MIMO Wiretap Channels: Secure Transmission Using Transmit Antenna Selection and Receive Generalized Selection Combining

Nan Yang, *Member, IEEE,* Phee Lep Yeoh, *Member, IEEE,* Maged Elkashlan, *Member, IEEE,* Robert Schober, *Fellow, IEEE,* and Jinhong Yuan, *Senior Member, IEEE*

***Abstract*—We propose and analyze transmit antenna selection with receive generalized selection combining (TAS/GSC) for physical layer security enhancement in multiple-input multiple-output wiretap channels. In this protocol, a single antenna out of $N_{\rm A}$ antennas is selected at the transmitter and $L_{\rm B}$ antennas out of $N_{\rm B}$ antennas are combined at the legitimate receiver. We characterize the physical layer secrecy of TAS/GSC via our new closed-form expressions for the exact and the asymptotic secrecy outage probability. We demonstrate that the maximum secrecy outage diversity gain of $N_{\rm A}N_{\rm B}$ is achieved.**

***Index Terms*—Multiple-input multiple-output wiretap channel, transmit antenna selection, generalized selection combining.**

I. Introduction

SECURITY in the physical layer domain is a prominent frontier in wireless networks where the communication between the transmitter and the legitimate receiver is vulnerable to eavesdropping [1, 2]. In such a wiretap channel, secure information transmission based on the physical layer characteristics of wireless channels is instrumental to complement the key management and cryptographic algorithms at higher layers [3].

Motivated by the practical importance of multiple antennas, physical layer security in multiple-input multiple-output (MIMO) wiretap channels has attracted considerable interests from an information-theoretic perspective, e.g., [4]. Based on these seminal studies, the secrecy outage probability was characterized in [5, 6] for a single antenna at the transmitter and multiple antennas at the legitimate receiver and/or the eavesdropper. Transmit beamforming (TBF) was considered in [7–9] as a means of providing secure transmission in wiretap channels with multiple antennas at the transmitter and the eavesdropper and a single antenna at the legitimate receiver. Different from TBF which requires the feedback of channel state information (CSI) and signal processing for all transmit antennas, transmit antenna selection (TAS) achieves lower feedback and computational overheads as it only requires feedback and signal processing for a single transmit antenna [10–12]. Motivated by these benefits, the secrecy outage probability of transmit antenna selection (TAS) was derived in [10]. More recently, TAS with receive selection combining (TAS/SC) and TAS with receive maximal-ratio combining (TAS/MRC) was examined in [11] for multiple antennas at the transmitter, the legitimate receiver, and the eavesdropper. Considering MRC at the legitimate receiver and the eavesdropper, [12] characterized the effect of antenna correlation on the secrecy performance.

In this letter, we propose transmit antenna selection with receive generalized selection combining (TAS/GSC) in MIMO wiretap channels to bridge the secrecy gap between TAS/SC and TAS/MRC. In the proposed protocol, a single antenna from $N_{\rm A}$ available antennas is selected at the transmitter to maximize the signal-to-noise ratio (SNR) at the legitimate receiver. At the legitimate receiver, GSC is applied to select the $L_{\rm B}$ antennas with the highest SNRs from $N_{\rm B}$ available antennas [13, 14]. During the transmission, an unauthorized eavesdropper attempts to intercept the signal by selecting $L_{\rm E}$ from $N_{\rm E}$ available antennas using GSC[1]. We first derive a new exact closed-form expression for the secrecy outage probability with TAS/GSC over Rayleigh fading channels. Importantly, this expression provides a generalized framework to bridge the gap between TAS/MRC and TAS/SC presented in [11]. We then derive a new compact expression for the asymptotic secrecy outage probability. This result confirms that the secrecy outage diversity gain is equal to $N_{\rm A}N_{\rm B}$, which indicates that TAS/GSC achieves the same secrecy outage diversity gain as TAS/SC and TAS/MRC in MIMO wiretap channels. We further highlight that the tradeoff between each of the protocols is characterized as a concise ratio of their respective secrecy outage SNR gains. For the same secrecy outage probability, the SNR gap between TAS/GSC and TAS/SC is derived as $(10/N_{\rm B})\log(L_{\rm B}^{N_{\rm B}-L_{\rm B}}L_{\rm B}!)$ dB. The SNR gap between TAS/GSC and TAS/MRC is derived as $(10/N_{\rm B})\log(L_{\rm B}^{N_{\rm B}-L_{\rm B}}L_{\rm B}!/N_{\rm B}!)$ dB. Finally, we show that the secrecy rate of TAS is close to that of TBF when $N_{\rm A}$ is small without added feedback and signal processing complexities.

II. Protocol Description

We consider a MIMO wiretap channel with $N_{\rm A}$ antennas at the transmitter (Alice), $N_{\rm B}$ antennas at the legitimate receiver (Bob), and $N_{\rm E}$ antennas at the eavesdropper (Eve). We focus on quasi-static fading channels with independent identically distributed (i.i.d.) block Rayleigh fading in the main channel from Alice to Bob, and in the eavesdropper's channel from Alice to Eve. In both channels, we assume that

[1]The use of GSC at the eavesdropper is motivated by the fact that it is a generalized antenna configuration which covers SC ($L_{\rm E}=1$) and MRC ($L_{\rm E}=N_{\rm E}$) as special cases.

Manuscript received May 6, 2013. The associate editor coordinating the review of this letter and approving it for publication was W. Xu.

This work was supported by an Australian Research Council (ARC) Discovery Project grant (DP120102607).

N. Yang and J. Yuan are with the School of Electrical Engineering and Telecommunications, The University of New South Wales, NSW 2052, Australia (e-mail: {nan.yang, j.yuan}@unsw.edu.au).

P. L. Yeoh is with the Dept. of Electrical and Electronic Engineering, The University of Melbourne, VIC 3010, Australia (e-mail: phee.yeoh@unimelb.edu.au).

M. Elkashlan is with the School of Electronic Engineering and Computer Science, Queen Mary, University of London, London E1 4NS, UK (e-mail: maged.elkashlan@eecs.qmul.ac.uk).

R. Schober is with the Dept. of Electrical, Electronics, and Communication Engineering, Friedrich-Alexander University of Erlangen-Nuremberg, 91054 Erlangen, Germany (e-mail: schober@lnt.de).

Digital Object Identifier 10.1109/LCOMM.2013.071813.131048

the transmission block length is less than or equal to the coherence time. Furthermore, we consider the practical passive eavesdropping scenario where the CSI of the eavesdropper's channel is not available to either Alice or Bob.

In the main channel, a single transmit antenna is selected at Alice to maximize the received SNR at Bob. At Bob, GSC is applied such that the L_{B} *strongest* antennas out of the N_{B} available antennas are combined. We denote the complex channel coefficient from the jth transmit antenna to the l_{B}th receive antenna as $h_{jl_{\mathrm{B}}}$, where $1 \leq j \leq N_{\mathrm{A}}$ and $1 \leq l_{\mathrm{B}} \leq N_{\mathrm{B}}$. Based on the rules of GSC, let $|h_{j1}|^2 \geq |h_{j2}|^2 \geq \cdots \geq |h_{jN_{\mathrm{B}}}|^2$ be the order statistics from arranging $\{|h_{jl_{\mathrm{B}}}|^2\}_{l_{\mathrm{B}}=1}^{N_{\mathrm{B}}}$ in descending order of magnitude. Combining the first L_{B} $(1 \leq L_{\mathrm{B}} \leq N_{\mathrm{B}})$ variable(s) in the order statistics, Bob obtains $\theta_j = \sum_{l_{\mathrm{B}}=1}^{L_{\mathrm{B}}} |h_{jl_{\mathrm{B}}}|^2$. As such, the index of the selected antenna is determined by Bob as $j^* = \mathrm{argmax}_{1 \leq j \leq N_{\mathrm{A}}} \{\theta_j\}$. Bob then feeds back j^* and $\theta_{j^*} = \sum_{l_{\mathrm{B}}=1}^{L_{\mathrm{B}}} |h_{j^* l_{\mathrm{B}}}|^2$ to Alice using a small number of bits via a low-rate feedback channel. Here, j^* allows Alice to select the strongest transmit antenna and θ_{j^*} allows Alice to determine the size of the codebook with random binning for secure transmission [2]. As such, the feedback overhead of TAS is lower than that of TBF since TBF necessitates CSI feedback of $N_{\mathrm{A}} L_{\mathrm{B}}$ complex numbers.

To perform secure transmission, Alice encodes each message $\mathbf{w}$ into a codeword $\mathbf{x} = [x(1), \cdots, x(i), \cdots, x(n)]$, where n is the length of $\mathbf{x}$. The transmitted codeword is subject to an average power constraint $\frac{1}{n}\sum_{i=1}^{n} \mathbb{E}\left[|x(i)|^2\right] \leq P_{\mathrm{A}}$. The received signal vector at Bob at time i is given by $\mathbf{y}(i) = \mathbf{h}x(i) + \mathbf{n}_{\mathrm{B}}$, where $\mathbf{h} = [h_{j^*1}, h_{j^*2}, \cdots, h_{j^*N_{\mathrm{B}}}]^T$ denotes the main channel vector between the j^*th transmit antenna at Alice and the N_{B} receive antennas at Bob, and $\mathbf{n}_{\mathrm{B}}$ is the $N_{\mathrm{B}} \times 1$ additive white Gaussian noise (AWGN) vector at Bob satisfying $\mathbb{E}\left[\mathbf{n}_{\mathrm{B}}\mathbf{n}_{\mathrm{B}}^{\dagger}\right] = \mathbf{I}_{N_{\mathrm{B}}}\sigma^2$, where $\mathbb{E}[\cdot]$ denotes the expectation, $\mathbf{I}_{N_{\mathrm{B}}}$ denotes the $N_{\mathrm{B}} \times N_{\mathrm{B}}$ identity matrix, and σ^2 is the noise variance at each receive antenna. The instantaneous SNR of the main channel is given by $\gamma_{\mathrm{B}} = \sum_{l_{\mathrm{B}}=1}^{L_{\mathrm{B}}} \gamma_{(l_{\mathrm{B}})}$, where $\gamma_{(1)} \geq \gamma_{(2)} \geq \ldots \geq \gamma_{(N_{\mathrm{B}})}$ are the order statistics from arranging $\{\gamma_{(l_{\mathrm{B}})} = |h_{j^* l_{\mathrm{B}}}|^2 P_{\mathrm{A}}/\sigma^2\}_{l_{\mathrm{B}}=1}^{N_{\mathrm{B}}}$ in descending order of magnitude. We further denote $\overline{\gamma}_{\mathrm{B}} = \mathbb{E}[\gamma_{\mathrm{B}}]/L_{\mathrm{B}}$ as the average SNR per antenna at Bob. In the eavesdropper's channel, the received signal vector at Eve at time i is given by $\mathbf{z}(i) = \mathbf{g}x(i) + \mathbf{n}_{\mathrm{E}}$, where $\mathbf{g} \triangleq \mathbf{g}_{j^*} = [g_{j^*1}, g_{j^*2}, \cdots, g_{j^*N_{\mathrm{E}}}]^T$ is the eavesdropper's channel vector between the j^*th transmit antenna at Alice and the N_{E} receive antennas at Eve, and $\mathbf{n}_{\mathrm{E}}$ is the $N_{\mathrm{E}} \times 1$ AWGN vector at Eve which satisfies $\mathbb{E}\left[\mathbf{n}_{\mathrm{E}}\mathbf{n}_{\mathrm{E}}^{\dagger}\right] = \mathbf{I}_{N_{\mathrm{E}}}\sigma^2$. Since the antenna index j^* is independent of $\mathbf{g}$, the strongest transmit antenna for Bob corresponds to a random transmit antenna for Eve. At Eve, we consider GSC to combine the L_{E} *strongest* antennas from N_{E} available antennas. As such, the instantaneous SNR of the eavesdropper's channel is given by $\gamma_{\mathrm{E}} = \sum_{l_{\mathrm{E}}=1}^{L_{\mathrm{E}}} \gamma_{(l_{\mathrm{E}})}$, where $\gamma_{(1)} \geq \gamma_{(2)} \geq \ldots \geq \gamma_{(N_{\mathrm{E}})}$ are the order statistics from arranging $\{\gamma_{(l_{\mathrm{E}})} = |g_{j^* l_{\mathrm{E}}}|^2 P_{\mathrm{A}}/\sigma^2\}_{l_{\mathrm{E}}=1}^{N_{\mathrm{E}}}$ in descending order of magnitude. We further denote $\overline{\gamma}_{\mathrm{E}} = \mathbb{E}[\gamma_{\mathrm{E}}]/L_{\mathrm{E}}$ as the average SNR per antenna at Eve.

III. Secrecy Performance of TAS/GSC

The achievable secrecy rate of this MIMO wiretap channel is defined as $C_S = [\log(1+\gamma_{\mathrm{B}}) - \log(1+\gamma_{\mathrm{E}})]^+$ [2], where $[x]^+$ denotes $\max\{0, x\}$. In passive eavesdropping, the transmission from Alice is performed at a constant code rate R_S. When $C_S > R_S$, the transmission from Alice guarantees perfect secrecy. When $C_S < R_S$, the transmission is vulnerable to eavesdropping and perfect secrecy is not guaranteed. This indicates that the rate at the eavesdropper is not zero. As such, the secrecy outage probability is a relevant performance measure for passive eavesdropping [2, 10–12].

We first present the statistics of γ_{B} and γ_{E}. The cumulative distribution function (cdf) of γ_{B} is obtained using [13, eq. (4)] and the polynomial expansion as

$$F_{\gamma_{\mathrm{B}}}(\gamma) = \sum_{S_k \in \mathcal{S}} \alpha_k \gamma^{\beta_k} e^{-\delta_k \frac{\gamma}{\overline{\gamma}_{\mathrm{B}}}}, \tag{1}$$

where $\mathcal{S} = \left\{S_k | \sum_{n=0}^{N} n_{k,n} = N_{\mathrm{A}}\right\}$ with $\{n_{k,n}\} \in \mathbb{Z}^+$,

$$\alpha_k = N_{\mathrm{A}}! \prod_{l_{\mathrm{B}}=1}^{L_{\mathrm{B}}} \left(\frac{\epsilon_{l_{\mathrm{B}}}}{(l_{\mathrm{B}}-1)!}\right)^{n_{k,l_{\mathrm{B}}}} \frac{\prod_{l_{\mathrm{B}}=L_{\mathrm{B}}+1}^{N_{\mathrm{B}}} \epsilon_{l_{\mathrm{B}}}^{n_{k,l_{\mathrm{B}}}}}{\prod_{n=0}^{N_{\mathrm{B}}} n_{k,n}!}, \tag{2}$$

$$\beta_k = \sum_{l_{\mathrm{B}}=1}^{L_{\mathrm{B}}} (l_{\mathrm{B}}-1)\, n_{k,l_{\mathrm{B}}}, \tag{3}$$

and

$$\delta_k = \sum_{l_{\mathrm{B}}=1}^{L_{\mathrm{B}}} n_{k,l_{\mathrm{B}}} + \sum_{l_{\mathrm{B}}=L_{\mathrm{B}}+1}^{N_{\mathrm{B}}} \frac{l_{\mathrm{B}} n_{k,l_{\mathrm{B}}}}{L_{\mathrm{B}}}. \tag{4}$$

In (2), we define ϵ_{l_ρ} for $\rho \in \{\mathrm{B}, \mathrm{E}\}$ as

$$\epsilon_{l_\rho} = \begin{cases} 1 & l_\rho = 0 \\ \frac{1}{\overline{\gamma}_\rho^{1-l_\rho}} \left[-1 + \sum_{k=L_\rho+1}^{N_\rho} (-1)^{k-l_\rho} \times \frac{\binom{N_\rho}{N_\rho-k}\binom{k-1}{k-L_\rho-1}}{\left(\frac{k}{L_\rho}-1\right)^{L_\rho-l_\rho+1}}\right] & 1 \leq l_\rho < L_\rho \\ -\overline{\gamma}_\rho^{1-L_\rho}\binom{N_\rho}{N_\rho-L_\rho} & l_\rho = L_\rho \\ \frac{(-1)^{l_\rho}\binom{N_\rho}{N_\rho-l_\rho}\binom{l_\rho-1}{l_\rho-L_\rho-1}}{\left(\frac{l_\rho}{L_\rho}-1\right)^{L_\rho}} & L_\rho < l_\rho \leq N_\rho. \end{cases} \tag{5}$$

Based on [13, eq. (4)], the cdf of γ_{E} with a random transmit antenna at Alice and GSC at Eve is given by

$$F_{\gamma_{\mathrm{E}}}(\gamma) = \epsilon_0 + \sum_{l_{\mathrm{E}}=1}^{L_{\mathrm{E}}} \frac{\epsilon_{l_{\mathrm{E}}} \gamma^{l_{\mathrm{E}}-1} e^{-\frac{\gamma}{\overline{\gamma}_{\mathrm{E}}}}}{\Gamma(l_{\mathrm{E}})} + \sum_{l_{\mathrm{E}}=L_{\mathrm{E}}+1}^{N_{\mathrm{E}}} \epsilon_{l_{\mathrm{E}}} e^{-\frac{l_{\mathrm{E}}\gamma}{L_{\mathrm{E}}\overline{\gamma}_{\mathrm{E}}}}. \tag{6}$$

A. Exact Secrecy Performance

In this subsection, we quantify the exact secrecy performance achieved by TAS/GSC by deriving the exact secrecy outage probability in closed-form. The secrecy outage probability is given by

$$\begin{aligned} P_{\mathrm{out}}(R_S) &= \Pr(C_S < R_S | \gamma_{\mathrm{B}} > \gamma_{\mathrm{E}}) \Pr(\gamma_{\mathrm{B}} > \gamma_{\mathrm{E}}) \\ &\quad + \Pr(C_S < R_S | \gamma_{\mathrm{B}} < \gamma_{\mathrm{E}}) \Pr(\gamma_{\mathrm{B}} < \gamma_{\mathrm{E}}) \\ &= \int_0^{\infty} \int_{\gamma_{\mathrm{E}}}^{2^{R_S}(1+\gamma_{\mathrm{E}})-1} f_{\gamma_{\mathrm{E}}}(\gamma_{\mathrm{E}}) f_{\gamma_{\mathrm{B}}}(\gamma_{\mathrm{B}})\, d\gamma_{\mathrm{B}} d\gamma_{\mathrm{E}} \\ &\quad + \int_0^{\infty} \int_0^{\gamma_{\mathrm{E}}} f_{\gamma_{\mathrm{E}}}(\gamma_{\mathrm{E}}) f_{\gamma_{\mathrm{B}}}(\gamma_{\mathrm{B}})\, d\gamma_{\mathrm{B}} d\gamma_{\mathrm{E}}. \end{aligned} \tag{7}$$

where $f_{\gamma_{\rm B}}(\cdot)$ and $f_{\gamma_{\rm E}}(\cdot)$ denote the probability density functions (pdfs) of $\gamma_{\rm B}$ and $\gamma_{\rm E}$, respectively. Taking the first derivative of $F_{\gamma_{\rm B}}(\gamma)$ in (1) and $F_{\gamma_{\rm E}}(\gamma)$ in (6), we obtain $f_{\gamma_{\rm B}}(\gamma)$ and $f_{\gamma_{\rm E}}(\gamma)$, respectively. Substituting these pdfs into (7) and applying [15, eq. (3.326.2)] to solve the resultant integrals, we derive the exact secrecy outage probability in closed-form as

$$P_{\rm out}(R_S) = \hbar_1 - \hbar_2 - \hbar_3, \tag{8}$$

where $\hbar_1$, $\hbar_2$, and $\hbar_3$ are easy-to-handle finite sums of standard functions defined as

$$\hbar_1 = \sum_{l_{\rm E}=1}^{L_{\rm E}} \frac{\epsilon_{l_{\rm E}}(l_{\rm E}-1)}{\Gamma(l_{\rm E})} \sum_{S_k\in\mathcal{S}} \sum_{\eta=0}^{\beta_k} \frac{\Xi\Gamma(\eta+l_{\rm E}-1)}{\left(\frac{2^{R_S}\delta_k}{\overline{\gamma}_{\rm B}}+\frac{1}{\overline{\gamma}_{\rm E}}\right)^{\eta+l_{\rm E}-1}}, \tag{9}$$

$$\hbar_2 = \sum_{l_{\rm E}=1}^{L_{\rm E}} \frac{\epsilon_{l_{\rm E}}}{\Gamma(l_{\rm E})\overline{\gamma}_{\rm E}} \sum_{S_k\in\mathcal{S}} \sum_{\eta=0}^{\beta_k} \frac{\Xi\Gamma(\eta+l_{\rm E})}{\left(\frac{2^{R_S}\delta_k}{\overline{\gamma}_{\rm B}}+\frac{1}{\overline{\gamma}_{\rm E}}\right)^{\eta+l_{\rm E}}}, \tag{10}$$

and

$$\hbar_3 = \sum_{l_{\rm E}=L_{\rm E}+1}^{N_{\rm E}} \frac{\epsilon_{l_{\rm E}} l_{\rm E}}{L_{\rm E}\overline{\gamma}_{\rm E}} \sum_{S_k\in\mathcal{S}} \sum_{\eta=0}^{\beta_k} \frac{\Xi\Gamma(\eta+1)}{\left(\frac{2^{R_S}\delta_k}{\overline{\gamma}_{\rm B}}+\frac{l_{\rm E}}{L_{\rm E}\overline{\gamma}_{\rm E}}\right)^{\eta+1}}. \tag{11}$$

In (9), (10), and (11), we define Ξ as

$$\Xi = \alpha_k \binom{\beta_k}{\eta} \left(2^{R_S}-1\right)^{\beta_k} e^{-\frac{\left(2^{R_S}-1\right)\delta_k}{\overline{\gamma}_{\rm B}}} \left(\frac{2^{R_S}}{2^{R_S}-1}\right)^{\eta}, \tag{12}$$

where α_k, β_k, and δ_k, are functions of $L_{\rm B}$ given in (2), (3), and (4), respectively. Notably, the expression for $P_{\rm out}(R_S)$ in (8) is derived in closed-form and is valid for general scenarios with arbitrary SNRs and arbitrary numbers of antennas.

Based on (8), we are able to calculate other secrecy performance metrics. For example, the probability of positive secrecy is evaluated as $\Pr(C_S>0) = \Pr(\gamma_{\rm B}>\gamma_{\rm E}) = 1 - P_{\rm out}(0)$. We can also examine the ε-outage secrecy rate, $R_S^{\max}$, which specifies the maximum secrecy rate when the secrecy outage probability is less than ε [6, 11]. According to (8), the ε-outage secrecy rate is determined as $P_{\rm out}(R_S^{\max}) = \varepsilon$.

B. Asymptotic Secrecy Performance

The purpose of this subsection is to examine the asymptotic behavior of the secrecy outage probability in the high SNR regime with $\overline{\gamma}_{\rm B} \to \infty$[2]. The asymptotic result allows us to determine the secrecy outage diversity gain and the secrecy outage SNR gain, which are two factors governing the secrecy outage probability at high SNRs.

We proceed by deriving the first order expansion of $F_{\gamma_{\rm B}}(\gamma)$ in (1). Applying the expansion [15, eq. (1.211.1)], the first order expansion of $F_{\gamma_{\rm B}}(\gamma)$ is derived as $F_{\gamma_{\rm B}}^{\infty}(\gamma) \approx 1/\left(L_{\rm B}^{N_{\rm A}(N_{\rm B}-L_{\rm B})}(L_{\rm B}!)^{N_{\rm A}}\right)(\gamma/\overline{\gamma}_{\rm B})^{N_{\rm A}N_{\rm B}}$. Based on this result, we obtain the asymptotic secrecy outage probability as

$$P_{\rm out}^{\infty}(R_S) \approx (G_a\overline{\gamma}_{\rm B})^{-G_d}, \tag{13}$$

[2]When $\overline{\gamma}_{\rm E}$ is higher than $\overline{\gamma}_{\rm B}$, the probability of successful eavesdropping approaches one as $\overline{\gamma}_{\rm E}\to\infty$. In this case, the secrecy outage probability can be derived using $F_{\gamma_{\rm B}}(\gamma)$ in (1) and the first order expansion of $F_{\gamma_{\rm E}}(\gamma)$ given by $F_{\gamma_{\rm E}}^{\infty}(\gamma) \approx 1/(L_{\rm E}^{(N_{\rm E}-L_{\rm E})}L_{\rm E}!)(\gamma/\overline{\gamma}_{\rm E})^{N_{\rm E}}$. The result is omitted due to page limits.

where the secrecy outage diversity gain is

$$G_d = N_{\rm A}N_{\rm B}, \tag{14}$$

and the secrecy outage SNR gain is

$$G_a = \Lambda^{-\frac{1}{N_{\rm A}N_{\rm B}}}. \tag{15}$$

In (15), we define Λ as

$$\Lambda = \frac{\left(2^{R_S}-1\right)^{N_{\rm A}N_{\rm B}}}{\left(L_{\rm B}^{N_{\rm B}-L_{\rm B}}L_{\rm B}!\right)^{N_{\rm A}}} \sum_{\eta=0}^{N_{\rm A}N_{\rm B}} \binom{N_{\rm A}N_{\rm B}}{\eta} \left(\frac{2^{R_S}\overline{\gamma}_{\rm E}}{2^{R_S}-1}\right)^{\eta} \times \left(-\eta \sum_{l_{\rm E}=1}^{L_{\rm E}} \frac{\epsilon_{l_{\rm E}}\Gamma(\eta+l_{\rm E}-1)}{\Gamma(l_{\rm E})\overline{\gamma}_{\rm E}^{1-l_{\rm E}}} - \sum_{l_{\rm E}=L_{\rm E}+1}^{N_{\rm E}} \frac{\epsilon_{l_{\rm E}}\Gamma(\eta+1)L_{\rm E}^{\eta}}{l_{\rm E}^{\eta}}\right). \tag{16}$$

According to (13), we offer the following remarks to provide insights into the use of TAS/GSC in the main channel.

Remark 1: The secrecy outage probability approaches zero as $\overline{\gamma}_{\rm B}$ approaches infinity.

Remark 2: The maximum secrecy outage diversity gain of $N_{\rm A}N_{\rm B}$ is achieved. This diversity gain is entirely dependent on the main channel.

Remark 3: The secrecy outage diversity gain is not affected by the choice of $L_{\rm B}$ and $L_{\rm E}$. The impact of $L_{\rm B}$ and $L_{\rm E}$ is only reflected in the secrecy outage SNR gain.

C. Secrecy Performance Tradeoff

We now examine the secrecy outage tradeoff between TAS/GSC, TAS/SC (i.e., $L_{\rm B}=1$), and TAS/MRC (i.e., $L_{\rm B}=N_{\rm B}$) at the legitimate receiver. From (14), we confirm that TAS/GSC has the same diversity gain as TAS/SC and TAS/MRC. As such, the tradeoff between them is solely characterized by their respective secrecy outage SNR gains. Maintaining the use of GSC at the eavesdropper, we present the SNR gap between TAS/GSC and TAS/SC in the main channel as $\Delta_1 = (10/N_{\rm B})\log\left(L_{\rm B}^{N_{\rm B}-L_{\rm B}}L_{\rm B}!\right)$ dB. We confirm that $\Delta_1>0$ and the SNR gap increases as $L_{\rm B}$ increases. We also present the SNR gap between TAS/GSC and TAS/MRC as $\Delta_2 = (10/N_{\rm B})\log\left(L_{\rm B}^{N_{\rm B}-L_{\rm B}}L_{\rm B}!/N_{\rm B}!\right)$ dB. We confirm that the SNR gap decreases as $L_{\rm B}$ increases. Observing Δ_1 and Δ_2, we find that these SNR gaps are entirely dependent on $N_{\rm B}$ and $L_{\rm B}$. Notably, they are not affected by $N_{\rm E}$ and $L_{\rm E}$.

IV. Simulations and Discussions

In this section, we examine the secrecy performance of TAS/GSC. Fig. 1 plots the secrecy outage probability versus $\overline{\gamma}_{\rm B}$ for $R_S=1$. Notably, our asymptotic curves from (13) accurately represent the secrecy outage diversity gain and the secrecy outage SNR gain, and our exact curves from (8) are well-validated by Monte Carlo simulations marked with '•'. We first see that the secrecy outage diversity gain is $G_d=8$ regardless of $L_{\rm B}$. We also see that the secrecy outage probability improves with increasing $L_{\rm B}$. As expected, we see that the secrecy outage probability approaches one when $\overline{\gamma}_{\rm B} < \overline{\gamma}_{\rm E}$. Importantly, we highlight that TAS/GSC brings a significant SNR advantage relative to TAS/SC. We also highlight that TAS/GSC provides comparable secrecy outage to TAS/MRC. Since GSC has a lower complexity than MRC and a higher complexity than SC, this figure confirms that

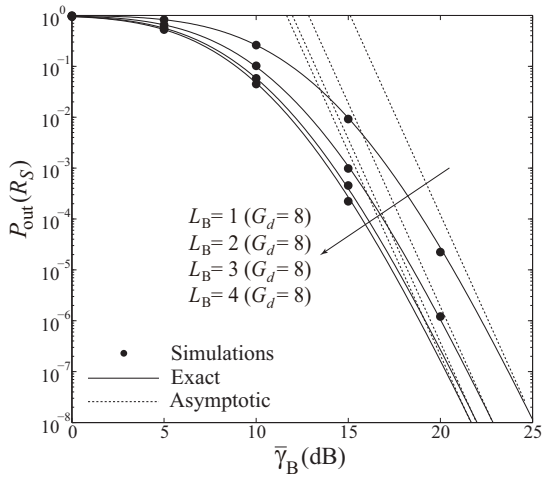

Fig. 1. The secrecy outage probability versus $\overline{\gamma}_{\text{B}}$ for $N_{\text{A}} = 2$, $N_{\text{B}} = 4$, $\overline{\gamma}_{\text{E}} = 5$ dB, $N_{\text{E}} = 3$, and $L_{\text{E}} = 2$.

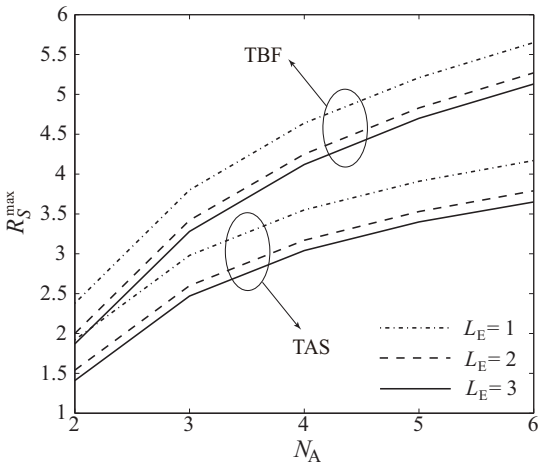

Fig. 2. Comparison of ε-outage secrecy rate between TAS and TBF versus N_{A} for $\overline{\gamma}_{\text{B}} = 20$ dB, $N_{\text{B}} = 1$, $\overline{\gamma}_{\text{E}} = 0$ dB, and $N_{\text{E}} = 3$.

TAS/GSC provides a cost-performance tradeoff in physical layer security enhancement.

Fig. 2 compares the ε-outage secrecy rate of TAS with that of TBF versus N_{A} for $\varepsilon = 0.01$. We consider the same TBF as in [9] where maximal ratio transmission is used at Alice and a single antenna is equipped at Bob. As such, we consider $N_{\text{B}} = 1$ in Fig. 2 for the sake of a fair comparison. To facilitate this comparison, we derive a new expression for the secrecy outage probability of TBF with GSC at the eavesdropper by applying $F_{\gamma_{\text{E}}}(\gamma)$ in (6) with [9, eq. (38)], which results in

$$P_{\text{out}}(R_S)_{\text{TBF}} = 1 - \sum_{n=1}^{N_{\text{A}}} \binom{N_{\text{A}}}{n} (-1)^n e^{-\frac{n\left(2^{R_S}-1\right)}{\overline{\gamma}_{\text{B}}}} \times \left[2^{R_S} n \sum_{l_{\text{E}}=1}^{L_{\text{E}}} \frac{\epsilon_{l_{\text{E}}}}{\overline{\gamma}_{\text{B}}} \left(\frac{2^{R_S} n}{\overline{\gamma}_{\text{B}}} + \frac{1}{\overline{\gamma}_{\text{E}}} \right)^{-l_{\text{E}}} - \sum_{l_{\text{E}}=L_{\text{E}}+1}^{N_{\text{E}}} \frac{\epsilon_{l_{\text{E}}} l_{\text{E}}}{L_{\text{E}} \overline{\gamma}_{\text{E}}} \left(\frac{2^{R_S} n}{\overline{\gamma}_{\text{B}}} + \frac{l_{\text{E}}}{L_{\text{E}} \overline{\gamma}_{\text{E}}} \right)^{-1} \right]. \quad (17)$$

As expected, Fig. 2 shows that $R_S^{\max}$ increases with N_{A} for both TAS and TBF. Notably, we observe that $R_S^{\max}$ of TAS is close to $R_S^{\max}$ of TBF when N_{A} is small. We also observe that the rate advantage of TBF over TAS increases with N_{A}. However, this advantage comes at the cost of higher feedback and signal processing overheads for TBF. Importantly, the feedback and signal processing overheads for TBF increase with N_{A}, while those for TAS remain unchanged.

V. Conclusion

We proposed TAS/GSC for physical layer security enhancement in MIMO wiretap channels. We derived new closed-form expressions for the exact and the asymptotic secrecy outage probability, which demonstrate that the maximum secrecy outage diversity gain of $N_{\text{A}}N_{\text{B}}$ is achieved. The tradeoff of TAS/GSC relative to TAS/SC and TAS/MRC is characterized by their respective secrecy outage SNR gains.

References

[1] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Commun. Mag.*, pp. 66–74, Apr. 2011.

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

[3] H. V. Poor, "Information and inference in the wireless physical layer," *IEEE Commun. Mag.*, pp. 40–47, Feb. 2012.

[4] 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.

[5] F. He, H. Man, and W. Wang, "Maximal ratio diversity combining enhanced security," *IEEE Commun. Lett.*, vol. 15, no. 5, pp. 509–511, May 2011.

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

[7] 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.

[8] G. Geraci, M. Egan, J. Yuan, A. Razi, and I. B. Collings, "Secrecy sum-rates for multi-user MIMO regularized channel inversion precoding," *IEEE Trans. Commun.*, vol. 60, no. 11, pp. 3472–3482, Nov. 2012.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] X. Cai and G. B. Giannakis, "Performance analysis of combined transmit selection diversity and receive generalized selection combining in Rayleigh fading channels," *IEEE Trans. Wireless Commun.*, vol. 3, no. 6, pp. 1980–1983, Nov. 2004.

[14] R. K. Mallik, P. Gupta, and Q. T. Zhang, "Minimum selection GSC in independent Rayleigh fading," *IEEE Trans. Veh. Technol.*, vol. 54, no. 3, pp. 1013–1021, May 2005.

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