-antenna eavesdroppers: Characterization of the outage probability and ε-outage secrecy capacity," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 853–860, Sep. 2011.

Nan Yang (S'09–M'11) received the B.S. degree in electronics from China Agricultural University in 2005, and the M.S. and Ph.D. degrees in electronic engineering from the Beijing Institute of Technology in 2007 and 2011, respectively. He is currently a Future Engineering Research Leadership Fellow and Lecturer in the Research School of Engineering at the Australian National University. Prior to this he was a Postdoctoral Research Fellow at the University of New South Wales (2012–2014) and a Postdoctoral Research Fellow at the Commonwealth Scientific and Industrial Research Organization (2010–2012). He received the IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award in 2014, the Exemplary Reviewer Certificate of the IEEE Wireless Communications Letters in 2014, the Exemplary Reviewer Certificate of the IEEE Communications Letters in 2012 and 2013, and the Best Paper Award at the IEEE 77th Vehicular Technology Conference in 2013. He serves as an editor of the TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGIES. His general research interests lie in the areas of communications theory and signal processing, with specific interests in collaborative networks, network security, massive multi-antenna systems, millimeter wave communications, and molecular communications.

Shihao Yan (S'11) received the B.S. in Communication Engineering and the M.S. in Communication and Information Systems from Shandong University, Jinan, China, in 2009 and 2012, respectively. He is currently a Ph.D. student in the School of Electrical Engineering and Telecommunications, The University of New South Wales, Sydney, NSW, Australia. He is supported by The University of New South Wales and China Scholarship Council. His current research interests are in the areas of wireless communications and signal processing, including physical-layer security, location security and location verification algorithms.

Jinhong Yuan (M'02–SM'11) received the B.E. and Ph.D. degrees in electronics engineering from the Beijing Institute of Technology, Beijing, China, in 1991 and 1997, respectively. From 1997 to 1999, he was a Research Fellow with the School of Electrical Engineering, University of Sydney, Sydney, Australia. In 2000, he joined the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, Australia, where he is currently a Telecommunications Professor with the School. He has published two books, three book chapters, over 200 papers in telecommunications journals and conference proceedings, and 40 industrial reports. He is a co-inventor of one patent on MIMO systems and two patents on low-density-parity-check codes. He has co-authored three Best Paper Awards and one Best Poster Award, including the Best Paper Award from the IEEE Wireless Communications and Networking Conference, Cancun, Mexico, in 2011, and the Best Paper Award from the IEEE International Symposium on Wireless Communications Systems, Trondheim, Norway, in 2007. He is currently serving as an Associate Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS. He serves as the IEEE NSW Chair of Joint Communications/Signal Processions/Ocean Engineering Chapter. His current research interests include error control coding and information theory, communication theory, and wireless communications.

Robert Malaney (M'03) is currently an Associate Professor in the School of Electrical Engineering and Telecommunications at the University of New South Wales, Australia. He holds a Bachelor of Science in Physics from the University of Glasgow, and a PhD in Physics from the University of St. Andrews, Scotland. He has over 150 publications. He has previously held research positions at Caltech, UC Berkeley – National Labs, and the University of Toronto. He is a former Principal Research Scientist at the Commonwealth Scientific and Industrial Research Organization (CSIRO).

Ramanan Subramanian (S'03–M'09) obtained his M.S. and Ph.D. in Electrical Engineering from Georgia Institute of Technology, Atlanta, GA, USA in 2006 and 2009, respectively. Since 2009, he has been a Research Fellow at the Institute for Telecommunications Research (ITR), University of South Australia. His research interests include information theory and stochastic modeling applied to cooperative and multi-user communication, and physical-layer security.

Ingmar Land (M'00–SM'12) is Principal Researcher at the Mathematical and Algorithmic Sciences Lab, French Research Center, Huawei Technologies Co. Ltd., Paris. Before joining Huawei, he held positions as Senior Research Fellow and Research Fellow at the Institute for Telecommunications Research, University of South Australia, Adelaide, 2007-2014, and as Assistant Professor at Aalborg University, Denmark, 2005-2006. Dr. Land received his Dr.-Ing. degree in 2004 from the University of Kiel, Germany, and studied for his Dipl.-Ing. degree at the University of Ulm and the University of Erlangen-Nürnberg, Germany. His research interests are coding and information theory in the areas of cooperative communications, multiuser communications, physical-layer security, distributed source coding and distributed storage.