Physical Layer Security with Threshold-Based Multiuser Scheduling in Multi-antenna Wireless Networks

Yang, M., Guo, D., Huang, Y., Duong, T. Q., & Zhang, B. (2016). Physical Layer Security with Threshold-Based Multiuser Scheduling in Multi-antenna Wireless Networks. *IEEE Transactions on Communications*. Advance online publication. https://doi.org/10.1109/TCOMM.2016.2606396

Published in:
IEEE Transactions on Communications

Document Version:
Peer reviewed version

Physical Layer Security with Threshold-Based Multiuser Scheduling in Multi-antenna Wireless Networks

Maoqiang Yang, *Student Member*, *IEEE*, Daoxing Guo, *Member*, *IEEE*, Yuzhen Huang, *Member*, *IEEE*, Trung Q. Duong, *Senior Member*, *IEEE*, and Bangning Zhang

***Abstract*—In this paper, we consider a multiuser downlink wiretap network consisting of one base station (BS) equipped with $A_{\rm A}$ antennas, $N_{\rm B}$ single-antenna legitimate users, and $N_{\rm E}$ single-antenna eavesdroppers over Nakagami-m fading channels. In particular, we introduce a joint secure transmission scheme that adopts transmit antenna selection (TAS) at the BS and explores threshold-based selection diversity (tSD) scheduling over legitimate users to achieve a good secrecy performance while maintaining low implementation complexity. More specifically, in an effort to quantify the secrecy performance of the considered system, two practical scenarios are investigated, i.e., Scenario I: the eavesdropper's channel state information (CSI) is unavailable at the BS, and Scenario II: the eavesdropper's CSI is available at the BS. For Scenario I, novel exact closed-form expressions of the secrecy outage probability are derived, which are valid for general networks with an arbitrary number of legitimate users, antenna configurations, number of eavesdroppers, and the switched threshold. For Scenario II, we take into account the ergodic secrecy rate as the principle performance metric, and derive novel closed-form expressions of the exact ergodic secrecy rate. Additionally, we also provide simple and asymptotic expressions for secrecy outage probability and ergodic secrecy rate under two distinct cases, i.e., Case I: the legitimate user is located close to the BS, and Case II: both the legitimate user and eavesdropper are located close to the BS. Our important findings reveal that the secrecy diversity order is $A_{\rm A}m_{\rm A}$ and the slope of secrecy rate is one under Case I, while the secrecy diversity order and the slope of secrecy rate collapse to zero under Case II, where the secrecy performance floor occurs. Finally, when the switched threshold is carefully selected, the considered scheduling scheme outperforms other well known existing schemes in terms of the secrecy performance and complexity tradeoff.**

***Index Terms*—Physical layer security, multiuser switched diversity, threshold-based scheduling scheme, secrecy outage probability, ergodic secrecy rate.**

I. Introduction

SECURITY and privacy have attracted enormous attention in the wireless communications since the inherent broadcast nature of radio propagation makes the data transmission particularly susceptible to malicious attacks [1]. To address intricate secure problems, many researchers have investigated various cryptographic protocols in the upper layer, from which an error-free link of physical layer was assumed to guarantee the reliability of data transmission. As being well-known, the key idea behind traditional cryptographic techniques lies in the complex mathematical operations, which, however, have become increasingly insecure due to the fact that the computational ability of eavesdropper becomes more and more powerful. Motivated by this limitation, physical layer security (PLS) has been introduced as an attractive approach to defend against malicious attack and wiretapping by exploiting the distinct characteristics of different wireless channels. The concept of PLS was pioneered by Shannon in [2], and further extended by Wyner in [3], where the condition of perfect secrecy was analyzed in view of an information-theoretic prospective. Later on, various advanced techniques, i.e., multiple antennas, multiuser diversity, and cooperative relaying, have been broadly exploited to improve the PLS of wireless transmissions.

In recent years, significant research efforts have been devoted to incorporating multi-antenna techniques to improve the performance of wireless communication systems. Specifically, transmit antenna selection (TAS) has been widely investigated due to the low realization complexity of radio frequency (RF) chains while achieving full diversity [4]–[6]. The authors in [7] analyzed the secrecy performance in multiple-input multiple-output (MIMO) wiretap channels with TAS and different receiver combining schemes. In [8], TAS with Alamouti coding and power allocation was addressed in MIMO wiretap channels. Additionally, TAS and receive generalized selection combining (TAS/GSC) was proposed for improving the security in the MIMO wiretap channels [9]. Furthermore, the work [10] investigated the secrecy performance for TAS and maximal ratio combining (TAS/MRC) system with imperfect feedback. More recently, TAS was also carried out both at the multi-antenna primary and secondary transmitter (ST) in cognitive wiretap systems [11], [12], where the ST acts as a friendly jammer to confound the eavesdropper and is granted to share the spectrum of the primary network as a reward. Besides these works, the secrecy performance of antenna-selection-aided MIMO system was addressed in [13] in terms of the probability of zero secrecy capacity and generalized secrecy diversity.

On the other hand, multiuser diversity technique has aroused

This work was supported by the National Science Foundation of China (No. 61401508) and the Jiangsu Provincial Natural Science Foundation of China (No. BK20150719). The work of T. Q. Duong was supported in part by the U.K. Royal Academy of Engineering Research Fellowship under Grant RF1415\14\22.

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

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

much attention from both academia and industry. Different from single user communication systems, multiuser communication systems are more susceptible to malicious attacks [14]–[17]. In [14], the secrecy outage performance of multiuser MIMO systems with TAS and arbitrary number of eavesdroppers was addressed. In [15], the authors investigated the secrecy performance of multiuser downlink networks with the artificial noise by designing an optimal power allocation to maximize the total ergodic secrecy capacity of the system. In [16], to increase the secure degrees of freedom of the main channel, different opportunistic jammer selection schemes were proposed in multiuser wiretap networks. In [17], an optimal user selection scheme for multiuser relaying networks with cooperative jamming was analyzed in terms of the ergodic secrecy rate. In addition, the impact of different scheduling schemes on the secrecy performance of multiuser wiretapping networks has been investigated in [18]–[20]. Particularly, in [18], the authors have explored the PLS of cognitive radio networks with different scheduling schemes and made a comprehensive comparison for the achievable secrecy rate. Later, in [19], an *on-off* opportunistic beamforming for the multiuser downlink channels with a passive eavesdropper was investigated. In [20], two opportunistic scheduling algorithms of multiuser uplink wiretap networks taking into consideration of the fairness among legitimate users were designed. Albeit the above-mentioned works have improved our understanding on the impact of user scheduling on the secrecy performance, the main limitation behind these works is the high complexity of the scheduling schemes owing to the continuous estimation for the channel state information (CSI) of the main channel. As a result, a significant proportion of the air-link resource and battery life of the mobile terminals are utilized for the CSI feedback instead of valuable data transmission.

In an effort to reduce the CSI feedback load of traditional scheduling schemes, the concept of multiuser switched-diversity opportunistic scheduling was firstly proposed in [21], which is to find any acceptable user instead of the best one by exploiting a threshold-based and ordered scheduling mechanism. The main idea behind switched diversity is to trade off part of desired multiuser diversity gains for considerable savings with regard to the CSI feedback requirements. In recent years, extensive efforts have been devoted to incorporating switched diversity in wireless communication systems [22]–[27]. However, few works have addressed the secure transmission issue of the switched diversity based opportunistic scheduling scheme. A recent work [28] firstly addressed a threshold-based branch selection scheme, namely switch-and-examine combining (SEC), to achieve a better tradeoff between the secrecy outage performance and implementation cost in classical wiretap networks. In [29], [30], a more preferred alternative termed SEC with post-examining selection (SECps) was investigated in the multiuser downlink wiretap networks. To be specific, the SEC or SECps scheme examines the signal-to-noise ratio (SNR) of each branch in one by one manner with a predefined switched threshold. Once any branch exceeds the switched threshold, it will be selected for data transmission. The difference between SEC and SECps scheme exists in their last step where SEC keeps the last examined branch, while SECps selects the best one instead. In particular, an improved threshold-based switched diversity (termed tSD) strategy was proposed in [31] and extended to different communication scenarios. Different from SEC and SECps scheme, the tSD scheme first examines whether the previous selected branch exceeds the predetermined switched threshold. If this is the case, this branch is kept, otherwise the scheduler switches to the branch that yields the best channel quality.

While the aforementioned works have laid a solid foundation for the investigation of threshold-based switched diversity scheduling in multiuser downlink networks, the PLS issues in multiuser multi-antenna networks with multiple eavesdroppers are still not well understood and the channel fading severity on the secrecy performance of these networks remains unknown.

With this in mind, in this paper, we introduce a hybrid scheme combining TAS with threshold-based selection diversity opportunistic scheduling, namely TAS/tSD, in a multiuser multi-antenna wiretap network over Nakagami-m channels. More specifically, we present a comprehensive secrecy performance analysis of the considered network under two practical eavesdropping scenarios, i.e., Scenario I: The CSI of eavesdropping channel is not available at the base station (BS), and Scenario II: The CSI of the eavesdropping channel is available at the BS[1]. The main contributions of this paper are summarized as follows:

- For Scenario I, we first derive novel exact closed-form expressions for the secrecy outage probability and non-zero secrecy rate with arbitrary transmit antenna configurations and channel fading severity, the number of legitimate users, and the number of eavesdroppers as well as the switched threshold, from which the impact of key system parameters on the secrecy performance of multiuser wiretap networks with TAS/tSD can be readily evaluated.
- For Scenario I, in order to achieve more insights, we derive new closed-form approximate expressions of the secrecy outage probability in high SNR regimes for two different cases, i.e., Case I: the legitimate user is located close to the BS and Case II: both the legitimate user and eavesdropper are located close to the BS. According to the derived expressions, we find that for Case I, the secrecy diversity order is decided by the number of transmit antennas and the channel fading severity of main channel, while for Case II, the secrecy diversity order collapses to zero and the secrecy performance floor occurs.
- For Scenario II, we derive new exact closed-form expressions for the ergodic secrecy rate, from which we can accurately examine the impact of the system parameters on the ergodic secrecy rate of the considered networks with TAS/tSD scheme.
- For Scenario II, we derive new closed-form approximate expressions of the ergodic secrecy rate in the high SNR

[1]Similarly as in [1], [9], [33], [34], [40], we consider the case that the CSIs of the eavesdropper's channels are obtained at the BS, which potentially demonstrates that their transmissions can be monitored.

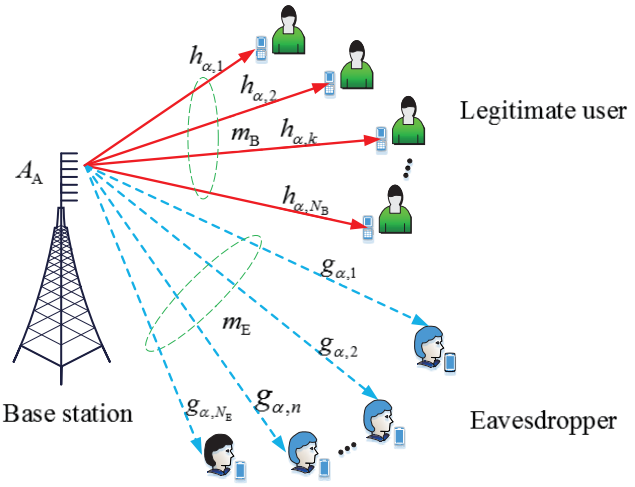


Fig. 1: System model

regime. Based on the derived results, we characterize the asymptotic ergodic secrecy rate in terms of the high SNR slope and high SNR power offset. Our findings demonstrate that the high SNR slope remains one for Case I, while collapses to zero for Case II. However, the high SNR power offset depends on the number of transmit antennas and the fading severity of main channel as well as the involved parameters of the eavesdropping channel.

- Our results also demonstrate that the considered TAS/tSD scheme achieves a better secrecy performance than the TAS/SECps scheme at the expense of negligible increasing complexity. In addition, compared to the best scheduling scheme, the TAS/tSD scheduling scheme achieves a similar secrecy performance, while the average number of user examinations of TAS/tSD scheme is significantly reduced.

Notation: We utilize bold lower/upper case symbols to represent vectors/matrics. We denote $|\cdot|$ the absolute value and $\binom{\cdot}{\cdot}$ is the binomial coefficient. The notation $O(\cdot)$ represents higher order function, $\Pr[\cdot]$ is the probability, the cumulative distribution function (CDF) and the probability distribution function (PDF) of random variable (RV) X are denoted as $F_X(x)$ and $f_X(x)$, respectively. $\mathrm{Ei}(\cdot)$ denotes the one-argument exponential integral function. $\mathbb{E}[\cdot]$ stands for the expectation operator and $\Gamma(\cdot)$ denotes the Gamma function.

II. System and Channel Models

Let us consider a multiuser downlink wiretap network as in Fig. 1, which consists of one BS equipped with A_{A} antennas, N_{B} single-antenna legitimate users (Bobs), and N_{E} single-antenna eavesdroppers (Eves). The system considered in this paper is applicable to practical multiuser scenarios, for instance, the Internet of Things (IoT) and Wireless Sensor Networks (WSN). The main link and eavesdropper's link are assumed to be quasi-static independent and non-identically distributed (i.n.i.d.) block Nakagami-m fading, and remain unchanged during the coherence time. In addition, each block transmission time, being equal to the channel coherence time, is composed of two parts, i.e., guard interval and data transmission interval. During the guard interval phase, BS first selects a desired legitimate user and transmit antenna pair according to the considered TAS/tSD scheme. After that, the data transmission is completed between the selected legitimate user and transmit antenna in the following interval.

To achieve secrecy, the BS encodes the message block $\mathbf{w}$ into the codeword $\mathbf{x} = [x(1), ..., x(i), ...x(n)]$ with $\frac{1}{n}\sum_{i=1}^{n}\mathbb{E}\left[|x(i)|^2\right] \leq P$ according to capacity achieving codebook for the wiretap channel. As such, the received instantaneous SNRs at the k-th legitimate user and at the n-th Eve associated with the α-th transmit antenna are expressed, respectively, as

$$\gamma_{\alpha,k}^{\mathrm{b}} = \frac{P|h_{\alpha,k}|^2}{\sigma_{\mathrm{b}}^2} \tag{1}$$

and

$$\gamma_{\alpha,n}^{\mathrm{e}} = \frac{P|g_{\alpha,n}|^2}{\sigma_{\mathrm{e}}^2} \tag{2}$$

where P denotes the transmit power of the BS, $h_{\alpha,k}$ denotes the channel coefficient between the α-th antenna and the k-th legitimate user, $g_{\alpha,n}$ represents the channel coefficient between α-th antenna and the n-th eavesdropper, σ_{b}^2 and σ_{e}^2 denote the additive white Gaussian noise (AWGN) variance at each legitimate user and eavesdropper, respectively.

In the following, we describe the basic principle of TAS/tSD scheme [31] in detail, from which an acceptable legitimate user is selected by the BS associated with a specific antenna.

- We begin with the first transmit antenna ($\alpha = 1$) of the tSD scheme. The BS estimates whether the instantaneous SNR $\gamma_{\alpha,k}^{\mathrm{b}}$ of the previously selected legitimate user for this transmit antenna exceeds the predetermined threshold γ_{T}, i.e., if $\gamma_{\mathrm{B},\alpha}^{\mathrm{tSD}} = \gamma_{\alpha,k}^{\mathrm{b}} > \gamma_{\mathrm{T}}$, the processing procedure of tSD terminates for this transmit antenna.
- Otherwise, once the instantaneous SNR of the previously selected legitimate user is below the threshold, i.e., $\gamma_{\alpha,k}^{\mathrm{b}} < \gamma_{\mathrm{T}}$, the legitimate user with the highest SNR is selected for this transmit antenna, wherein $\gamma_{\mathrm{B},\alpha}^{\mathrm{tSD}} = \max\left(\gamma_{\alpha,1}^{\mathrm{b}}, \gamma_{\alpha,2}^{\mathrm{b}}, ..., \gamma_{\alpha,N_{\mathrm{B}}}^{\mathrm{b}}\right)$. The same user scheduling operation repeats for the remaining transmit antennas sequentially.
- As per the TAS scheme, the transmit antenna and legitimate user pair that results in the largest instantaneous SNR is selected for the following transmission interval. The index of selected transmit antenna α^* is given by

$$\alpha^* = \underset{1\leq\alpha\leq A_{\mathrm{A}}}{\arg\max}\left(\gamma_{\mathrm{B},\alpha}^{\mathrm{tSD}}\right) \tag{3}$$

Without loss of generality, we assume that the selection procedure of legitimate user and transmit antenna pair is done at a central scheduler (i.e., at the BS). Meanwhile, the requirement of feedback information includes not only legitimate user indexes, but also the received SNRs. Different from the conventional application without secrecy constraint, the resulting largest SNR is exploited by the BS for the

construction of wiretap code[2].

We also remark that selecting the best antenna at the BS is optimal for the legitimate channels, however, it corresponds to a random transmit antenna in the perspective of eavesdroppers. As such, the Eves could hardly achieve any additional transmit diversity from the selected antenna.

Due to the fact that each eavesdropper has received the signal from BS, we consider the most powerful colluding eavesdropper attacking scenario, where the eavesdroppers can share their available observations to decode the confidential messages. From the eavesdropper's design perspective, the colluding eavesdropping scenario yields the best possible performance of illegitimate link while it represents the worst case scenario in the viewpoint of secure transmission [35]–[37]. Additionally, all Eves are assumed to be perfectly colluded where the inter-eavesdropper channels are considered error-free. In doing so, the maximal ratio combining (MRC) scheme is adopted among the eavesdroppers to achieve the best wiretapping performance.

III. Secrecy Performance Analysis

In this section, we present a comprehensive analysis on the secrecy performance of the considered system with TAS/tSD scheme. Before delving into the detailed analysis, we first present the statistical characteristics of legitimate channel and eavesdropping channel.

A. Preliminaries

Based on the aforementioned TAS/tSD scheme, it is obvious that the events of selecting an acceptable user are mutually exclusive for a specific transmit antenna α, therefore, the CDF of the end-to-end instantaneous SNR $\gamma_{\mathrm{B},\alpha}^{\mathrm{tSD}}$ is given by [31]

$$F_{\gamma_{\mathrm{B},\alpha}^{\mathrm{tSD}}}(\gamma)=\Pr\left[\gamma_{\mathrm{B},\alpha}^{\mathrm{tSD}}\leq\gamma\right]=\sum_{k=1}^{N_{\mathrm{B}}}\Pr\left[\gamma_{\mathrm{B},\alpha}^{\mathrm{tSD}}=\gamma_{\alpha,k}^{\mathrm{b}}\&\gamma_{\alpha,k}^{\mathrm{b}}\leq\gamma\right] \tag{4}$$

Besides, each legitimate link is assumed to follow independent and identically distributed (i.i.d.) Nakagami-m distribution[3]. Following the same steps as developed in [31], thus the CDF of $\gamma_{\mathrm{B},\alpha}^{\mathrm{tSD}}$ can be rewritten as

$$F_{\gamma_{\mathrm{B},\alpha}^{\mathrm{tSD}}}(\gamma)=\begin{cases}F_{\gamma_{\alpha,k}^{\mathrm{b}}}(\gamma)-F_{\gamma_{\alpha,k}^{\mathrm{b}}}(\gamma_{\mathrm{T}})\\ \quad+F_{\gamma_{\alpha,k}^{\mathrm{b}}}(\gamma_{\mathrm{T}})\left[F_{\gamma_{\alpha,k}^{\mathrm{b}}}(\gamma)\right]^{N_{\mathrm{B}}-1}, & \gamma\geq\gamma_{\mathrm{T}}\\ \left[F_{\gamma_{\alpha,k}^{\mathrm{b}}}(\gamma)\right]^{N_{\mathrm{B}}}, & \gamma<\gamma_{\mathrm{T}}\end{cases} \tag{5}$$

where

$$F_{\gamma_{\alpha,k}^{\mathrm{b}}}(\gamma)=1-\exp\left(-\frac{m_{\mathrm{B}}}{\bar{\gamma}_{\mathrm{B}}}\gamma\right)\sum_{k=0}^{m_{\mathrm{B}}-1}\frac{1}{k!}\left(\frac{m_{\mathrm{B}}}{\bar{\gamma}_{\mathrm{B}}}\gamma\right)^{k} \tag{6}$$

and

$$f_{\gamma_{\alpha,k}^{\mathrm{b}}}(\gamma)=\left(\frac{m_{\mathrm{A}}}{\bar{\gamma}_{\mathrm{B}}}\right)^{m_{\mathrm{B}}}\frac{\gamma^{m_{\mathrm{B}}-1}}{\Gamma(m_{\mathrm{B}})}\exp\left(-\frac{m_{\mathrm{B}}}{\bar{\gamma}_{\mathrm{B}}}\gamma\right) \tag{7}$$

denote the CDF and PDF of $\gamma_{\alpha,k}^{\mathrm{b}}$, respectively. Moreover, $\bar{\gamma}_{\mathrm{B}}=\mathbb{E}\left[\gamma_{\alpha,k}^{\mathrm{b}}\right]$ represents the average SNR of each legitimate link and m_{B} is the fading severity of the legitimate channel.

Let us define γ_{B} as the end-to-end instantaneous SNR of TAS/tSD scheme. According to the principle of TAS, γ_{B} can be presented as $\gamma_{\mathrm{B}}=\max\left(\gamma_{\mathrm{B},\alpha}^{\mathrm{tSD}}\right)$. Therefore, the CDF of γ_{B} is given by

$$F_{\gamma_{\mathrm{B}}}(\gamma)=\left[F_{\gamma_{\mathrm{B},\alpha}^{\mathrm{tSD}}}(\gamma)\right]^{A_{\mathrm{A}}} \tag{8}$$

Moreover, resorting to binomial theorem [41, Eq.(1.111)], the CDF of γ_{B} can be rewritten as (9).

On the other hand, since MRC scheme is adopted at the colluding eavesdroppers, the end-to-end instantaneous SNR of the colluding eavesdroppers is $\gamma_{\mathrm{E}}=\sum_{n=1}^{N_{\mathrm{E}}}\gamma_{\alpha^*,n}^{\mathrm{e}}$, where α^* represents the selected antenna at the BS. Thus, the CDF and PDF of γ_{E} are, respectively, expressed as

$$F_{\gamma_{\mathrm{E}}}(\gamma)=1-\exp\left(-\frac{m_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{E}}}\gamma\right)\sum_{k=0}^{N_{\mathrm{E}}m_{\mathrm{E}}-1}\frac{1}{k!}\left(\frac{m_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{E}}}\gamma\right)^{k} \tag{10}$$

and

$$f_{\gamma_{\mathrm{E}}}(\gamma)=\left(\frac{m_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{E}}}\right)^{N_{\mathrm{E}}m_{\mathrm{E}}}\frac{\gamma^{N_{\mathrm{E}}m_{\mathrm{E}}-1}}{\Gamma(N_{\mathrm{E}}m_{\mathrm{E}})}\exp\left(-\frac{m_{\mathrm{E}}}{\bar{\gamma}_{\mathrm{E}}}\gamma\right) \tag{11}$$

where $\bar{\gamma}_{\mathrm{E}}=\mathbb{E}\left[\gamma_{\alpha^*,n}^{\mathrm{e}}\right]$ denotes the average SNR of eavesdropper's channel and m_{E} denotes the fading severity of the wiretap channel.

The instantaneous secrecy rate C_{s} of the considered system is given by

$$C_{\mathrm{s}}=[C_{\mathrm{B}}-C_{\mathrm{E}}]^{+}=[\log(1+\gamma_{\mathrm{B}})-\log(1+\gamma_{\mathrm{E}})]^{+} \tag{12}$$

where

$$[u]^{+}=\max(u,0)=\begin{cases}u, & u>0\\ 0, & u\leq 0\end{cases} \tag{13}$$

while $C_{\mathrm{B}}=\log(1+\gamma_{\mathrm{B}})$ and $C_{\mathrm{E}}=\log(1+\gamma_{\mathrm{E}})$ represent the instantaneous rate of the legitimate channel and wiretap channel, respectively. According to [34], [38], when the eavesdropper's CSI is not available at the BS, i.e., the passive eavesdropping scenario, BS has no choice but to assume the instantaneous rate of the eavesdropping channel as $\tilde{C}_{\mathrm{E}}=C_{\mathrm{B}}-R_{\mathrm{s}}$ to achieve secure transmission, where R_{s} denotes a constant secrecy rate chosen by the BS. Then, the BS constructs the wiretap codes by exploiting C_{B} and $\tilde{C}_{\mathrm{E}}$. If $R_{\mathrm{s}}\leq C_{\mathrm{s}}$ (i.e., $\tilde{C}_{\mathrm{E}}\geq C_{\mathrm{E}}$), the codewords insure a perfect secrecy. Otherwise, if $R_{\mathrm{s}}>C_{\mathrm{s}}$ (i.e., $\tilde{C}_{\mathrm{E}}<C_{\mathrm{E}}$), the confidential data can be overheard by the eavesdroppers and the secrecy is compromised. Hence, the secrecy outage probability is adopted as a useful and well-acceptable secrecy performance metric under this scenario.

[2]Similar as in [31], we assume in the following analysis that there is no feedback error or delay in the transmission, while each legitimate user has perfect CSI of its own.

[3]Similar to the work in [23], [32], we assume the i.i.d. fading channels where legitimate users are located approximately the same distance from the BS, or they are distributed in the whole cluster and slow power control protocol is employed.

$$F_{\gamma_{\rm B}}(\gamma)=\begin{cases}\sum\limits_{q=0}^{A_{\rm A}}\binom{A_{\rm A}}{q}\left[F_{\gamma^{\rm b}_{\alpha,k}}(\gamma_{\rm T})\right]^{q}\sum\limits_{q_1=0}^{q}\binom{q}{q_1}(-1)^{q_1}\sum\limits_{q_2=0}^{(N_{\rm B}-1)(q-q_1)+A_{\rm A}-q}\binom{(N_{\rm B}-1)(q-q_1)+A_{\rm A}-q}{q_2}(-1)^{q_2}\\ \qquad\times\exp\left(-\frac{m_{\rm B}q_2\gamma}{\bar{\gamma}_{\rm B}}\right)\Theta_{{\rm B},q_2}\left(\frac{m_{\rm B}}{\bar{\gamma}_{\rm B}}\right)^{\phi_{\rm B}}\gamma^{\phi_{\rm B}},\gamma\geq\gamma_{\rm T} & (9)\\ \sum\limits_{q=0}^{A_{\rm A}N_{\rm B}}\binom{A_{\rm A}N_{\rm B}}{q}(-1)^{q}\exp\left(-\frac{m_{\rm B}q\gamma}{\bar{\gamma}_{\rm B}}\right)\Theta_{{\rm B},q}\left(\frac{m_{\rm B}}{\bar{\gamma}_{\rm B}}\right)^{\phi_{\rm B}}\gamma^{\phi_{\rm B}}, & \gamma<\gamma_{\rm T}\end{cases}$$

where

$$\Theta_{{\rm B},q}=\sum_{n_1=0}^{q}\sum_{n_2=0}^{n_1}\cdots\sum_{n_{m_{\rm B}-1}=0}^{n_{m_{\rm B}-2}}\frac{q!}{n_{m_{\rm B}-1}!}\prod_{t=1}^{m_{\rm B}-1}\left[\frac{(t!)^{n_{t+1}-n_t}}{(n_{t-1}-n_t)!}\right],n_0=q,n_{m_{\rm B}}=0,\phi_{\rm B}=\sum_{p=1}^{m_{\rm B}-1}n_p$$

B. Secrecy Outage Probability

According to [1], [34], the secrecy outage probability is defined as $P_{\rm out}(R_{\rm s})=\Pr(C_{\rm s}<R_{\rm s})$. Mathematically, the secrecy outage probability can be formulated as

$$\begin{aligned}P_{\rm out}(R_{\rm s})=&\Pr(C_{\rm s}<R_{\rm s}|\gamma_{\rm B}>\gamma_{\rm E})\Pr(\gamma_{\rm B}>\gamma_{\rm E})\\&+\Pr(\gamma_{\rm B}<\gamma_{\rm E})\end{aligned}\quad(14)$$

Following the detailed algebraic manipulations in [1], we have

$$\begin{aligned}P_{\rm out}(R_{\rm s})&=\int_0^{\infty}\int_0^{2^{R_{\rm s}}(1+y)-1}f_{\gamma_{\rm B}}(x)f_{\gamma_{\rm E}}(y)\,dxdy\\&=\int_0^{\infty}F_{\gamma_{\rm B}}\left(2^{R_{\rm s}}(1+y)-1\right)f_{\gamma_{\rm E}}(y)\,dy\end{aligned}\quad(15)$$

where $f_{\gamma_{\rm B}}(x)$ is the PDF of $\gamma_{\rm B}$. Due to the fact that the switched threshold $\gamma_{\rm T}$ is incorporated in the CDF of $\gamma_{\rm B}$ as shown in (9), there exists relationship between the term $2^{R_{\rm s}}(1+y)-1$ and $\gamma_{\rm T}$ in (15), i.e., $2^{R_{\rm s}}(1+y)-1\geq\gamma_{\rm T}$ or $2^{R_{\rm s}}(1+y)-1<\gamma_{\rm T}$. To facilitate the analysis in (15), here we introduce a bound point as ${\rm H}(\gamma_{\rm T})=2^{-R_{\rm s}}(1+\gamma_{\rm T})-1$. As such, the secrecy outage probability can be converted to a piecewise one with respect to the bound point as

$$P_{\rm out}(R_{\rm s})=\begin{cases}\int_0^{{\rm H}(\gamma_{\rm T})}F_{\gamma_{\rm B}}\left(\Phi_y\right)f_{\gamma_{\rm E}}(y)\,dy+\int_{{\rm H}(\gamma_{\rm T})}^{\infty}F_{\gamma_{\rm B}}\left(\Phi_y\right)\\ \qquad\times f_{\gamma_{\rm E}}(y)\,dy, & {\rm H}(\gamma_{\rm T})\geq 0\\ \int_0^{\infty}F_{\gamma_{\rm B}}\left(\Phi_y\right)f_{\gamma_{\rm E}}(y)\,dy, & {\rm H}(\gamma_{\rm T})<0\end{cases}\quad(16)$$

where $\Phi_y=2^{R_{\rm s}}(1+y)-1$. In what follows, by substituting (7) and (9) into (16) and utilizing the results in [41, Eqs. (1.111), (3.351.2) and (3.351.3)], the exact closed-form expression of secrecy probability can be obtained in the following theorem.

Theorem 1. *The secrecy outage probability of multiuser multi-antenna wiretap networks with TAS/tSD scheme is given as* (17)*, where $\gamma(\cdot,\cdot)$ and $\Gamma(\cdot,\cdot)$ denote the lower and upper incomplete Gamma function [41, Eqs. (8.350.1) and (8.350.2)], respectively.*

It is worth mentioning that other secrecy performance metrics can be conveniently calculated from (17). For instance, the probability of positive secrecy can be easily evaluated by setting $R_{\rm s}=0$ into (17), i.e., $\Pr(C_{\rm s}>0)=1-P_{\rm out}(0)$.

In general, due to the complexity of the involved expressions, it is difficult to explore the effect of system parameters on the secrecy performance from (17). In order to achieve more insights from (17), we provide an asymptotic secrecy outage analysis in the high SNR regime via the following key corollaries.

Corollary 1. *When $\bar{\gamma}_{\rm B}\to\infty$ and $\bar{\gamma}_{\rm E}$ is fixed, the asymptotic secrecy outage probability of multiuser multi-antenna wiretap networks with TAS/tSD scheme is given by*

$$P_{\rm out}(R_{\rm s})=(\Xi\cdot\bar{\gamma}_{\rm B})^{-\Psi}+O\left(\bar{\gamma}_{\rm B}^{-\Psi}\right),\quad(18)$$

where the secrecy diversity order is $\Psi=A_{\rm A}m_{\rm B}$, and the secrecy array gain Ξ is given by (19)*.*

Proof: A detailed proof is provided in Appendix A. ■

From Corollary 1, we highlight that the secrecy diversity gain is determined by the number of transmit antennas at the BS and the fading severity of the legitimate channel, which is independent of the number of legitimate users or eavesdroppers, (i.e., $N_{\rm B}$ or $N_{\rm E}$), and the average SNR of eavesdropping channel $\bar{\gamma}_{\rm E}$. However, the effect of these involved parameters on the secrecy outage performance can be described by the secrecy array gain.

In what follows, we consider the case of $\bar{\gamma}_{\rm B}\to\infty$ and $\bar{\gamma}_{\rm E}\to\infty$ with a fixed main-to-eavesdropper ratio (MER), i.e., $\frac{\bar{\gamma}_{\rm B}}{\bar{\gamma}_{\rm E}}=\lambda_{\rm be}$.

Corollary 2. *In the case of $\bar{\gamma}_{\rm B}\to\infty$ and $\bar{\gamma}_{\rm E}\to\infty$ with $\frac{\bar{\gamma}_{\rm B}}{\bar{\gamma}_{\rm E}}=\lambda_{\rm be}$, both legitimate user and eavesdropper are located close to the BS, the asymptotic secrecy outage probability with TAS/tSD scheme is derived as*

$$\begin{aligned}P^{\infty}_{\rm out}(R_{\rm s})\approx&\sum_{q=0}^{A_{\rm A}}\binom{A_{\rm A}}{q}(-1)^{q}\Theta_{{\rm B},q}\left(\frac{m_{\rm B}2^{R_{\rm s}}}{m_{\rm E}}\right)^{\phi_{\rm B}}(\lambda_{\rm be})^{\phi_{\rm B}}\\&\times\left(\frac{m_{\rm B}2^{R_{\rm s}}q}{m_{\rm E}}\lambda_{\rm be}+1\right)^{-(N_{\rm E}m_{\rm E}+\phi_{\rm B})}\frac{\Gamma(N_{\rm E}m_{\rm E}+\phi_{\rm B})}{\Gamma(N_{\rm E}m_{\rm E})}\end{aligned}\quad(20)$$

Proof: Based on (17), the asymptotic secrecy outage probability can be easily derived after some algebraic manipulations. ■

According to (20), we confirm that the secrecy outage probability approaches a constant at high SNR value, which implies that the secrecy diversity gain is not achievable for

$$P_{\rm out}\left(R_{\rm s}\right)=\begin{cases}\left(\frac{m_{\rm E}}{\bar{\gamma}_{\rm E}}\right)^{N_{\rm E}m_{\rm E}}\frac{1}{\Gamma(N_{\rm E}m_{\rm E})}\left\{\sum\limits_{q=0}^{A_{\rm A}N_{\rm B}}\binom{A_{\rm A}N_{\rm B}}{q}(-1)^q\exp\left(-\frac{m_{\rm B}q}{\bar{\gamma}_{\rm B}}\left(2^{R_{\rm s}}-1\right)\right)\Theta_{{\rm B},q}\left(\frac{m_{\rm B}\left(2^{R_{\rm s}}-1\right)}{\bar{\gamma}_{\rm B}}\right)^{\phi_{\rm B}}\sum\limits_{s=0}^{\phi_{\rm B}}\binom{\phi_{\rm B}}{s}\left(\frac{2^{R_{\rm s}}}{2^{R_{\rm s}}-1}\right)^s\right.\\ \times\left(\frac{m_{\rm E}}{\bar{\gamma}_{\rm E}}+\frac{m_{\rm B}2^{R_{\rm s}}q}{\bar{\gamma}_{\rm B}}\right)^{-(N_{\rm E}m_{\rm E}+s)}\gamma\left(N_{\rm E}m_{\rm E}+s,\left(\frac{m_{\rm E}}{\bar{\gamma}_{\rm E}}+\frac{m_{\rm B}2^{R_{\rm s}}q}{\bar{\gamma}_{\rm B}}\right)\mathrm{H}\left(\gamma_{\rm T}\right)\right)+\sum\limits_{q=0}^{A_{\rm A}}\binom{A_{\rm A}}{q}\left[F_{\gamma^{\rm b}_{\alpha,k}}\left(\gamma_{\rm T}\right)\right]^q\sum\limits_{q_1=0}^{q}\binom{q}{q_1}\\ \times(-1)^{q_1}\sum\limits_{q_2=0}^{[(N_{\rm B}-1)(q-q_1)+A_{\rm A}-q]}\binom{(N_{\rm B}-1)(q-q_1)+A_{\rm A}-q}{q_2}(-1)^{q_2}\exp\left(-\frac{m_{\rm B}q_2}{\bar{\gamma}_{\rm B}}\left(2^{R_{\rm s}}-1\right)\right)\Theta_{{\rm B},q_2}\left(\frac{m_{\rm B}\left(2^{R_{\rm s}}-1\right)}{\bar{\gamma}_{\rm B}}\right)^{\phi_{\rm B}}\\ \left.\times\sum\limits_{s=0}^{\phi_{\rm B}}\binom{\phi_{\rm B}}{s}\left(\frac{2^{R_{\rm s}}}{2^{R_{\rm s}}-1}\right)^s\Gamma\left(N_{\rm E}m_{\rm E}+s,\left(\frac{m_{\rm B}2^{R_{\rm s}}q_2}{\bar{\gamma}_{\rm B}}+\frac{m_{\rm E}}{\bar{\gamma}_{\rm E}}\right)\mathrm{H}\left(\gamma_{\rm T}\right)\right)\left(\frac{m_{\rm B}2^{R_{\rm s}}q_2}{\bar{\gamma}_{\rm B}}+\frac{m_{\rm E}}{\bar{\gamma}_{\rm E}}\right)^{-(N_{\rm E}m_{\rm E}+s)}\right\},\mathrm{H}\left(\gamma_{\rm T}\right)\geq 0\\ \left(\frac{m_{\rm E}}{\bar{\gamma}_{\rm E}}\right)^{N_{\rm E}m_{\rm E}}\frac{1}{\Gamma(N_{\rm E}m_{\rm E})}\left\{\sum\limits_{q=0}^{A_{\rm A}}\binom{A_{\rm A}}{q}\left[F_{\gamma^{\rm b}_{\alpha,k}}\left(\gamma_{\rm T}\right)\right]^q\sum\limits_{q_1=0}^{q}\binom{q}{q_1}(-1)^{q_1}\sum\limits_{q_2=0}^{[(N_{\rm B}-1)(q-q_1)+A_{\rm A}-q]}\binom{(N_{\rm B}-1)(q-q_1)+A_{\rm A}-q}{q_2}\right.\\ \times\left(-1\right)^{q_2}\exp\left(-\frac{m_{\rm B}q_2}{\bar{\gamma}_{\rm B}}\left(2^{R_{\rm s}}-1\right)\right)\Theta_{{\rm B},q}\left(\frac{m_{\rm B}\left(2^{R_{\rm s}}-1\right)}{\bar{\gamma}_{\rm B}}\right)^{\phi_{\rm B}}\sum\limits_{s=0}^{\phi_{\rm B}}\binom{\phi_{\rm B}}{s}\left(\frac{2^{R_{\rm s}}}{2^{R_{\rm s}}-1}\right)^s\left(\frac{m_{\rm B}2^{R_{\rm s}}q_2}{\bar{\gamma}_{\rm B}}+\frac{m_{\rm E}}{\bar{\gamma}_{\rm E}}\right)^{-(N_{\rm E}m_{\rm E}+s)}\\ \left.\times\Gamma\left(N_{\rm E}m_{\rm E}+s\right)\right\},\qquad\qquad\mathrm{H}\left(\gamma_{\rm T}\right)<0\end{cases}\tag{17}$$

$$\Xi=\begin{cases}\left[\frac{1}{\Gamma(N_{\rm E}m_{\rm E})}\left(\frac{m_{\rm B}{}^{m_{\rm B}}}{m_{\rm B}\,!}\right)^{A_{\rm A}}\sum\limits_{q=0}^{A_{\rm A}}\binom{A_{\rm A}}{q}(-1)^q(\gamma_{\rm T})^{m_{\rm B}q}\left(2^{R_s}-1\right)^{m_{\rm B}(A_{\rm A}-q)}\sum\limits_{q_1=0}^{m_{\rm B}(A_{\rm A}-q)}\binom{m_{\rm B}(A_{\rm A}-q)}{q_1}\right.\\ \left.\times\left(\frac{2^{R_{\rm s}}}{2^{R_{\rm s}}-1}\right)^{q_1}\left(\frac{m_{\rm E}}{\bar{\gamma}_{\rm E}}\right)^{-q_1}\Gamma\left(N_{\rm E}m_{\rm E}+q_1,\frac{m_{\rm E}}{\bar{\gamma}_{\rm E}}\mathrm{H}\left(\gamma_{\rm T}\right)\right)\right]^{-1},\mathrm{H}\left(\gamma_{\rm T}\right)\geq 0\\ \left[\frac{1}{\Gamma(N_{\rm E}m_{\rm E})}\left(\frac{m_{\rm B}{}^{m_{\rm B}}}{m_{\rm B}\,!}\right)^{A_{\rm A}}\sum\limits_{q=0}^{A_{\rm A}}\binom{A_{\rm A}}{q}(-1)^q(\gamma_{\rm T})^{m_{\rm B}q}\left(2^{R_s}-1\right)^{m_{\rm B}(A_{\rm A}-q)}\sum\limits_{q_1=0}^{m_{\rm B}(A_{\rm A}-q)}\binom{m_{\rm B}(A_{\rm A}-q)}{q_1}\right.\\ \left.\times\left(\frac{2^{R_{\rm s}}}{2^{R_{\rm s}}-1}\right)^{q_1}\left(\frac{m_{\rm E}}{\bar{\gamma}_{\rm E}}\right)^{-q_1}\Gamma\left(N_{\rm E}m_{\rm E}+q_1\right)\right]^{-1},\qquad\mathrm{H}\left(\gamma_{\rm T}\right)<0\end{cases}\tag{19}$$

this particular case. Besides, it is noteworthy that increasing the transmit power at the BS does not improve the secrecy performance.

C. Ergodic Secrecy Rate

In this subsection, we concentrate on the scenario where the CSI of the eavesdropping channel is available at BS. As such, the BS adjusts the transmission rate adaptively with the wiretap coding scheme. More specifically, any average transmission rate below the ergodic secrecy rate of the channel is achievable in principle [1], [9]. Different from the Scenario I, here we take the ergodic secrecy rate as a principal metric to evaluate the secrecy performance of the considered system with TAS/tSD scheme.

According to [9], the ergodic secrecy rate is given by

$$\overline{C}_{\rm s}=\int_0^\infty\int_y^\infty\left[\log_2\left(1+x\right)-\log_2\left(1+y\right)\right]\times f_{\gamma_{\rm B}}\left(x\right)f_{\gamma_{\rm E}}\left(y\right)dxdy\tag{21}$$

To solve the above double integral, we follow the similar procedures as introduced in [9]. First, the inner integral can be evaluated with the adoption of integration by parts, and then applying some mathematical manipulations, the ergodic secrecy rate can be further written as in [9, Eq. (15)]

$$\overline{C}_{\rm s}=\frac{1}{\ln 2}\int_0^\infty\frac{F_{\gamma_{\rm E}}\left(y\right)}{1+y}\left[1-F_{\gamma_{\rm B}}\left(y\right)\right]dy\tag{22}$$

Moreover, by taking the switched threshold $\gamma_{\rm T}$ into account, the ergodic secrecy rate can be re-expressed as

$$\overline{C}_{\rm s}=\frac{1}{\ln 2}\left[\int_0^{\gamma_{\rm T}}\frac{F_{\gamma_{\rm E}}\left(y\right)}{1+y}\left[1-F_{\gamma_{\rm B}}\left(y\right)\right]dy+\int_{\gamma_{\rm T}}^\infty\frac{F_{\gamma_{\rm E}}\left(y\right)}{1+y}\left[1-F_{\gamma_{\rm B}}\left(y\right)\right]dy\right]\tag{23}$$

Now, by substituting (9) and (10) into (23), resorting to the new derived formulae of integration (44), (46) and (48) in Appendix B and performing some algebraic manipulations, the ergodic secrecy rate can be derived in the following theorem.

Theorem 2. *The exact ergodic secrecy rate of multiuser multi-antenna wiretap networks with TAS/tSD scheme is given as*

$$\overline{C}_{\rm s}=\frac{1}{\ln 2}\left(\overline{C}_1+\overline{C}_2\right)\tag{24}$$

where $\overline{C}_1$ *and* $\overline{C}_2$ *are expressed in* (25) *and* (26)*, respectively.*

In what follows, to evaluate the impact of key system parameters on the ergodic secrecy rate, we also look into the ergodic secrecy rate in the high SNR regime. We first consider the asymptotic ergodic secrecy rate in the case of $\bar{\gamma}_{\rm B}\to\infty$ and a fixed $\bar{\gamma}_{\rm E}$.

$$\overline{C}_1 = \Bigg\{ - \sum_{q=1}^{A_{\rm A}N_{\rm B}} \binom{A_{\rm A}N_{\rm B}}{q} (-1)^q \Theta_{{\rm B},q} \left(\frac{m_{\rm B}}{\bar{\gamma}_{\rm B}}\right)^{\phi_{\rm B}} \exp\left(\frac{m_{\rm B}q}{\bar{\gamma}_{\rm B}}\right) \sum_{k=0}^{\phi_{\rm B}} \binom{\phi_{\rm B}}{k} (-1)^{\phi_{\rm B}-k} \left(\frac{m_{\rm B}q}{\bar{\gamma}_{\rm B}}\right)^{-k} \Big[\Gamma\left(k, \frac{m_{\rm B}q}{\bar{\gamma}_{\rm B}}\right) - \Gamma\left(k, \frac{m_{\rm B}q}{\bar{\gamma}_{\rm B}}\left(\gamma_{\rm T}+1\right)\right)\Big] \sum_{k=0}^{N_{\rm E}m_{\rm E}-1} \frac{1}{k!} \left(\frac{m_{\rm E}}{\bar{\gamma}_{\rm E}}\right)^k \sum_{q=1}^{A_{\rm A}N_{\rm B}} \binom{A_{\rm A}N_{\rm B}}{q} (-1)^q \Theta_{{\rm B},q} \left(\frac{m_{\rm B}}{\bar{\gamma}_{\rm B}}\right)^{\phi_{\rm B}} \exp\left(\frac{m_{\rm B}q}{\bar{\gamma}_{\rm B}} + \frac{m_{\rm E}}{\bar{\gamma}_{\rm E}}\right) \times \sum_{k_1=0}^{\phi_{\rm B}+k} \binom{\phi_{\rm B}+k}{k_1} (-1)^{\phi_{\rm B}+k-k_1} \left(\frac{m_{\rm B}q}{\bar{\gamma}_{\rm B}} + \frac{m_{\rm E}}{\bar{\gamma}_{\rm E}}\right)^{-k_1} \left[\Gamma\left(k_1, \frac{m_{\rm B}q}{\bar{\gamma}_{\rm B}} + \frac{m_{\rm E}}{\bar{\gamma}_{\rm E}}\right) - \Gamma\left(k_1, \left(\frac{m_{\rm B}q}{\bar{\gamma}_{\rm B}} + \frac{m_{\rm E}}{\bar{\gamma}_{\rm E}}\right)\left(\gamma_{\rm T}+1\right)\right)\right] \Bigg\} \tag{25}$$

$$\begin{aligned}\overline{C}_2 = \Bigg\{ & - \sum_{q_0=1}^{A_{\rm A}} \binom{A_{\rm A}}{q_0} (-1)^{q_0} \Theta_{{\rm B},q_0} \left(\frac{m_{\rm B}}{\bar{\gamma}_{\rm B}}\right)^{\phi_{\rm B}} \exp\left(\frac{m_{\rm B}q_0}{\bar{\gamma}_{\rm B}}\right) \sum_{k_1=0}^{\phi_{\rm B}} \binom{\phi_{\rm B}}{k_1} (-1)^{\phi_{\rm B}-k_1} \left(\frac{m_{\rm B}q_0}{\bar{\gamma}_{\rm B}}\right)^{-k_1} \Gamma\left(k_1, \frac{m_{\rm B}q_0}{\bar{\gamma}_{\rm B}}\left(\gamma_{\rm T}+1\right)\right) \\ & + \sum_{k=0}^{N_{\rm E}m_{\rm E}-1} \frac{1}{k!} \left(\frac{m_{\rm E}}{\bar{\gamma}_{\rm E}}\right)^k \sum_{q_0=1}^{A_{\rm A}} \binom{A_{\rm A}}{q_0} (-1)^{q_0} \Theta_{{\rm B},q_0} \left(\frac{m_{\rm B}}{\bar{\gamma}_{\rm B}}\right)^{\phi_{\rm B}} \exp\left(\frac{m_{\rm B}q_0}{\bar{\gamma}_{\rm B}} + \frac{m_{\rm E}}{\bar{\gamma}_{\rm E}}\right) \sum_{k_1=0}^{k+\phi_{\rm B}} \binom{A_{\rm A}}{k_1} (-1)^{k+\phi_{\rm B}-k_1} \\ & \times \left(\frac{m_{\rm B}q_0}{\bar{\gamma}_{\rm B}} + \frac{m_{\rm E}}{\bar{\gamma}_{\rm E}}\right)^{-k_1} \Gamma\left(k_1, \left(\frac{m_{\rm B}q_0}{\bar{\gamma}_{\rm B}} + \frac{m_{\rm E}}{\bar{\gamma}_{\rm E}}\right)\left(\gamma_{\rm T}+1\right)\right) - \sum_{q=1}^{A_{\rm A}} \binom{A_{\rm A}}{q} \left[F_{\gamma^{\rm b}_{\alpha,k}}\left(\gamma_{\rm T}\right)\right]^q \sum_{q_1=0}^{q} \binom{q}{q_1} (-1)^{q_1} \sum_{q_2=0}^{[(N_{\rm B}-1)(q-q_1)+A_{\rm A}-q]} \\ & \times \binom{(N_{\rm B}-1)(q-q_1)+A_{\rm A}-q}{q_2} (-1)^{q_2} \Theta_{{\rm B},q_2} \left(\frac{m_{\rm B}}{\bar{\gamma}_{\rm B}}\right)^{\phi_{\rm B}} \exp\left(\frac{m_{\rm B}q_2}{\bar{\gamma}_{\rm B}}\right) \sum_{k_1=0}^{\phi_{\rm B}} \binom{\phi_{\rm B}}{k_1} (-1)^{\phi_{\rm B}-k_1} \left(\frac{m_{\rm B}q_2}{\bar{\gamma}_{\rm B}}\right)^{-k_1} \Gamma\left(k_1, \frac{m_{\rm B}q_2}{\bar{\gamma}_{\rm B}}\left(\gamma_{\rm T}+1\right)\right) \\ & + \sum_{k=0}^{N_{\rm E}m_{\rm E}-1} \frac{1}{k!} \left(\frac{m_{\rm E}}{\bar{\gamma}_{\rm E}}\right)^k \sum_{q=1}^{A_{\rm A}} \binom{A_{\rm A}}{q} \left[F_{\gamma^{\rm b}_{\alpha,k}}\left(\gamma_{\rm T}\right)\right]^q \sum_{q_1=0}^{q} \binom{q}{q_1} (-1)^{q_1} \sum_{q_2=0}^{[(N_{\rm B}-1)(q-q_1)+A_{\rm A}-q]} \binom{(N_{\rm B}-1)(q-q_1)+A_{\rm A}-q}{q_2} (-1)^{q_2} \Theta_{{\rm B},q_2} \\ & \times \left(\frac{m_{\rm B}}{\bar{\gamma}_{\rm B}}\right)^{\phi_{\rm B}} \exp\left(\frac{m_{\rm B}q_0}{\bar{\gamma}_{\rm B}} + \frac{m_{\rm E}}{\bar{\gamma}_{\rm E}}\right) \sum_{k_1=0}^{k+\phi_{\rm B}} \binom{k+\phi_{\rm B}}{k_1} (-1)^{k+\phi_{\rm B}-k_1} \left(\frac{m_{\rm B}q_0}{\bar{\gamma}_{\rm B}} + \frac{m_{\rm E}}{\bar{\gamma}_{\rm E}}\right)^{-k_1} \Gamma\left(k_1, \left(\frac{m_{\rm B}q_0}{\bar{\gamma}_{\rm B}} + \frac{m_{\rm E}}{\bar{\gamma}_{\rm E}}\right)\left(\gamma_{\rm T}+1\right)\right) \Bigg\}\end{aligned} \tag{26}$$

Corollary 3. *When $\bar{\gamma}_{\rm B} \to \infty$ and $\bar{\gamma}_{\rm E}$ is fixed, the asymptotic ergodic secrecy rate of multiuser multi-antenna wiretap networks with TAS/tSD scheme is given by*

$$\overline{C}^{\infty}_{{\rm s},1} = \Delta_1^{\infty} + \Delta_2^{\infty} \tag{27}$$

where Δ_1^{∞} and Δ_2^{∞} is provided by (28) *and* (29)*, respectively.*

Proof: A detailed proof is provided in Appendix C. ∎

In order to gain more insights, we also provide two metrics i.e., the high SNR slope and the high SNR power offset, to describe the asymptotic behavior of the ergodic secrecy rate in the high SNR regime. We adopt a general form to rewrite the asymptotic ergodic secrecy rate as [1]

$$\overline{C}^{\infty}_{{\rm s},1} = S_{\infty}\left(\log_2\bar{\gamma}_{\rm B} - \zeta_{\infty}\right) \tag{30}$$

where S_{∞} denotes the high SNR slope in bits/s/Hz (3dB) and ζ_{∞} is the high SNR power offset in 3dB units. According to [1], the high SNR slope is given by

$$S_{\infty} = \lim_{\bar{\gamma}_{\rm B}\to\infty} \frac{\overline{C}^{\infty}_{{\rm s},1}}{\log_2\bar{\gamma}_{\rm B}} \tag{31}$$

Substituting (27) into (31) and performing some algebraic manipulations, we have

$$S_{\infty} = 1 \tag{32}$$

From (32), we find that the key parameters, such as the number of legitimate users $N_{\rm B}$ and of eavesdroppers $N_{\rm E}$ as well as the switched threshold $\gamma_{\rm T}$, have no impact on the high SNR slope. Next, we turn our attention to the high SNR power offset ζ_{∞}, which can be easily derived as follows:

$$\zeta_{\infty} = \lim_{\bar{\gamma}_{\rm B}\to\infty} \left(\log_2\bar{\gamma}_{\rm B} - \frac{\overline{C}^{\infty}_{{\rm s},1}}{S_{\infty}}\right) \tag{33}$$

It is noted that (33) reflects the impact of main channel and eavesdropping channel on the ergodic secrecy rate. Therefore, inserting (30) and (31) into (33), ζ_{∞} can be further expressed as

$$\zeta_{\infty} = \zeta_{\infty}\left(A_{\rm A}, m_{\rm B}\right) + \zeta_{\infty}\left(N_{\rm E}, m_{\rm E}, \bar{\gamma}_{\rm E}\right), \tag{34}$$

where

$$\begin{aligned}\zeta_{\infty}\left(A_{\rm A}, m_{\rm B}\right) = & \frac{-A_{\rm A}}{\Gamma(m_{\rm B})} \sum_{q=0}^{A_{\rm A}-1} \binom{A_{\rm A}-1}{q} (-1)^q \Theta_{{\rm B},q} \Gamma\left(m_{\rm B}+\phi_{\rm B}\right) \\ & \times (1+q)^{-(m_{\rm B}+\phi_{\rm B})} \left[\frac{\psi(m_{\rm B}+\phi_{\rm B})}{\ln 2} - \log_2\left(m_{\rm B}\left(1+q\right)\right)\right]\end{aligned} \tag{35}$$

and

$$\zeta_{\infty}\left(N_{\rm E}, m_{\rm E}, \bar{\gamma}_{\rm E}\right) = \Delta_2^{\infty} \tag{36}$$

Based on the analysis above, we can draw the conclusion that the high SNR offset is independent of $\bar{\gamma}_{\rm B}$. Besides, the positive impact of main channel on ergodic secrecy rate is characterized by $\zeta_{\infty}\left(A_{\rm A}, m_{\rm B}\right)$, which is related to the key system parameters of the legitimate channel, i.e., $A_{\rm A}$ and $m_{\rm B}$. On the other hand, the negative impact of eavesdropper's channel is characterized by $\zeta_{\infty}\left(N_{\rm E}, m_{\rm E}, \bar{\gamma}_{\rm E}\right)$, which is associated with the parameters of eavesdropping channel, i.e., $N_{\rm E}, m_{\rm E}$ and $\bar{\gamma}_{\rm E}$. In addition, $\zeta_{\infty}\left(N_{\rm E}, m_{\rm E}, \bar{\gamma}_{\rm E}\right)$ also explicitly quantifies the loss of ergodic secrecy rate due to the behavior of the wiretapping at Eves.

In the sequel, we take into account the case of $\bar{\gamma}_{\rm B} \to \infty$ and $\bar{\gamma}_{\rm E} \to \infty$ with a fixed MER $\frac{\bar{\gamma}_{\rm B}}{\bar{\gamma}_{\rm E}} = \lambda_{\rm be}$ and provide the following corollary.

Corollary 4. *The asymptotic ergodic secrecy rate at $\bar{\gamma}_{\rm B} \to \infty$ and $\bar{\gamma}_{\rm E} \to \infty$ with $\frac{\bar{\gamma}_{\rm B}}{\bar{\gamma}_{\rm E}} = \lambda_{\rm be}$ of multiuser multi-antenna wiretap networks with TAS/tSD scheme is given by* (37)*.*

$$\Delta_1^{\infty} = \frac{A_{\rm A}}{\Gamma(m_{\rm B})} \sum_{q=0}^{A_{\rm A}-1} \binom{A_{\rm A}-1}{q} (-1)^q \Theta_{{\rm B},q} \Gamma\left(m_{\rm B}+\phi_{\rm B}\right) (1+q)^{-(m_{\rm B}+\phi_{\rm B})} \left[\frac{\psi(m_{\rm B}+\phi_{\rm B})}{\ln 2} - \log_2\left(m_{\rm B}\left(1+q\right)\right)\right] + \log_2\left(\bar{\gamma}_{\rm B}\right) \quad (28)$$

$$\Delta_2^{\infty} = \frac{1}{\ln 2} \sum_{k=0}^{N_{\rm E} m_{\rm E}-1} \frac{1}{k!} \left(\frac{m_{\rm E}}{\bar{\gamma}_{\rm E}}\right)^k \left[(-1)^{k-1} \exp\left(\frac{m_{\rm E}}{\bar{\gamma}_{\rm E}}\right) {\rm Ei}\left(-\frac{m_{\rm E}}{\bar{\gamma}_{\rm E}}\right) + \sum_{k_1=1}^{k} (k_1-1)! (-1)^{k-k_1} \left(\frac{m_{\rm E}}{\bar{\gamma}_{\rm E}}\right)^{-k_1}\right] \quad (29)$$

Proof: A detailed proof is provided in Appendix D. ■

As can be observed from (37) that a rate ceiling exists in this particular case. Once again, it demonstrates that increasing the transmit power at the BS does not have a positive impact on the ergodic secrecy rate when the eavesdropper is located close to the transmitter.

D. Average Number of User Examinations

Compared with the best scheduling scheme, i.e., SC scheme, where all the $N_{\rm B}$ legitimate users are examined to select the best one, tSD scheme only examines the legitimate user adopted in the previous time slot. Once it is acceptable, there is no need to check out the remaining $(N_{\rm B}-1)$ legitimate users. Hence, the average number of user examinations can be expressed as [31]:

$$N_{\rm TAS/tSD}^{\rm avg} = \sum_{\alpha=1}^{A_{\rm A}} \left[1 + (N_{\rm B}-1) F_{\gamma_{\alpha,k}^{\rm b}}(\gamma_{\rm T})\right] \quad (38)$$

For the SECps scheme, it examines the SNRs of additional main links only if necessary. Once the SNR of the k-th legitimate user is acceptable, there is no need to check out the remaining SNRs of $(N_{\rm B}-k)$ legitimate users. Hence, the average number of user examinations can be characterized as [22]

$$N_{\rm TAS/SECps}^{\rm avg} = \sum_{\alpha=1}^{A_{\rm A}} \sum_{k=0}^{N_{\rm B}-1} \left[F_{\gamma_{\alpha,k}^{\rm b}}(\gamma_{\rm T})\right]^k \quad (39)$$

On the other hand, since $0 \le F_{\gamma_{\alpha,k}^{\rm b}}(\gamma_{\rm T}) \le 1$, we have

$$\left[F_{\gamma_{\alpha,k}^{\rm b}}(\gamma_{\rm T})\right]^k < F_{\gamma_{\alpha,k}^{\rm b}}(\gamma_{\rm T}), k \in \{1,2,...,N_{\rm B}-1\} \quad (40)$$

By jointly taking (38), (39) and (40) into account, we have

$$N_{\rm TAS/SECps}^{\rm avg} \le N_{\rm TAS/tSD}^{\rm avg} \le A_{\rm A} N_{\rm B} \quad (41)$$

As a result, the implementation cost of TAS/tSD scheme is higher than that of TAS/SECps scheme, while it is lower than TAS/SC scheme.

IV. Simulations and Discussion

In this section, we present some numerical results to validate the aforementioned secrecy analysis and analyze the joint impact of key parameters on the secrecy performance of the considered system.

Fig. 2 presents the secrecy outage probability and asymptotic secrecy outage probability versus different average legitimate user's SNR $\bar{\gamma}_{\rm B}$ in Case I. It is observed from the figure that the theoretical results of secrecy outage probability

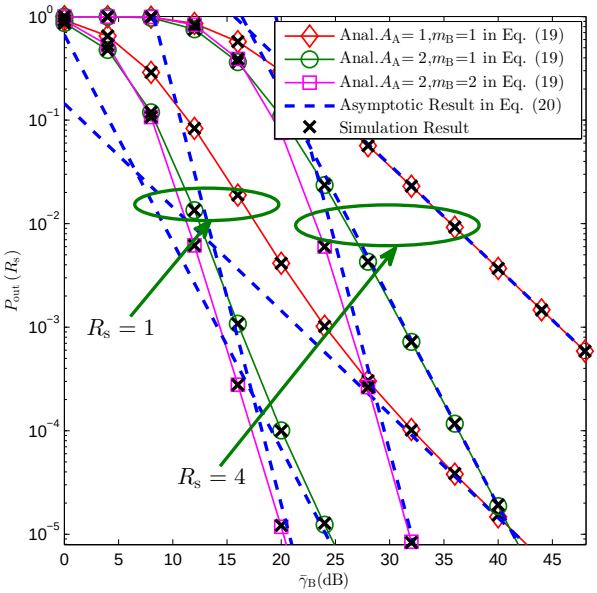


Fig. 2: Secrecy outage probability in Case I versus different $\bar{\gamma}_{\rm B}$ for $\bar{\gamma}_{\rm E}=0$dB, $\gamma_{\rm T}=10$dB, $m_{\rm E}=1$ and $N_{\rm B}=N_{\rm E}=2$.

in (17) match precisely with the Monte Carlo simulations and the high SNR curves given by (18) agree very well with the exact ones in the high SNR regime and accurately predict the secrecy diversity order and secrecy array gain. Furthermore, increasing the number of antennas at the BS and the channel fading severity parameter of legitimate channel have positive impact on the secrecy performance. This is due to the fact that more number of transmit antennas results in larger transmit diversity gains and the higher $m_{\rm B}$ means the better channel quality of legitimate channel. Additionally, as can be expected, the secrecy outage probability of TAS/tSD scheme degrades with the increment of the predefined secrecy rate $R_{\rm s}$, and increasing $R_{\rm s}$ does not influence the secrecy diversity order as indicated by the parallel slopes of the asymptotes.

Fig. 3 illustrates the secrecy outage probability of the system with different $N_{\rm B}$. As illustrated in the figure, we observe that the secrecy performance can be improved as increasing $N_{\rm B}$ for the particular case when $\overline{\gamma}_{\rm B} \le \gamma_{\rm T}$. However, when $\overline{\gamma}_{\rm B} \ge \gamma_{\rm T}$, increasing the number of legitimate users $N_{\rm B}$ has marginal impact on the secrecy outage performance due to no additional secrecy diversity order. Moreover, the better secrecy performance can be achieved with the larger predefined switched threshold $\gamma_{\rm T}$, while the TAS/tSD scheme and TAS/SECps scheme turn into the TAS/SC scheme as $\gamma_{\rm T}$

$$\overline{C}_{\mathrm{s},2}^{\infty} = \log_2(\lambda_{\mathrm{be}}) + A_{\mathrm{A}} \sum_{q=0}^{A_{\mathrm{A}}-1} \binom{A_{\mathrm{A}}-1}{q} (-1)^q \Theta_{\mathrm{B},q} \frac{\Gamma(m_{\mathrm{B}}+\phi_{\mathrm{B}})}{\Gamma(m_{\mathrm{B}})} (1+q)^{-(m_{\mathrm{B}}+\phi_{\mathrm{B}})} \left[\frac{\psi(m_{\mathrm{B}}+\phi_{\mathrm{B}})}{\ln 2} - \log_2(m_{\mathrm{B}}(1+q)) \right] - \frac{\psi(N_{\mathrm{E}} m_{\mathrm{E}})}{\ln 2} + \log_2(m_{\mathrm{E}}) \quad (37)$$

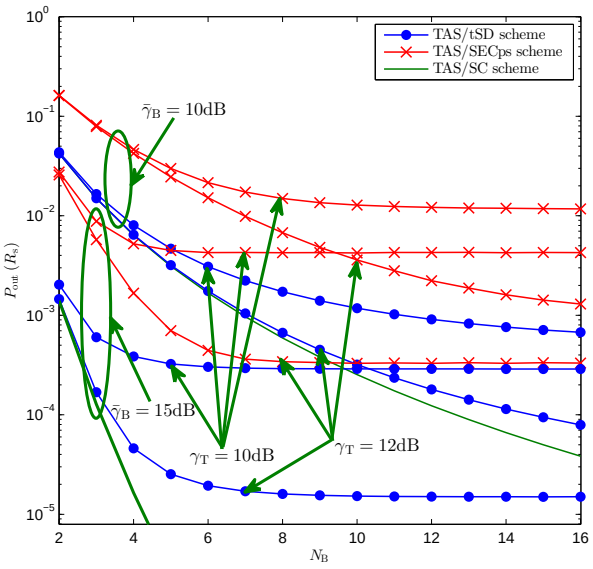


Fig. 3: Secrecy outage probability versus N_{B} with different $\bar{\gamma}_{\mathrm{B}}$ and γ_{T} for $A_{\mathrm{A}} = 2$, $m_{\mathrm{B}} = m_{\mathrm{E}} = 1$, $N_{\mathrm{E}} = 2$, $R_{\mathrm{s}} = 1$ and $\bar{\gamma}_{\mathrm{E}} = 0$dB.

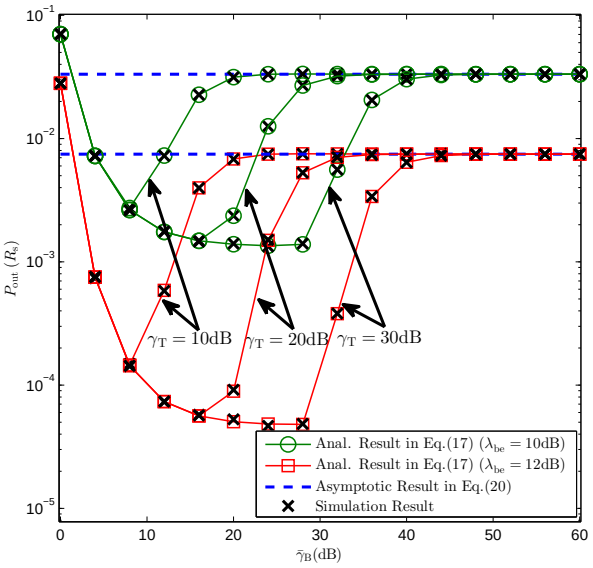


Fig. 4: Secrecy outage probability in Case II versus $\bar{\gamma}_{\mathrm{B}}$ for $A_{\mathrm{A}} = 3, N_{\mathrm{B}} = 4, N_{\mathrm{E}} = 2, m_{\mathrm{B}} = 2, m_{\mathrm{E}} = 1, R_{\mathrm{s}} = 1$ with different γ_{T} and λ_{be}.

approaches to infinite.

Fig. 4 shows the secrecy outage probability versus $\bar{\gamma}_{\mathrm{B}}$ with different γ_{T} and λ_{be} in Case II. As shown obviously in the figure, the larger switched threshold γ_{T} results in better secrecy performance since more legitimate users have been examined. It can also be observed that at a fixed MER λ_{be}, the secrecy outage probability improves with $\bar{\gamma}_{\mathrm{B}}$ in the low SNR area, however the improvement tends to be saturated in the medium and high SNR area. This is attributed to the fact that the MER is the bottleneck of the secrecy outage probability. In addition, we can see that the secrecy outage probability floor decreases with the increment of MER.

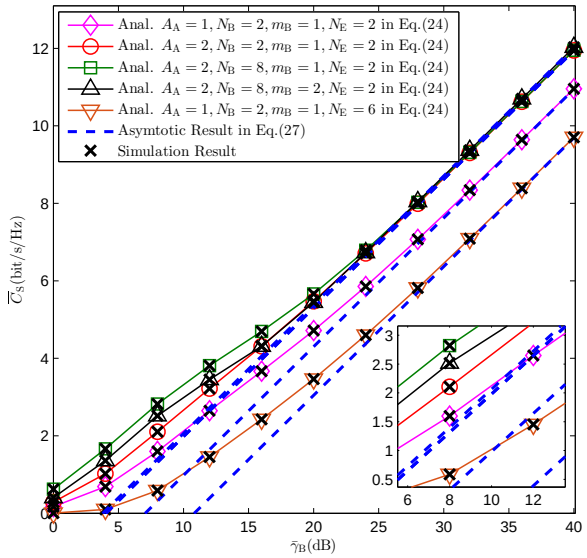


Fig. 5: Ergodic secrecy rate versus $\bar{\gamma}_{\mathrm{B}}$ with different $A_{\mathrm{A}}, N_{\mathrm{B}}$ and m_{B} settings as well as $\gamma_{\mathrm{T}} = 10$dB, $N_{\mathrm{E}} = 2$ and $m_{\mathrm{E}} = 2$.

Fig. 5 depicts the ergodic secrecy rate of the system with TAS/tSD scheme against different N_{B} in Case I. It can be observed that the curves of ergodic secrecy rate generated by (24) are in exact agreement with the Monte Carlo simulations and the curves of asymptotic ergodic secrecy rate in (27) well approximate the analytical ones in the high SNR regimes. We also observe that, both the number of legitimate users N_{B} and antenna configurations contribute to the improvement of ergodic secrecy rate in the low $\bar{\gamma}_{\mathrm{B}}$ regime, where the TAS/tSD scheme is equal to N_{B}-legitimate users TAS/SC scheme and multiuser diversity gain is achieved. However, in the high $\bar{\gamma}_{\mathrm{B}}$ regime, BS intends to schedule the first user, and thus the ergodic secrecy rate is independent of the number of legitimate users N_{B}. From another point of view, the high power offset ζ_{∞} in (34) is not relevant to the number of legitimate users N_{B} under this case. It needs to be pointed out that, in contrast with the secrecy outage probability, increasing the fading severity parameter of the legitimate channel slightly degrades

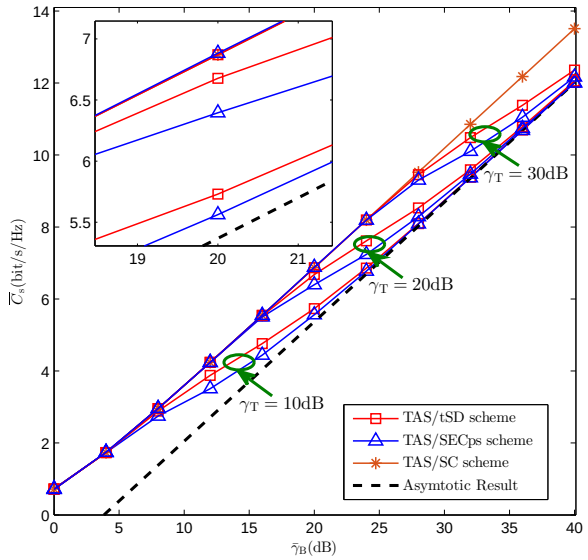


Fig. 6: Ergodic secrecy rate versus $\bar{\gamma}_B$ with different γ_T for $A_A = 2$, $N_B = 8$, $N_E = 2$, $m_B = m_E = 1$ and $\bar{\gamma}_E = 0$dB.

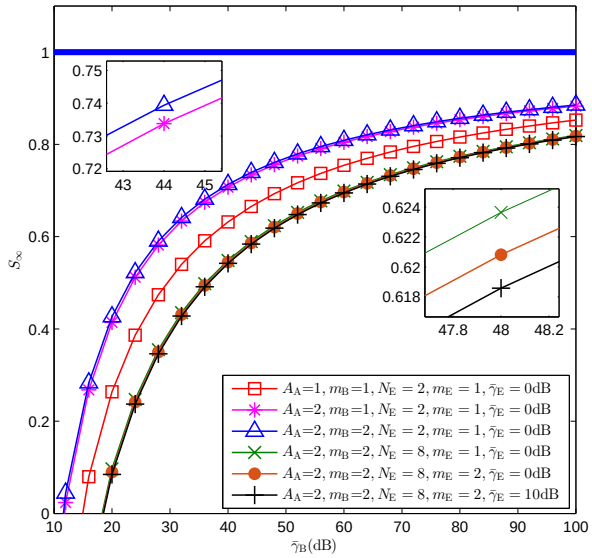


Fig. 7: High SNR slope S_∞ versus $\bar{\gamma}_B$ with different system parameters.

the ergodic secrecy rate. In addition, as can be expected, increasing the number of eavesdroppers can considerably improve the wiretapping capability of colluding eavesdropper, which leads to the increment of the high power offset ζ_∞, and thus degrades secrecy performance of the considered systems.

Fig. 6 shows that the ergodic secrecy rate improves with the increase of the switched threshold γ_T. This is due to the fact that the scheduler has more opportunities to adopt TAS/SC scheme as the switched threshold increases, thus it yields a better performance at the expense of higher complexity. That is to say, when γ_T comes close to infinity, the TAS/tSD scheme

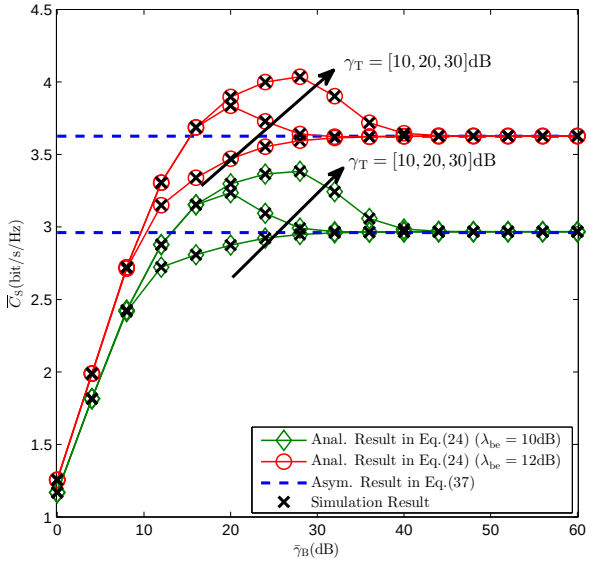


Fig. 8: Ergodic secrecy rate in Case II versus $\bar{\gamma}_B$ for $A_A = 2, N_B = 2, N_E = 2, m_B = 2, m_E = 1$ with different γ_T and λ_{be}.

completely turns into the TAS/SC scheme. In addition, it is observed that the TAS/tSD scheme outperforms the TAS/SECps scheme regardless of switched threshold γ_T. Fig. 7 presents the impact of key system parameters A_A, m_B, N_E, m_E and $\bar{\gamma}_E$ on the high SNR slope S_∞. As illustrated in the figure, the key system parameters of the legitimate channel A_A and m_B have a positive impact on the high SNR slope. However, when the parameters related with eavesdropping channel, i.e., N_E, m_E or $\bar{\gamma}_E$ increases, the speed of convergence to 1 slows down. This is because that the second term on the right hand side of (34) has a great impact on the high SNR slope S_∞.

Fig. 8 shows the ergodic secrecy rate versus $\bar{\gamma}_B$ with different γ_T and λ_{be} in Case II. It is shown in Fig. 8 that the exact curves of (24) are still in good agreement with the Monte Carlo simulations, and the asymptotic results in (20) predict the exact ones precisely in the high SNR area. Similar to the secrecy outage probability in Case II, we find that the increment of switched threshold γ_T contributes to the improvement of the ergodic secrecy rate. It can be observed that at a fixed MER λ_{be}, the ergodic secrecy rate increases with $\bar{\gamma}_B$ in the low SNR area, but tends to a rate ceiling in the medium and high SNR area. This is due to the fact that the MER is the bottleneck of the ergodic secrecy rate under this case. Furthermore, we also find that increasing the MER leads to the reduction of rate ceiling.

Fig. 9 presents the saving percentage of the number of legitimate user estimations, i.e., $\left(1 - N^{\text{avg}}_{\text{TAS/tSD}}/A_A/N_B\right)$. As illustrated in this figure, the saving percentage of TAS/tSD scheme reduces to zero as the switched threshold increases. By jointly considering Fig. 3, Fig. 6 and Fig. 9, we find that the TAS/tSD scheme achieves better secrecy performance than the TAS/SECps scheme at the expense of negligible complexity cost, and achieves a similar performance as TAS/SC scheme

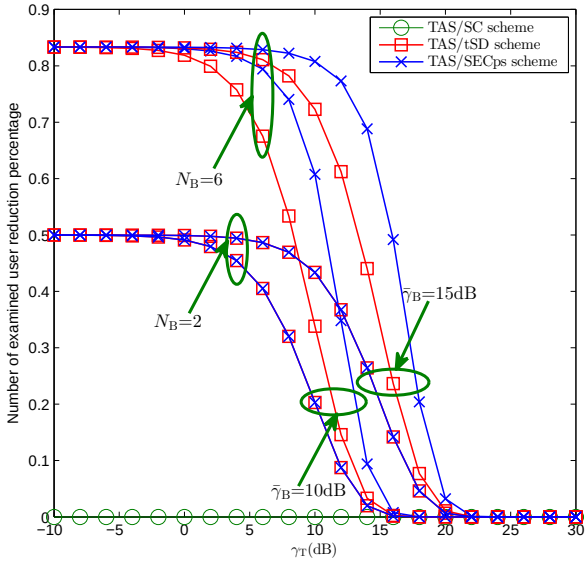


Fig. 9: The reduced percentage of number of user examinations versus switched thresholds $\gamma_{\rm T}$ with different $N_{\rm B}$ and $\bar{\gamma}_{\rm B}$, where $A_{\rm A}=2$ and $m_{\rm B}=2$.

while maintaining a lower number of user estimations load compared with TAS/SC scheme.

V. Conclusions

In this paper, we have presented a comprehensive secrecy performance analysis of multiuser multi-antenna wiretap networks with the TAS/tSD scheme. Particularly, the secrecy performance of two practical scenarios was addressed with respect to the availability of the CSI of the eavesdropping channel at the BS. When the BS has the full knowledge of the eavesdropper's CSI, we have derived closed-form exact expressions of the secrecy outage probability and the probability of non-zero secrecy capacity, which provides a fast and efficient way to evaluate the secrecy performance of the system. Moreover, simple and informative high SNR approximations for the secrecy outage probability were derived under two distinct cases, which enable us to exploit more insights about the impact of the key parameters on the secrecy performance. For the case of eavesdropper's CSI is not available at the BS, we have investigated in detail the ergodic secrecy rate achieved by the system with TAS/tSD scheme. In doing so, novel closed-form expressions for the exact and asymptotic ergodic secrecy rate were derived. Our results demonstrate that when the switched threshold being carefully selected, the TAS/tSD scheme outperforms the TAS/SECps scheme in terms of the secrecy performance at the expense of little complexity cost, while maintaining a lower number of user estimations load compared with TAS/SC scheme.

Appendix A
A Detailed Derivation for Corollary 1

In the high SNR regime, i.e., $\bar{\gamma}_{\rm B}\to\infty$ with a fixed $\bar{\gamma}_{\rm E}$, the CDF of $\gamma^{\rm b}_{\alpha,k}$ can be approximated as

$$F_{\gamma^{\rm b}_{\alpha,k}}(x)\approx\frac{{m_{\rm B}}^{m_{\rm B}}}{(m_{\rm B})!}\left(\frac{x}{\bar{\gamma}_{\rm B}}\right)^{m_{\rm B}} \tag{42}$$

By inserting (42) into (8) and using the law of binomial theorem, we have

$$F_{\gamma_{\rm B}}(x)=\begin{cases}\sum\limits_{q=0}^{A_{\rm A}}\binom{A_{\rm A}}{q}\left[\frac{{m_{\rm B}}^{m_{\rm B}}}{(m_{\rm B})!}\left(\frac{\gamma_{\rm T}}{\bar{\gamma}_{\rm B}}\right)^{m_{\rm B}}\right]^q\sum\limits_{q_1=0}^{q}\binom{q}{q_1}(-1)^{q_1} & \\ \times\left[\frac{{m_{\rm B}}^{m_{\rm B}}}{(m_{\rm B})!}\left(\frac{x}{\bar{\gamma}_{\rm B}}\right)^{m_{\rm B}}\right]^{(N_{\rm B}-1)(q-q_1)+A_{\rm A}-q}, & x\geq\gamma_{\rm T}\\ \left[\frac{{m_{\rm B}}^{m_{\rm B}}}{(m_{\rm B})!}\left(\frac{x}{\bar{\gamma}_{\rm B}}\right)^{m_{\rm B}}\right]^{A_{\rm A}N_{\rm B}}, & x<\gamma_{\rm T}\end{cases} \tag{43}$$

As such, by plugging (43) into (16) and neglecting the higher order terms, with the help of [41, Eqs. (3.381.3) and (3.351.3)], the desired asymptotic outage probability $P_{\rm out}(R_{\rm s})$ can be easily derived as (18) after some simple mathematical manipulations.

Appendix B
A Derivation for Some Integral Equations

In this Appendix, we present some useful results on the solution of some integrals, which will be frequently adopted to evaluate some performance metrics.

Consider the following first integral

$$\int_0^v\frac{\exp(-ux)\,x^k}{1+x}dx \tag{44}$$
$$=\exp(u)\sum_{k_1=0}^{k}\binom{k}{k_1}(-1)^{k-k_1}\times u^{-k_1}\left[\Gamma(k_1,u)-\Gamma(k_1,u(v+1))\right]$$

Proof: Let $y=1+x$, then we have

$$\int_0^v\frac{\exp(-ux)\,x^k}{1+x}dx=\int_1^{v+1}\frac{\exp(-u(y-1))\,(y-1)^k}{y}dy \tag{45a}$$

By adopting the binomial theorem, the above expression can be further expanded as

$$\int_0^v\frac{\exp(-ux)\,x^k}{1+x}dx \tag{45b}$$
$$=\exp(u)\sum_{k_1=0}^{k}\binom{k}{k_1}(-1)^{k-k_1}\int_1^{v+1}\exp(-uy)\,y^{k_1-1}dy$$
$$=\exp(u)\sum_{k_1=0}^{k}\binom{k}{k_1}(-1)^{k-k_1}\times\left(\int_1^{\infty}\exp(-ux)\,x^{k_1-1}dx-\int_{v+1}^{\infty}\exp(-ux)\,x^{k_1-1}dx\right) \tag{45c}$$

With the aid of variable substitution operation $y = ux$, and resorting to the upper incomplete gamma function in [41, Eq. (8.350.2)] as $\Gamma(\alpha,\mu) = \int_{\mu}^{\infty} e^{-t} t^{\alpha-1} dt$, we obtain

$$\int_{1}^{v+1} \exp(-ux)\, x^{k_1-1} dx = u^{-k_1} \left[\Gamma(k_1, u) - \Gamma(k_1, u(v+1))\right] \tag{45d}$$

Finally, by substituting (45d) into (45b), therefore we complete the proof of (44). ∎

Consider the following second integral

$$\int_{v}^{\infty} \frac{\exp(-ux)}{1+x} dx = \exp(u)\, \Gamma(0, u(1+v)) \tag{46}$$

Proof: Similarly, with the operation of variable substitution $y = 1 + x$, we have

$$\int_{v}^{\infty} \frac{\exp(-ux)}{1+x} dx = \int_{1+v}^{\infty} \frac{\exp(-u(y-1))}{y} dy \tag{47a}$$

and then let $z = uy$, we have

$$\int_{v}^{\infty} \frac{\exp(-ux)}{1+x} dx = \exp(u) \int_{u(1+v)}^{\infty} \frac{\exp(-z)}{z} dz \tag{47b}$$

Resorting to the upper incomplete gamma function in [41, Eq. (8.350.2)], the desired result can be derived. ∎

Consider the following third integral

$$\int_{v}^{\infty} \frac{\exp(-ux)\, x^{k}}{1+x} dx = \exp(u) \sum_{k_1=0}^{k} \binom{k}{k_1} (-1)^{k-k_1} \left[\frac{1}{u^{k_1}} \Gamma(k_1, u(v+1))\right] \tag{48}$$

Proof: Similar to the proofs above, arming with variable substitution $y = 1 + x$, $z = uy$ and resorting to the upper incomplete gamma function in [41, Eq. (8.350.2)], we obtain the important integral equations. ∎

APPENDIX C
A DETAILED DERIVATION FOR COROLLARY 3

Before probing into the analysis of the asymptotic ergodic secrecy rate, we first rewrite the CDF of γ_{E} as $F_{\gamma_{\mathrm{E}}}(y) = 1 - \varphi_{\gamma_{\mathrm{E}}}(y)$, where

$$\varphi_{\gamma_{\mathrm{E}}}(y) = \exp\left(-\frac{m_{\mathrm{E}} y}{\bar{\gamma}_{\mathrm{E}}}\right) \sum_{k=0}^{N_{\mathrm{E}} m_{\mathrm{E}} - 1} \frac{1}{k!} \left(\frac{m_{\mathrm{E}} y}{\bar{\gamma}_{\mathrm{E}}}\right)^{k} \tag{49}$$

To this end, with the help of (49), the ergodic secrecy rate can be re-expressed as

$$\overline{C}_{\mathrm{s},1} = \frac{1}{\ln 2} \int_{0}^{\infty} \int_{0}^{x} \frac{1 - \varphi_{\gamma_{\mathrm{E}}}(y)}{1+y} dy\, f_{\gamma_{\mathrm{B}}}(x)\, dx = \Delta_1 + \Delta_2 \tag{50}$$

where

$$\Delta_1 = \frac{1}{\ln 2} \int_{0}^{\infty} \ln(1+x) f_{\gamma_{\mathrm{B}}}(x)\, dx \tag{51}$$

and

$$\Delta_2 = -\frac{1}{\ln 2} \int_{0}^{\infty} \int_{0}^{x} \frac{\varphi_{\gamma_{\mathrm{E}}}(y)}{1+y} f_{\gamma_{\mathrm{B}}}(x)\, dy dx \tag{52}$$

Now, in the following, we discuss the characteristics of Δ_1 and Δ_2 in the high SNR regime, respectively. According to the basic idea of tSD scheme, when $\bar{\gamma}_{\mathrm{B}} \to \infty$, the probability that each SNR of the main link γ_k^{b} exceeds the predefined threshold γ_{T} approaches one. That is to say, the instantaneous SNR of the main channel reduces to $\gamma_{\mathrm{B}} = \gamma_{\alpha,k}^{\mathrm{b}}$, the PDF of which can be characterized by

$$f_{\gamma_{\mathrm{B}}}(x) \approx \frac{A_{\mathrm{A}}}{\Gamma(m_{\mathrm{B}})} \sum_{q=0}^{A_{\mathrm{A}}-1} \binom{A_{\mathrm{A}}-1}{q} (-1)^{q} \Theta_{\mathrm{B},q} \left(\frac{m_{\mathrm{B}}}{\bar{\gamma}_{\mathrm{B}}}\right)^{m_{\mathrm{B}}+\phi_{\mathrm{B}}} \times x^{\,m_{\mathrm{B}}+\phi_{\mathrm{B}}-1} \exp\left(-\frac{m_{\mathrm{B}}(q+1)}{\bar{\gamma}_{\mathrm{B}}} x\right) \tag{53}$$

As $x \to \infty$, we have $\ln(1+x) \approx x$, thus, Δ_1 asymptotically turns into

$$\begin{aligned}\Delta_1^{\infty} &= \int_{0}^{\infty} \left[\log_2(\bar{\gamma}_{\mathrm{B}}) + \log_2\left(\frac{x}{\bar{\gamma}_{\mathrm{B}}}\right)\right] f_{\gamma_{\mathrm{B}}}(x)\, dx \\ &= \log_2(\bar{\gamma}_{\mathrm{B}}) + \int_{0}^{\infty} \log_2\left(\frac{x}{\bar{\gamma}_{\mathrm{B}}}\right) f_{\gamma_{\mathrm{B}}}(x)\, dx \end{aligned} \tag{54}$$

Now, by utilizing the PDF of γ_{B} and resorting to [41, Eq.(4.352.1)], we have Δ_1^{∞} as (28), where $\psi(\cdot)$ denotes the digamma function [42].

In what follows, by exchanging the order of integration in Δ_2, therefore, Δ_2 can be rewritten as

$$\begin{aligned}\Delta_2 &= -\frac{1}{\ln 2} \int_{0}^{\infty} \int_{0}^{x} \frac{\varphi_{\gamma_{\mathrm{E}}}(y)}{1+y} f_{\gamma_{\mathrm{B}}}(x)\, dy dx \\ &= -\frac{1}{\ln 2} \int_{0}^{\infty} \frac{\varphi_{\gamma_{\mathrm{E}}}(y)}{1+y} (1 - F_{\gamma_{\mathrm{B}}}(x))\, dy \end{aligned} \tag{55}$$

Depending on the CDF expression in (8), as $\bar{\gamma}_{\mathrm{B}} \to \infty$, we have $F_{\gamma_{\mathrm{B}}}(x) \to 0$. Hence, Δ_2 can be further expressed as

$$\Delta_2^{\infty} = -\frac{1}{\ln 2} \int_{0}^{\infty} \frac{\varphi_{\gamma_{\mathrm{E}}}(y)}{1+y} dy \tag{56}$$

As such, by utilizing (49) and resorting to [41, Eq. (3.353.5)], the asymptotic expression of Δ_2 can be derived as (29) after some mathematical manipulations. Finally, summing up Δ_1^{∞} and Δ_2^{∞} yields the asymptotic ergodic secrecy rate $C_{\mathrm{s},1}^{\infty}$.

APPENDIX D
A DETAILED DERIVATION FOR COROLLARY 4

When $\bar{\gamma}_{\mathrm{B}} \to \infty$ and $\bar{\gamma}_{\mathrm{E}} \to \infty$ with $\frac{\bar{\gamma}_{\mathrm{B}}}{\bar{\gamma}_{\mathrm{E}}} = \lambda_{\mathrm{be}}$, the asymptotic ergodic secrecy rate can be conveniently achieved according to the proof of Corollary 3 in Appendix E. To be specific, what we need to do is just considering the asymptotic behavior for Δ_2^{∞} as $\bar{\gamma}_{\mathrm{B}} \to \infty$. Following the similar procedure developed in [40] and observing Δ_1^{∞} in (54), the asymptotic expression for Δ_2^{∞} is given by

$$\Delta_{2,2}^{\infty} = -\log_2(\bar{\gamma}_{\mathrm{E}}) - \int_{0}^{\infty} \log_2\left(\frac{y}{\bar{\gamma}_{\mathrm{E}}}\right) f_{\gamma_{\mathrm{E}}}(y)\, dy \tag{57}$$

By plugging the PDF of γ_{B} in (53) into (57) and capitalizing on the equation [41, Eq.(4.352.1)], we have

$$\Delta_{2,2}^{\infty} = -\log_2(\bar{\gamma}_{\mathrm{E}}) - \frac{\psi(N_{\mathrm{E}} m_{\mathrm{E}})}{\ln 2} + \log_2(m_{\mathrm{E}}) \tag{58}$$

Therefore, by summing up the new asymptotic result (58) for Δ_2^{∞} and (28) into (50), we eventually obtain (37) and complete the proof.

ACKNOWLEDGMENTS

The authors wish to thank the reviewers for valuable and constructive suggestions that improved and clarified the paper.

REFERENCES

[1] Y. Huang, F. S. Al-Qahtani, T. Q. Duong, and J. Wang, "Secure transmission in MIMO wiretap channels using general-order transmit antenna selection with outdated CSI," *IEEE Trans. Commun.*, vol. 63, no. 8, pp. 2959-2971, Aug. 2015.

[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Technol. J.*, vol. 28, no. 4, pp. 656-715, Oct. 1949.

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

[4] F. A. Khan, K. Tourki, M.-S. Alouini, and K. A. Qaraqe, "Outage and SER performance of spectrum sharing system with TAS/MRC," in *Proc. IEEE Commun. Conf.*, pp. 381-385, Jun. 2013.

[5] F. A. Khan, K. Tourki, M.-S. Alouini, and K. A. Qaraqe, "Performance analysis of a power limited spectrum sharing system with TAS/MRC," *IEEE Trans. Signal Process.*, vol. 62, no. 4, pp. 954-967, Feb. 2014.

[6] K. Tourki, F. A. Khan, K. A. Qaraqe, H. -C. Yang, and M.-S. Alouini, "Exact performance analysis of MIMO cognitive radio systems using transmit antenna selection," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 3, pp. 425-438, Mar. 2014.

[7] 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.

[8] 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.

[9] 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. Commun.*, vol. 13, no. 11, pp. 6054-6067, Nov. 2014.

[10] J. Xiong, Y. Tang, D. Ma, P. Xiao, and K. K. Wong, "Secrecy performance analysis for TAS-MRC system with imperfect feedback," *IEEE Trans. Inf. Forensics Security*, vol. 10, No. 8, pp. 1617-1629, Aug. 2015.

[11] K. Tourki and M. O. Hasna, "Proactive spectrum sharing incentive for physical layer security enhancement," in *Proc. IEEE Global Commun. Conf.*, pp. 1-6, Dec. 2015.

[12] K. Tourki and M. O. Hasna, "Proactive spectrum sharing incentive for physical layer security enhancement using outdated CSI," *IEEE Trans. Wireless Commun.*, accepted for publication, in 2016.

[13] J. Zhu, Y. Zou, G. Wang, Y. D. Yao, and G. K. Karagiannidis, "On secrecy performance of antenna-selection-aided MIMO systems against eavesdropping," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 214-225, Jan. 2016.

[14] Y. Hu and X. Tao, "Secrecy outage analysis of MU-MIMO transmit antenna selection systems with arbitrary number of eavesdropping users," *Electron. Lett.*, vol. 51, no. 11, pp. 874-876, May. 2015

[15] N. Li, X. Tao, and H. Wu, "Large system analysis of artificial noise assisted communication in the multiuser downlink: ergodic secrecy sum-rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, accepted for publication, in 2016.

[16] J. Lee and C. Wan, "Multiuser diversity for secrecy communications using opportunistic jammer selection: Secure DoF and jammer scaling law," *IEEE Trans. Signal Process.*, vol. 62, no. 4, pp. 828-839, Feb. 2014.

[17] K. Sung-Il, K. Il-Min, and H. Jun, "Secure transmission for multiuser relay networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 3724-3737, Jul. 2015.

[18] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 5103-5113, Dec. 2013.

[19] M. Pei, A. L. Swindlehurst, D. Ma, and J. Wei, "On ergodic secrecy rate for MISO wiretap broadcast channels with opportunistic scheduling," *IEEE Commun. Lett.*, vol. 18, no. 1, pp. 50-53, Jan. 2014.

[20] X. Ge, H. Jin, X. Li, and V. C. M. Leung, "Opportunistic fair resource sharing with secrecy considerations in uplink wiretap channels," in *Proc. IEEE Wireless Commun. and Networking Conf.*, New Orleans, LA, Mar. 2015, pp. 1422-1427.

[21] B. Holter, M.-S. Alouini, G. E. Oien, and H. -C. Yang, "Multiuser switched diversity transmission," in *Proc. IEEE Veh. Technol. Conf.*, Sep. 2004, pp. 2038-2043.

[22] H. -C. Yang and M.-S. Alouini, "Improving the performance of switched diversity with post-examining selection," *IEEE Trans. Wireless Commun.*, vol. 5, no. 1, pp. 67-71, Jan. 2006.

[23] Y. S. Al-harthi, A. H. Tewfik, and M.-S. Alouini, "Multiuser diversity with quantized feedback," *IEEE Trans. Wireless Commun.*, vol. 6, no. 1, pp. 330-337, Jan. 2007.

[24] S. S. Nam, M.-S. Alouini, H. -C. Yang, and K. A. Qaraqe, "Threshold-based parallel multiuser scheduling," *IEEE Trans. Wireless Commun.*, vol. 8, no. 4, pp. 2150-2159, Apr. 2009.

[25] H. Nam and M.-S. Alouini, "Multiuser switched diversity scheduling systems with per-user threshold," *IEEE Trans. Commun.*, vol. 58, no. 5, pp. 1321-1326, May. 2010.

[26] M. Shaqfeh, H. Alnuweiri, and M.-S. Alouini, "Multiuser switched diversity scheduling schemes," *IEEE Trans. Commun.*, vol. 60, no. 9, pp. 2499-2510, Sep. 2012.

[27] Z. Bouida, K. Tourki, A. Ghrayeb, K. Qaraqe, and M.-S. Alouini, "Power adaptation for joint switched diversity and adaptive modulation schemes in spectrum sharing systems," *IEEE Commun. Lett.*, vol. 16, no. 9, pp. 1482-1485, Sep. 2012.

[28] Y. Hu, X. Tao, J. Xu, and Q. Cui, "Secrecy outage analysis of transmit antenna selection with switch-and-examine combining over rayleigh fading," in *Proc. IEEE Veh. Technol. Conf.*, Vancouver, BC, Sep. 2014, pp. 1-5.

[29] M. Yang, B. Zhang, Y. Huang, D. Guo, and X. Yi, "Ergodic secrecy capacity for downlink multiuser networks using switch-and-examine combining with post-selection scheduling scheme," *Electron. Lett.*, vol. 52, no. 9, pp. 720-722, Apr. 2016.

[30] M. Yang, B. Zhang, Y. Huang, and D. Guo, "Secrecy outage analysis of multiuser downlink wiretap networks with SECps scheduling in Nakagami-m channel," *IEEE Wireless Commun. Lett.*, accepted for publication, in 2016.

[31] P. S. Bithas, A. A. Rontogiannis, and G. K. Karagiannidis, "An improved threshold-based channel selection scheme for wireless communication systems," in *IEEE Trans. Wireless Commun.*, accepted for publication, in 2016.

[32] L. Fan, N. Yang, T. Duong, M. Elkashlan, and G. Karagiannidis, "Exploiting direct links for physical layer security in multi-user multi-relay networks," *IEEE Trans. Wireless Commun.*, accepted for publication, in 2016.

[33] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875-1888, Mar. 2010.

[34] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information theoretic security," *IEEE Trans. Inf. Theory*, vol. 5, no. 6, pp. 2515-2534, Jun. 2008.

[35] X. Zhou, R. K. Ganti, and J. G. Andrews, "Secure wireless network connectivity with multi-antenna transmission," in *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 425-430, Feb. 2011.

[36] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 3000-3015, May. 2012.

[37] Y. Zhang, Y. Shen, H. Wang, J. Yong, and X. Jiang, "On secure wireless communications for IoT under eavesdropper collusion," *IEEE Trans. Autom. Sci. Eng.*, to be published, in 2016.

[38] J. Hu, Y. Cai, N. Yang, and W. Yang, "A New secure transmission scheme with outdated antenna selection," *IEEE Trans. Inf. Forensics and Security*, vol. 10, no. 11, pp. 2435-2446, Nov. 2015.

[39] L. Wang, N. Yang, M. Elkashlan, P. Yeoh, and J. Yuan, "Physical layer security of maximal ratio combining in two-wave with diffuse power fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 2, pp. 247-258, Feb. 2014.

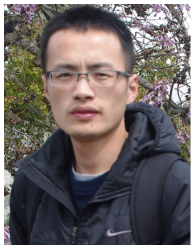
[40] L. Wang, K. J. Kim, T. Q. Duong, M. Elkashlan, and H. V. Poor, "Security enhancement of cooperative single carrier systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 1, pp. 90-103, Jan. 2015

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

[42] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tables*, 9th ed. New York, NY, USA: Dover, 1972.

Maoqiang Yang received his B.S. degree from South China University of Technology, Guangzhou, China, in 2010 and the M.S. degree from PLA University of Science and Technology, Nanjing, China, in 2013. He is currently working toward his Ph.D. degree in PLA University of Science and Technology. His research interests focus on nonlinear signal processing, MIMO communications systems, multiuser communication systems, cooperative communications and physical layer security.

Daoxing Guo received the B.S. degree, M.S. degree and ph.D. degree from Institute of Communications Engineering (ICE), Nanjing, China, in 1995, 1999 and 2002, respectively. He is currently a Full Professor and also a Ph.D. Supervisor with PLA University of Science and Technology. He has authored and coauthored more than 40 conference and journal papers and has been granted over 20 patents in his research areas. He has served as a reviewer for several journals in communication field. His current research interests include satellite communications systems and Transmission technologies, communication anti-jamming technologies, communication anti-interception technologies including physical layer security and so on.



Yuzhen Huang received his B.S. degree in Communications Engineering, and Ph.D. degree in Communications and Information Systems from College of Communications Engineering, PLA University of Science and Technology, in 2008 and 2013 respectively. He has been with College of Communications Engineering, PLA University of Science and Technology since 2013, and currently as an Assistant Professor. His research interests focus on channel coding, MIMO communications systems, cooperative communications, physical layer security, and cognitive radio systems. He has published nearly 20 research papers in international journals and conferences such as IEEE TCOM, IEEE TVT, IEEE CL, WCNC, etc. He and his coauthors have been awarded a Best Paper Award at the WCSP 2013. He received an IEEE COMMUNICATIONS LETTERS exemplary reviewer certificate for 2014.

Trung Q. Duong (S'05, M'12, SM'13) received his Ph.D. degree in Telecommunications Systems from Blekinge Institute of Technology (BTH), Sweden in 2012. Since 2013, he has joined Queen's University Belfast, UK as a Lecturer (Assistant Professor). His current research interests include physical layer security, energy-harvesting communications, cognitive relay networks. He is the author or co-author of more than 200 technical papers published in scientific journals (105 articles) and presented at international conferences.

Dr. Duong currently serves as an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE COMMUNICATIONS LETTERS, IET COMMUNICATIONS, WILEY TRANSACTIONS ON EMERGING TELECOMMUNICATIONS TECHNOLOGIES, and ELECTRONICS LETTERS. He has also served as the Guest Editor of the special issue on some major journals including IEEE JOURNAL IN SELECTED AREAS ON COMMUNICATIONS, IET COMMUNICATIONS, IEEE WIRELESS COMMUNICATIONS MAGAZINE, IEEE COMMUNICATIONS MAGAZINE, EURASIP JOURNAL ON WIRELESS COMMUNICATIONS AND NETWORKING, EURASIP JOURNAL ON ADVANCES SIGNAL PROCESSING. He was awarded the Best Paper Award at the IEEE Vehicular Technology Conference (VTC-Spring) in 2013, IEEE International Conference on Communications (ICC) 2014. He is the recipient of prestigious Royal Academy of Engineering Research Fellowship (2015-2020)

Bangning Zhang received the B.S. degree and M.S. degree in Institute of Communications Engineering (ICE), Nanjing, China, in 1984 and 1987, respectively. He is currently a Full Professor and the Head of College of Communications Engineering. He has authored and coauthored more than 80 conference and journal papers and and has been granted over 20 patents in his research areas. He has served as a reviewer for several journals in communication field. His current research interests include communication anti-jamming technologies, microwave technologies, satellite communications systems, cooperative communications and physical layer security.