Three Artificial-Noise-Aided Secure Transmission Schemes in Wiretap Channels

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

***Abstract*—We examine the secrecy performance of three artificial-noise-aided secure transmission schemes, namely, the partially-adaptive, fully-adaptive, and on-off schemes. To this end, we provide new analysis to facilitate the optimization of the fraction ϕ of the transmit power allocated to the useful signal and redundancy rate R_{E}. Surprisingly, our examination indicates that the partially-adaptive scheme, in which only the codeword rate R_{B} varies with the instantaneous channel gains, significantly outperforms the on-off scheme, in which both R_{B} and R_{E} vary. This performance gain can be characterized in terms of a higher average secrecy rate, subject to an upper bound on the secrecy outage probability. Furthermore, our results also demonstrate that the partially-adaptive scheme can achieve almost the same secrecy performance as the fully-adaptive scheme, which is of a much higher complexity, where ϕ, R_{B}, and R_{E} all vary with the instantaneous channel gains.**

***Index Terms*—Physical layer security, artificial noise, power allocation, wiretap code rates, secure transmission.**

I. Introduction and Related Work

Security and privacy are critical in existing and future wireless networks since a large amount of confidential information is wirelessly transferred over the open medium [1]. Against this background, as a compatible and complementary technique to the conventional cryptography, physical layer security has been developed to address the security issues in wireless communications (e.g. [2–4]). Physical layer security offers progressively higher levels of security, conditioned on assumptions about the system model and adversary capabilities. In physical layer security, an eavesdropper (Eve) attempts to intercept the data transmission from a transmitter (Alice) to a legitimate receiver (Bob). The recent development of physical layer security in the context of multiple-input multiple-output (MIMO) techniques is in conjunction with artificial-noise-aided secure transmissions. Collectively, these techniques provide robustness and other desirable performance attributes in the passive eavesdropping scenario (e.g., [5, 6]).

In the literature, three different artificial-noise-aided secure transmission schemes, namely, partially-adaptive, fully-adaptive, and on-off schemes, have been proposed [7–9]. In the partially-adaptive scheme, only the codeword rate R_{B} is adaptively chosen based on the instantaneous channel state information (CSI) of the main channel from Alice to Bob, while the parameter ϕ, which denotes the fraction of the transmit power allocated to the useful signal ($1-\phi$ of the transmit power is allocated to the artificial noise (AN)), and the redundancy rate R_{E} are fixed [7]. In the fully-adaptive scheme, R_{B}, R_{E}, and ϕ are all adaptively varied with the instantaneous CSI of the main channel [8]. In the on-off scheme, both R_{B} and R_{E} are adaptively chosen as per the instantaneous CSI of the main channel, while ϕ is fixed [9]. This on-off scheme is different from the non-adaptive encoding scheme proposed and analyzed in [10, 11], where R_{B}, R_{E}, and ϕ are all fixed and independent of the instantaneous CSI of the main channel. As such, the complexity of the non-adaptive encoding scheme is lower than that of the on-off scheme and thus its secrecy performance would not be better than that of the on-off scheme. Therefore, we do not adopt the non-adaptive encoding scheme but the on-off scheme as one benchmark.

The secrecy performance comparison between the on-off and fully-adaptive schemes has been conducted in [8], which, as expected, shows that the fully-adaptive scheme outperforms the on-off scheme at the cost of a much higher complexity. The authors of [11] examined the secrecy performance of the non-adaptive encoding scheme and the fully-adaptive scheme, which demonstrates that the fully-adaptive scheme achieves a higher throughput than the non-adaptive encoding scheme. However, the secrecy performance of the partially-adaptive scheme compared with that of other schemes has never been thoroughly examined. This leaves an important gap in our understanding on the AN-aided secure transmission schemes and motivates this work.

In this work, we thoroughly examine the secrecy performance of the partially-adaptive scheme with the fully-adaptive and on-off schemes as benchmarks. To this end, we conduct novel analysis to facilitate the optimization of the power allocation parameter ϕ and the redundancy rate R_{E} in the partially-adaptive and fully-adaptive schemes. Specifically, we derive the closed-form expression for the average secrecy rate in the high signal-to-noise ratio (SNR) regime and prove the existence and uniqueness of the optimal R_{E} for any given ϕ in the partially-adaptive scheme. In addition, the optimal R_{E} and ϕ are analytically obtained for the fully-adaptive scheme in two asymptotic scenarios, where the requirement on the instantaneous CSI of the main channel is determined for secure transmission. Surprisingly, our examinations indicate that the partially-adaptive scheme significantly outperforms the on-off

S. Yan and N. Yang are with the Research School of Engineering, The Australian National University, Canberra, ACT, Australia (emails: {shihao.yan, nan.yang}@anu.edu.au). I. Land is with the French Research Centre, Huawei Technologies, Paris, France (email: ingmar.land@ieee.org). R. Malaney and J. Yuan are with the School of Electrical Engineering and Telecommunications, The University of New South Wales, Sydney, NSW, Australia (emails: {r.malaney, j.yuan}@unsw.edu.au). This work was supported by the Australian Research Council's Discovery Projects (DP150103905).

scheme in terms of achieving a much higher average secrecy rate subject to the constraint on the secrecy outage probability, while the complexity of these two schemes are similar. Furthermore, the partially-adaptive scheme can achieve almost the same secrecy performance as the fully-adaptive scheme that is of a much higher complexity.

II. System Model

We consider a wiretap channel where communication from an N-antenna Alice to a single-antenna Bob is overheard by a single-antenna Eve. We denote the main channel as the $1 \times N$ complex-valued vector $\mathbf{h}$ and the eavesdropper's channel from Alice to Eve as the $1 \times N$ complex-valued vector $\mathbf{g}$. Each entry of $\mathbf{h}$ and $\mathbf{g}$ is modeled as an independent and identically distributed (i.i.d.) Gaussian random variable. Considering passive eavesdropping, we assume that $\mathbf{g}$ is not available at Alice. We also assume that $\mathbf{h}$ is known exactly by Bob and fed back to Alice perfectly. We further assume that $\mathbf{h}$ is perfectly available at Eve, since the feedback from Bob to Alice may not be secure.

We next detail the AN-aided secure transmission in the considered wiretap channel. Alice transmits an information signal s_{I} in conjunction with an $(N-1) \times 1$ AN vector $\mathbf{s}_{\mathrm{N}}$ to Bob, where the variance of s_{I} is χ_{I} and each entry of $\mathbf{s}_{\mathrm{N}}$ has the variance χ_{N} [8]. We assume that the total transmit power used by Alice is P_{t}. We denote the fraction of the power allocated to s_{I} as ϕ such that $\chi_{\mathrm{I}} = \phi P_{\mathrm{t}}$, where $0 \leq \phi \leq 1$. Since Alice does not know $\mathbf{g}$, she equally distributes the transmit power of AN 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. To determine $\mathbf{V}$, Alice performs the eigenvalue decomposition of $\mathbf{F} \triangleq \mathbf{h}^H \mathbf{h}$, where $\mathbf{h}^H$ is the Hermitian transpose of $\mathbf{h}$. Then Alice chooses $\mathbf{v}_{\mathrm{I}}$ as the principal eigenvector corresponding to the largest eigenvalue of $\mathbf{F}$ and chooses $\mathbf{V}_{\mathrm{N}}$ as the remaining $N-1$ eigenvectors of $\mathbf{F}$ such that $\mathbf{V}_{\mathrm{N}}$ lies in the nullspace of $\mathbf{h}^H$. 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 satisfying $\mathbb{E}\left[n_{\mathrm{B}} n_{\mathrm{B}}^H\right] = \sigma_{\mathrm{B}}^2$. Based on (2), the instantaneous SNR at Bob is given by $\gamma_{\mathrm{B}} = \phi \overline{\gamma}_{\mathrm{B}} \|\mathbf{h}\|^2$, where $\overline{\gamma}_{\mathrm{B}} = P_{\mathrm{t}}/\sigma_{\mathrm{B}}^2$. As such, the probability density function (pdf) of γ_{B} is [8]

$$f_{\gamma_B}(\gamma) = \frac{\gamma^{N-1} e^{-\frac{\gamma}{\phi \overline{\gamma}_{\mathrm{B}}}}}{(\phi \overline{\gamma}_{\mathrm{B}})^N \Gamma(N)}, \tag{3}$$

and the cumulative distribution function (cdf) of γ_{B} is

$$F_{\gamma_B}(\gamma) = 1 - \frac{\Gamma\left(N, \frac{\gamma}{\phi \overline{\gamma}_{\mathrm{B}}}\right)}{\Gamma(N)} = 1 - e^{-\frac{\gamma}{\phi \overline{\gamma}_{\mathrm{B}}}} \sum_{n=0}^{N-1} \frac{1}{n!} \left(\frac{\gamma}{\phi \overline{\gamma}_{\mathrm{B}}}\right)^n. \tag{4}$$

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

$$z = \mathbf{g}\mathbf{x} + n_{\mathrm{E}} = \mathbf{g}\mathbf{v}_{\mathrm{I}} s_{\mathrm{I}} + \mathbf{g}\mathbf{V}_{\mathrm{N}} \mathbf{s}_{\mathrm{N}} + n_{\mathrm{E}}, \tag{5}$$

where n_{E} is the AWGN at Eve satisfying $\mathbb{E}\left[n_{\mathrm{E}} n_{\mathrm{E}}^H\right] = \sigma_{\mathrm{E}}^2$. It is crucial to clarify that although Eve knows $\mathbf{h}$ and $\mathbf{V}$, she cannot eliminate the interference caused by $\mathbf{V}_{\mathrm{N}} \mathbf{s}_{\mathrm{N}}$ due to the existence of n_{E} (i.e., a non-zero σ_{E}^2). If $\sigma_{\mathrm{E}}^2 = 0$, i.e., Eve is a noise-free device, she can eliminate this interference when she is equipped with more antennas than Alice. Following (5), the instantaneous signal-to-interference-plus-noise ratio (SINR) at Eve is given by [8]

$$\gamma_{\mathrm{E}} = \frac{\phi \overline{\gamma}_{\mathrm{E}} \|\mathbf{g}\mathbf{v}_{\mathrm{I}}\|^2}{\frac{1-\phi}{N-1} \overline{\gamma}_{\mathrm{E}} \|\mathbf{g}\mathbf{V}_{\mathrm{N}}\|^2 + 1}, \tag{6}$$

where $\overline{\gamma}_{\mathrm{E}} = P_{\mathrm{t}}/\sigma_{\mathrm{E}}^2$. In the wiretap channel, we assume that $\overline{\gamma}_{\mathrm{B}}$ and $\overline{\gamma}_{\mathrm{E}}$ are publicly known. If Alice does not know them, she is still able to perform the AN-aided secure data transmission, but not able to calculate the secrecy performance metrics. Following (6), the cdf of γ_{E} is obtained as [8]

$$F_{\gamma_E}(\gamma) = 1 - \left(1 + \frac{(1-\phi)\gamma}{\phi(N-1)}\right)^{1-N} e^{-\frac{\gamma}{\phi \overline{\gamma}_{\mathrm{E}}}}. \tag{7}$$

III. Three AN-Aided Secure Transmission Schemes

In this section, we first detail the three AN-aided secure transmission schemes. We then formalize the optimization of the power allocation parameter ϕ and redundancy rate R_{E} for the three schemes. We also provide novel analysis on the relationship between ϕ and R_{E} in the partially-adaptive and fully-adaptive schemes to facilitate the optimization.

A. Partially-Adaptive Scheme

In the partially-adaptive scheme, R_{B} is set such as $R_{\mathrm{B}} = C_{\mathrm{B}}$ and R_{E} is fixed for each pair of $\overline{\gamma}_{\mathrm{B}}$ and $\overline{\gamma}_{\mathrm{E}}$, where $C_{\mathrm{B}} = \log_2(1+\gamma_{\mathrm{B}})$ [7]. A secure transmission requires a positive secrecy rate, i.e., $R_s = C_{\mathrm{B}} - R_{\mathrm{E}} > 0$, and thus Alice only transmits signals when $C_{\mathrm{B}} > R_{\mathrm{E}}$. As such, the transmission probability of the partially-adaptive scheme is

$$P_p(\phi, R_{\mathrm{E}}) = \Pr(C_{\mathrm{B}} > R_{\mathrm{E}}) = \frac{\Gamma\left(N, \frac{2^{R_{\mathrm{E}}}-1}{\phi \overline{\gamma}_{\mathrm{B}}}\right)}{\Gamma(N)}. \tag{8}$$

Then, for given ϕ and R_{E} its average secrecy rate is

$$\begin{aligned} \overline{R}_p(\phi, R_{\mathrm{E}}) &= \mathbb{E}\left[C_{\mathrm{B}} - R_{\mathrm{E}}\right]^+ \\ &= \int_{2^{R_{\mathrm{E}}}-1}^{\infty} \left[C_{\mathrm{B}} - R_{\mathrm{E}}\right]^+ f_{\gamma_{\mathrm{B}}}(\gamma_{\mathrm{B}}) d\gamma_{\mathrm{B}}, \end{aligned} \tag{9}$$

where $[x]^+ = \max\{0, x\}$. The closed-form expression for $\overline{R}_p(\phi, R_{\mathrm{E}})$ is mathematically intractable due to the complicated integration in (9). As such, we derive a compact expression for $\overline{R}_p(\phi, R_{\mathrm{E}})$ for the high SNR regime in the following proposition.

Proposition 1: In the high SNR regime, the average secrecy rate of the partially-adaptive scheme is derived as

$$\begin{aligned} \overline{R}_p(\phi, R_{\mathrm{E}}) = & \frac{1}{\ln(2)\Gamma(N)} \mathbf{G}_{2,3}^{3,0}\left(\begin{matrix} 1,1 \\ 0,0,N \end{matrix} \middle| \frac{2^{R_{\mathrm{E}}}-1}{\overline{\gamma}_{\mathrm{B}}} \right) \\ & + \frac{\log_2(2^{R_{\mathrm{E}}}-1)}{\Gamma(N)} \Gamma\left(N, \frac{2^{R_{\mathrm{E}}}-1}{\phi \overline{\gamma}_{\mathrm{B}}}\right) - \frac{R_{\mathrm{E}} \Gamma\left(N, \frac{2^{R_{\mathrm{E}}}-1}{\phi \overline{\gamma}_{\mathrm{B}}}\right)}{\Gamma(N)}, \end{aligned} \tag{10}$$

where $\mathbf{G}_{m,n}^{p,q}\left(\begin{array}{c} a_1,\dots,a_p \\ b_1,\dots,b_q \end{array} \middle| \, x \right)$ is the Meijer's G-Function given by [12, Eq. (9.301)].

Proof: In the high SNR regime, we can approximte C_{B} as $C_{\text{B}} = \log_2(\gamma_{\text{B}})$. Then, substituting (3) and (4) into (9), we have

$$\begin{aligned}\overline{R}_p(\phi, R_{\text{E}}) &= \int_{2^{R_{\text{E}}-1}}^{\infty} C_{\text{B}} f_{\gamma_{\text{B}}}(\gamma_{\text{B}}) d\gamma_{\text{B}} - R_{\text{E}} \left(1 - F_{\gamma_{\text{B}}}\left(2^{R_{\text{E}}} - 1\right)\right), \\ &= \int_{2^{R_{\text{E}}-1}}^{\infty} \frac{\ln(\gamma_{\text{B}})}{\ln(2)} \frac{\gamma_{\text{B}}^{N-1} e^{-\frac{\gamma_{\text{B}}}{\phi\overline{\gamma}_{\text{B}}}}}{(\phi\overline{\gamma}_{\text{B}})^N \Gamma(N)} d\gamma_{\text{B}} - \frac{R_{\text{E}} \Gamma\left(N, \frac{2^{R_{\text{E}}}-1}{\phi\overline{\gamma}_{\text{B}}}\right)}{\Gamma(N)}.\end{aligned} \tag{11}$$

Following the definition of the Meijer's G-Function, we have

$$\begin{aligned}&\frac{1}{b^n} \int_{a}^{\infty} \ln(x) x^{n-1} e^{-\frac{x}{b}} dx \\ &= \mathbf{G}_{2,3}^{3,0}\left(\begin{array}{c} 1,1 \\ 0,0,n \end{array} \middle| \, \frac{a}{b} \right) + \ln(a)\Gamma\left(n, \frac{a}{b}\right).\end{aligned} \tag{12}$$

Then, substituting (12) into (11) we obtain the desired result in (10) after some algebraic manipulations, which completes the proof of this proposition. ■

The compact expression given in (10) allows us to efficiently examine the secrecy performance of the partially-adaptive scheme, based on which some system parameters can be optimized via numerical search methods, without incurring time-consuming Monte Carlo simulations.

In the partially-adaptive scheme, the secrecy outage occurs when $C_{\text{E}} > R_{\text{E}}$ conditioned on a transmission, where $C_{\text{E}} = \log_2(1+\gamma_{\text{E}})$. Thus, its secrecy outage probability is given by

$$\begin{aligned}\mathcal{O}_p(\phi, R_{\text{E}}) &= \Pr(C_{\text{E}} > R_{\text{E}} | C_{\text{B}} > R_{\text{E}}) = \Pr(C_{\text{E}} > R_{\text{E}}) \\ &= 1 - F_{\gamma_{\text{E}}}\left(2^{R_{\text{E}}} - 1\right) = \tau^{1-N} e^{-\frac{\left(2^{R_{\text{E}}-1}\right)}{\phi\overline{\gamma}_{\text{E}}}},\end{aligned} \tag{13}$$

where

$$\tau = 1 + \frac{(1-\phi)\left(2^{R_{\text{E}}} - 1\right)}{\phi(N-1)}, \tag{14}$$

since C_{B} and C_{E} are independent from each other.

In the partially-adaptive scheme, in addition to R_{E}, ϕ is fixed for each pair of $\overline{\gamma}_{\text{B}}$ and $\overline{\gamma}_{\text{E}}$. The optimal values of R_{E} and ϕ in the partially-adaptive scheme can be obtained through

$$(\phi^{\dagger}, R_{\text{E}}^{\dagger}) = \underset{0<\phi\leq 1, R_{\text{E}}}{\operatorname{argmax}} \overline{R}_p(\phi, R_{\text{E}}), \text{s.t. } \mathcal{O}_p(\phi, R_{\text{E}}) \leq p_0. \tag{15}$$

Due to the intractable expression of $\overline{R}_p(\phi, R_{\text{E}})$, it is hard, if not impossible, to prove the concavity of (15) with respect to both R_{E} and ϕ. Noting the closed interval of ϕ (i.e., $0 \leq \phi \leq 1$), in the following proposition we analytically prove that for any given ϕ there is a unique solution to R_{E} that maximizes $\overline{R}_p(\phi, R_{\text{E}})$ subject to $\mathcal{O}_p(\phi, R_{\text{E}}) \leq p_0$.

Proposition 2: For any given ϕ, there is a unique value of R_{E} that maximizes $\overline{R}_p(\phi, R_{\text{E}})$ subject to $\mathcal{O}_p(\phi, R_{\text{E}}) \leq p_0$ and this value is the one that guarantees $\mathcal{O}_p(\phi, R_{\text{E}}) = p_0$.

Proof: If we can prove that for any given ϕ, both $\overline{R}_p(\phi, R_{\text{E}})$ and $\mathcal{O}_p(\phi, R_{\text{E}})$ are monotonic decreasing functions of R_{E}, this proposition can be proved. As such, we next derive the first derivatives of $\overline{R}_p(\phi, R_{\text{E}})$ and $\mathcal{O}_p(\phi, R_{\text{E}})$ with respect to R_{E}, respectively. Following (9) and the Leibniz's rule, we have

$$\begin{aligned}\frac{\partial \overline{R}_p(\phi, R_{\text{E}})}{\partial R_{\text{E}}} &= -[C_{\text{B}} - R_{\text{E}}]^{+} f_{\gamma_{\text{B}}}(\gamma_{\text{B}}) 2^{R_{\text{E}}} \ln(2) \\ &\quad - \int_{2^{R_{\text{E}}}-1}^{\infty} f_{\gamma_{\text{B}}}(\gamma_{\text{B}}) d\gamma_{\text{B}}.\end{aligned} \tag{16}$$

By noting that $[C_{\text{B}} - R_{\text{E}}]^{+} \geq 0$ and $f_{\gamma_{\text{B}}}(\gamma_{\text{B}}) \geq 0$, we find that $\partial \overline{R}_p(\phi, R_{\text{E}}) / \partial R_{\text{E}} < 0$, which proves that $\overline{R}_p(\phi, R_{\text{E}})$ monotonically decreases with R_{E}. Following (13), the first derivative of $\mathcal{O}_p(\phi, R_{\text{E}})$ with respect to R_{E} is derived as

$$\begin{aligned}\frac{\partial \mathcal{O}_p(\phi, R_{\text{E}})}{\partial R_{\text{E}}} &= -\frac{2^{R_{\text{E}}} \ln(2)}{\phi\overline{\gamma}_{\text{E}}} e^{-\frac{\left(2^{R_{\text{E}}-1}\right)}{\phi\overline{\gamma}_{\text{E}}}} \tau^{1-N} \\ &\quad - \frac{1-\phi}{\phi} e^{-\frac{\left(2^{R_{\text{E}}-1}\right)}{\phi\overline{\gamma}_{\text{E}}}} \tau^{-N}.\end{aligned} \tag{17}$$

By noting $\tau > 0$ as per (14) due to $N > 1$, we find that $\partial \mathcal{O}_p(\phi, R_{\text{E}}) / \partial R_{\text{E}} < 0$, which proves that $\mathcal{O}_p(\phi, R_{\text{E}})$ is a monotonic decreasing function of R_{E}. ■

According to Proposition 2, we conclude that for any given ϕ the optimal R_{E} can be searched by increasing R_{E} from zero to the value of it that ensures $\mathcal{O}_p(\phi, R_{\text{E}}) = p_0$. Then, the optimization problem in (15) can be solved by a two-dimension numerical search method. To further facilitate the numerical search, we derive closed-form expressions for R_{E} as functions of ϕ in the following asymptotic scenarios, which can reduce the two-dimensional numerical search to a one-dimensional numerical search.

Proposition 3: As $N \to \infty$, the optimal R_{E} for a given ϕ is given by

$$R'_{\text{E}}(\phi) = \log_2\left(1 - \frac{\phi\overline{\gamma}_{\text{E}} \ln p_0}{(1-\phi)\overline{\gamma}_{\text{E}} + 1}\right). \tag{18}$$

Proof: As $N \to \infty$, $F_{\gamma_E}(\gamma)$ in (7) is approximated as

$$F_{\gamma_E}(\gamma) \approx 1 - e^{-\left(\frac{1-\phi}{\phi} + \frac{1}{\phi\overline{\gamma}_{\text{E}}}\right)\gamma}. \tag{19}$$

Then, by setting $\mathcal{O}_p(\phi, R_{\text{E}}) = p_0$ we achieve the desirable result in (18). ■

Proposition 4: As $\overline{\gamma}_{\text{E}} \to \infty$, the optimal R_{E} for a given ϕ is given by

$$R'_{\text{E}}(\phi) = \log_2\left(1 + \frac{\phi(N-1)\left(p_0^{1/(1-N)} - 1\right)}{1-\phi}\right). \tag{20}$$

Proof: As $\overline{\gamma}_{\text{E}} \to \infty$, $F_{\gamma_E}(\gamma)$ in (7) is approximated as

$$F_{\gamma_E}(\gamma) \approx 1 - \left(1 + \frac{(1-\phi)\gamma}{\phi(N-1)}\right)^{1-N}, \tag{21}$$

which leads to the desirable result in (20). ■

B. Fully-Adaptive Scheme

In the fully-adaptive scheme, R_{B} is chosen such that $R_{\text{B}} = C_{\text{B}}$ and R_{E} is adaptively chosen for each $\tilde{\gamma}_{\text{B}} = \overline{\gamma}_{\text{B}} \|\mathbf{h}\|^2$ [8]. Thus, its instantaneous secrecy rate as a function of ϕ and R_{E} is given by

$$R_s(\phi, R_{\text{E}}) = [C_{\text{B}} - R_{\text{E}}]^{+} = [\log_2(1 + \phi\tilde{\gamma}_{\text{B}}) - R_{\text{E}}]^{+}. \tag{22}$$

Since R_{B}, R_{E}, and ϕ are all adaptively chosen, $R_s(\phi, R_{\mathrm{E}}) > 0$ can be always guaranteed in the fully-adaptive scheme. As such, without considering any constraint on the secrecy outage probability, Alice always transmits confidential information to Bob with a positive $R_s(\phi, R_{\mathrm{E}})$. However, a secrecy outage occurs when $C_{\mathrm{E}} > R_{\mathrm{E}}$. Thus, the secrecy outage probability of the fully-adaptive scheme is

$$\mathcal{O}_f(\phi, R_{\mathrm{E}}) = \Pr(C_{\mathrm{E}} > R_{\mathrm{E}}) = \tau^{1-N} e^{-\frac{\left(2^{R_{\mathrm{E}-1}}\right)}{\phi \overline{\gamma}_{\mathrm{E}}}}. \tag{23}$$

In the fully-adaptive scheme, both ϕ and R_{E} are to be optimized in order to maximize the instantaneous secrecy rate $R_s(\phi, R_{\mathrm{E}})$ for each $\widetilde{\gamma}_{\mathrm{B}}$, subject to an upper bound on $\mathcal{O}_f(\phi, R_{\mathrm{E}})$. Then, the optimal values of ϕ and R_{E} in the fully-adaptive scheme can be obtained through

$$\begin{aligned}(\phi^{\ddagger}, R_{\mathrm{E}}^{\ddagger}) = & \underset{0<\phi\leq 1, 0<R_{\mathrm{E}}<C_{\mathrm{B}}}{\operatorname{argmax}} \; R_s(\phi, R_{\mathrm{E}}), \\ & \text{s.t. } \mathcal{O}_f(\phi, R_{\mathrm{E}}) \leq p_0. \end{aligned} \tag{24}$$

Noting $\mathcal{O}_f(\phi, R_{\mathrm{E}}) = \mathcal{O}_p(\phi, R_{\mathrm{E}})$ and that $R_s(\phi, R_{\mathrm{E}})$ monotonically decreases with R_{E} as per (22), according to Proposition 2 we can conclude that for any given ϕ, there is a unique value of R_{E} that maximizes $R_s(\phi, R_{\mathrm{E}})$ subject to $\mathcal{O}_f(\phi, R_{\mathrm{E}}) \leq p_0$ and this value is the one that guarantees $\mathcal{O}_f(\phi, R_{\mathrm{E}}) = p_0$. Since the optimization is conducted for each $\widetilde{\gamma}_B$ in (24), the signal processing complexity for the fully-adaptive scheme is much higher than those for the partially-adaptive and on-off schemes. We would like to highlight that $\phi^{\ddagger}$ and $R_{\mathrm{E}}^{\ddagger}$ can be derived in closed-form expressions for each $\widetilde{\gamma}_B$ in the following asymptotic scenarios. Such closed-form expressions are analytical solutions to (24).

***Proposition** 5:* As $N \to \infty$, the optimal values of ϕ and R_{E} are given by

$$\begin{aligned} \phi^{\ddagger} &= \sqrt{\frac{\ln p_0 \left[(1 + \ln p_0 + \widetilde{\gamma}_{\mathrm{B}})\overline{\gamma}_{\mathrm{E}} + \widetilde{\gamma}_{\mathrm{B}}\right]}{-\overline{\gamma}_{\mathrm{E}}^2 \widetilde{\gamma}_{\mathrm{B}} (1 + \ln p_0)^2 (\overline{\gamma}_{\mathrm{E}} + 1)^{-1}}} - \frac{\overline{\gamma}_{\mathrm{E}} + 1}{\overline{\gamma}_{\mathrm{E}}(1 + \ln p_0)}, \\ R_{\mathrm{E}}^{\ddagger} &= \log_2 \left(1 - \frac{\phi^{\ddagger} \overline{\gamma}_{\mathrm{E}} \ln p_0}{(1 - \phi^*)\overline{\gamma}_{\mathrm{E}} + 1}\right), \end{aligned}$$

where $\widetilde{\gamma}_{\mathrm{B}} > -\overline{\gamma}_{\mathrm{E}} \ln p_0 / (\overline{\gamma}_{\mathrm{E}} + 1)$.

Proof: Due to $\mathcal{O}_f(\phi, R_{\mathrm{E}}) = \mathcal{O}_p(\phi, R_{\mathrm{E}})$, Proposition 3 is also valid for the fully-adaptive scheme. Substituting (18) into $R_s(\phi, R_{\mathrm{E}})$ in (22), we have the instantaneous secrecy rate as

$$R_s(\phi, R_{\mathrm{E}}^{\dagger}(\phi)) = \log_2(1 + \phi \widetilde{\gamma}_{\mathrm{B}}) - \log_2 \left(1 - \frac{\phi \overline{\gamma}_{\mathrm{E}} \ln p_0}{(1-\phi)\overline{\gamma}_{\mathrm{E}} + 1}\right). \tag{25}$$

Guaranteeing $R_s(\phi, R_{\mathrm{E}}^{\dagger}(\phi)) > 0$ leads to

$$\widetilde{\gamma}_{\mathrm{B}} > -\frac{\overline{\gamma}_{\mathrm{E}} \ln p_0}{(1 - \phi)\overline{\gamma}_{\mathrm{E}} + 1} > -\frac{\overline{\gamma}_{\mathrm{E}} \ln p_0}{\overline{\gamma}_{\mathrm{E}} + 1}. \tag{26}$$

Following (25), we define

$$g(\phi) \triangleq 2^{R_s(\phi, R_{\mathrm{E}}^{\dagger}(\phi))} = A\phi + B + \frac{C}{D\phi + E}, \tag{27}$$

$$\begin{aligned} A &= \frac{\widetilde{\gamma}_{\mathrm{B}}}{1 + \ln p_0}, \; C = (\overline{\gamma}_{\mathrm{E}} + 1)(1 - B), \\ B &= \frac{\widetilde{\gamma}_{\mathrm{B}}(\overline{\gamma}_{\mathrm{E}} + 1)}{\overline{\gamma}_{\mathrm{E}}(1 + \ln p_0)^2} - \frac{\widetilde{\gamma}_{\mathrm{B}} - \overline{\gamma}_{\mathrm{E}} + \widetilde{\gamma}_{\mathrm{B}}\overline{\gamma}_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}(1 + \ln p_0)}, \\ D &= -\overline{\gamma}_{\mathrm{E}}(1 + \ln p_0), \; E = \overline{\gamma}_{\mathrm{E}} + 1. \end{aligned} \tag{28}$$

Maximizing $R_s(\phi, R_{\mathrm{E}}^{\dagger}(\phi))$ is equivalent to maximizing $g(\phi)$ as per (27). We next prove that $g(\phi)$ is a concave function of ϕ. Following (27), we have $\partial^2 g(\phi)/\partial^2 \phi = 2D^2 C/(D\phi + E)^3$. It is easy to prove that $(D\phi + E)^3 > 0$. Thus, the concavity only requires $C < 0$, which requires $1 - B < 0$, since $C = (\overline{\gamma}_{\mathrm{B}} + 1)(1 - B)$ and $\overline{\gamma}_{\mathrm{B}} + 1 > 0$. Following (28), we have

$$1 - B = \frac{\overline{\gamma}_{\mathrm{E}}(1 + \ln p_0)\ln p_0 + \widetilde{\gamma}_{\mathrm{B}}(1 + \overline{\gamma}_{\mathrm{E}})\ln p_0}{(1 + \ln p_0)^2 \overline{\gamma}_{\mathrm{E}}}. \tag{29}$$

Using (26) and noting $p_0 < 1$, we have

$$\widetilde{\gamma}_{\mathrm{B}}(1 + \overline{\gamma}_{\mathrm{E}}) \ln p_0 < -\overline{\gamma}_{\mathrm{E}}(\ln p_0)^2. \tag{30}$$

Substituting (30) into (29) and noting $p_0 < 1$, we have

$$1 - B < \frac{\ln p_0}{(1 + \ln p_0)^2} < 0. \tag{31}$$

As such, we have proved that $g(\phi)$ is a concave function of ϕ and we achieve the desirable results presented in Proposition 5 by setting $\mathcal{O}_f(\phi, R_{\mathrm{E}}) = p_0$ and $\partial g(\phi)/\partial \phi = 0$. ■

***Proposition** 6:* As $\overline{\gamma}_{\mathrm{E}} \to \infty$, the optimal values of ϕ and R_{E} are given by

$$\begin{aligned} \phi^{\ddagger} &= \sqrt{\frac{1}{\widetilde{\gamma}_{\mathrm{B}}} \left(\frac{2\widetilde{\gamma}_{\mathrm{B}}}{\alpha - 1} + \frac{\widetilde{\gamma}_{\mathrm{B}}}{(\alpha - 1)^2} - 1\right)} - \frac{1}{\alpha - 1}, \\ R_{\mathrm{E}}^{\ddagger} &= \log_2 \left(1 - \frac{\phi^{\ddagger}\alpha}{(1 - \phi^{\ddagger})}\right), \end{aligned}$$

where $\widetilde{\gamma}_{\mathrm{B}} > -\ln(p_0)$ and α is given by

$$\alpha = (N - 1)\left(p_0^{\frac{1}{1-N}} - 1\right). \tag{32}$$

Proof: The proof follows from Proposition 4 and is similar to that of Proposition 5, which is omitted here. ■

We note that the maximum instantaneous secrecy rate $R_s(\phi^{\ddagger}, R_{\mathrm{E}}^{\ddagger})$ is still a function of $\widetilde{\gamma}_{\mathrm{B}}$ (and thus of $\|\mathbf{h}\|$). In order to conduct the performance comparison among the three schemes, we have to calculate the average maximum secrecy rate of the fully-adaptive scheme over $\|\mathbf{h}\|$, which is given by

$$\overline{R}_f^{\ddagger} = \int_0^{\infty} R_s(\phi^{\ddagger}, R_{\mathrm{E}}^{\ddagger}) f_{\widetilde{\gamma}_{\mathrm{B}}}(\widetilde{\gamma}_{\mathrm{B}}) d\widetilde{\gamma}_{\mathrm{B}}, \tag{33}$$

where $f_{\widetilde{\gamma}_{\mathrm{B}}}(\widetilde{\gamma}_{\mathrm{B}})$ denotes the pdf of $\widetilde{\gamma}_{\mathrm{B}}$ given in [8].

C. On-Off Scheme

In the on-off scheme, R_{B} is set such that $R_{\mathrm{B}} = C_{\mathrm{B}}$ and the secrecy rate R_s is fixed for each pair of $\overline{\gamma}_{\mathrm{B}}$ and $\overline{\gamma}_{\mathrm{E}}$ [5]. Thus, we have the redundancy rate as $R_{\mathrm{E}} = C_{\mathrm{B}} - R_s$, which varies with C_{B} as well. Alice only transmits confidential information to Bob when $C_{\mathrm{B}} > R_s$, and thus the transmission probability of the on-off scheme is

$$P_o(\phi, R_s) = \Pr(C_{\mathrm{B}} > R_s) = \frac{\Gamma\left(N, \frac{2^{R_s} - 1}{\phi \overline{\gamma}_{\mathrm{B}}}\right)}{\Gamma(N)}. \tag{34}$$

Then, the average secrecy rate achieved by the on-off scheme can be written as

$$\overline{R}_o(\phi, R_s) = R_s P_o(\phi, R_s). \tag{35}$$

The secrecy outage probability conditioned on a transmission of the on-off scheme is given by

$$\mathcal{O}_o(\phi, R_s) = \Pr(C_{\rm E} > R_{\rm E} | C_{\rm B} > R_s) \\ = 1 - \frac{1 - \Pr(C_s < R_s)}{P_o(\phi, R_s)}, \quad (36)$$

where $\Pr(C_s < R_s)$ is the hybrid secrecy outage probability given by [8, Eq. (18)].

In the on-off scheme, in addition to R_s, ϕ is fixed for each pair of $\overline{\gamma}_{\rm B}$ and $\overline{\gamma}_{\rm E}$. Thus, the optimal values of ϕ and R_s in the on-off scheme can be achieved through

$$(\phi^*, R_s^*) = \underset{0<\phi\leq 1, R_s}{\operatorname{argmax}} \; \overline{R}_o(\phi, R_s), \text{ s.t. } \mathcal{O}_o(\phi, R_s) \leq p_0. \quad (37)$$

We note that $\overline{R}_o(\phi, R_s)$ is not a monotonic function of R_s, since $P_o(\phi, R_s)$ monotonically decreases with R_s. As such, in the optimization presented in (37) we may not have $\mathcal{O}_o(\phi, R_s) = p_0$. Due to the complicated expression of $\mathcal{O}_o(\phi, R_s)$ given in (36), the uniqueness of ϕ and R_s cannot be theoretically proved and thus we adopt a two-dimensional numerical search to solve the optimization problem in (37).

IV. Secrecy Performance Comparison

We present the secrecy performance comparison among the three different AN-aided secure transmission schemes in Fig. 1. We first observe that $\overline{R}_p(\phi^\dagger, R_{\rm E}^\dagger)$ is much higher than $\overline{R}_o(\phi^*, R_{\rm E}^*)$, which means that the partially-adaptive scheme dramatically outperforms the on-off scheme. This is due to the fact that when the main channel cannot support a fixed secrecy rate R_s^* under the secrecy constraint in the on-off scheme, a positive secrecy rate $C_{\rm B} - R_{\rm E}^\dagger$ can still be achieved in the partially-adaptive scheme. We note that the complexity of the partially-adaptive scheme is slightly lower than that of the on-off scheme, which is due to the fact that both $R_{\rm B}$ and $R_{\rm E}$ have to be adjusted for each $\|\mathbf{h}\|$ in the on-off scheme, while only $R_{\rm B}$ varies in the partially-adaptive scheme.

The negligible advantage of the the fully-adaptive scheme compared with the partially-adaptive scheme is unexpected, since ϕ, $R_{\rm B}$, and $R_{\rm E}$ are chosen adaptively for each $\mathbf{h}$ in the fully-adaptive scheme. The fact that only a minor advantage is forthcoming for the fully-adpative scheme can be explained as follows. Under the constraint $\mathcal{O}_f(\phi, R_{\rm E}) \leq p_0$, in the fully-adaptive scheme a positive secrecy rate is achievable only when $\widetilde{\gamma}_B$ is larger than some specific value, not for every $\widetilde{\gamma}_B$. This is explicitly confirmed by (26) in the asymptotic scenarios. Thus, under the constraint $\mathcal{O}_f(\phi, R_{\rm E}) \leq p_0$, Alice actually does not always transmit confidential information in the fully-adaptive scheme, which is similar to what incurs in the partially-adaptive scheme. We note that the complexity of the fully-adaptive scheme is much higher than those of the partially-adaptive and on-off schemes. This is due to the fact that ϕ and $R_{\rm E}$ (or R_s) are optimized for each instantaneous CSI of the main channel (i.e., $\|\mathbf{h}\|$) in the fully-adaptive scheme, while they only have to be optimized for each pair of the average SNRs (i.e., each pair of $\overline{\gamma}_{\rm B}$ and $\overline{\gamma}_{\rm E}$) in the partially-adaptive and on-off schemes.

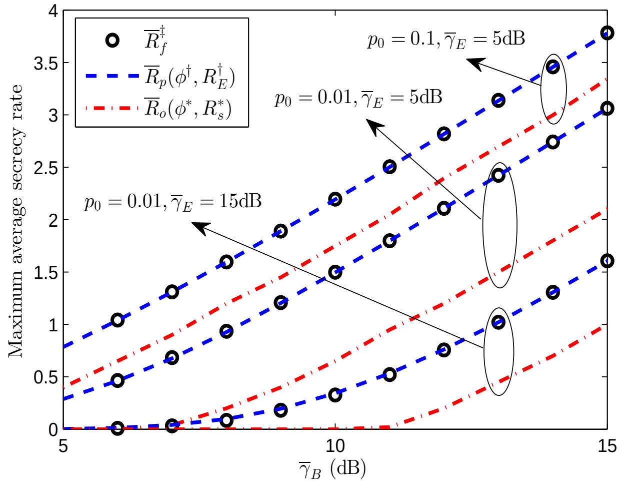

Fig. 1. Maximum average secrecy rate of the three schemes subject to the upper bound p_0 on the secrecy outage probability with $N = 4$ and 2 antennas at Eve with the minimum mean square error (MMSE) combiner.

V. Conclusion

This work thoroughly examined the secrecy performance of the partially-adaptive, fully-adaptive, and on-off schemes. Unexpectedly, our examination demonstrates that the partially-adaptive scheme significantly outperforms the on-off scheme, which is of a similar complexity, and achieves almost the same secrecy performance as the fully-adaptive scheme, which is of a much higher complexity.

References

[1] T. Q. Duong, X. Zhou, and H. V. Poor (Eds.), *Trusted communications with physical layer security for 5G and beyond*, UK: IET Publisher, 2016.

[2] 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. 37–375, Jun. 2012.

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

[4] P. Yeoh, K. Kim, T. Duong, G. Karagiannidis, "Transmit antenna selection in cognitive MIMO relaying with multiple primary transceivers," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 483–489, Jan. 2016.

[5] H. Wang, C. Wang, and D. W. K. Ng, "Artificial noise assisted secure transmission under training and feedback," *IEEE Trans. Signal Process.*, vol. 63, no. 23, pp. 6285–6298, Dec. 2015.

[6] Y. Deng, L. Wang, S. A. R. Zaidi, J. Yuan and M. Elkashlan, "Aritificial-noise aided secure transmission in large scale spectrum sharing networks," *IEEE Trans. Commun.*, vol. 64, no. 5, pp. 2116–2129, May 2016.

[7] R. Subramanian and I. Land, "The role of artificial noise in multi-antenna fading wiretap channels: Useful or harmful?" in *Proc. IEEE Information Theory Workshop*, Nov. 2014, pp. 641–645.

[8] N. Yang, S. Yan, J. Yuan, R. Malaney, R. Subramanian, and I. Land, "Artificial noise: Transmission optimization in Multi-Input Single-Output wiretap channels," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1771–1783, May 2015.

[9] T. Zheng, H. Wang, J. Yuan, D. Towsley, and M. H. Lee "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4347–4362, Nov. 2015.

[10] X. Zhang, X. Zhou, and M. R. McKay, "Benefits of multiple transmit antennas in secure communication: A secrecy outage viewpoint," in *Proc. Asilomar Conf. Signals Syst. Comput.*, Nov. 2011, pp. 212–216.

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

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