On Different Artificial-Noise Aided Transmission Schemes in MISOME Wiretap Channels

Shihao Yan, Ramanan Subramanian, Nan Yang, Ingmar Land, Robert Malaney, and Jinhong Yuan

***Abstract*—**

***Index Terms*—**

I. System Model

We consider an MISOME wiretap channel 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 $\mathbf{f}$ and denote the eavesdropper's channel between Alice and Eve as an $M \times N$ matrix $\mathbf{G}$. The entries of $\mathbf{f}$ and $\mathbf{G}$ are modeled as independent and identically distributed (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 block fading with equal block length. We further assume that $N > M$ since Eve is able to remove the artificial noise signals if $N \leq M$ [1]. In this wiretap channel, we consider that the instantaneous information of $\mathbf{G}$ is not available to Alice. Moreover, we consider that $\mathbf{f}$ is precisely estimated by Bob and fed back to Alice. We further consider that $\mathbf{f}$ 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} [1]. We assume that the total transmit power used by Alice is P_{T}. We denote the fraction of the power allocated to s_{I} by ϕ such that $\chi_{\mathrm{I}} = \phi P_{\mathrm{T}}$, where $0 < \phi \leq 1$. 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

$$\mathbf{V} = [\mathbf{v}_{\mathrm{I}}\ \mathbf{V}_{\mathrm{N}}], \tag{1}$$

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 $\mathbf{F} \triangleq \mathbf{f}^H\mathbf{f}$. 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

$$\mathbf{x} = [\mathbf{v}_{\mathrm{I}}\ \mathbf{V}_{\mathrm{N}}] \begin{bmatrix} s_{\mathrm{I}} \\ \mathbf{s}_{\mathrm{N}} \end{bmatrix} = \mathbf{v}_{\mathrm{I}} s_{\mathrm{I}} + \mathbf{V}_{\mathrm{N}}\mathbf{s}_{\mathrm{N}}. \tag{2}$$

According to (2), the received signal at Bob is given by

$$y = \mathbf{f}\mathbf{x} + n_{\mathrm{B}} = \mathbf{f}\mathbf{v}_{\mathrm{I}} s_{\mathrm{I}} + n_{\mathrm{B}}, \tag{3}$$

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 (3), the instantaneous received SNR at Bob is given by

$$\gamma_{\mathrm{B}} = \phi\overline{\gamma}_{\mathrm{B}} \left\|\mathbf{f}\right\|^2, \tag{4}$$

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

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

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 clarify that although Eve knows the exact instantaneous knowledge of $\mathbf{f}$ and $\mathbf{V}$, she cannot eliminate the interference caused by $\mathbf{V}_{\mathrm{N}}\mathbf{s}_{\mathrm{N}}$ if $N > M$. As such, the optimal received signal combiner chosen by Eve is a minimum mean-square error (MMSE) combiner, which gives the maximum received signal-to-interference-plus-noise ratio (SINR) [2]. Based on (5), the instantaneous received SINR at Eve is given by

$$\gamma_{\mathrm{E}} = \phi\mathbf{v}_{\mathrm{I}}^H\mathbf{G}^H \left(\frac{1-\phi}{N-1}\mathbf{G}\mathbf{V}_{\mathrm{N}}\mathbf{V}_{\mathrm{N}}^H\mathbf{G}^H + \frac{1}{\overline{\gamma}_{\mathrm{E}}}\mathbf{I}_M\right)^{-1} \mathbf{G}\mathbf{v}_{\mathrm{I}}, \tag{6}$$

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 secure data transmission using artificial noise but not able to calculate the secrecy performance metrics.

Based on (4), the CDF of γ_{B} is obtained as

$$F_{\gamma_B}(\gamma) = 1 - e^{-\frac{\gamma}{\phi\overline{\gamma}_{\mathrm{B}}}} \sum_{n=0}^{N-1} \frac{1}{n!}\left(\frac{\gamma}{\phi\overline{\gamma}_{\mathrm{B}}}\right)^n. \tag{7}$$

Based on (6), we find that the entries of $\mathbf{G}\mathbf{V}$ 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 [2], the CDF of γ_{E} is obtained as

$$F_{\gamma_E}(\gamma) = 1 - \frac{e^{-\frac{\gamma}{\phi\overline{\gamma}_{\mathrm{E}}}}}{\left(1+\frac{(1-\phi)\gamma}{\phi(N-1)}\right)^{N-1}} \sum_{p=1}^{M} \frac{1}{\Gamma(p)}\left(\frac{\gamma}{\phi\overline{\gamma}_{\mathrm{E}}}\right)^{p-1} \times \sum_{q=0}^{M-p} \binom{N-1}{q} \left(\frac{(1-\phi)\gamma}{\phi(N-1)}\right)^q. \tag{8}$$

II. Three Different Transmission Schemes

In this section, we first present the details of three different coding and transmission schemes. We then formalize the optimization procedure of the power allocation parameter ϕ and different wiretap code rates (e.g., R_E, R_S) for the three schemes. We also provide some analysis for the optimization of each scheme.

A. On-Off Transmission Scheme

In the on-off transmission scheme, both ϕ and R_s are fixed for each pair of $\overline{\gamma}_B$ and $\overline{\gamma}_E$. We choose R_B as $R_B = C_B$ and thus we have $R_E = C_B - R_s$. Alice only transmit signals when $C_B > R_s$, and thus the transmission probability of the on-off transmission scheme is

$$P_o^{tx}(\phi, R_s) = \Pr(C_B > R_s) = 1 - F_{\gamma_B}\left(2^{R_s} - 1\right). \quad (9)$$

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

$$\begin{aligned} P_o^{so}(\phi, R_s) &= \Pr(C_E > R_E | C_B > R_s) \\ &= 1 - \frac{1 - \Pr(C_s < R_s)}{P_o^{tx}(\phi, R_s)} \end{aligned} \quad (10)$$

where $\Pr(C_s < R_s)$ is the traditional secrecy outage probability, which has been derived in Jonas's MISOME paper. The average secrecy rate of the on-off transmission scheme over all realizations of γ_B for a given $\overline{\gamma}_B$ is

$$\mathcal{R}_o(\phi, R_s) = R_s P_o^{tx}(\phi, R_s). \quad (11)$$

In the on-off transmission scheme, we intend to optimize ϕ and R_s through maximizing $\mathcal{R}_o(\phi, R_s)$ subjective to a given secrecy outage probability. Mathematically, the optimization problem in the on-off transmission scheme is presented as

$$(\phi^*, R_s^*) = \underset{0<\phi\leq 1, R_s}{\operatorname{argmax}} \ \mathcal{R}_o(\phi, R_s), \ \text{s.t.} \ P_o^{so}(\phi, R_s) \leq p_0. \quad (12)$$

In Fig. 1, we plot $\mathcal{R}_o(\phi, R_s)$ and $P_o^{so}(\phi, R_s)$ with and without the constraint $P_o^{so}(\phi, R_s) \leq p_0$. We note that $\mathcal{R}_o(\phi, R_s)$ is not a monotonic function of R_s and thus in the optimization presented in (12) we may not have $P_o^{so}(\phi, R_s) = p_0$ for a large p_0 (e.g., $p_0 \to 1$). However, for a small p_0 (e.g., $p_0 = 0.1$) we still have $P_o^{so}(\phi, R_s) = p_0$, which is the reason why we have a sharp curve of $\mathcal{R}_o(\phi, R_s)$ versus R_s under the constraint $P_o^{so}(\phi, R_s) \leq p_0$. In this figure, we confirm that ϕ^* and R_s^* are unique for each pair of $\overline{\gamma}_B$ and $\overline{\gamma}_E$. As such, we can adopt griding numerical search to solve the optimization problem presented in (12). We note that for a given ϕ the secrecy outage probability $P_o^{so}(\phi, R_s)$ is a monotonic increasing function of R_s. As such, in the griding numerical search we can first set a value for ϕ all over $0 < \phi \leq 1$ and then increase R_s until we have $P_o^{so}(\phi, R_s) = p_0$ to obtain the upper bound of R_s.

B. Partial-Adaptive Transmission Scheme

In the partial-adaptive transmission scheme, we fix ϕ and R_E for each pair of $\overline{\gamma}_B$ and $\overline{\gamma}_E$. We choose R_B as $R_B = C_B$ and thus we have $R_s = C_B - R_E$. As such, R_s adaptively varies for each C_B while ϕ is fixed, which is the reason we

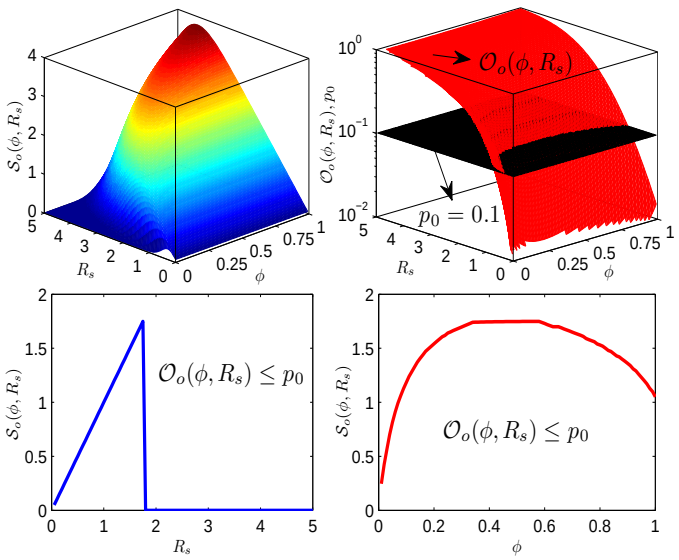

Fig. 1. Average secrecy rate and secrecy outage probability of the on-off transmission scheme with and without the constraint $P_o^{so}(\phi, R_s) \leq p_0$ for $N = 4$, $M = 2$, $\overline{\gamma}_B = 10$dB, $\overline{\gamma}_E = 5$dB, and $p_0 = 0.1$.

name this scheme as the partial-adaptive transmission scheme. Due to $R_s > 0$, Alice only transmits signals when $C_B > R_E$. Then, the transmission probability of the partial-adaptive transmission scheme is

$$P_p^{tx}(\phi, R_E) = \Pr(C_B > R_E) = 1 - F_{\gamma_B}\left(2^{R_E} - 1\right). \quad (13)$$

The secrecy outage occurs when $C_E > R_E$ conditioned on a transmission. Thus, the secrecy outage probability of the partial-adaptive transmission scheme is given by

$$P_p^{so}(\phi, R_E) = \Pr(C_E > R_E | C_B > R_E). \quad (14)$$

Since the main channel and the eavesdropper's channel are independent from each other, we further have

$$P_p^{so}(\phi, R_E) = \Pr(C_E > R_E) = 1 - F_{\gamma_E}\left(2^{R_E} - 1\right). \quad (15)$$

The average secrecy rate of the partial-adaptive transmission scheme over all realizations for one $\overline{\gamma}_B$ is

$$\begin{aligned} &\mathcal{R}_p(\phi, R_E) = \mathbb{E}\left[C_B - R_E\right]^+ \\ &= \int_{2^{R_E}-1}^{\infty} \left[C_B - R_E\right] f_{\gamma_B}(\gamma_B) d\gamma_B \\ &= R_e\left[F_{\gamma_B}\left(2^{R_E} - 1\right) - 1\right] + \int_{2^{R_E}-1}^{\infty} C_B f_{\gamma_B}(\gamma_B) d\gamma_B. \end{aligned} \quad (16)$$

In the partial-adaptive transmission scheme, we intend to optimize ϕ and R_E through maximizing $\mathcal{R}_p(\phi, R_E)$ subjective to a given secrecy outage probability. Mathematically, the optimization problem in the partial-adaptive transmission scheme can be presented as

$$(\phi^\dagger, R_E^\dagger) = \underset{0<\phi\leq 1, R_E}{\operatorname{argmax}} \ \mathcal{R}_p(\phi, R_E), \ \text{s.t.} \ P_p^{so}(\phi, R_E) \leq p_0. \quad (17)$$

For any given ϕ, both $\mathcal{R}_p(\phi, R_E)$ and $P_p^{so}(\phi, R_E)$ are monotonic decreasing functions of R_E, which is confirmed in Fig. 2. As such, for any given ϕ the optimal value of R_E

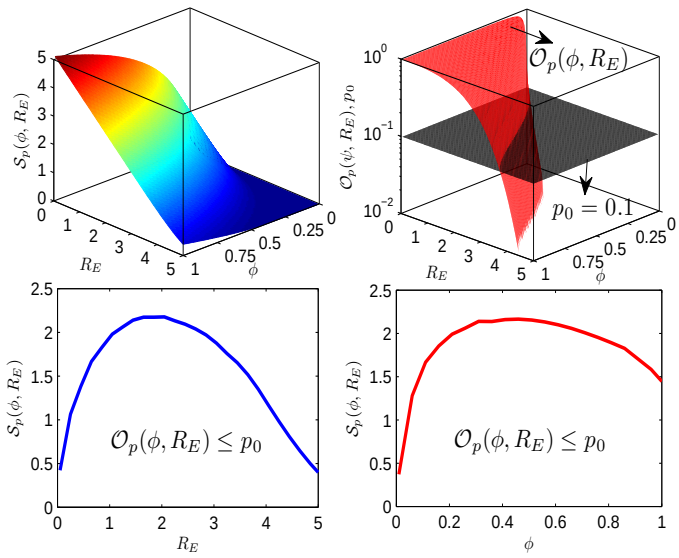

Fig. 2. Average secrecy rate and secrecy outage probability of the partial-adaptive transmission scheme with and without the constraint $P_p^{so}(\phi, R_E) \le p_0$ for $N = 4$, $M = 2$, $\overline{\gamma}_B = 10$dB, $\overline{\gamma}_E = 5$dB, and $p_0 = 0.1$.

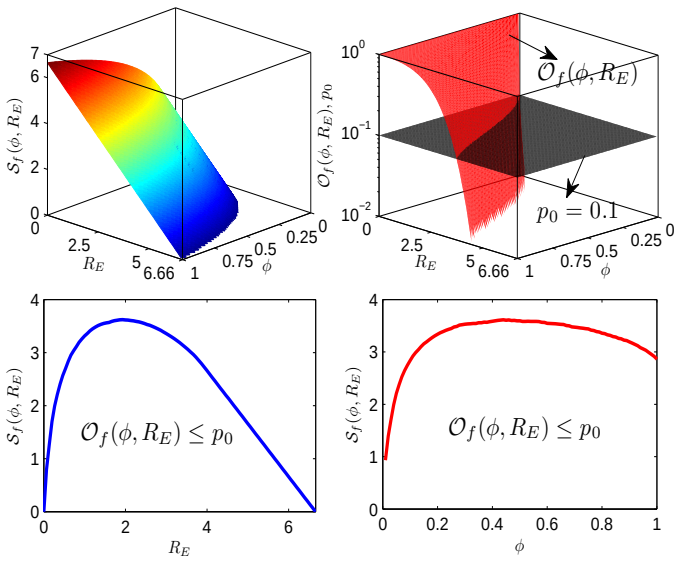

Fig. 3. Average secrecy rate and secrecy outage probability of the fully-adaptive transmission scheme with and without the constraint $P_f^{so}(\phi, R_E) \le p_0$ for $N = 4$, $M = 2$, $\widetilde{\gamma}_B = 20$dB, $\overline{\gamma}_E = 5$dB, and $p_0 = 0.1$.

is the minimum one that guarantees $P_p^{so}(\phi, R_E) = p_0$. This means that $P_p^{so}(\phi, R_E) = p_0$ is always guaranteed in such optimization, which determines a function between R_E and ϕ. Then, the two-dimension optimization problem presented in (17) can be reduced to a one-dimension optimization problem. We can adopt griding numerical search to solve the optimization problem, in which we first set a value for ϕ all over $0 < \phi \le 1$ and then increase R_E until we have $P_p^{so}(\phi, R_E) = p_0$. In Fig. 2, we confirm that $\phi^\dagger$ and $R_E^\dagger$ are unique for each pair of $\overline{\gamma}_B$ and $\overline{\gamma}_E$. To facilitate the numerical search, we are more interested in deriving a closed-form expression for R_E in terms of ϕ since we know the value range of ϕ. We would like to highlight that such a closed-form expression can be achieved for the following asymptotic scenarios.

***Corollary** 1:* For $M = 1$, as $N \to \infty$ the optimal R_E for a given ϕ is given by

$$R_E'(\phi) = \log_2\left(1 - \frac{\phi\overline{\gamma}_E \ln p_0}{(1-\phi)\overline{\gamma}_E + 1}\right). \quad (18)$$

Proof: For $M = 1$, as $N \to \infty$ the CDF of γ_E can be approximated as

$$F_{\gamma_E}(\gamma) \approx 1 - e^{-\left(\frac{1-\phi}{\phi} + \frac{1}{\phi\overline{\gamma}_E}\right)\gamma}. \quad (19)$$

Then, by setting $P_p^{so}(\phi, R_E) = p_0$ we achieve the desirable result in (18). ■

***Corollary** 2:* For $M = 1$, as $\overline{\gamma}_E \to \infty$ the optimal R_E for a given ϕ is given by

$$R_E'(\phi) = \log_2\left(1 + \frac{\phi(N-1)\left(p_0^{1/(1-N)} - 1\right)}{1-\phi}\right). \quad (20)$$

C. Fully-Adaptive Transmission Scheme

In the fully-adaptive transmission scheme, both ϕ and R_E are adaptively chosen for each $\widetilde{\gamma}_B = \overline{\gamma}_B\|\mathbf{f}\|^2$. We also choose R_B as $R_B = C_B$ and thus we have that the instantaneous secrecy rate is a function of ϕ and R_E, which is given by

$$R_s(\phi, R_E) = [C_B - R_E]^+ = [\log_2(1 + \phi\widetilde{\gamma}_B) - R_E]^+. \quad (21)$$

Alice only transmit signals when $R_s(\phi, R_E) > 0$. Thus, the transmission probability of the fully-adaptive transmission scheme is

$$P_f^{tx}(\phi, R_E) = \Pr(C_B > R_E) = 1 - F_{\gamma_B}\left(2^{R_E} - 1\right). \quad (22)$$

Similar to the partial-adaptive transmission scheme, the secrecy outage probability of the fully-adaptive transmission scheme is

$$P_f^{so}(\phi, R_E) = \Pr(C_E > R_E) = 1 - F_{\gamma_E}\left(2^{R_E} - 1\right). \quad (23)$$

In the fully-adaptive transmission scheme, we intend to maximize the instantaneous secrecy rate $R_s(\phi, R_E)$ for each $\widetilde{\gamma}_B$ subject to a given secrecy outage probability. Then, the optimization problem in the fully-adaptive transmission scheme is given by

$$(\phi^\ddagger, R_E^\ddagger) = \underset{0<\psi\le 1, 0<R_E<C_B}{\operatorname{argmax}} R_s(\phi, R_E), \text{ s.t. } \mathcal{O}_f(\phi, R_E) \le p_0. \quad (24)$$

In Fig. 3, we plot $R_s(\phi, R_E)$ and $P_f^{so}(\phi, R_E)$ with and without the constraint $P_f^{so}(\phi, R_E) \le p_0$. Again, we confirm that for any given ϕ both R_s and $\mathcal{O}_f(\phi, R_E)$ are monotonic decreasing functions of R_E. As such, the optimization procedure of the partial-adaptive transmission scheme can be applied to the fully-adaptive transmission scheme and $P_f^{so}(\phi, R_E) = p_0$ is always guaranteed in the optimization presented in (24). Since the optimization is conducted for each $\widetilde{\gamma}_B$, the complexity of the signal processing for the fully-adaptive transmission scheme is much higher than that for the partial-adaptive and on-off transmission schemes. We would

like to highlight that $\phi^{\ddagger}$ and $R_E^{\ddagger}$ can be achieved in closed-from expressions for each $\widetilde{\gamma}_B$ in the following asymptotic scenarios.

***Corollary** 3:* For $M = 1$, as $N \to \infty$ the optimal values of ϕ^* and R_E^* are given by

$$\phi^{\ddagger} = \sqrt{\frac{\ln p_0 \left[(1+\ln p_0+\widetilde{\gamma}_B)\overline{\gamma}_E+\widetilde{\gamma}_B\right]}{-\overline{\gamma}_E^2\widetilde{\gamma}_B(1+\ln p_0)^2(\overline{\gamma}_E+1)^{-1}}} - \frac{\overline{\gamma}_E+1}{\overline{\gamma}_E(1+\ln p_0)},$$

$$R_E^{\ddagger} = \log_2\left(1-\frac{\phi^{\ddagger}\overline{\gamma}_E\ln p_0}{(1-\phi^*)\overline{\gamma}_E+1}\right).$$

Proof: Since $P_f^{so}(\phi, R_E) = P_p^{so}(\phi, R_E)$, Corollary 1 is also valid for the fully-adaptive transmission scheme. Substituting (18) into $R_s(\phi, R_E)$ in (21), we have

$$R_s(\phi, R_E^{\dagger}(\phi)) = \log_2(1+\phi\widetilde{\gamma}_B) - \log_2\left(1-\frac{\phi\overline{\gamma}_E\ln p_0}{(1-\phi)\overline{\gamma}_E+1}\right). \tag{25}$$

We first note that we have to guarantee $R_s(\phi, R_E^{\dagger}(\phi)) > 0$, which results in

$$\widetilde{\gamma}_B > -\frac{\overline{\gamma}_E\ln p_0}{(1-\phi)\overline{\gamma}_E+1} > -\frac{\overline{\gamma}_E\ln p_0}{\overline{\gamma}_E+1}. \tag{26}$$

Following (25), we define

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

where

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

To maximize $R_s(\phi, R_E^{\dagger}(\phi))$ is equivalent to maximize $g(\phi)$. We next prove that $g(\phi)$ is a concave function with respective to ϕ. Using (27), we have

$$\frac{\partial^2 g(\phi)}{\partial^2\phi} = \frac{2D^2C}{(D\phi+E)^3}. \tag{29}$$

It is easy to prove that $(D\phi+E)^3 > 0$. Thus, we only have to prove $C < 0$, which means that we have to prove $1 - B < 0$ since $C = (\overline{\gamma}_B+1)(1-B)$ and $\overline{\gamma}_B+1 > 0$. Following (28), we have

$$1-B = \frac{\overline{\gamma}_E(1+\ln p_0)\ln p_0 + \widetilde{\gamma_B}(1+\overline{\gamma}_E)\ln p_0}{(1+\ln p_0)^2\overline{\gamma}_E}. \tag{30}$$

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

$$\widetilde{\gamma}_B(1+\overline{\gamma}_E)\ln p_0 < -\overline{\gamma}_E(\ln p_0)^2. \tag{31}$$

Substituting (31) into (30) and noting $p_0 < 1$, we have

$$1-B < \frac{\ln p_0}{(1+\ln p_0)^2} < 0. \tag{32}$$

As such, we have proved that $g(\phi)$ is a concave function of ϕ and we achieve the desirable results presented in Corollary 3 by setting $\partial g(\phi)/\partial\phi = 0$. ∎

***Corollary** 4:* For $M = 1$, as $\overline{\gamma}_E \to \infty$ the optimal values of ϕ^* and R_E^* are given by

$$\phi^{\ddagger} = \sqrt{\frac{1}{\widetilde{\gamma}_B}\left(\frac{2\widetilde{\gamma}_B}{\alpha-1}+\frac{\widetilde{\gamma}_B}{(\alpha-1)^2}-1\right)} - \frac{1}{\alpha-1},$$

$$R_E^{\ddagger} = \log_2\left(1-\frac{\phi^{\ddagger}\alpha}{(1-\phi^{\ddagger})}\right),$$

where α is given by

$$\alpha = (N-1)\left(p_0^{1/(1-N)}-1\right). \tag{33}$$

We note that the maximum instantaneous secrecy rate $R_s(\phi^{\ddagger}, R_E^{\ddagger})$ is still a function of $\widetilde{\gamma}_B$. In order to conduct the performance comparison among the three schemes, we have to calculate the average maximum secrecy rate of the fully-adaptive transmission scheme, which is given by

$$\mathcal{R}_f^{\ddagger} = \int_0^{\infty} R_s(\phi^{\ddagger}, R_E^{\ddagger}) f_{\widetilde{\gamma}_B}(\widetilde{\gamma}_B) d\widetilde{\gamma}_B, \tag{34}$$

where $f_{\widetilde{\gamma}_B}(\widetilde{\gamma}_B)$ denotes the pdf of $\widetilde{\gamma}_B$.

III. Performance Comparison of the Three Different Transmission Schemes

We present the performance comparison results of the three different transmission schemes in Fig. 4. We first observe that $\mathcal{R}_p(\phi^{\dagger}, R_E^{\dagger})$ is much higher than $\mathcal{R}_o(\phi^*, R_E^*)$, which means that the partial-adaptive transmission scheme dramatically outperforms the on-off transmission scheme. This can be explained by the fact that when the main channel cannot support a fixed secrecy rate R_s^* under the secrecy constraint in the on-off transmission scheme, a positive secrecy rate $C_B - R_E^{\dagger}$ can still be achieved under the secrecy constraint in the partial-adaptive transmission scheme. We would like to highlight that from a wiretap coding perspective point of view the complexity of the partial-adaptive transmission scheme is much lower than that of the on-off transmission scheme. This is due to the fact that both the codeword rate R_B and redundancy rate R_E have to be adjusted for each γ_B in the on-off transmission scheme while only the codeword rate R_B varies in the partial-adaptive transmission scheme. In the simulations to obtain Fig. 4, we confirm that $\mathcal{R}_f^{\ddagger}$ is slightly larger than $\mathcal{R}_p(\phi^{\dagger}, R_E^{\dagger})$, which is not obviously observed in this figure due to the large value range. The minor advantage of the fully-adaptive transmission scheme relative to the partial-adaptive transmission scheme is unexpected (we expect a large advantage since ϕ and R_E are adaptively chosen for each instantaneous SNR of the main channel). However, this is reasonable since as per (26) we know that a positive secrecy rate is achievable under the secrecy constraint only when $\widetilde{\gamma}_B$ is larger than some specific value, not for every $\widetilde{\gamma}_B$.

References

[1] 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.

[2] 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.

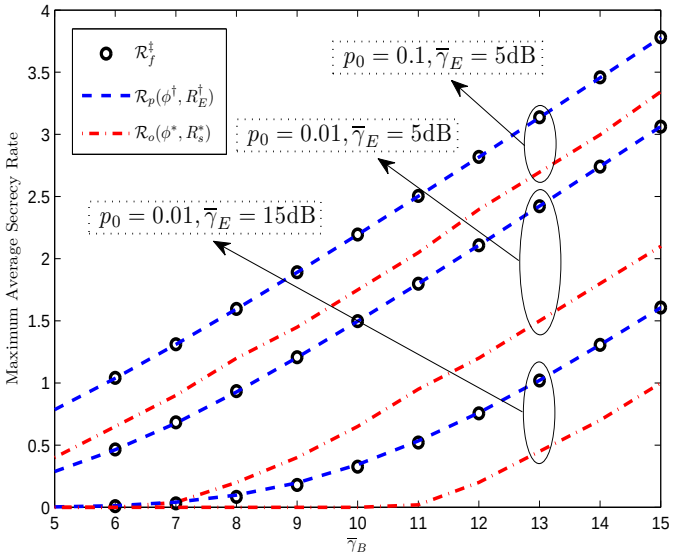

Fig. 4. Maximum average secrecy rate of the three different transmission schemes for $N = 4$, $M = 2$, and $p_0 = 0.1$.