Optimal Transmission with Artificial Noise in MISOME Wiretap Channels

Nan Yang, *Member, IEEE,* Maged Elkashlan, *Member, IEEE,* Trung Q. Duong, *Senior Member, IEEE,*
Jinhong Yuan, *Senior Member, IEEE,* and Robert Malaney, *Member, IEEE*

***Abstract*—We investigate the optimal physical layer secure transmission with artificial noise in the wiretap channel with N antennas at the transmitter, a single antenna at the receiver, and M antennas at the eavesdropper. We analyze the performance and determine the optimal transmission parameters for two distinct schemes: (1) an on-off transmission scheme and (2) an adaptive transmission scheme. For the on-off transmission scheme where a channel-realization-independent secrecy rate is used for all transmission periods, we derive closed-form expressions for the secure transmission probability, the hybrid outage probability, and the effective secrecy throughput. For the adaptive transmission scheme where a channel-realization-dependent secrecy rate is used for each transmission period, we derive closed-form expressions for the secure transmission probability, the secrecy outage probability, and the effective secrecy throughput. Using these closed-form expressions, we determine the optimal power allocation between information signals and artificial noise signals for both schemes in order to maximize the secure transmission probability. We also determine the optimal secrecy rate for both schemes in order to maximize the effective secrecy throughput. We explicitly examine the impact of N and M on the optimal power allocation and the optimal secrecy rate. Finally, we demonstrate the performance gain of the adaptive transmission scheme over the on-off transmission scheme.**

***Index Terms*—Artificial noise, MISOME wiretap channels, optimal power allocation, physical layer security.**

I. Introduction

TODAY the Internet is being increasingly accessed via the wireless infrastructure, e.g., cellular networks and Wi-Fi networks [1, 2]. In wireless communication networks, the fundamental characteristics of the wireless media – openness – makes wireless transmission vulnerable to potential eavesdropping. Many techniques to prevent such eavesdropping have been explored, with physical layer security being one which has attracted growing attention. In physical layer security techniques, we exploit the imperfections of communication channels (e.g., noise, fading, and interference) to provide secure communication between legitimate transmitters and receivers [3]. Importantly, such techniques overcome the difficulties and vulnerabilities inherent in traditional cryptographic methods, such as secret key distribution and management. As such, physical layer techniques are particularly suitable for emerging decentralized wireless networks where mobile nodes may randomly leave or join [4].

In the pioneering studies of physical layer security, it was revealed that a positive secrecy data rate is achieved if the transmitter-eavesdropper channel is a degraded version of the transmitter-receiver channel [5–8]. Inspired by these studies, the secrecy capacity of wiretap channels was examined from an information theoretic perspective [9–14]. More recently, an increasing amount of research effort has been directed towards designing practical transmission schemes to improve physical layer security, e.g., transmit beamforming (TBF) [15], secure on-off transmission [16], secure opportunistic scheduling [17], and transmit antenna selection [18–22]. Notably, the schemes in [15–22] relaxed the strong assumption mandated by the information theoretic studies, that the precise eavesdropper's CSI is available at the transmitter. It is worthwhile to stress that the effectiveness of these schemes lies in the improvement of the transmitter-receiver channel quality. In order to further deteriorate the eavesdropper's channel, the authors in [23] proposed artificial noise on top of the beamformed information signal to confuse the eavesdropper. From a quality-of-service-based perspective, [24–27] designed beamformers with artificial noise within predetermined signal-to-interference-plus-noise-ratio (SINR) targets at the desired receiver(s) and/or the eavesdropper. Motivated by these studies, some research efforts have been devoted to examine the secrecy rate achieved by transmitting artificial noise in fast fading [28–32]. Differing from [28–32], some research efforts have been directed toward a better understanding of the role of transmitting artificial noise in slow fading, where the secrecy outage probability is widely adopted as the performance metric [33–35].

Different from [33–35], this work prioritizes the *effective*

Manuscript received March 21, 2014; revised September 24, 2014 and February 3, 2015; accepted March 29, 2015. The work of N. Yang was supported by the Australian Research Council Discovery Projects (DP120102607 and DP150103905). The work of M. Elkashlan and T. Q. Duong was supported by the Vietnam National Foundation for Science and Technology Development (102.04-2013.13). The work of J. Yuan and R. Malaney was supported by the Australian Research Council Discovery Project (DP120102607). The review of this paper was coordinated by Prof. M. Cenk Gursoy.

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).

M. Elkashlan is with the School of Electronic Engineering and Computer Science, Queen Mary University of London, London E1 4NS, United Kingdom (email: maged.elkashlan@qmul.ac.uk).

T. Q. Duong is with the School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, Belfast BT7 1NN, United Kingdom (e-mail: trung.q.duong@qub.ac.uk).

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

Digital Object Identifier 10.1109/TVT.2015.2419318

secrecy throughput as a performance metric in the design of secure transmission using artificial noise over slow fading. The effective secrecy throughput is a relatively new and practical performance metric that jointly considers the secrecy transmission probability and the secrecy rate [36, 37]. As such, it allows for a quantification of the average secrecy rate at which the messages are securely transmitted. In order to obtain the effective secrecy throughput, we examine the *secure transmission probability* which evaluates the probability that the messages transmitted from the transmitter to the receiver are not leaked to the eavesdropper. The primary contribution of this work is to determine the optimal transmission parameters of artificial noise such that the maximum effective secrecy throughput is guaranteed for the general operating scenarios with arbitrary signal-to-noise ratios (SNRs). To the best knowledge of the authors, such work has not been reported in literature so far.

In this paper, we investigate the optimal transmission with artificial noise in the multiple-input, single-output, and multi-antenna eavesdropper (MISOME) wiretap channel. In such a channel, the transmitter is equipped with N antennas, the receiver is equipped with a single antenna, and the eavesdropper is equipped with M antennas. In order to perform secure data transmission, artificial noise signals are transmitted in conjunction with information signals at the transmitter. We consider slow fading between the transmitter and the receiver and between the transmitter and the eavesdropper. We also consider that the instantaneous CSI of the eavesdropper's channel is not available to the transmitter. As such, perfect secrecy cannot always be guaranteed in this channel. This motivates us to examine the secrecy outage probability and the effective secrecy throughput as key performance metrics. The key contributions of this paper are summarized as follows:

1) We derive closed-form expressions for the secure transmission probability and the effective secrecy throughput of two transmission schemes. The first scheme is an on-off transmission scheme where the transmitter chooses a fixed secrecy rate, which is independent of the transmitter-receiver channel realization, for all transmission periods. It follows that the transmitter either transmits or not, depending on whether the transmitter-receiver channel capacity is higher than the secrecy rate. Based on the secure transmission probability, we obtain the hybrid outage probability of the on-off transmission scheme which allows us to quantify the transmission outage probability and the secrecy outage probability. The second scheme is an adaptive transmission scheme where the transmitter chooses a variable secrecy rate for each transmission period. In this scheme, the secrecy rate depends on the transmitter-receiver channel realization and thus, the transmitter always transmits.
2) We optimize the secrecy performance of both the on-off transmission scheme and the adaptive transmission scheme. Using our closed-form results, we first determine the optimal power allocation between information signals and artificial noise signals that maximizes the secure transmission probability of each transmission scheme. Based on this optimal solution, we then determine the optimal secrecy rate that maximizes the effective secrecy throughput of each transmission scheme.

We present numerical results to corroborate our analysis. We highlight that our derived secrecy outage probability and determined optimal solutions are valid for arbitrary N, M, $\overline{\gamma}_{\mathrm{B}}$, and $\overline{\gamma}_{\mathrm{E}}$, where $\overline{\gamma}_{\mathrm{B}}$ denotes the average SNR between the transmitter and the receiver and $\overline{\gamma}_{\mathrm{E}}$ denotes the average SNR between the transmitter and the eavesdropper. Notably, our results establish a generalized criterion that is distinct from the previous studies, e.g., [28, 34][1]. Through numerical results, we evaluate the impact of N, M, $\overline{\gamma}_{\mathrm{B}}$, and $\overline{\gamma}_{\mathrm{E}}$ on the optimal power allocation and the optimal secrecy rate. In addition, we show that the adaptive transmission scheme offers a higher maximum effective secrecy throughput than the on-off transmission scheme.

Notation: Scalar variables are denoted by italic symbols. Vectors and matrices are denoted by lower-case and upper-case boldface symbols, respectively. Moreover, $(\cdot)^H$ denotes the complex conjugate transpose, $(\cdot)^{-1}$ denotes the inverse, $\mathbf{I}_m$ denotes the $m \times m$ identity matrix, and $\mathbb{E}[\cdot]$ denotes the expectation.

II. Secure Transmission with Artificial Noise in MISOME Wiretap Channels

Fig. 1 depicts the MISOME wiretap channel of interest where the communication between the N-antenna transmitter Alice and the single antenna receiver Bob is overheard by the M-antenna malicious eavesdropper Eve. In this wiretap channel, we denote the main channel between Alice and Bob as an $1 \times N$ vector $\mathbf{h}$ and denote the eavesdropper's channel between Alice and Eve as an $M \times N$ matrix $\mathbf{G}$. The entries of $\mathbf{h}$ are modeled as independent and identically distributed (i.i.d.) Rayleigh fading and the entries of $\mathbf{G}$ are modeled as i.i.d. Rayleigh fading. Of course, we preserve the practical assumption that the main channel and the eavesdropper's channel have different average SNRs. Moreover, we assume that both the main channel and the eavesdropper's channel are subject to slow fading where the fading coefficients remain constant during the channel coherence time. We further assume that $N > M$ since Eve is able to remove the artificial noise signals if $N \leq M$ [28]. In this wiretap channel, we consider the passive eavesdropping scenario where the instantaneous information of $\mathbf{G}$ is not available to Alice. Moreover, we consider that $\mathbf{h}$ is precisely estimated by Bob and fed back to Alice. We further consider that $\mathbf{h}$ is perfectly available at Eve since the feedback from Bob to Alice is not secure.

We next detail the secure data transmission using artificial noise in the MISOME wiretap channel. In this wiretap channel, Alice transmits an information signal s_{I} in conjunction with an $(N-1) \times 1$ artificial noise signal vector $\mathbf{s}_{\mathrm{N}}$ to Bob, where s_{I} has the variance χ_{I} and each entry of $\mathbf{s}_{\mathrm{N}}$ has the variance χ_{N} [28]. We assume that the total transmit power used by Alice is P_{T}. We denote ϕ as the power allocation factor[2],

[1] We note that [28] and [34] assumed zero noise at the eavesdropper, which makes their analysis and optimal solutions only valid for high SNRs.

[2] When $\phi = 1$, no artificial noise is transmitted and TBF [15] is adopted at Alice to transmit the information signal using maximal ratio transmission with P_{T}.

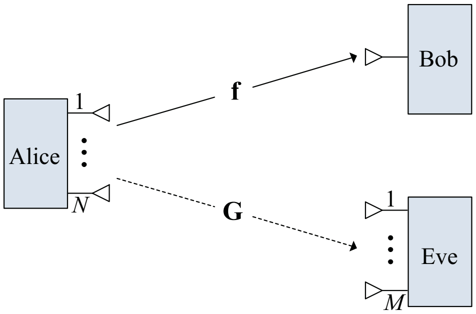

Fig. 1. A MISOME wiretap channel where Alice is equipped with N antennas, Bob is equipped with one antenna, and Eve is equipped with M antennas. The communication between Alice and Bob is overheard by Eve.

where $0 < \phi \leq 1$, which determines the fraction of the power allocated to s_{I} such that $\chi_{\mathrm{I}} = \phi P_{\mathrm{T}}$. Since Alice does not have the access of $\mathbf{G}$, she equally distributes the transmit power to each entry of $\mathbf{s}_{\mathrm{N}}$ such that $\chi_{\mathrm{N}} = (1-\phi) P_{\mathrm{T}} / (N-1)$. In order to transmit s_{I} and $\mathbf{s}_{\mathrm{N}}$, Alice designs an $N \times N$ beamforming matrix $\mathbf{V}$ given by $\mathbf{V} = [\mathbf{v}_{\mathrm{I}}\ \mathbf{V}_{\mathrm{N}}]$, where $\mathbf{v}_{\mathrm{I}}$ is used to transmit s_{I} and $\mathbf{V}_{\mathrm{N}}$ is used to transmit $\mathbf{s}_{\mathrm{N}}$. The aim of $\mathbf{V}$ is to degrade the eavesdropper's channel quality by transmitting $\mathbf{s}_{\mathrm{N}}$ in all directions except towards Bob. The design of $\mathbf{V}$ is based on the information of $\mathbf{h}$, which is fed back by Bob. To design $\mathbf{V}$, Alice defines $\mathbf{H} \triangleq \mathbf{h}^H \mathbf{h}$ and performs the eigenvalue decomposition of $\mathbf{H}$. Then Alice chooses $\mathbf{v}_{\mathrm{I}}$ as the principal eigenvector corresponding to the largest eigenvalue of $\mathbf{H}$ and chooses $\mathbf{V}_{\mathrm{N}}$ as the remaining $N-1$ eigenvectors of $\mathbf{H}$ such that $\mathbf{V}_{\mathrm{N}}$ lies in the nullspace of the main channel[3]. Therefore, the $N \times 1$ transmitted signal vector at Alice, $\mathbf{x}$, is given by

$$\mathbf{x} = [\mathbf{v}_{\mathrm{I}}\ \mathbf{V}_{\mathrm{N}}] \begin{bmatrix} s_{\mathrm{I}} \\ \mathbf{s}_{\mathrm{N}} \end{bmatrix} = \mathbf{v}_{\mathrm{I}} s_{\mathrm{I}} + \mathbf{V}_{\mathrm{N}} \mathbf{s}_{\mathrm{N}}. \tag{1}$$

According to (1), the received signal at Bob is given by

$$y = \mathbf{h}\mathbf{x} + n_{\mathrm{B}} = \mathbf{h}\mathbf{v}_{\mathrm{I}} s_{\mathrm{I}} + n_{\mathrm{B}}, \tag{2}$$

where n_{B} is additive white Gaussian noise (AWGN) at Bob with variance σ_{B}^2. Based on (2), the instantaneous received SNR at Bob is given by

$$\gamma_{\mathrm{B}} = \phi \overline{\gamma}_{\mathrm{B}} \left\| \mathbf{h} \right\|^2, \tag{3}$$

where $\overline{\gamma}_{\mathrm{B}} = P_{\mathrm{T}}/\sigma_{\mathrm{B}}^2$. According to (1), the received signal at Eve is given by

$$\mathbf{z} = \mathbf{G}\mathbf{x} + \mathbf{n}_{\mathrm{E}} = \mathbf{G}\mathbf{v}_{\mathrm{I}} s_{\mathrm{I}} + \mathbf{G}\mathbf{V}_{\mathrm{N}}\mathbf{s}_{\mathrm{N}} + \mathbf{n}_{\mathrm{E}}, \tag{4}$$

where $\mathbf{n}_{\mathrm{E}}$ is the $M \times 1$ AWGN vector at Eve satisfying $\mathbb{E}\left[\mathbf{n}_{\mathrm{E}}\mathbf{n}_{\mathrm{E}}^H\right] = \sigma_{\mathrm{E}}^2 \mathbf{I}_M$. It is crucial to note that Eve cannot eliminate the interference caused by $\mathbf{V}_{\mathrm{N}}\mathbf{s}_{\mathrm{N}}$ if $N > M$ [28]. This is due to the fact that $\mathbf{G}\mathbf{G}^H$ is invertible when $N > M$. Based on (4), the instantaneous received SINR at Eve is given by [26, 31]

$$\gamma_{\mathrm{E}} = \phi \mathbf{v}_{\mathrm{I}}^H \mathbf{G}^H \left(\frac{1-\phi}{N-1} \mathbf{G}\mathbf{V}_{\mathrm{N}}\mathbf{V}_{\mathrm{N}}^H \mathbf{G}^H + \frac{1}{\overline{\gamma}_{\mathrm{E}}} \mathbf{I}_M \right)^{-1} \mathbf{G}\mathbf{v}_{\mathrm{I}}, \tag{5}$$

where $\overline{\gamma}_{\mathrm{E}} = P_{\mathrm{T}}/\sigma_{\mathrm{E}}^2$. We clarify that the value of γ_{E} is not available at Alice since we consider a passive eavesdropping scenario in this work. In this scenario, the instantaneous knowledge of $\mathbf{G}$ is not available at Alice. We assume that $\overline{\gamma}_{\mathrm{B}}$ is available at Alice, due to the fact that Bob is an user served by Alice and thus his distances from Alice are known and the path loss exponents are known. We also assume that $\overline{\gamma}_{\mathrm{E}}$ is available at Alice[4]. If Alice does not know $\overline{\gamma}_{\mathrm{B}}$ and $\overline{\gamma}_{\mathrm{E}}$, she is still able to perform the secure data transmission using artificial noise but not able to calculate the secrecy performance metrics shown in the following sections.

In the MISOME wiretap channel, the achievable secrecy rate C_S is expressed as [12]

$$C_S = \begin{cases} C_{\mathrm{B}} - C_{\mathrm{E}} \ , & \gamma_{\mathrm{B}} > \gamma_{\mathrm{E}} \\ 0 \ , & \gamma_{\mathrm{B}} \leq \gamma_{\mathrm{E}}, \end{cases} \tag{6}$$

where $C_{\mathrm{B}} = \log_2(1+\gamma_{\mathrm{B}})$ is the capacity of the main channel and $C_{\mathrm{E}} = \log_2(1+\gamma_{\mathrm{E}})$ is the capacity of the eavesdropper's channel. Alice adopts wiretap codes [6] to perform secure transmission. To design wiretap codes, Alice has to choose the codeword transmission rate, R, and the secrecy rate, R_s. The rate difference between R and R_s, given by $R - R_s$, is the rate cost providing secrecy against Eve. Since Alice perfectly knows C_{B}, Alice chooses $R = C_{\mathrm{B}}$. Since C_{E} is not known to Alice, due to the consideration of the passive eavesdropping scenario, she assumes the capacity of the eavesdropper's channel to be $\hat{C}_{\mathrm{E}}$, where $\hat{C}_{\mathrm{E}} \neq C_{\mathrm{E}}$. Alice then constructs the wiretap codes using C_{B} and $\hat{C}_{\mathrm{E}}$. If $\hat{C}_{\mathrm{E}} \geq C_{\mathrm{E}}$, the codeword guarantees perfect secrecy. If $\hat{C}_{\mathrm{E}} < C_{\mathrm{E}}$, secrecy is compromised.

III. Optimized On-Off Transmission

In this section, we investigate the optimized on-off transmission scheme in MISOME wiretap channels. To this end, we first present the procedure of the on-off transmission scheme. We then derive new closed-form expressions that quantify the secrecy performance of this scheme. Based on these expressions, the optimal power allocation factor and the optimal secrecy rate are determined to achieve the best secrecy performance.

A. Transmission Procedure for On-Off Transmission

In the on-off transmission scheme, Alice selects a constant secrecy rate R_s for the design of wiretap code and a constant

[3] We note that the generation of $\mathbf{V}_{\mathrm{N}}$ is different from that in [32]. This is due to the fact that the aim of [32] is to maximize the secrecy rate in MISOSE wiretap channel with fast fading. Differently, we consider the MISOME wiretap channel with slow fading such that the optimization problem in [32] may not be directly applied to our work.

[4] One scenario in which knowledge of $\overline{\gamma}_{\mathrm{E}}$ would be available is when Eve is part of a multiuser system. In such a system, Eve becomes an active legitimate user in alternate time slots and thus will feedback her CSI to Alice for the time slot in which she is being served. This CSI allows Alice to determine the average SNR of Eve in the time slots she is not being served. Another scenario in which knowledge of $\overline{\gamma}_{\mathrm{E}}$ would be available is when information on the location of the eavesdropper is known (e.g., [38]). We note many previous works in physical layer security have assumed that $\overline{\gamma}_{\mathrm{E}}$ is known (e.g., [18–21, 34–37]). We also note other works have modeled the statistical distribution of $\overline{\gamma}_{\mathrm{E}}$ (e.g., [39]).

power allocation factor ϕ for secure transmission. The values of R_s and ϕ are determined based on $\overline{\gamma}_{\rm B}$ and $\overline{\gamma}_{\rm E}$ and kept constant during all transmission periods. Moreover, the values of R_s and ϕ do not depend on the instantaneous realization of the main channel.

We clarify that in the on-off transmission scheme, Alice does not transmit when $C_{\rm B} \leq R_s$. In this case the wiretap codes cannot be constructed using $C_{\rm B}$ and R_s and thus transmission outage occurs. When $C_{\rm B} > R_s$, Alice transmits. Secrecy outage occurs if $\hat{C}_{\rm E} < C_{\rm E}$ (or equivalently, $C_S < R_s$). Therefore, secure transmission is carried out when $C_S \geq R_s$. Based on these outage events, we examine the secure transmission probability in the next subsection, defined as the probability that the messages are securely transmitted from Alice to Bob but not leaked to Eve. We also examine the hybrid outage probability, defined as the complimentary probability of the secure transmission probability. Notably, the hybrid outage probability characterizes two mutually exclusive outage probabilities: i) transmission outage probability which quantifies the probability that Alice does not transmit and ii) secrecy outage probability which quantifies the probability that Alice transmits but secrecy is compromised.

B. Secrecy Performance

We first derive a new closed-form expression for the secure transmission probability. We then obtain the expression for the hybrid outage probability, based on which the expressions are presented for the transmission outage probability and the secrecy outage probability. Using the secure transmission probability, we obtain the expression for the effective secrecy throughput.

1) Secure transmission probability: According to definition, the secure transmission probability is

$$\begin{aligned} P_{\rm sec}\left(R_s\right) =& \Pr\left(C_S \geq R_s\right) \\ =& \Pr\left(\gamma_{\rm B} \geq 2^{R_s}\left(1+\gamma_{\rm E}\right)-1\right). \end{aligned} \tag{7}$$

We can re-express (7) as

$$\begin{aligned} P_{\rm sec}\left(R_s\right) =& \int_0^\infty \int_{2^{R_s}(1+\gamma_{\rm E})-1}^\infty f_{\gamma_{\rm B}}\left(\gamma_{\rm B}\right) f_{\gamma_{\rm E}}\left(\gamma_{\rm E}\right) d\gamma_{\rm B} d\gamma_{\rm E} \\ =& 1-\int_0^\infty \int_0^{2^{R_s}(1+\gamma_{\rm E})-1} f_{\gamma_{\rm B}}\left(\gamma_{\rm B}\right) f_{\gamma_{\rm E}}\left(\gamma_{\rm E}\right) d\gamma_{\rm B} d\gamma_{\rm E}, \end{aligned} \tag{8}$$

where $f_{\gamma_{\rm B}}(\gamma)$ and $f_{\gamma_{\rm E}}(\gamma)$ denote the probability density functions (PDFs) of $\gamma_{\rm B}$ and $\gamma_{\rm E}$, respectively. In order to determine (8), we first obtain $f_{\gamma_{\rm B}}(\gamma)$ and $f_{\gamma_{\rm E}}(\gamma)$. Observing $\gamma_{\rm B}$ in (3), we find that $\gamma_{\rm B}$ follows a chi-squared distribution, which is due to the fact that $\|\mathbf{h}\|^2$ is a sum of the squares of N independent Gaussian random variables. Therefore, the PDF of $\gamma_{\rm B}$ is obtained as [40]

$$f_{\gamma_{\rm B}}(\gamma) = \frac{e^{-\frac{\gamma}{\phi\overline{\gamma}_{\rm B}}}\gamma^{N-1}}{\left(\phi\overline{\gamma}_{\rm B}\right)^N \Gamma(N)}, \tag{9}$$

where $\Gamma(\cdot)$ denotes the gamma function. Based on (5), we find that the entries of $\mathbf{GV}$ are i.i.d. zero-mean complex Gaussian random variables since the entries of $\mathbf{G}$ are i.i.d. zero-mean complex Gaussian random variables and $\mathbf{V}$ is a unitary matrix. With the aid of [41], the PDF of $\gamma_{\rm E}$ is obtained as (13), at the top of the next page, where

$$\tau_1 = \frac{1}{\phi\overline{\gamma}_{\rm E}} e^{-\frac{\gamma}{\phi\overline{\gamma}_{\rm E}}}\gamma^{p-1+q}\varrho^{-(N-1)}, \tag{10}$$

$$\tau_2 = (p-1+q)\, e^{-\frac{\gamma}{\phi\overline{\gamma}_{\rm E}}}\gamma^{p-2+q}\varrho^{-(N-1)}, \tag{11}$$

and

$$\tau_3 = \frac{1-\phi}{\phi} e^{-\frac{\gamma}{\phi\overline{\gamma}_{\rm E}}}\gamma^{p-1+q}\varrho^{-N}, \tag{12}$$

with $\varrho = 1+\frac{\gamma(1-\phi)}{\phi(N-1)}$. We next use (9) and (13) to derive the secure transmission probability.

1. The case of $0<\phi<1$: In this case, we substitute (9) and (13) with $0<\phi<1$ into (8) and obtain $P_{\rm sec}(R_s)$ as

$$\begin{aligned} P_{\rm sec}^{\dagger}\left(R_s\right) =& e^{-\frac{2^{R_s}-1}{\phi\overline{\gamma}_{\rm B}}} \sum_{n=0}^{N-1} \frac{\left(2^{R_s}-1\right)^n}{n!\left(\phi\overline{\gamma}_{\rm B}\right)^n} \sum_{l=0}^{n} \binom{n}{l} \left(\frac{2^{R_s}}{2^{R_s}-1}\right)^l \\ & \times \sum_{p=1}^{M} \frac{1}{\Gamma(p)\left(\phi\overline{\gamma}_{\rm E}\right)^{p-1}} \sum_{q=0}^{M-p} \binom{N-1}{q} \frac{\theta_1-\theta_2+\theta_3}{\chi^q}. \end{aligned} \tag{14}$$

In (14), we derive θ_1 as

$$\begin{aligned} \theta_1 =& \frac{1}{\phi\overline{\gamma}_{\rm E}} \int_0^\infty e^{-\left(\frac{2^{R_s}}{\overline{\gamma}_{\rm B}}+\frac{1}{\overline{\gamma}_{\rm E}}\right)\frac{\gamma_{\rm E}}{\phi}} \frac{\gamma_{\rm E}^{l+p-1+q}}{\left(1+\frac{\gamma_{\rm E}}{\chi}\right)^{N-1}} d\gamma_{\rm E} \\ \overset{a}{=}& \frac{\chi^{\mu_1}}{\phi\overline{\gamma}_{\rm E}} \int_0^\infty e^{-\left(\frac{2^{R_s}}{\overline{\gamma}_{\rm B}}+\frac{1}{\overline{\gamma}_{\rm E}}\right)\frac{(N-1)t}{1-\phi}} \frac{t^{l+p-1+q}}{(1+t)^{N-1}} dt \\ \overset{b}{=}& \frac{\chi^{\mu_1}}{\phi\overline{\gamma}_{\rm E}} \Gamma\left(\mu_1\right) \Phi\left(\mu_1, \mu_2+1, \mu_3\right), \end{aligned} \tag{15}$$

where $\chi = \frac{\phi(N-1)}{1-\phi}$, $\mu_1 = l+p+q$, $\mu_2 = -N+l+p+q+1$, $\mu_3 = \left(\frac{2^{R_S}}{\overline{\gamma}_{\rm B}}+\frac{1}{\overline{\gamma}_{\rm E}}\right)\frac{N-1}{1-\phi}$, and $\Phi(\cdot,\cdot,\cdot)$ is the Tricomi's (confluent hypergeometric) function [42, Eq. (9.211.4)]. In (15), the equality a is obtained by applying $\gamma_{\rm E} = t\chi$, and the equality b is derived with the aid of [42, Eq. (9.211.4)]. We highlight that the value of $\Phi(\cdot,\cdot,\cdot)$ can be evaluated. We then derive θ_2 as

$$\begin{aligned} \theta_2 =& (p-1+q) \int_0^\infty e^{-\left(\frac{2^{R_s}}{\overline{\gamma}_{\rm B}}+\frac{1}{\overline{\gamma}_{\rm E}}\right)\frac{\gamma_{\rm E}}{\phi}} \frac{\gamma_{\rm E}^{l+p-2+q}}{\left(1+\frac{\gamma_{\rm E}}{\chi}\right)^{N-1}} d\gamma_{\rm E} \\ =& (p-1+q)\, \chi^{\mu_1-1} \Gamma\left(\mu_1-1\right) \Phi\left(\mu_1-1, \mu_2, \mu_3\right), \end{aligned} \tag{16}$$

and derive θ_3 as

$$\begin{aligned} \theta_3 =& \frac{1-\phi}{\phi} \int_0^\infty e^{-\left(\frac{2^{R_s}}{\overline{\gamma}_{\rm B}}+\frac{1}{\overline{\gamma}_{\rm E}}\right)\frac{\gamma_{\rm E}}{\phi}} \frac{\gamma_{\rm E}^{l+p-1+q}}{\left(1+\frac{\gamma_{\rm E}}{\chi}\right)^{N}} d\gamma_{\rm E} \\ =& \frac{1-\phi}{\phi} \chi^{\mu_1} \Gamma\left(\mu_1\right) \Phi\left(\mu_1, \mu_2, \mu_3\right). \end{aligned} \tag{17}$$

$$f_{\gamma_{\rm E}}\left(\gamma\right)=\left\{\begin{array}{ll}\sum_{p=1}^{M}\frac{1}{\Gamma(p)(\phi\overline{\gamma}_{\rm E})^{p-1}}\sum_{q=0}^{M-p}\binom{N-1}{q}\left(\tau_1-\tau_2+\tau_3\right)\left(\frac{1-\phi}{\phi(N-1)}\right)^{q} & , \quad 0<\phi<1\\ \frac{e^{-\frac{\gamma}{\overline{\gamma}_{\rm E}}}\gamma^{M-1}}{(\overline{\gamma}_{\rm E})^{M}\Gamma(M)} \quad , & \quad\phi=1.\end{array}\right. \tag{13}$$

2. The case of $\phi = 1$: In this case, we substitute (9) and (13) with $\phi = 1$ into (8) and obtain $P_{\rm sec}\left(R_s\right)$ as

$$\begin{aligned}P_{\rm sec}^{\ddagger}\left(R_s\right)=&\frac{e^{-\frac{2^{R_s}-1}{\overline{\gamma}_{\rm B}}}}{\Gamma\left(M\right)\overline{\gamma}_{\rm E}^{M}}\sum_{n=0}^{N-1}\frac{\left(2^{R_s}-1\right)^n}{n!\overline{\gamma}_{\rm B}^{n}}\sum_{l=0}^{n}\binom{n}{l}\\ &\times\left(\frac{2^{R_s}}{2^{R_s}-1}\right)^{l}\int_0^\infty e^{-\left(\frac{2^{R_s}}{\overline{\gamma}_{\rm B}}+\frac{1}{\overline{\gamma}_{\rm E}}\right)\gamma_{\rm E}}\gamma_{\rm E}^{M-1+l}d\gamma_{\rm E}\\ \overset{c}{=}&\frac{e^{-\frac{2^{R_s}-1}{\overline{\gamma}_{\rm B}}}}{\Gamma\left(M\right)\overline{\gamma}_{\rm E}^{M}}\sum_{n=0}^{N-1}\frac{1}{n!\overline{\gamma}_{\rm B}^{n}}\sum_{l=0}^{n}\binom{n}{l}2^{lR_s}\left(2^{R_s}-1\right)^{n-l}\\ &\times\Gamma\left(M+l\right)\left(\frac{2^{R_s}}{\overline{\gamma}_{\rm B}}+\frac{1}{\overline{\gamma}_{\rm E}}\right)^{-(M+l)},\end{aligned} \tag{18}$$

where the equality c is derived with the aid of [42, Eq. (3.381.4)].

Combining (14) and (18), we obtain the secure transmission probability of on-off transmission as

$$P_{\rm sec}\left(R_s\right)=\left\{\begin{array}{ll}P_{\rm sec}^{\dagger}\left(R_s\right) & , \quad 0<\phi<1\\ P_{\rm sec}^{\ddagger}\left(R_s\right) & , \quad \phi=1.\end{array}\right. \tag{19}$$

2) Hybrid outage probability: According to definition, the hybrid outage probability is

$$P_{\rm out}\left(R_s\right)=1-P_{\rm sec}\left(R_s\right). \tag{20}$$

With the aid of (19), the hybrid outage probability can be obtained in closed-form. We highlight that our new expressions in (19) and (20) are derived in closed-form as they involve power functions, exponential functions, and Tricomi's (confluent hypergeometric) functions, the values of which can be easily evaluated via computational software. Moreover, (19) and (20) are valid for general operating scenarios with arbitrary N, arbitrary M, arbitrary $\overline{\gamma}_{\rm B}$, and arbitrary $\overline{\gamma}_{\rm E}$. Notably, (19) and (20) represent an advancement over the result in [33] which examined $\log_2\left(1+\gamma_{\rm B}\right)-\log_2\left(1+\gamma_{\rm E}\right)$ numerically.

We clarify that the hybrid outage probability allows us to examine two mutually exclusive outage probabilities: i) transmission outage probability, denoted by $T_{\rm out}\left(R_s\right)$, and ii) secrecy outage probability, denoted by $S_{\rm out}\left(R_s\right)$. We note that the transmission outage occurs when $C_{\rm B} \leq R_s$ while the secrecy outage occurs when $C_{\rm B} > R_s$ and $C_S < R_s$. As such, we have

$$P_{\rm out}\left(R_s\right)=T_{\rm out}\left(R_s\right)+S_{\rm out}\left(R_s\right). \tag{21}$$

According to definition, we obtain $T_{\rm out}\left(R_s\right)$ as

$$\begin{aligned}T_{\rm out}\left(R_s\right)=&\Pr\left(C_{\rm B}\leq R_s\right)\\ =&\Pr\left(\gamma_{\rm B}\leq 2^{R_s}-1\right)\\ =&F_{\gamma_{\rm B}}\left(2^{R_s}-1\right)\\ =&1-e^{-\frac{2^{R_s}-1}{\phi\overline{\gamma}_{\rm B}}}\sum_{n=0}^{N-1}\frac{1}{n!}\left(\frac{2^{R_s}-1}{\phi\overline{\gamma}_{\rm B}}\right)^n,\end{aligned} \tag{22}$$

where $F_{\gamma_{\rm B}}\left(\cdot\right)$ denotes the cumulative distribution function (CDF) of $\gamma_{\rm B}$. Moreover, we use (19) and (22) to obtain the secrecy outage probability is obtained as

$$S_{\rm out}\left(R_s\right)=\left\{\begin{array}{ll}1-P_{\rm sec}^{\dagger}\left(R_s\right)-T_{\rm out}\left(R_s\right) & , \quad 0<\phi<1\\ 1-P_{\rm sec}^{\ddagger}\left(R_s\right)-T_{\rm out}\left(R_s\right) & , \quad \phi=1.\end{array}\right. \tag{23}$$

3) Effective secrecy throughput: The effective secrecy throughput quantifies the average rate of the messages that are securely transmitted from Alice to Bob in the passive eavesdropping scenario [36, 37]. In such a scenario, the CSI of the eavesdropper's channel cannot be accessed by Alice and thus perfect secrecy is not guaranteed. Therefore, the effective secrecy throughput is defined as the product of R_s and the secure transmission probability. We clarify that the effective secrecy throughput is different from the ergodic secrecy rate. The ergodic secrecy rate applies to delay-tolerant applications which allow for the adoption of an ergodic version of the fading channel [11, 43]. In addition, the effective secrecy throughput is different from the throughput investigated in [16, 34, 44]. In [16, 34, 44], the throughput is defined as the product of R_s and the transmission probability. Thus, the throughput evaluates the average rate of message transmissions but does not examine how much of the transmitted messages are secure on average.

Using (19), we formulate the effective secrecy throughput as

$$U\left(\phi,R_s\right)=\left\{\begin{array}{ll}R_sP_{\rm sec}^{\dagger}\left(R_s\right) & , \quad 0<\phi<1\\ R_sP_{\rm sec}^{\ddagger}\left(R_s\right) & , \quad \phi=1.\end{array}\right. \tag{24}$$

Substituting (19) into (24), we obtain a closed-form expression for the effective secrecy throughput of the on-off transmission scheme.

C. Performance Optimization

1) Optimal ϕ for minimum $P_{out}\left(R_s\right)$: We first determine the optimal power allocation factor, ϕ^*, that maximizes the secure transmission probability for a given R_s. It is easy to find from (21) that maximizing the secure transmission probability is equivalent to minimizing the hybrid outage probability. We express ϕ^* as

$$\phi^*=\underset{0<\phi\leq 1}{\operatorname{argmin}}\,P_{\rm out}\left(R_s\right). \tag{25}$$

We first analytically determine the first-order derivative of $P_{\text{out}}(R_s)$ with respect to ϕ for a given R_s. We numerically find that $\partial P_{\text{out}}(R_s)/\partial\phi$ is first negative and then positive. We then analytically determine the second-order derivative of $P_{\text{out}}(R_s)$ with respect to ϕ for a given R_s. We numerically find that $\partial^2 P_{\text{out}}(R_s)/\partial^2\phi$ is always positive when $0 < \phi < 1$. Therefore, we *conjecture* that there is a unique value of ϕ within $0 < \phi < 1$, referred to as ϕ_t^*, which achieves the minimum $P_{\text{out}}(R_s)$ (or equivalently, the maximum $P_{\text{sec}}(R_s)$). This conjecture will be supported by the numerical results in Section III-D. Although a closed-form solution for ϕ_t^* is mathematically intractable, we are able to determine ϕ_t^* by using the exhaustive search method. After finding ϕ_t^*, we compare $P_{\text{out}}(R_s)_{\phi=\phi_t^*}$ with $P_{\text{out}}(R_s)_{\phi=1}$. If $P_{\text{out}}(R_s)_{\phi=\phi_t^*} < P_{\text{out}}(R_s)_{\phi=1}$, we have $\phi^* = \phi_t^*$. Otherwise we have $\phi^* = 1$.

We clarify that the solution of ϕ^* allows us to achieve two important goals: 1) Achieve the minimum hybrid outage probability for a given R_s and 2) Facilitate the maximization of the effective secrecy throughput, as will be shown in Section III-C2. We denote $P_{\text{out}}^*(R_s) \triangleq P_{\text{out}}(R_s)_{\phi=\phi^*}$ and $P_{\text{sec}}^*(R_s) \triangleq P_{\text{sec}}(R_s)_{\phi=\phi^*}$ as the optimal hybrid outage probability and the optimal secure transmission probability for a given R_s, respectively. We further denote $U^*(\phi^*, R_s) \triangleq R_s P_{\text{sec}}^*(R_s)$ as the effective secrecy throughput achieved by ϕ^* for a given R_s. It is easy to verify that $U^*(\phi^*, R_s)$ is the maximum effective secrecy throughput for a given R_s.

2) Optimal R_s for maximum $U^*(\phi^*, R_s)$: We now determine the optimal secrecy rate, R_s^*, that maximizes the effective secrecy throughput achieved by ϕ^*. R_s^* is expressed as

$$R_s^* = \underset{R_s>0}{\operatorname{argmax}}\, U^*(\phi^*, R_s). \tag{26}$$

We numerically find that $U^*(\phi^*, R_s)$ first increases and then decreases as R_s increases (see Section III-D). This finding is not surprising since $P_{\text{sec}}^*(R_s)$ is a decreasing function of R_s. When R_s is low, the behavior of $U^*(\phi^*, R_s)$ is dominated by R_s and thus $U^*(\phi^*, R_s)$ increases as R_s increases. When R_s is high, the behavior of $U^*(\phi^*, R_s)$ is dominated by $P_{\text{sec}}^*(R_s)$ and thus $U^*(\phi^*, R_s)$ decreases as R_s increases. Based on this finding, we conjecture that the optimal value of R_s that maximizes $U^*(\phi^*, R_s)$, i.e., R_s^*, is unique. This conjecture will be supported by the numerical results in Section III-D. With the aid of the exhaustive search method, we are able to determine R_s^*. Since $U^*(\phi^*, R_s)$ appears to be a quasi-concave function of R_s, as shown in the numerical results in Section III-D, the optimal value of R_s that maximizes $U^*(\phi^*, R_s)$ may converge to a local optimum, but not global optimum [45]. We denote $\phi^{*\circ}$ as the value of ϕ^* for $P_{\text{sec}}^*(R_s^*)$. Finally, we denote $U^{*\circ} \triangleq U^*(\phi^{*\circ}, R_s^*)$ as the maximum effective secrecy throughput.

D. Numerical Results

In this subsection, numerical results are presented to examine the impact of the number of antennas, i.e., N and M, and the average SNRs, i.e., $\overline{\gamma}_{\text{B}}$ and $\overline{\gamma}_{\text{E}}$, on the secrecy performance of the on-off transmission scheme.

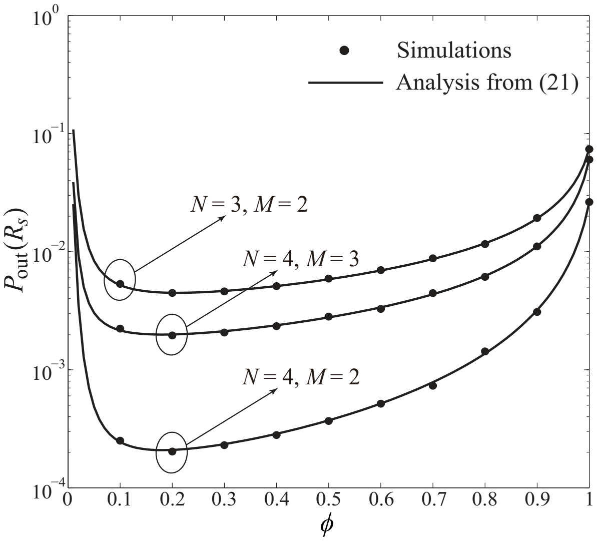

Fig. 2. The hybrid outage probability for $R_s = 1$, $\overline{\gamma}_{\text{B}} = 20$ dB, and $\overline{\gamma}_{\text{E}} = \overline{\gamma}_{\text{B}}/5$.

1) Impact of system parameters on $P_{out}(R_s)$: Fig. 2 plots the hybrid outage probability versus ϕ. In this figure, the analytical curve is obtained from (20). We first see that the hybrid outage probability first decreases and then increase as ϕ increases, which implies that there is a unique ϕ that minimizes the hybrid outage probability, i.e., ϕ^*. This supports our conjecture on ϕ^* in Section III-C1. Second, we find that an increasing N brings a significant reduction in the hybrid outage probability, which demonstrates that the multi-antenna benefit at Alice is preserved when artificial noise signals are incorporated in the transmission. Third, we find that an increasing M leads to an increase in the hybrid outage probability, which shows the detrimental effect of multiple antennas at Eve. Fourth, it is clearly seen that the scheme using ϕ^* achieves a lower hybrid outage probability than that using equal power allocation with $\phi = 0.5$. This demonstrates the effectiveness of our optimal power allocation factor in (25). Fifth, it is evident that the simulation points, marked by '•', precisely agree with the analysis, which substantiates the accuracy of our results. In addition, although not shown in the figure, we find that $\phi^* \to 1$ when $\overline{\gamma}_{\text{B}}$ is low. This indicates that the entire power is allocated to transmit information signals in the low SNR regime, which is in accordance with [33, Corollary 4].

2) Impact of system parameters on ϕ^*: In Figs. 3 and 4, we examine the impact of N, M, $\overline{\gamma}_{\text{B}}$, and $\overline{\gamma}_{\text{E}}$ on the optimal power allocation factor. We first focus on the system parameters that can be managed by Alice, namely, N and $\overline{\gamma}_{\text{B}}$. Fig. 3 plots ϕ^* versus N for different values of $\overline{\gamma}_{\text{B}}$. We observe that an increase in N or $\overline{\gamma}_{\text{B}}$ leads to a rapidly decreasing ϕ^*. For example, when $\overline{\gamma}_{\text{B}} = 10$ dB, increasing N from 3 to 6 decreases ϕ^* from 0.442 to 0.327. When $N = 4$, increasing $\overline{\gamma}_{\text{B}}$ from 5 dB to 15 dB decreases ϕ^* from 0.413 to 0.329. These observations imply that Alice should allocate more power to artificial noise signals in order to minimize the hybrid outage probability (or equivalently, maximize the

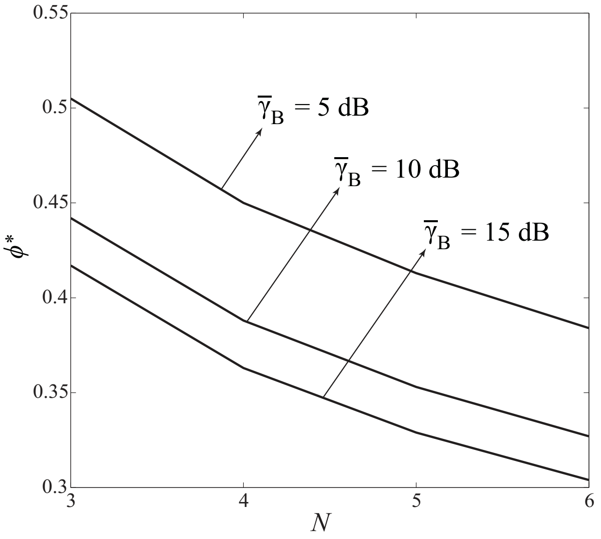

Fig. 3. The value of ϕ^* for $M = 2$, $R_s = 1$, and $\overline{\gamma}_{\mathrm{E}} = 5$ dB.

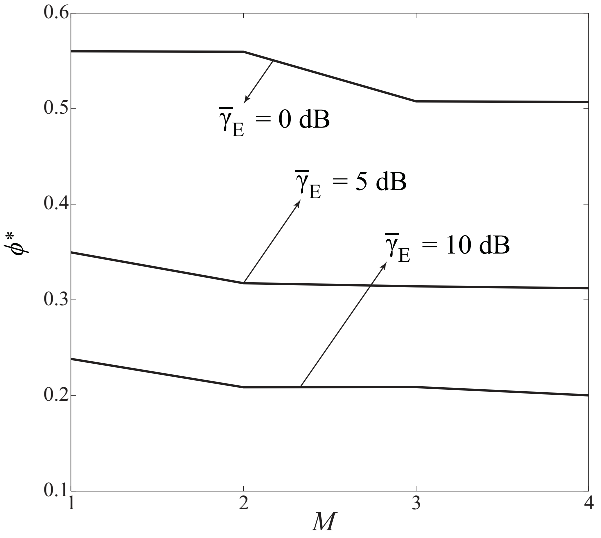

Fig. 4. The value of ϕ^* for $N = 5$, $R_s = 1$, and $\overline{\gamma}_{\mathrm{B}} = 20$ dB.

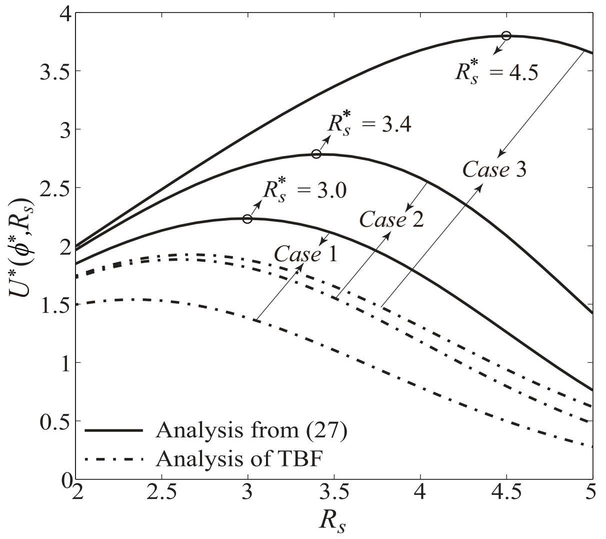

Fig. 5. The effective secrecy throughput achieved by ϕ^* of the on-off transmission scheme with $\overline{\gamma}_{\mathrm{E}} = \overline{\gamma}_{\mathrm{B}}/5$ for three cases: *Case* 1: $N = 3$, $M = 2$, and $\overline{\gamma}_{\mathrm{B}} = 15$ dB,*Case* 2: $N = 4$, $M = 2$, and $\overline{\gamma}_{\mathrm{B}} = 15$ dB, and *Case* 3: $N = 4$, $M = 2$, and $\overline{\gamma}_{\mathrm{B}} = 20$ dB.

secure transmission probability) for larger N or higher $\overline{\gamma}_{\mathrm{B}}$ in the on-off transmission scheme. We note that this conclusion is different from the optimal power allocation for the non-adaptive encoder Φ^* in [34]. In [34], it was found that Φ^* increases with N, which indicates that when more transmit antennas are used, less power should be allocated to artificial noise signals, under the required security level. The difference in the conclusion between our work and [34] is not surprising since the aim of optimization, the target performance metric, and the design of secrecy rate are different.

We next focus on the system parameters that cannot be managed by Alice, namely, M and $\overline{\gamma}_{\mathrm{E}}$. Fig. 4 plots ϕ^* versus M for different values of $\overline{\gamma}_{\mathrm{E}}$. In this figure, it is seen that a pronounced decrease in ϕ^* is caused by increasing $\overline{\gamma}_{\mathrm{E}}$. For example, when $M = 3$, increasing $\overline{\gamma}_{\mathrm{E}}$ from 0 dB to 10 dB decreases ϕ^* from 0.508 to 0.209. Moreover, we see a slight decrease in ϕ^* is caused by increasing M. For example, when $\overline{\gamma}_{\mathrm{E}} = 5$ dB, increasing M from 1 to 4 decreases ϕ^* from 0.349 to 0.312. These observations imply that Alice should allocate more power to artificial noise signals in order to minimize the hybrid outage probability (or equivalently, maximize the secure transmission probability) for larger M or higher $\overline{\gamma}_{\mathrm{E}}$ in the on-off transmission scheme.

3) Impact of system parameters on $U^*(\phi^*, R_s)$: In Figs. 5 and 6, we examine the impact of N, M, $\overline{\gamma}_{\mathrm{B}}$, and $\overline{\gamma}_{\mathrm{E}}$ on the effective secrecy throughput determined using ϕ^*, $U^*(\phi^*, R_s)$. In both figures, we see that $U^*(\phi^*, R_s)$ first increases and then decreases as R_s increases, which supports our conjecture on R_s^* in Section III-C2. We first focus on the impact of N and $\overline{\gamma}_{\mathrm{B}}$. Fig. 5 plots $U^*(\phi^*, R_s)$ versus R_s for *Cases* 1–3. We find that a higher effective secrecy throughput is achieved when either N or $\overline{\gamma}_{\mathrm{B}}$ increases. Moreover, we see that the effective secrecy throughput achieved by artificial noise is higher than that achieved by TBF, which demonstrates the superiority of the use of artificial noise over TBF. Furthermore, we observe that R_s^* shifts to the right when either N or $\overline{\gamma}_{\mathrm{B}}$ increases. For example, comparing *Case* 1 and *Case* 2, we find that increasing N from 3 to 4 increases R_s^* from 3.0 to 3.4. Comparing *Case* 2 and *Case* 3, we find that increasing $\overline{\gamma}_{\mathrm{B}}$ from 15 dB to 20 dB increases R_s^* from 3.4 to 4.5. This observation implies that Alice supports a higher secrecy rate for larger N or higher $\overline{\gamma}_{\mathrm{B}}$ in the on-off transmission scheme.

We now focus on the impact of M and $\overline{\gamma}_{\mathrm{E}}$. Fig. 6 plots $U^*(\phi^*, R_s)$ achieved by ϕ^* versus R_s for *Cases* 4–6. Evidently, this figure shows that increasing M or $\overline{\gamma}_{\mathrm{E}}$ leads to a lower effective secrecy throughput. Moreover, it shows that R_s^* shifts to the left when either M or $\overline{\gamma}_{\mathrm{E}}$ increases. For example, comparing *Case* 4 and *Case* 5, we find that increasing M from 2 to 3 decreases R_s^* from 3.7 to 3.3. Comparing *Case* 5 and *Case* 6, we find that increasing $\overline{\gamma}_{\mathrm{E}}$ from $\overline{\gamma}_{\mathrm{B}}/10$ to $\overline{\gamma}_{\mathrm{B}}/5$

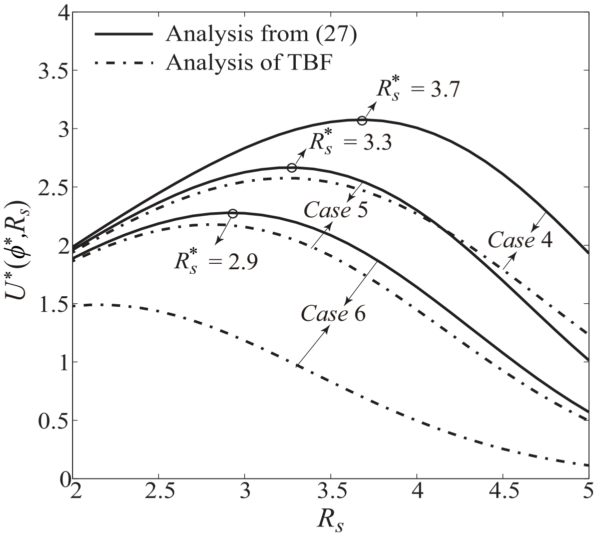

Fig. 6. The effective secrecy throughput achieved by ϕ^* of the on-off transmission scheme with $\overline{\gamma}_{\mathrm{B}} = 15$ dB for three cases: *Case* 4: $N = 4$, $M = 2$, and $\overline{\gamma}_{\mathrm{E}} = \overline{\gamma}_{\mathrm{B}}/10$, *Case* 5: $N = 4$, $M = 3$, and $\overline{\gamma}_{\mathrm{E}} = \overline{\gamma}_{\mathrm{B}}/10$, and *Case* 6: $N = 4$, $M = 3$, and $\overline{\gamma}_{\mathrm{E}} = \overline{\gamma}_{\mathrm{B}}/5$.

decreases R_s^* from 3.3 to 2.9. This observation implies that Alice supports a lower secrecy rate for larger M or higher $\overline{\gamma}_{\mathrm{E}}$ in the on-off transmission scheme.

IV. Optimized Adaptive Transmission

In this section, we investigate the optimized adaptive transmission scheme in MISOME wiretap channels. For this purpose, we first present the procedure of the adaptive transmission scheme. New closed-form expressions are then derived to quantify the secrecy performance of the scheme. Using these expressions, we determine the optimal power allocation factor and the optimal secrecy rate that achieve the optimum secrecy performance.

A. Transmission Procedure for Adaptive Transmission

In the adaptive transmission scheme, Alice uses a variable secrecy rate R_s for the design of wiretap code and a variable power allocation factor ϕ for secure transmission. The values of R_s and ϕ are determined based on $\tilde{\gamma}_{\mathrm{B}} = \overline{\gamma}_{\mathrm{B}} \left\|\mathbf{h}\right\|^2$ and $\overline{\gamma}_{\mathrm{E}}$ and thus vary from one transmission period to another. Different from the on-off transmission scheme, the values of R_s and ϕ in the adaptive transmission scheme depend on the instantaneous realization of the main channel. Here, $\tilde{\gamma}_{\mathrm{B}}$ is the instantaneous SNR of the main channel without power allocation, which is calculated at Alice, based on the information of $\mathbf{h}$ fed back by Bob, before power allocation between information signals and artificial noise signals.

We clarify that in the adaptive transmission scheme, Alice always transmit since Alice chooses R_s within $0 < R_s < \tilde{C}_{\mathrm{B}}$ for each $\tilde{C}_{\mathrm{B}}$, where $\tilde{C}_{\mathrm{B}} = \log_2(1+\tilde{\gamma}_{\mathrm{B}})$. This indicates that the transmission outage probability is zero. This also indicates that there is only one outage event in the adaptive transmission scheme, which is secrecy outage. Secrecy outage occurs when $\hat{C}_{\mathrm{E}} < C_{\mathrm{E}}$ (or equivalently, $C_{\mathrm{B}} - R_s < C_{\mathrm{E}}$). Based on this outage event, we examine two probabilities to quantify the secrecy performance of the adaptive transmission scheme. The first one is the secure transmission probability, which is defined as the probability that Alice securely transmits messages to Bob. The second one is the secrecy outage probability, which is defined as the complimentary probability of the secure transmission probability. Such a probability quantifies the probability that the messages are leaked to Eve.

B. Secrecy Performance

We first derive new closed-form expressions for the secure transmission probability and the secrecy outage probability. Based on these probabilities, we obtain the expression for the effective secrecy throughput. These probabilities and the effective secrecy throughput are based on a given $\tilde{\gamma}_{\mathrm{B}}$, which is required by the procedure of the adaptive transmission scheme.

1) Secure transmission probability: According to definition, the secure transmission probability is given by

$$\begin{aligned}\mathcal{P}_{\mathrm{sec}}\left(R_s\right) &= \Pr\left(C_{\mathrm{E}} \le C_{\mathrm{B}} - R_s\right)\\ &= \Pr\left(\gamma_{\mathrm{E}} \le \frac{(1+\phi\tilde{\gamma}_{\mathrm{B}})}{2^{R_s}} - 1\right). \end{aligned} \tag{27}$$

Observing γ_{E} in (5), it is found that the entries of $\mathbf{GV}$ are i.i.d. zero-mean complex Gaussian random variables. Based on [41, Eqs. (11)–(12)], we obtain $\mathcal{P}_{\mathrm{sec}}\left(R_s\right)$ as

$$\begin{aligned}\mathcal{P}_{\mathrm{sec}}\left(R_s\right) =& F_{\gamma_{\mathrm{E}}}\left(\frac{\kappa}{2^{R_s}}\right)\\ =& 1 - e^{-\frac{\kappa}{\phi\overline{\gamma}_{\mathrm{E}}2^{R_s}}}\left(1+\frac{(1-\phi)\,\kappa}{\phi\,(N-1)\,2^{R_s}}\right)^{-(N-1)}\\ &\times\sum_{p=1}^{M}\frac{1}{\Gamma\left(p\right)}\left(\frac{\kappa}{\phi\overline{\gamma}_{\mathrm{E}}2^{R_s}}\right)^{p-1}\\ &\times\sum_{q=0}^{M-p}\binom{N-1}{q}\left(\frac{(1-\phi)\,\kappa}{\phi\,(N-1)\,2^{R_s}}\right)^{q}, \end{aligned} \tag{28}$$

where $F_{\gamma_{\mathrm{E}}}(\cdot)$ is the CDF of γ_{E} and $\kappa = 1 + \phi\tilde{\gamma}_{\mathrm{B}} - 2^{R_s}$.

2) Secrecy outage probability: According to definition, the secrecy outage probability is formulated as

$$\mathcal{S}_{\mathrm{out}}\left(R_s\right) = 1 - \mathcal{P}_{\mathrm{sec}}\left(R_s\right), \tag{29}$$

which can be obtained using (28). We clarify that (28) and (29) are valid for $\frac{2^{R_s-1}}{\tilde{\gamma}_{\mathrm{B}}} < \phi \le 1$.

3) Effective secrecy throughput: According to definition, we obtain the effective secrecy throughput as

$$\mathcal{U}\left(\phi, R_s\right) = R_s\mathcal{P}_{\mathrm{sec}}\left(R_s\right). \tag{30}$$

Substituting (28) into (30), the effective secrecy throughput of the adaptive transmission scheme is obtained in closed-form.

C. Performance Optimization

1) Optimal ϕ for minimum $\mathcal{S}_{out}\left(R_s\right)$: We first determine the optimal power allocation factor, ϕ', that minimizes the secrecy outage probability (or equivalently, maximizes the secure transmission probability) for a given R_s and the realization of $\tilde{\gamma}_{\rm B}$. The value of ϕ' is

$$\phi' = \underset{\frac{2^{R_s-1}}{\tilde{\gamma}_{\rm B}}<\phi\leq 1}{\operatorname{argmin}} \ \mathcal{S}_{\rm out}\left(R_s\right). \quad (31)$$

We first analytically determine the first-order derivative of $\mathcal{S}_{\rm out}\left(R_s\right)$ with respect to ϕ for a given R_s. We numerically find that $\partial\mathcal{S}_{\rm out}\left(R_s\right)/\partial\phi$ is first negative and then positive. We then analytically determine the second-order derivative of $\mathcal{S}_{\rm out}\left(R_s\right)$ with respect to ϕ for a given R_s, We numerically find that $\partial^2\mathcal{S}_{\rm out}\left(R_s\right)/\partial^2\phi$ is always positive when $\frac{2^{R_s-1}}{\tilde{\gamma}_{\rm B}} < \phi \leq 1$. Based on these findings we conjecture that there is a unique value of ϕ that minimizes $\mathcal{S}_{\rm out}\left(R_s\right)$ (or equivalently, maximizes $\mathcal{P}_{\rm sec}\left(R_s\right)$), which is ϕ'. This conjecture will be supported by the numerical results in Section IV-D. Using the exhaustive search method, the value of ϕ' can be determined. The solution of ϕ' enables us to evaluate the minimum secrecy outage probability for a target R_s. It also facilitate us to maximize the effective secrecy throughput, as will be shown in Section IV-C2. Based on ϕ', we denote $\mathcal{S}'_{\rm out}\left(R_s\right) \triangleq \mathcal{S}_{\rm out}\left(R_s\right)|_{\phi=\phi'}$ and $\mathcal{P}'_{\rm sec}\left(R_s\right) \triangleq \mathcal{P}_{\rm set}\left(R_s\right)|_{\phi=\phi'}$ as the optimal secrecy outage probability achieved by ϕ' and the optimal secure transmission probability achieved by ϕ' for a given R_s, respectively. In addition, $\mathcal{U}'\left(\phi', R_s\right) \triangleq R_s\mathcal{P}'_{\rm sec}\left(R_s\right)$ as the effective secrecy throughput achieved by ϕ'. Evidently, $\mathcal{U}'\left(\phi', R_s\right)$ is the maximum effective secrecy throughput for a given R_s.

2) Optimal R_s for maximum $\mathcal{U}'\left(\phi', R_s\right)$: We now determine the optimal secrecy rate, R'_s, that maximizes the effective secrecy throughput achieved by ϕ'. R'_s is expressed as

$$R'_s = \underset{0<R_s<\tilde{C}_{\rm B}}{\operatorname{argmax}}\, \mathcal{U}'\left(\phi', R_s\right). \quad (32)$$

It is numerically found that $\mathcal{U}'\left(\phi', R_s\right)$ first increases and then decreases as R_s increases. We believe that this finding is expected since $\mathcal{P}'_{\rm sec}\left(R_s\right)$ decreases as R_s increases. When R_s is low, the behavior of $\mathcal{U}'\left(\phi', R_s\right)$ is dominated by R_s and thus $\mathcal{U}'\left(\phi', R_s\right)$ increases as R_s increases. When R_s is high, the behavior of $\mathcal{U}'\left(\phi', R_s\right)$ is dominated by $\mathcal{U}'\left(\phi', R_s\right)$ and thus $\mathcal{U}'\left(\phi', R_s\right)$ decreases as R_s increases. From this finding we conjecture that the optimal value of R_s that maximizes $\mathcal{U}'\left(\phi', R_s\right)$, i.e., R'_s, is unique. This conjecture will be supported by the numerical results in Section IV-D. The value of R'_s can be determined by using the exhaustive search method. We denote ϕ'° as the value of ϕ' for $\mathcal{P}'_{\rm sec}\left(R'_s\right)$. As shown in the numerical results in Section III-D, $\mathcal{U}'\left(\phi', R_s\right)$ appears to be a quasi-concave function of R_s, which leads to the fact that the optimal value of R_s that maximizes $\mathcal{U}'\left(\phi', R_s\right)$ may converge to a local optimum, but not global optimum [45]. Using ϕ'° and R'_s, we denote $\mathcal{U}'^{\circ} \triangleq \mathcal{U}\left(\phi'^{\circ}, R'_s\right)$ as the maximum effective secrecy throughput. We note that $\mathcal{U}'^{\circ}$ depends on the value of $\tilde{\gamma}_{\rm B}$. Therefore, we finally denote $\bar{\mathcal{U}}'^{\circ}$ as the average maximum effective secrecy throughput, where $\bar{\mathcal{U}}'^{\circ}$ takes expectation of $\mathcal{U}'^{\circ}$ over $\tilde{\gamma}_{\rm B}$, i.e., $\bar{\mathcal{U}}'^{\circ} = \mathbb{E}_{\tilde{\gamma}_{\rm B}}\left[\mathcal{U}'^{\circ}\right]$.

D. Numerical Results

In this subsection, numerical results are presented to examine the impact of the number of antennas, i.e., N and M, and the SNRs, i.e., $\tilde{\gamma}_{\rm B}$ and $\overline{\gamma}_{\rm E}$, on the secrecy performance of the adaptive transmission scheme.

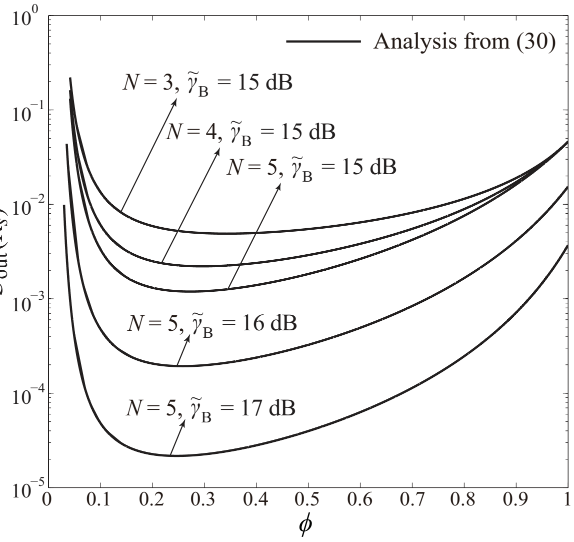

Fig. 7. The secrecy outage probability for $M = 2$, $R_s = 1$, and $\overline{\gamma}_{\rm E} = 5$ dB.

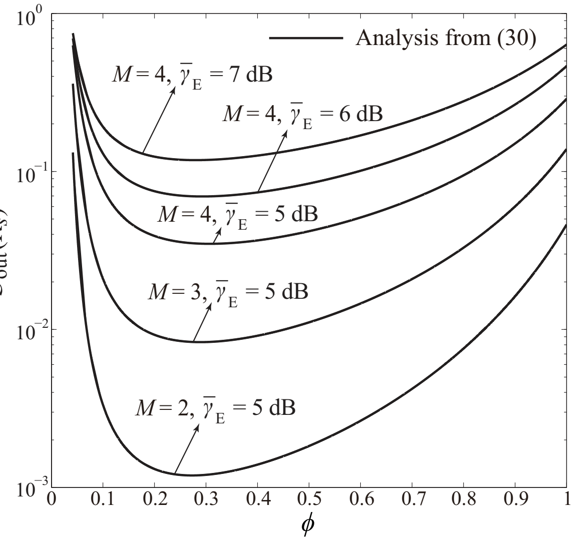

Fig. 8. The secrecy outage probability for $N = 5$, $R_s = 1$, and $\tilde{\gamma}_{\rm B} = 15$ dB.

1) Impact of system parameters on $\mathcal{S}_{out}\left(R_s\right)$: In Figs. 7 and 8, we examine the impact of N, M, $\tilde{\gamma}_{\rm B}$, and $\overline{\gamma}_{\rm E}$ on the secrecy outage probability $\mathcal{S}_{\rm out}\left(R_s\right)$ and the optimal power allocation factor ϕ'. In these figures, the analytical curve is obtained from (29). We find from both figures that $\mathcal{S}_{\rm out}\left(R_s\right)$ first increases and then decreases as ϕ increases. As such, there is a unique ϕ that minimizes the secrecy outage probability, which supports our conjecture on ϕ' in Section IV-C1. We first focus on N and $\tilde{\gamma}_{\rm B}$. Fig. 7 plots $\mathcal{S}_{\rm out}\left(R_s\right)$ versus ϕ. First, we see that the value of ϕ' decreases as N increases for a given $\tilde{\gamma}_{\rm B}$. For example, when $\tilde{\gamma}_{\rm B} = 15$ dB, increasing N from 3 to 5 decreases ϕ' from 0.34 to 0.27. Second, we find that the value of ϕ' decreases as $\tilde{\gamma}_{\rm B}$ increases for a given N. For example, when $N = 5$, increasing $\tilde{\gamma}_{\rm B}$ from 15 dB to 17 dB decreases

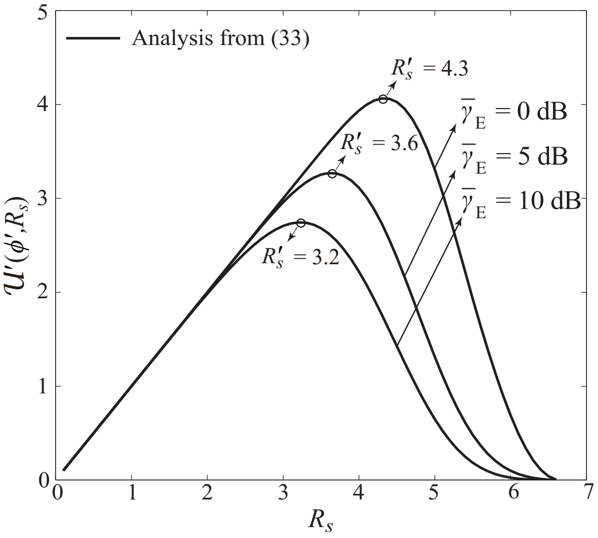

Fig. 9. The effective secrecy throughput achieved by ϕ' of adaptive transmission between artificial noise for $N = 4$, $M = 2$, and $\tilde{\gamma}_{\rm B} = 20$ dB.

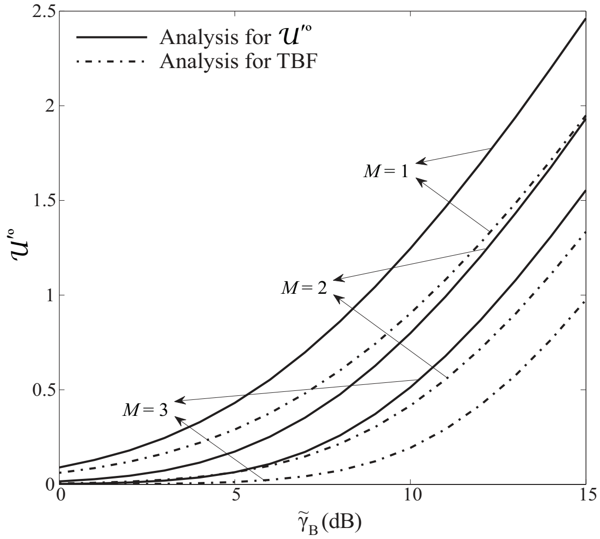

Fig. 10. Maximum effective secrecy throughput of adaptive transmission between artificial noise and TBF for $N = 5$ and $\overline{\gamma}_{\rm E} = 5$ dB.

ϕ' from 0.27 to 0.25. These observations indicate that Alice should allocate more power to artificial noise signals in order to maximize the secure transmission probability for larger N or higher $\tilde{\gamma}_{\rm B}$ in the adaptive transmission scheme.

We next focus on M and $\overline{\gamma}_{\rm E}$. Fig. 8 plots $\mathcal{S}_{\rm out}(R_s)$ versus ϕ. In this figure, we first observe that the value of ϕ' increases as M increases for a given $\tilde{\gamma}_{\rm B}$. For example, when $\overline{\gamma}_{\rm E} = 5$ dB, increasing M from 2 to 4 increases ϕ' from 0.27 to 0.30. Second, we see that the value of ϕ' decreases as $\overline{\gamma}_{\rm E}$ increases for a given M. For example, when $M = 4$, increasing $\overline{\gamma}_{\rm E}$ from 5 dB to 7 dB decreases ϕ' from 0.30 to 0.28. These observations indicate that Alice should allocate less power to artificial noise signals in order to maximize the secure transmission probability for larger M, but more power to artificial noise signals in order to maximize the secure transmission probability for higher $\overline{\gamma}_{\rm E}$ in the adaptive transmission scheme.

2) Impact of system parameters on $\mathcal{U}'(\phi', R_s)$ and $\mathcal{U}'^{\circ}$: In Fig. 9, we examine the impact of $\overline{\gamma}_{\rm E}$ and R_s on the effective secrecy throughput determined using ϕ', $\mathcal{U}'(\phi', R_s)$. Fig. 9 plots $\mathcal{U}'(\phi', R_s)$ versus R_s for different values of $\overline{\gamma}_{\rm E}$. From this figure we find that $\mathcal{U}'(\phi', R_s)$ first increases and then decreases as R_s increases. Therefore, there is a unique R_s that maximizes $\mathcal{U}'(\phi', R_s)$, which supports our conjecture on R'_s in Section IV-C2. We also find that a lower effective secrecy throughput is achieved when $\overline{\gamma}_{\rm E}$ increases. This implies that Alice supports a lower secrecy rate for higher $\overline{\gamma}_{\rm E}$ in the adaptive transmission scheme. Although not shown, we confirm that a higher effective secrecy throughput is achieved when N or $\tilde{\gamma}_{\rm B}$ increases. This implies that Alice supports a higher secrecy rate for larger N or higher $\tilde{\gamma}_{\rm B}$ in the adaptive transmission scheme.

In Fig. 10, we examine the impact of M and $\tilde{\gamma}_{\rm B}$ on the maximum effective secrecy throughput $\mathcal{U}'^{\circ}$, which is achieved by ϕ'° and R'_s as given in (32). Also, we compare the maximum effective secrecy throughput achieved by the adaptive transmission scheme with artificial noise to that achieved by the adaptive transmission scheme with TBF in this figure. Here, we obtain the maximum effective secrecy throughput achieved by the adaptive transmission scheme with TBF as $\mathcal{U}'^{\circ}_{\rm TBF}(R_s) = \max_{R_s} \mathcal{U}_{\rm TBF}(R_s)$, where $\mathcal{U}_{\rm TBF}$ is defined as the effective secrecy throughput achieved by the adaptive transmission scheme with TBF. Using (28) with $\phi = 1$, we obtain $\mathcal{U}_{\rm TBF}$ as

$$\mathcal{U}_{\rm TBF}(R_s) = R_s\left(1 - e^{-\frac{\kappa}{2^{R_s}\overline{\gamma}_{\rm E}}}\sum_{p=1}^{M}\frac{\kappa^{p-1}}{\Gamma(p)\left(2^{R_s}\overline{\gamma}_{\rm E}\right)^{p-1}}\right). \quad (33)$$

Fig. 10 compares the maximum effective secrecy throughput between artificial noise and TBF versus $\tilde{\gamma}_{\rm B}$ for different values of M. We first observe in this figure that $\mathcal{U}'^{\circ}$ increases as $\tilde{\gamma}_{\rm B}$ increases. We then observe that $\mathcal{U}'^{\circ}$ decreases as M increases. Furthermore, we find that artificial noise achieves a higher $\mathcal{U}'^{\circ}$ than TBF. In particular, the performance gain of artificial noise over TBF slightly increases with M for a given $\tilde{\gamma}_{\rm B}$. This observation indicates that artificial noise provides a minor increase in the effective secrecy throughput gain over TBF when M increases. Although not shown in this paper, we confirm that $\mathcal{U}'^{\circ}$ increases as $\tilde{\gamma}_{\rm B}$ increases or $\overline{\gamma}_{\rm E}$ decreases.

3) Comparison between on-off transmission and adaptive transmission: Finally, we conduct a secrecy throughput comparison between the on-off transmission scheme and the adaptive transmission scheme. Fig. 11 plots the maximum effective secrecy throughput of the on-off transmission scheme, $U^{*\circ}$, and the average maximum effective secrecy throughput of the adaptive transmission scheme, $\bar{\mathcal{U}}'^{\circ}$, versus $\overline{\gamma}_{\rm B}$. Importantly, we observe that the adaptive transmission scheme achieves a higher effective secrecy throughput than the on-off transmission scheme. This is caused by the fact that the adaptive transmission scheme optimizes α and R_s based on $\tilde{\gamma}_{\rm B}$ in each transmission period. For the on-off transmission scheme, α and R_s are optimized based on $\overline{\gamma}_{\rm B}$ only once and used for all transmission periods. We also observe that the performance

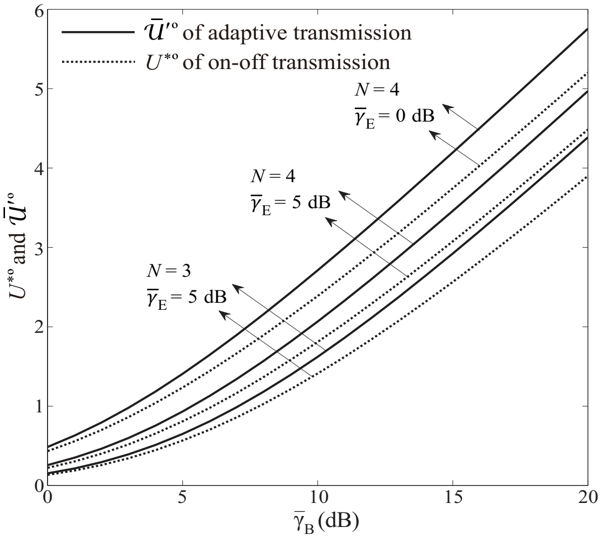

Fig. 11. Maximum effective secrecy throughput comparison between on-off transmission and adaptive transmission for $M = 2$.

gain of the adaptive transmission scheme over the on-off transmission scheme remains constant when $\bar{\gamma}_B$ is high.

V. Conclusions

In this work, we considered MISOME wiretap channels and investigated two transmission schemes with artificial noise, namely, the on-off transmission scheme and the adaptive transmission scheme. In order to determine the optimal transmission parameters, we analyzed the secure transmission probability and the effective secrecy throughput of both transmission schemes by deriving closed-form expressions. Built on these expressions, the optimal power allocation factor was first determined such that the secure transmission probability is maximized. The optimal secrecy rate were then determined such that the effective secrecy throughput is maximized. We verified our analysis with the aid of numerical results. Furthermore, we provided valuable insights into the impact of the number of antennas and the SNRs on the secrecy performance.

References

[1] D. Raychaudhuri and N. B. Mandayam, "Frontiers of wireless and mobile communications," *Proc. IEEE*, vol. 100, no. 4, pp. 824–840, Apr. 2012.

[2] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, "Communication security for smart grid distribution networks," *IEEE Commun. Mag.*, vol. 51, no. 1, pp. 42–49, Jan. 2013.

[3] 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 Signal Process. Mag.*, vol. 30, no. 5, pp. 29–40, Sept. 2013.

[4] B. Schneier, "Cryptographic design vulnerabilities," *Computer*, vol. 31, no. 9, pp. 29–33, Sept. 1998.

[5] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Techn. J.*, vol. 28, pp. 656–715, Oct. 1949.

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

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

[8] 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, July 1978.

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

[10] 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, June 2008.

[11] 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.

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

[13] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas–Part II: The MIMOME wireltap 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] B. He and X. Zhou, "Secure on-off transmission design with channel estimation errors," *Trans.Inf. Forensics Security.*, vol. 8, no. 12, pp. 1923–1936, Dec. 2013.

[17] I. Krikidis and B. Ottersten, "Secrecy sum-rate for orthogonal random beamforming with opportunistic scheduling," *IEEE Signal Process. Lett.*, vol. 20, no. 2, pp. 141–144, Feb. 2013.

[18] 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, June 2012.

[19] 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.

[20] 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.

[21] 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, Sept. 2013.

[22] 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.

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

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

[25] A. Mukherjee and A. L. Swindlehurst, "Utility of beamforming strategies for secrecy in multiuser MIMO wiretap channels," in *Proc. Allerton 2009*, Monticello, IL, Oct. 2009, pp. 1134–1141.

[26] 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.

[27] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.

[28] 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.

[29] 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.

[30] Y. Yang, W. Wang, H. Zhao, and L. Zhao, "Transmitter beamforming and artificial noise with delayed feedback: Secrecy rate and power allocation," *J. Commun. Netw.*, vol. 14, no. 4, pp. 374–384, Aug. 2012.

[31] 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.

[32] 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. Selected Areas Commun.*, vol. 31, no. 9, pp. 1728–1740, Sep. 2013.

[33] 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.

[34] 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, June 2013.

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

[36] 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. 993–998.

[37] 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. 2190–2196.

[38] N. Romero-Zurita, D. McLemon, M. Ghogho, and A. Swami, "PHY layer security based on protected zone and artificial noise," *IEEE Sig. Process. Lett.*, vol. 20, no. 5, pp. 487–490, May 2013.

[39] M. Ghogho and A. Swami, "Characterizing physical-layer secrecy with unknown eavesdropper locations and channels," in *Proc. IEEE ICASSP 2011*, Prague, Czech Republic, May 2011, pp. 3432–3435.

[40] T. Lo, "Maximal-ratio transmission," *IEEE Trans. Commun.*, vol. 47, no. 10, pp. 1458–1461, Oct. 1999.

[41] H. Gao, P. J. Smith, and M. V. Clark, "Theoretical reliability of MMSE linear diversity combining in Rayleigh-fading additive interference channels," *IEEE Trans. Commun.*, vol. 46, no. 5, pp. 666–672, May 1998.

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

[43] J. Li and A. P. Petropulu, "On ergodic secrecy rate for Gaussian MISO wiretap channels," *IEEE Trans. Wireless Commun.*, vol. 10, no. 4, pp. 1176–1187, Apr. 2011.

[44] X. Zhou, M. R. McKay, B. Maham, and A. Hjørungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, no. 3, pp. 302–305, Mar. 2011.

[45] S. Boyd and L. Vandenberghe, *Convex Optimization*, 1st ed., Cambridge University Press, Cambridge, UK, 2004.

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.

Maged Elkashlan (M'06) received the Ph.D. degree in Electrical Engineering from the University of British Columbia, Canada, 2006. From 2006 to 2007, he was with the Laboratory for Advanced Networking at University of British Columbia. From 2007 to 2011, he was with the Wireless and Networking Technologies Laboratory at Commonwealth Scientific and Industrial Research Organization (CSIRO), Australia. During this time, he held an adjunct appointment at University of Technology Sydney, Australia. In 2011, he joined the School of Electronic Engineering and Computer Science at Queen Mary University of London, UK, as an Assistant Professor. He also holds visiting faculty appointments at the University of New South Wales, Australia, and Beijing University of Posts and Telecommunications, China. His research interests fall into the broad areas of communication theory, wireless communications, and statistical signal processing for distributed data processing, millimeter wave communications, cognitive radio, and wireless security.

Dr. Elkashlan currently serves as an Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and the IEEE COMMUNICATIONS LETTERS. He also serves as the Lead Guest Editor for the special issue on "Green Media: The Future of Wireless Multimedia Networks" of the IEEE WIRELESS COMMUNICATIONS MAGAZINE, Lead Guest Editor for the special issue on "Millimeter Wave Communications for 5G" of the IEEE COMMUNICATIONS MAGAZINE, Guest Editor for the special issue on "Energy Harvesting Communications" of the IEEE COMMUNICATIONS MAGAZINE, and Guest Editor for the special issue on "Location Awareness for Radios and Networks" of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. He received the Best Paper Award at the IEEE Vehicular Technology Conference (VTC-Spring) in 2013. He received the Exemplary Reviewer Certificate of the IEEE Communications Letters in 2012.

Trung Q. Duong (S'05–M'12–SM'13) received his Ph.D. degree in Telecommunications Systems from Blekinge Institute of Technology (BTH), Sweden in 2012. Since 2013, he has joined Queen's University Belfast, UK as a Lecturer (Assistant Professor). His current research interests include cooperative communications, cognitive radio networks, physical layer security, massive MIMO, cross-layer design, mm-waves communications, and localization for radios and networks. He is the author or co-author of 170 technical papers published in scientific journals and presented at international conferences.

Dr. Duong currently serves as an Editor for the IEEE COMMUNICATIONS LETTERS, IET COMMUNICATIONS, and TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGIES. He has also served as the Guest Editor of the special issue on some major journals including IEEE JOURNAL IN SELECTED AREAS ON COMMUNICATIONS, IET COMMUNICATIONS, IEEE WIRELESS COMMUNICATIONS MAGAZINE, IEEE COMMUNICATIONS MAGAZINE, EURASIP JOURNAL ON WIRELESS COMMUNICATIONS AND NETWORKING, EURASIP JOURNAL ON ADVANCES SIGNAL PROCESSING. He was awarded the Best Paper Award at the IEEE Vehicular Technology Conference (VTC-Spring) in 2013 and the IEEE International Conference on Communications (ICC) in 2014.

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).