Secrecy Enhancement of Multiuser MISO Networks Using OSTBC and Artificial Noise

Maoqiang Yang, *Student Member, IEEE*, Bangning Zhang, *Member, IEEE*, Yuzhen Huang, *Member, IEEE*, Nan Yang, *Member, IEEE*, Daniel Benevides da Costa, *Senior Member, IEEE*, and Daoxing Guo, *Member, IEEE*

***Abstract*—In this paper, we propose a novel physical layer strategy to improve the secrecy performance of multiuser multiple-input single-output networks. In this strategy, orthogonal space-time block code (OSTBC) is employed at an A_A-antenna base station (BS) and artificial noise (AN) is employed at an A_J-antenna cooperative relay to enhance the security level of the network. Moreover, two opportunistic scheduling schemes, namely, selection combining (SC) and scan-and-wait combining (SWC), are leveraged to select one legitimate user for data transmission. To evaluate the secrecy performance of the proposed OSTBC-SC-AN and OSTBC-SWC-AN schemes, we derive new exact closed-form expressions for the secrecy outage probability and the effective secrecy throughput. Using numerical results, we show that the OSTBC-SWC-AN scheme outperforms the OSTBC-SC-AN scheme when the switching threshold is carefully chosen. We also show that increasing A_A brings down the secrecy performance in the presence of a high switching threshold.**

***Index Terms*—Physical layer security, orthogonal space-time block codes, artificial noise, secrecy performance.**

I. Introduction

The information security has become an increasingly important issue in the design and implementation of wireless networks, due to the broadcast nature of the wireless medium. By exploiting the spatio-temporal characteristics of the wireless medium, physical layer security (PLS) has been extensively investigated to provide additional confidentiality protection for wireless networks in recent years [1].

Remarkably, various advanced signal processing techniques, e.g., multiple-input multiple-output (MIMO) techniques, relay-aided techniques, and multiuser diversity, have been explored to improve the secrecy performance of wireless communications systems. Considering MIMO wiretap channels, [2] studied the PLS achieved by using orthogonal space-time block code (OSTBC) with arbitrary transmit/receive antenna correlation. The impact of transmit antenna selection (TAS) on the PLS performance was established in [3, 4]. Focusing on Nakagami-m fading channels, [5] evaluated TAS with receive generalized selection combining. Very recently, [6, 7] designed the optimal artificial noise (AN)-based secure transmission schemes. Considering relay-aided wiretap channels, [8] proposed a two-stage scheme to boost the security of cooperative single-carrier systems via joint relay and destination selection. Differing from [8], [9] exploited the cooperative beamforming and user selection techniques for secrecy improvement. Building upon the aforementioned studies on the single-user wiretap channel, the secrecy performance of the multiuser wiretap channels has recently been evaluated. For example, [10] examined the impact of TAS and threshold-based selection diversity (tSD) on the secrecy performance over Nakagami-m fading. [11] studied the secure multiuser communications with TAS and cooperative jamming in wireless sensor networks, where the switch-and-stay combining (SSC) scheduling scheme is exploited over the sensor nodes.

We note that the scan-and-wait combining (SWC) scheme, proposed in [12], is an effective approach to realize multiuser diversity with a low implementation complexity and achieve a tradeoff between performance and delay. Specifically, this scheme conducts a sequential scan of all the available diversity branches and selects the first branch whose channel quality is not less than a predefined switching threshold as the acceptable branch. If no branch meets the required channel quality, the SWC scheme waits for a channel coherence time and then repeats the scanning. Despite the potential benefits, the secrecy performance achieved by the SWC scheme in multiuser MISO networks has not been examined thus far.

In this paper, we propose a novel PLS strategy for multiuser MISO networks where both the A_A-antenna base station (BS) and the A_J-antenna cooperative relay help the secure transmission in the presence of an A_E-antenna eavesdropper. In the proposed strategy, OSTBC is used at the BS to enable transmit multi-antenna diversity [13] and AN is explored at the cooperative relay to boost the security level of the considered network. Moreover, the selection combining (SC) scheme and the SWC scheme are adopted among the legitimate users to

This work was supported by the National Science Foundation of China (No. 61501507). Jiangsu Provincial Natural Science Foundation of China (No. BK20150719), and China Postdoctoral Science Foundation Funded Project (No. 2017M610066). The work of Nan Yang is supported by the Australian Research Council Discovery Project (DP150103905).

M. Yang, B. Zhang, and D. Guo are with the College of Communications Engineering, PLA University of Science and Technology, Nanjing 210007, China (e-mails: yyypub@163.com; zbnpub@163.com; nsagfg@163.com)

Y. Huang is with the College of Communications Engineering, PLA University of Science and Technology, Nanjing 210007, China, and also with the School of Information and Communication, Beijing University of Posts and Telecommunications, Beijing 100876, China (e-mail: yzh_huang@sina.com).

N. Yang is with the Research School of Engineering, Australian National University, Canberra, ACT 2601, Australia (email: nan.yang@anu.edu.au.)

D. B. da Costa is with the Department of Computer Engineering, Federal University of Ceará (UFC), Campus Sobral, Ceará, Brazil (e-mail: danielbcosta@ ieee.org).

Corresponding author: D. Guo.

Digital Object Identifier 10.1109/TVT.2017.2725643

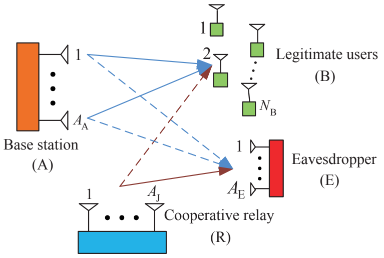

Fig. 1. The illustration of the multiuser MISO network where both the BS and the cooperative relay help the secure transmission to one selected legitimate user in the presence of an eavesdropper.

select one user for data transmission. We derive new exact closed-form expressions for the secrecy outage probability and the effective secrecy throughput to examine the secrecy performance achieved by the OSTBC-SC-AN and OSTBC-SWC-AN schemes. Numerical results are provided to demonstrate the validity of our derived expressions and reveal the impact of key network parameters on the secrecy performance.

II. System Model

As illustrated in Fig. 1, we consider the downlink of a multiuser MISO network, in which one BS with A_A antennas serves N_B single-antenna legitimate users in the presence of an A_E-antenna eavesdropper. In order to strengthen the eavesdropping capability, we assume that the eavesdropper adopts maximal ratio combining (MRC) scheme to wiretap the messages. In this network, one A_J-antenna cooperative relay acts as a friendly jammer. We use A, R, B, and E to represent the BS, cooperative relay, legitimate users, and eavesdropper, respectively. We assume that the A → B link, A → E link, and R → E link are subject to independent and non-identically distributed (i.n.i.d) quasi-static Rayleigh fading, where the fading coefficients are constant over a frame of consecutive $2L$ symbols and varies from one frame to another. We also assume that the frame length keeps the same for all the channels and is long enough to allow capacity-achieving codes within each frame.

We propose that OSTBC is employed at the BS and AN is employed at the cooperative relay to enhance the security level of the network. Moreover, we consider the use of SC or SWC to schedule one out of N_B legitimate users for data transmission. The transmission process of the OSTBC-SC-AN and OSTBC-SWC-AN schemes are detailed as follows:

The BS first selects L transmit symbols, $s_1, s_2, ..., s_L$, with $\mathbb{E}\left[|s_l|^2\right] = \mathcal{P}_\mathrm{A}, \forall l$, where $\mathbb{E}[\cdot]$ represents expectation and $\mathcal{P}_\mathrm{A}$ denotes the transmit power at the BS. Then, an $A_\mathrm{A} \times T$ OSTBC is adopted at the BS in T times slots. With the aid of [2, 13], the received SNR at the k-th user ($1 \leq k \leq N_\mathrm{B}$) is given by

$$\gamma_{\mathrm{B},k} = \frac{\mathcal{P}_\mathrm{A}}{\sigma_\mathrm{B}^2} \left\|\mathbf{h}_{\mathrm{AB},k}\right\|_F^2, \tag{1}$$

where $\mathbf{h}_{\mathrm{AB},k}$ denotes the $A_\mathrm{A} \times 1$ channel vector for the BS to k-th legitimate user channel whose entries follow i.i.d. Rayleigh fading, $\|\cdot\|_F^2$ represents the Frobenius norm and σ_B^2 is the variance of additive white Gaussian noise (AWGN) at the legitimate user.

When the SC scheme is employed, the user with the best channel quality is selected. Thus, we have the received SNR at the selected user as $\gamma_\mathrm{B} = \max_{1 \leq k \leq N_\mathrm{B}} \{\gamma_{\mathrm{B},k}\}$. When the SWC scheme is employed, the first user compares its received SNR $\gamma_{\mathrm{B},1}$ with the predefined threshold γ_T. If $\gamma_{\mathrm{B},1} \geq \gamma_\mathrm{T}$, then this user is selected for transmission in the upcoming data burst and $\gamma_\mathrm{B} = \gamma_{\mathrm{B},1}$. Otherwise, the next user compares its received SNR, $\gamma_{\mathrm{B},2}$, with γ_T. This procedure repeats until either an acceptable user is found or all the users have been examined. In the latter case, the BS waits for a period of time to buffer the input data instead of transmitting. After the waiting period ends, the BS re-initiates the same procedure. We note that in our context the selected legitimate user feeds its received SNR back to the BS through a specific uplink for wiretap codes construction, which is different from the scenario without secrecy consideration.

We assume that the selected legitimate user transmits pilot signals to the cooperative relay at the same frequency as that of B → R link, and the relay obtains the $A_\mathrm{J} \times 1$ precise CSI vector of the R → B link, $\mathbf{h}_\mathrm{RB}$ through channel reciprocity. To enable the cooperative relay to send AN signals, we first design an $A_\mathrm{J} \times A_\mathrm{J}$ unitary beamforming matrix as $\mathbf{W} = [\mathbf{w}_\mathrm{RB}, \mathbf{W}_\mathrm{RE}]$, where $\mathbf{w}_\mathrm{RB}$ is an $A_\mathrm{J} \times 1$ vector used for the R → B link and $\mathbf{W}_\mathrm{RE}$ is an $A_\mathrm{J} \times (A_\mathrm{J} - 1)$ matrix used for the remaining directions. We then choose $\mathbf{w}_\mathrm{RB}$ as the main eigenvector corresponding to the largest eigenvalue of $\mathbf{h}_\mathrm{RB}\mathbf{h}_\mathrm{RB}^\dagger$. We further choose $\mathbf{W}_\mathrm{RE}$ as the remaining $A_\mathrm{J} - 1$ eigenvectors of $\mathbf{h}_\mathrm{RB}\mathbf{h}_\mathrm{RB}^\dagger$ such that $\mathbf{W}_\mathrm{RE}$ lies in the nullspace of $\mathbf{h}_\mathrm{RB}$, i.e., $\mathbf{h}_\mathrm{RB}\mathbf{W}_\mathrm{RE} = \mathbf{0}$. Using $\mathbf{W}$, the cooperative relay transmits AN signals in all directions except towards the selected legitimate user within the data burst. We further assume that $A_\mathrm{J} > A_\mathrm{E}$, thus the eavesdropper cannot remove the AN signals [7, 14].

Without loss of generality, we take into account the practical assumption where the relay has no knowledge about the CSI of the R → E link. Thus, the relay uniformly allocates its transmit power $\mathcal{P}_\mathrm{J}$ across the $(A_\mathrm{J} - 1)$ transmit antennas. It follows that the instantaneous signal-to-interference plus noise ratio (SINR) at the eavesdropper is expressed as

$$\gamma_\mathrm{E} = \frac{\frac{\mathcal{P}_\mathrm{A}}{\sigma_\mathrm{E}^2} \left\|\mathbf{H}_\mathrm{AE}\right\|_F^2}{\frac{\mathcal{P}_\mathrm{J}}{(A_\mathrm{J}-1)\sigma_\mathrm{E}^2} \left\|\mathbf{H}_\mathrm{RE}\mathbf{W}_\mathrm{RE}\right\|_F^2 + 1}, \tag{2}$$

where $\mathbf{H}_\mathrm{AE}$ denotes the $A_\mathrm{E} \times A_\mathrm{A}$ channel matrix of the A → E link and $\mathbf{H}_\mathrm{RE}$ denotes the $A_\mathrm{E} \times A_\mathrm{J}$ channel matrix of the R → E link, whose entries follow i.i.d. Rayleigh fading. σ_E^2 represents the variance of AWGN at the eavesdropper.

Using γ_B and γ_E, we define $\mathcal{C}_\mathrm{B} \triangleq \log(1 + \gamma_\mathrm{B})$ and $\mathcal{C}_\mathrm{E} \triangleq \log(1 + \gamma_\mathrm{E})$ as the instantaneous rate of the legitimate channel and the eavesdropper's channel, respectively. Therefore, the achievable secrecy rate of the multiuser MISO network is given by $\mathcal{C}_\mathrm{s} = [\mathcal{C}_\mathrm{B} - \mathcal{C}_\mathrm{E}]^+$, where $[u]^+ = \max(u, 0)$. For simplicity, we define $\overline{\gamma}_\mathrm{B} = \mathcal{P}_\mathrm{A}/\sigma_\mathrm{B}^2, \overline{\gamma}_\mathrm{E} = \mathcal{P}_\mathrm{A}/\sigma_\mathrm{E}^2$, and $\overline{\gamma}_\mathrm{J} = \mathcal{P}_\mathrm{J}/\sigma_\mathrm{E}^2$. In addition, we denote λ_BE as the main-to-eavesdropper ratio (MER), where $\lambda_\mathrm{BE} = \overline{\gamma}_\mathrm{B}/\overline{\gamma}_\mathrm{E}$.

III. Secrecy Performance Analysis

In this section, we first derive new exact closed-form expressions for the secrecy outage probability achieved by the OSTBC-SC-AN and OSTBC-SWC-AN schemes. Based on these expressions, we then evaluate the effective secrecy throughput of the considered network.

A. Preliminaries

Based on (1) and using the statistics of a Rayleigh faded SNR, the cumulative distribution function (CDF) of $\gamma_{\mathrm{B},k}$ is derived as

$$F_{\gamma_{\mathrm{B},k}}\left(x\right) = 1 - \exp\left(-\frac{x}{\overline{\gamma}_{\mathrm{B}}}\right) \sum_{n=0}^{A_{\mathrm{A}}-1} \frac{1}{n!}\left(\frac{x}{\overline{\gamma}_{\mathrm{B}}}\right)^{n}. \tag{3}$$

We now make the assumption that all the legitimate channels undergo independent and identical distribution (i.i.d.) Rayleigh fading[1]. When the SC scheme is adopted, we obtain the CDF of γ_{B} using the multinomial theorem, which gives

$$F^{\mathrm{I}}_{\gamma_{\mathrm{B}}}\left(x\right) = \sum_{q=0}^{N_{\mathrm{B}}} \binom{N_{\mathrm{B}}}{q} (-1)^{q} \exp\left(-\frac{qx}{\overline{\gamma}_{\mathrm{B}}}\right) \Theta_{A_{\mathrm{A}},q}\left(\frac{x}{\overline{\gamma}_{\mathrm{B}}}\right)^{\phi}, \tag{4}$$

where

$$\Theta_{A_{\mathrm{A}},q} = \sum_{n_1=0}^{q}\sum_{n_2=0}^{n_1}\cdots\sum_{n_{A_{\mathrm{A}}-1}=0}^{n_{A_{\mathrm{A}}-2}} \frac{q!}{n_{A_{\mathrm{A}}-1}!} \prod_{t=1}^{A_{\mathrm{A}}-1} \frac{(t!)^{n_{t+1}-n_t}}{(n_{t-1}-n_t)!},$$

with $n_0 = q, n_{A_{\mathrm{A}}} = 0$, and $\phi = \sum_{q_0=1}^{A_{\mathrm{A}}-1} n_{q_0}$. When the SWC scheme is used, according to [12], the CDF of γ_{B} is given by

$$F^{\mathrm{II}}_{\gamma_{\mathrm{B}}}\left(x\right) = \begin{cases} 0, & x < \gamma_{\mathrm{T}} \\ \frac{F_{\gamma_{\mathrm{B},k}}(\gamma_{\mathrm{T}})}{1-F_{\gamma_{\mathrm{B},k}}(\gamma_{\mathrm{T}})}\left(\frac{F_{\gamma_{\mathrm{B},k}}(x)}{F_{\gamma_{\mathrm{B},k}}(\gamma_{\mathrm{T}})}-1\right), & x \geq \gamma_{\mathrm{T}}. \end{cases} \tag{5}$$

We further examine the probability density function (PDF) of γ_{E}. According to (2), the PDF of γ_{E} is derived as

$$f_{\gamma_{\mathrm{E}}}\left(x\right) = \frac{x^{A_{\mathrm{A}}A_{\mathrm{E}}-1}\exp\left(-\frac{x}{\overline{\gamma}_{\mathrm{E}}}\right)}{\Gamma\left(A_{\mathrm{A}}A_{\mathrm{E}}\right)\Gamma\left(A_{\mathrm{E}}\rho\right)\overline{\gamma}_{\mathrm{J}}^{A_{\mathrm{E}}\rho}\overline{\gamma}_{\mathrm{E}}^{A_{\mathrm{A}}A_{\mathrm{E}}}} \sum_{n=0}^{A_{\mathrm{A}}A_{\mathrm{E}}} \binom{A_{\mathrm{A}}A_{\mathrm{E}}}{n} \times \frac{\Gamma\left(A_{\mathrm{E}}\left(A_{\mathrm{A}}+\rho\right)-n\right)}{\rho^{A_{\mathrm{A}}A_{\mathrm{E}}-n}}\left(\frac{x}{\overline{\gamma}_{\mathrm{E}}\rho}+\frac{1}{\overline{\gamma}_{\mathrm{J}}}\right)^{-\left(A_{\mathrm{E}}\left(A_{\mathrm{A}}+\rho\right)-n\right)}, \tag{6}$$

where $\rho = A_{\mathrm{J}} - 1$ and $\Gamma\left(\cdot\right)$ represents the gamma function.

Proof: For the sake of clarity, we first define $\mathcal{X} = \overline{\gamma}_{\mathrm{E}}\left\|\mathbf{H}_{\mathrm{AE}}\right\|_F^2$ and $\mathcal{Y} = \overline{\gamma}_{\mathrm{J}}\left\|\mathbf{H}_{\mathrm{RE}}\mathbf{W}_{\mathrm{RE}}\right\|_F^2$ in (2). With the help of [15], the PDF of $\mathcal{Y}$ is given by

$$f_{\mathcal{Y}}\left(y\right) = \frac{y^{A_{\mathrm{E}}\rho-1}}{\Gamma\left(A_{\mathrm{E}}\rho\right)\overline{\gamma}_{\mathrm{J}}^{A_{\mathrm{E}}\rho}}\exp\left(-\frac{y}{\overline{\gamma}_{\mathrm{J}}}\right). \tag{7}$$

By applying order statistics, the CDF of γ_{E} is derived as

$$F_{\gamma_{\mathrm{E}}}\left(z\right) = \Pr\left[\frac{\mathcal{X}}{\frac{\mathcal{Y}}{\rho}+1} < z\right] = \int_0^{\infty} F_{\mathcal{X}}\left(z\left(\frac{y}{\rho}+1\right)\right) f_{\mathcal{Y}}\left(y\right)dy. \tag{8}$$

Then we take derivative of (8) to obtain the PDF of γ_{E} as

$$f_{\gamma_{\mathrm{E}}}\left(z\right) = \int_0^{\infty}\left(\frac{y}{\rho}+1\right) f_{\mathcal{X}}\left(z\left(\frac{y}{\rho}+1\right)\right) f_{\mathcal{Y}}\left(y\right)dy. \tag{9}$$

We further obtain the PDF of $\mathcal{X}$ as

$$f_{\mathcal{X}}\left(x\right) = \frac{x^{A_{\mathrm{A}}A_{\mathrm{E}}-1}}{\Gamma\left(A_{\mathrm{A}}A_{\mathrm{E}}\right)\overline{\gamma}_{\mathrm{E}}^{A_{\mathrm{A}}A_{\mathrm{E}}}}\exp\left(-\frac{x}{\overline{\gamma}_{\mathrm{E}}}\right). \tag{10}$$

By substituting (7) and (10) into (9), and utilizing [16, Eq. (3.326.2)] to perform some mathematical manipulations, we obtain (6), which completes the proof. ■

B. Secrecy Outage Probability

According to the definition in [3], the secrecy outage probability is characterized as the probability that the achievable secrecy rate $\mathcal{C}_{\mathrm{s}}$ is less than a predetermined secrecy transmission rate R_{s}. Therefore, we express the secrecy outage probability as

$$\begin{aligned} P_{\mathrm{out}}\left(R_{\mathrm{s}}\right) &= \Pr\left[\mathcal{C}_{\mathrm{s}} < R_{\mathrm{s}}\right] \\ &= \int_0^{\infty} F_{\gamma_{\mathrm{B}}}\left(2^{R_{\mathrm{s}}}\left(1+y\right)-1\right) f_{\gamma_{\mathrm{E}}}\left(y\right)dy, \end{aligned} \tag{11}$$

We next present the secrecy outage probability for the proposed schemes.

1) OSTBC-SC-AN Scheme: By substituting (4) and (6) into (11) and applying [16, Eq. (9.211.4)], the exact closed-form expression for the secrecy outage probability of the OSTBC-SC-AN scheme $P^{\mathrm{I}}_{\mathrm{out}}\left(R_{\mathrm{s}}\right)$ is derived as (12).

2) OSTBC-SWC-AN Scheme: We first rewrite (11) as

$$P_{\mathrm{out}}\left(R_{\mathrm{s}}\right) = \begin{cases} \int_0^{\Omega_{\gamma_{\mathrm{T}}}} F_{\gamma_{\mathrm{B}}}\left(\theta\left(x\right)\right) f_{\gamma_{\mathrm{E}}}\left(x\right)dx \\ \quad + \int_{\Omega_{\gamma_{\mathrm{T}}}}^{\infty} F_{\gamma_{\mathrm{B}}}\left(\theta\left(x\right)\right) f_{\gamma_{\mathrm{E}}}\left(x\right)dx, & \Omega_{\gamma_{\mathrm{T}}} > 0 \\ \int_0^{\infty} F_{\gamma_{\mathrm{B}}}\left(\theta\left(x\right)\right) f_{\gamma_{\mathrm{E}}}\left(x\right)dx, & \Omega_{\gamma_{\mathrm{T}}} \leq 0 \end{cases}, \tag{13}$$

where $\theta\left(x\right) = 2^{R_{\mathrm{s}}}\left(1+x\right)-1$ and $\Omega_{\gamma_{\mathrm{T}}} = 2^{-R_{\mathrm{s}}}\left(1+\gamma_{\mathrm{T}}\right)-1$. By substituting (5) and (6) into (13) and performing mathematical manipulations using [16, Eqs. (1.111) and (9.211.4)], we derive the exact closed-form expression for the secure outage probability of the OSTBC-SWC-AN scheme as

$$P^{\mathrm{II}}_{\mathrm{out}}\left(R_{\mathrm{s}}\right) = \begin{cases} P^{\text{II-A}}_{\mathrm{out}}\left(R_{\mathrm{s}}\right), & \Omega_{\gamma_{\mathrm{T}}} > 0 \\ P^{\text{II-B}}_{\mathrm{out}}\left(R_{\mathrm{s}}\right), & \Omega_{\gamma_{\mathrm{T}}} \leq 0 \end{cases}, \tag{14}$$

where $P^{\text{II-A}}_{\mathrm{out}}\left(R_{\mathrm{s}}\right)$ and $P^{\text{II-B}}_{\mathrm{out}}\left(R_{\mathrm{s}}\right)$ are given by (15) and (16), respectively, and $\Gamma\left(\cdot,\cdot\right)$ and $\Psi\left(\cdot,\cdot,\cdot\right)$ denote the upper incomplete Gamma function [16, Eq. (8.350.2)] and the confluent hypergeometric function of the second kind [16, Eq. (9.211.4)], respectively.

We clarify that the derived exact expressions in (12), (15), and (16) only obtain easy-to-compute functions. Moreover, these expressions hold for general networks with arbitrary A_{A}, A_{E}, A_{J}, and N_{B}.

C. Effective Secrecy Throughput

Based on its definition in [6, 7], the effective secrecy throughput is defined as the product of the complementary probability of $P_{\mathrm{out}}\left(R_{\mathrm{s}}\right)$ and the predetermined secrecy rate R_{s}. Thus, the effective secrecy throughput is given

[1] We assume that the legitimate users are located relatively close together, e.g., in a clustered structure. This assumption is commonly adopted in the context of cooperative multiuser systems.

$$P_{\mathrm{out}}^{\mathrm{I}}\left(R_{\mathrm{s}}\right)=\sum_{q=0}^{N_{\mathrm{B}}}\binom{N_{\mathrm{B}}}{q}(-1)^{q}\exp\left(-\frac{2^{R_{\mathrm{s}}}-1}{\overline{\gamma}_{\mathrm{B}}}q\right)\frac{\Theta_{A_{\mathrm{A}},q}}{\overline{\gamma}_{\mathrm{B}}^{\phi}}\sum_{q_1=0}^{\phi}\binom{\phi}{q_1}\left(2^{R_{\mathrm{s}}}\overline{\gamma}_{\mathrm{E}}\right)^{q_1}\left(2^{R_{\mathrm{s}}}-1\right)^{\phi-q_1}\sum_{n=0}^{A_{\mathrm{A}}A_{\mathrm{E}}}\binom{A_{\mathrm{A}}A_{\mathrm{E}}}{n}\left(\frac{\rho}{\overline{\gamma}_{\mathrm{J}}}\right)^{q_1+n}$$
$$\times\frac{\Gamma\left(A_{\mathrm{E}}\left(A_{\mathrm{A}}+\rho\right)-n\right)}{\Gamma\left(A_{\mathrm{A}}A_{\mathrm{E}}\right)\Gamma\left(A_{\mathrm{E}}\rho\right)}\Gamma\left(A_{\mathrm{A}}A_{\mathrm{E}}+q_1\right)\Psi\left(A_{\mathrm{A}}A_{\mathrm{E}}+q_1,q_1+n-A_{\mathrm{E}}\rho+1;\left(\frac{2^{R_{\mathrm{s}}}q}{\overline{\gamma}_{\mathrm{B}}}+\frac{1}{\overline{\gamma}_{\mathrm{E}}}\right)\frac{\rho\overline{\gamma}_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{J}}}\right). \tag{12}$$

$$P_{\mathrm{out}}^{\mathrm{II\text{-}A}}\left(R_{\mathrm{s}}\right)=\sum_{n=0}^{A_{\mathrm{A}}A_{\mathrm{E}}}\binom{A_{\mathrm{A}}A_{\mathrm{E}}}{n}\frac{\Gamma\left(A_{\mathrm{E}}\left(A_{\mathrm{A}}+\rho\right)-n\right)}{\Gamma\left(A_{\mathrm{A}}A_{\mathrm{E}}\right)\Gamma\left(A_{\mathrm{E}}\rho\right)}\exp\left(\frac{\rho}{\overline{\gamma}_{\mathrm{J}}}\right)\sum_{q_1=0}^{A_{\mathrm{A}}A_{\mathrm{E}}-1}\binom{A_{\mathrm{A}}A_{\mathrm{E}}-1}{q_1}(-1)^{q_1}\left(\frac{\rho}{\overline{\gamma}_{\mathrm{J}}}\right)^{q_1+A_{\mathrm{E}}\rho}$$
$$\times\Gamma\left(n-q_1-A_{\mathrm{E}}\rho,\frac{\rho}{\overline{\gamma}_{\mathrm{J}}}\left(1+\frac{\overline{\gamma}_{\mathrm{J}}\Omega_{\gamma_{\mathrm{T}}}}{\rho\overline{\gamma}_{\mathrm{E}}}\right)\right)-\frac{\exp\left(-\frac{2^{R_{\mathrm{s}}}-1}{\overline{\gamma}_{\mathrm{B}}}\right)}{1-F_{\gamma_{\mathrm{B},k}}\left(\gamma_{\mathrm{T}}\right)}\sum_{m=0}^{A_{\mathrm{A}}-1}\frac{1}{m!}\sum_{t=0}^{m}\binom{m}{t}\left(\frac{2^{R_{\mathrm{s}}}\overline{\gamma}_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{B}}}\right)^{t}\left(\frac{2^{R_{\mathrm{s}}}-1}{\overline{\gamma}_{\mathrm{B}}}\right)^{m-t}$$
$$\times\sum_{n=0}^{A_{\mathrm{A}}A_{\mathrm{E}}}\binom{A_{\mathrm{A}}A_{\mathrm{E}}}{n}\left(\frac{\overline{\gamma}_{\mathrm{J}}}{\rho}\right)^{-(t+n)}\frac{\Gamma\left(A_{\mathrm{E}}\left(A_{\mathrm{A}}+\rho\right)-n\right)}{\Gamma\left(A_{\mathrm{A}}A_{\mathrm{E}}\right)\Gamma\left(A_{\mathrm{E}}\rho\right)}\exp\left(\left(\frac{2^{R_{\mathrm{s}}}}{\overline{\gamma}_{\mathrm{B}}}+\frac{1}{\overline{\gamma}_{\mathrm{E}}}\right)\frac{\rho\overline{\gamma}_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{J}}}\right)\sum_{q_1=0}^{A_{\mathrm{A}}A_{\mathrm{E}}+t-1}\binom{A_{\mathrm{A}}A_{\mathrm{E}}+t-1}{q_1}$$
$$\times(-1)^{q_1}\left(\left(\frac{2^{R_{\mathrm{s}}}}{\overline{\gamma}_{\mathrm{B}}}+\frac{1}{\overline{\gamma}_{\mathrm{E}}}\right)\frac{\rho\overline{\gamma}_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{J}}}\right)^{-(n+t-q_1-A_{\mathrm{E}}\rho)}\Gamma\left(n+t-q_1-A_{\mathrm{E}}\rho,\left(\frac{2^{R_{\mathrm{s}}}}{\overline{\gamma}_{\mathrm{B}}}+\frac{1}{\overline{\gamma}_{\mathrm{E}}}\right)\frac{\rho\overline{\gamma}_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{J}}}\left(1+\frac{\overline{\gamma}_{\mathrm{J}}\Omega_{\gamma_{\mathrm{T}}}}{\rho\overline{\gamma}_{\mathrm{E}}}\right)\right). \tag{15}$$

$$P_{\mathrm{out}}^{\mathrm{II\text{-}B}}\left(R_{\mathrm{s}}\right)=\sum_{n=0}^{A_{\mathrm{A}}A_{\mathrm{E}}}\binom{A_{\mathrm{A}}A_{\mathrm{E}}}{n}\left(\frac{\rho}{\overline{\gamma}_{\mathrm{J}}}\right)^{n}\frac{\Gamma\left(A_{\mathrm{E}}\left(A_{\mathrm{A}}+\rho\right)-n\right)}{\Gamma\left(A_{\mathrm{E}}\rho\right)}\Psi\left(A_{\mathrm{A}}A_{\mathrm{E}},n-A_{\mathrm{E}}\rho+1;\frac{\rho}{\overline{\gamma}_{\mathrm{J}}}\right)-\frac{\exp\left(-\frac{2^{R_{\mathrm{s}}}-1}{\overline{\gamma}_{\mathrm{B}}}\right)}{1-F_{\gamma_{\mathrm{B},k}}\left(\gamma_{\mathrm{T}}\right)}\sum_{m=0}^{A_{\mathrm{A}}-1}\frac{1}{m!}$$
$$\times\sum_{t=0}^{m}\binom{m}{t}\left(\frac{2^{R_{\mathrm{s}}}\overline{\gamma}_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{B}}}\right)^{t}\left(\frac{2^{R_{\mathrm{s}}}-1}{\overline{\gamma}_{\mathrm{B}}}\right)^{m-t}\sum_{n=0}^{A_{\mathrm{A}}A_{\mathrm{E}}}\binom{A_{\mathrm{A}}A_{\mathrm{E}}}{n}\left(\frac{\rho}{\overline{\gamma}_{\mathrm{J}}}\right)^{t+n}\frac{\Gamma\left(A_{\mathrm{E}}\left(A_{\mathrm{A}}+\rho\right)-n\right)\Gamma\left(A_{\mathrm{A}}A_{\mathrm{E}}+t\right)}{\Gamma\left(A_{\mathrm{A}}A_{\mathrm{E}}\right)\Gamma\left(A_{\mathrm{E}}\rho\right)}$$
$$\times\Psi\left(A_{\mathrm{A}}A_{\mathrm{E}}+t,t+n+1-A_{\mathrm{E}}\rho;\left(\frac{2^{R_{\mathrm{s}}}}{\overline{\gamma}_{\mathrm{B}}}+\frac{1}{\overline{\gamma}_{\mathrm{E}}}\right)\frac{\rho\overline{\gamma}_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{J}}}\right). \tag{16}$$

by $T_{\mathrm{sec}}^{\mathrm{I}}\left(R_{\mathrm{s}}\right)=\left(1-P_{\mathrm{out}}^{\mathrm{I}}\left(R_{\mathrm{s}}\right)\right)R_{\mathrm{s}}$ for the OSTBC-SC-AN scheme and $T_{\mathrm{sec}}^{\mathrm{II}}\left(R_{\mathrm{s}}\right)=\left(1-P_{\mathrm{out}}^{\mathrm{II}}\left(R_{\mathrm{s}}\right)\right)R_{\mathrm{s}}$ for the OSTBC-SWC-AN scheme.

The effective secrecy throughput is a meaningful performance metric since it quantifies the average rate of the messages that are sent from the transmitter to the legitimate user securely in the passive eavesdropping case. We remark that the effective secrecy throughput is different from the widely adopted conventional throughput definition in [17–19], where the throughput quantifies how much of transmitted messages on average but does not evaluate the average amount of the secure transmitted messages.

IV. Numerical Results and Discussions

In this section, we provide representative numerical results to verify our performed theoretical analysis and to evaluate the impact of network parameters on the secrecy performance achieved by the proposed schemes. In Figs. 3-5, we use solid lines and dashed lines to represent the secrecy performance achieved by the OSTBC-SWC-AN scheme and the OSTBC-SC-AN scheme, respectively.

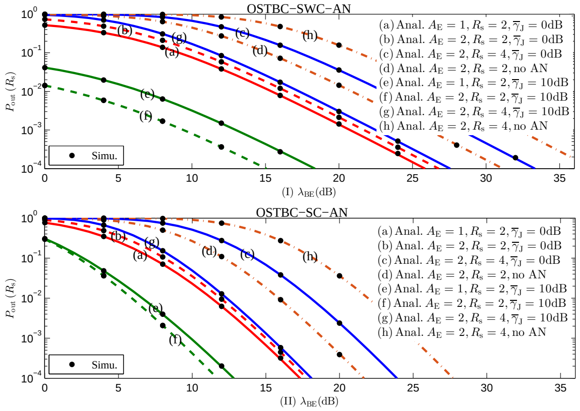

Fig. 2. Secrecy outage probability versus λ_{BE} with $\overline{\gamma}_{\mathrm{E}}=5$dB, $A_{\mathrm{A}}=2$, $A_{\mathrm{J}}=4$, $N_{\mathrm{B}}=2$, and $\gamma_{\mathrm{T}}=10$dB.

Fig. 2 depicts the secrecy outage probability versus MER λ_{BE}. We first observe that the theoretical curves of both proposed schemes match precisely with the Monte Carlo simulations, which validates the accuracy of our derivation. Second, we observe that the secrecy outage probability decreases sharply when λ_{BE} increases and the secrecy performance improves when the secrecy rate R_{s} decreases, e.g., curve (b) and (c), (f) and (g). Third, we remark that if the improved useful signal dominates, the secrecy performance becomes worse when the eavesdropper's antenna number increases, e.g., curve (a) and (b), and if the improved artificial noise dominates, the secrecy performance becomes better when the eavesdropper's antenna number increases, e.g., curve (e) and (f). The dominating factor depends on λ_{BE} and $\overline{\gamma}_{\mathrm{J}}$. Finally, we find that the secrecy performance of the proposed schemes is better than that of the naive cases without AN, e.g., curve (b) and (d), (g) and (h), which demonstrates the effectiveness of our proposed schemes.

Fig. 3 depicts the secrecy outage probability versus the switching threshold γ_{T}. As observed in this figure, the secrecy performance of the OSTBC-SC-AN scheme is independent of γ_{T}, while that of the OSTBC-SWC-AN scheme improves

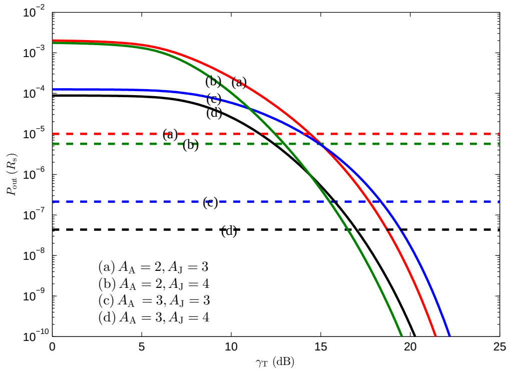

Fig. 3. Secrecy outage probability versus γ_{T} with $R_{\mathrm{s}}=2$, A_{E}=2, $N_{\mathrm{B}}=2$, $\lambda_{\mathrm{BE}}=15$dB, $\overline{\gamma}_{\mathrm{J}}$=10dB, and $\overline{\gamma}_{\mathrm{E}}=5$dB.

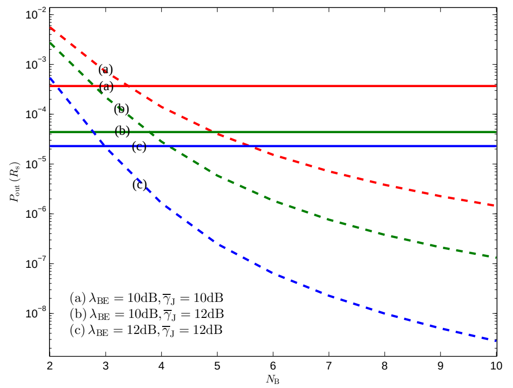

Fig. 4. Secrecy outage probability versus N_{B} with $R_{\mathrm{s}}=3$, $\gamma_{\mathrm{T}}=15$dB, $A_{\mathrm{A}}=A_{\mathrm{E}}=2$, $A_{\mathrm{J}}=4$, and $\overline{\gamma}_{\mathrm{E}}=5$dB.

significantly when γ_{T} increases. We also observe that the OSTBC-SWC-AN scheme outperforms the OSTBC-SC-AN scheme when γ_{T} is higher than a certain value, which implies that the OSTBC-SWC-AN scheme can achieve a better secrecy performance at the cost of time delay for signal retransmission. Third, we observe the curve (a) and (c) for the OSTBC-SWC-AN scheme and find that curve (c) is firstly lower than curve (a) and then slightly higher than curve (a) when γ_{T} increases.

Fig. 4 depicts the secrecy outage probability versus the number of legitimate users N_{B}. We first observe that the secrecy performance of the OSTBC-SWC-AN scheme is independent of N_{B}. We also observe that the secrecy performance of OSTBC-SC-AN scheme improves when N_{B} increases. We further observe that increasing λ_{BE} or the average SNR of jammer's channel, $\overline{\gamma}_{\mathrm{J}}$, brings about a superior secrecy performance for both schemes.

Fig. 5 plots the effective secrecy throughput versus the secrecy rate R_{s}. It is observed that the effective secrecy throughput first increases and then decreases as R_{s} increases from 3 to 7 for both schemes, which reveals that there exists an optimum R_{s}^{*} that yields the maximum effective secrecy throughput. Moreover, we observe that the effective secrecy throughput of the OSTBC-SC-AN scheme is higher than that of the OSTBC-SWC-AN scheme when $\gamma_{\mathrm{T}}=10$ dB, but lower than that of the OSTBC-SWC-AN scheme when $\gamma_{\mathrm{T}}=25$ dB. Furthermore, by observing the effective secrecy throughput of the OSTBC-SC-AN scheme with $\gamma_{\mathrm{T}}=10$ or 25 dB and the effective secrecy throughput of the OSTBC-SWC-AN scheme with $\gamma_{\mathrm{T}}=10$ dB, we find that increasing A_{A} and A_{J} shifts R_{s}^{*} to the right. This reveals that the BS is capable of supporting a larger secure transmission rate when the BS or the cooperative relay can accommodate a larger number of antennas under the considered network parameters.

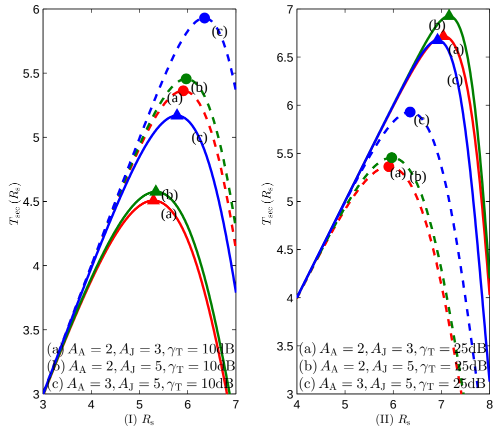

Fig. 5. Effective secrecy throughput versus R_{s} with $\overline{\gamma}_{\mathrm{E}}=5$dB, $\lambda_{\mathrm{BE}}=15$dB, $\overline{\gamma}_{\mathrm{J}}=10$dB, $A_{\mathrm{E}}=2$ and $N_{\mathrm{B}}=2$.

V. Conclusion

We designed new secure transmission schemes for multiuser MISO networks, where OSTBC and AN were exploited at the BS and the cooperative relay, respectively, to enhance the security level and the SC and SWC schemes were explored for user scheduling. We derived new exact closed-form expressions for the secrecy outage probability and the effective secrecy throughput to evaluate the secrecy performance achieved by the proposed OSTBC-SC-AN and OSTBC-SWC-AN schemes. Our results revealed that the OSTBC-SWC-AN scheme outperforms the OSTBC-SC-AN scheme when the switching threshold is carefully chosen. Considering a high switching threshold, we found that increasing the number of antennas at the BS brings down the secrecy performance. Finally, we would like to consider the adoption of AN at the BS as our future work.

References

[1] 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.

[2] N. S. Ferdinand, D. B. da Costa, and M. Latva-aho, "Physical layer security in MIMO OSTBC line-of-sight wiretap channels with arbitrary transmit/receive antenna correlation," *IEEE Wireless Commu. Lett.*, vol. 2, no. 5, pp. 467-470, Oct. 2013.

[3] 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.

[4] 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.

[5] L. Wang, M. Elkashlan, J. Huang, R. Schober, and R. K. Mallik, "Secure transmission with antenna selection in MIMO Nakagami-m fading channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6054-6067, Nov. 2014.

[6] 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.

[7] N. Yang, M. Elkashlan, T. Q. Duong, J. Yuan, and R. Malaney, "Optimal transmission with artificial noise in MISOME wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2170-2181, Apr. 2016.

[8] L. Wang, K. J. Kim, T. Q. Duong, M. Elkashlan, and H. V. Poor, "Security enhancement of cooperative single carrier systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 1, pp. 90-103, Jan. 2015.

[9] T. M. Hoang, T. Q. Duong, H. A. Suraweera, C. Tellambura, and H. V. Poor, "Cooperative beamforming and user selection for improving the security of relay-aided systems," *IEEE Trans. Commun.*, vol. 63, no. 12, pp. 5039-5051, Dec. 2015.

[10] M. Yang, D. Guo, Y. Huang, T. Q. Duong, and B. Zhang, "Physical layer security with threshold-based multiuser scheduling in multi-antenna wireless networks," *IEEE Trans. Commun.*, vol. 64, no. 12, pp. 5189-5202, Dec. 2016.

[11] M. Yang, B. Zhang, Y. Huang, N. Yang, D. Guo, and B. Gao, "Secure multiuser communications in wireless sensor networks with TAS and cooperative jamming," *Sensors*, vol. 16, no. 1908, pp. 1-16, Nov. 2016.

[12] H. -C. Yang, M. K. Simon, and M. S. Alouini, "Scan and wait combining (SWC): A switch and examine strategy with a performance-delay tradeoff," *IEEE Trans. Wireless Commun.*, vol. 5, no. 9, pp. 2477-2483, Sep. 2006.

[13] M. K. Arti and S. K. Jindal, "OSTBC transmission in shadowed-rician land mobile satellite links," *IEEE Trans. Veh. Technol.*, vol. 65, no. 7, pp. 5771-5777, Jul. 2016.

[14] 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.

[15] Y. Huang, J. Wang, C. Zhong, T. Q. Duong, and G. K. Karagiannidis, "Secure transmission in cooperative relaying networks with multiple antennas," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6843-6856, Oct. 2016.

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

[17] 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. on Veh. Technol.*, vol. 62, pp. 2170-2181, Jun. 2013.

[18] B. He and X. Zhou, "Secure On-Off transmission design with channel estimation errors," *IEEE Trans. Inf. Forensics Security*, vol. 8, pp. 1923-1936, Dec. 2013.

[19] X. Zhou, M. R. McKay, B. Maham, and A. Hjorungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Commun. Lett.*, vol. 15, pp. 302-304, Mar. 2011.