Secure Multiuser Scheduling in Downlink Dual-hop Regenerative Relay Networks over Nakagami-m Fading Channels

Secure Multiuser Scheduling in Downlink Dual-hop Regenerative Relay Networks over Nakagami-m Fading Channels

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 investigate the secrecy performance of multiuser dual-hop relay networks where a base station (BS) communicates with multiple legitimate users via the assistance of a trustful regenerative relay in the presence of multiple eavesdroppers. Particularly, the maximal ratio transmission (MRT) scheme is exploited at the BS and a threshold-based multiuser scheduling scheme is employed over the legitimate users, while concerning the imperfect decoding at the regenerative relay. To evaluate the secrecy performance of the considered system, two practical situations are addressed based on the availability of eavesdropper's channel state information (CSI), i.e., Scenario I, where the eavesdropper's CSI is not available at the relay, and Scenario II, where the eavesdropper's CSI is available at the relay. For both scenarios, we further consider two eavesdropping modes, i.e., colluding eavesdropping and non-colluding eavesdropping. For Scenario I, new exact and asymptotic closed-form expressions of the secrecy outage probability (SOP) are derived. For Scenario II, we derive new exact and asymptotic closed-form expressions of ergodic secrecy rate (ESR). The asymptotic SOPs demonstrate that the secrecy diversity order is independent of the number of legitimate users N_{B} and eavesdroppers N_{E}, the number of antennas equipped at eavesdroppers A_{E} as well as fading factor of the wiretap channel m_{E}. Furthermore, we also determine the secrecy multiplexing gain and the power cost to explicitly quantify the impact of the legitimate channel and wiretap channel on ergodic secrecy rate. Our findings demonstrate that increasing the switching threshold, the number of antennas at the BS, and the number of legitimate users have a positive impact on secrecy performance.**

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

I. Introduction

SECURE information transmission has aroused extensive interest from the wireless communications community in order to prevent eavesdroppers from taking advantage of the broadcast nature of radio propagation medium to intercept confidential messages. Conventionally, various cryptographic protocols have been developed and applied in the upper layers to achieve transmission security on the assumption of an error-free link in the physical layer. Nevertheless, the limitations behind these cryptographic protocols lie in secret key distribution and management, as well as its extreme computational complexity of mathematical operations [1]. Alternatively, physical layer security (PLS) has been introduced as an attractive means to guarantee secure transmission by exploiting the distinct characteristics of wireless channels (e.g., fading or noise). The concept of PLS was first introduced in Shannon's pioneering work [2] from an information theoretic perspective. Subsequently, wiretap channel was introduced in [3], where it demonstrated that perfect security can be obtained when the quality of legitimate channel is superior to that of the wiretap channel.

In recent years, a considerable amount of research has been devoted to incorporating multiple-antenna techniques, which provide additional spatial degrees of freedom (DoF), to further improve PLS. To be specific, maximal ratio transmission (MRT) or transmit antenna selection (TAS) schemes can be exploited at the transmitter to leverage the advantages of multiple antennas [4]–[8]. The authors in [4] proposed and analyzed TAS for PLS multiple-input multiple-output (MIMO) wiretap channels with receiver combining schemes. Later on, in [5], secure transmission of multiple-input multiple-output multiple eavesdropper (MIMOME) wiretap channels was addressed by employing TAS with receive generalized selection combining over Nakagami-m channels. Besides, considering the outdated channel state information (CSI) at the transmitter, general-order TAS was proposed to enhance the secrecy performance of MIMOME [6]. Furthermore, the work in [7] studied the secrecy outage performance of multiple-input single-output (MISO) wiretap channel, where MRT scheme is adopted at the BS with outdated CSI of the main channel. More recently, regarding a wirelessly powered wiretap channel, both MRT and TAS schemes at the source have been investigated in terms of achievable secrecy outage probability and average secrecy rate in [8].

Meanwhile, cooperative relaying techniques have aroused extensive research interest due to its ability of increasing

This work was supported by the National Science Foundation of China (No. 61501507) 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. This paper was presented in part at the 16th International Symposium on Communications and Information Technologies (ISCIT2016), Qingdao, China, Sep. 2016.

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

reliability and extending range of wireless networks with low energy budget [11]. Recently, several cooperative relaying schemes, for instance, decode-and-forward (DF), amplify-and-forward (AF) and cooperative jamming (CJ), were exploited to improve the security of dual-hop cooperative relaying systems. Considering individual power constraint and no eavesdropper's CSI, a joint cooperative beamforming and jamming scheme was proposed in [12] to enhance the security of an amplify-and-forward (AF) relay network. In [13], hybrid cooperative beamforming and jamming scheme was designed to improve the PLS of two-way relay networks. For securing a decode-and-forward (DF) two-hop cooperative network, the work in [14] proposed an opportunistic relaying and artificial jamming scheme with power allocation. Moreover, the work in [15] coped with relay selection in cooperative networks with secrecy constraint, where two nodes are selected to forward source data and transmit an intentional interference signal, respectively. In [16], two novel opportunistic relay selection techniques incorporating the quality of the relay-eavesdropper links were investigated for DF cooperative relay networks. More recently, the security of cooperative single carrier systems with multiple relays and multiple destinations was examined in [17], where a two-stage relay and destination selection scheme was proposed. Besides, in [18], PLS in DF relaying cooperative wireless networks was studied, where the cooperative nodes can be assigned as either jammers or relays in an attempt to minimize the secrecy outage probability. Among the aforementioned works, high SNR assumption at the relay was considered, therefore the relay can decode the information correctly. This hypothesis of decoding without errors at the relays is not applicable throughout the SNR range. It is highlighting that the quality of the first hop also has a significant impact on the PLS of wireless relaying networks [19], [20]. In [19], the PLS of dual-hop relaying networks employing DF protocol was investigated, where only a set of relays are assumed to be able to successfully decode the message. Specifically, in a very recent work [20], the secrecy outage performance of dual-hop regenerative multi-relay systems with relay selection was investigated. In this work, the authors assumed that the relay may suffer from a wrong decision, and thus the rate is limited by the minimum quality of the dual-hop links. Additionally, in [21], outage constrained secrecy throughput maximization for DF relay networks was investigated, where two-hop signals are both taken into consideration to guarantee the transmission security.

In an effort to further enhance the secrecy performance of wireless networks, a plethora of works have suggested the idea of incorporating multiuser diversity techniques into the system. Recently, in [22], the PLS of cognitive radio networks with different multiuser scheduling schemes was investigated in terms of the achievable secrecy rate and intercept probability. Moreover, in [23], an optimal user selection scheme for multiuser relaying scheme with cooperative jamming (MUCJ) was proposed and optimized by maximizing the secrecy rate. Besides, in [24], the secrecy performance of multiuser downlink networks with the help of the artificial noise was addressed by designing an optimal power allocation to maximize the total ergodic secrecy rate of the system. Notably, the key limitations behind [22]–[24] are the high complexity and feedback load of scheduling algorithms due to the continuous estimation of the legitimate links. Specifically, in a recent work [25], a threshold-based branch selection scheme termed as switch-and-examine combining (SEC) was introduced to make a good tradeoff between secrecy performance and implementation complexity for MIMO wiretap channels. Later, a more preferable alternative namely SEC with post-examining selection (SECps) was designed to achieve a better secrecy performance in multiuser downlink wiretap networks [26], [27]. In [28], the physical layer security with TAS and threshold-based selection diversity (tSD) scheme was investigated in multiuser multi-antenna wireless networks. The key difference between SEC and SECps scheduling schemes is that SEC scheme selects any branch randomly when no acceptable one is found after examining all the legitimate links, whereas the best branch is selected in the SECps scheme, which guarantees the secrecy performance particularly for the case when the switching threshold is a high value. Noteworthy, in some practical scenarios, the legitimate users and eavesdroppers may be far away from the BS or in a deep shadow fading environment [29]–[33]. Therefore, it is of importance to seek the assistance of a trusted cooperative relay to perform the complete transmission. However, to the best of the authors' knowledge, the cooperative relay assisted multiuser multi-antenna secure transmission with SECps scheduling scheme has not been studied yet. Moreover, the impact of both antenna configurations at each terminal and the fading severity of involved channels on the secrecy performance remains unexplored. Additionally, due to the fact that the confidential messages for the legitimate users have been overheard by multiple multi-antenna eavesdroppers, and thus how the eavesdropping modes adopted at the wiretappers affect the secrecy performance of the considered network has not been reported in the literature.

Enlightened by the above observations, in this paper, we investigate secure transmission in dual-hop regenerative relaying multiuser multiple antenna networks over Nakagami-m channels. To exploit the advantages of multiple antennas, a maximal ratio transmission (MRT) scheme is adopted at the BS to improve the channel quality of the first hop. In order to reduce the feedback load and implementation complexity, the SECps scheme is utilized to select an acceptable user for transmission without continuous estimations of all the main channels' quality in the second hop. Besides, we consider a rather realistic assumption of imperfect decoding at the relays, i.e., the messages decoded at relays may be incorrect. Finally, due to the fact that malicious eavesdropping attacks significantly threaten the security of multiuser wireless communications, we take into account two different eavesdropping scenarios, i.e., the colluding and non-colluding eavesdropping modes [34], [35]. For such a practical system model, we pursue a comprehensive investigation on the secrecy performance for two different cases based on the availability of the eavesdropper's CSI, i.e., Case I, where the eavesdropper's CSI is unavailable at the relay, and Case II, where the relay has full knowledge about the eavesdropper's CSI. The main contributions of this paper are summarized as follows:

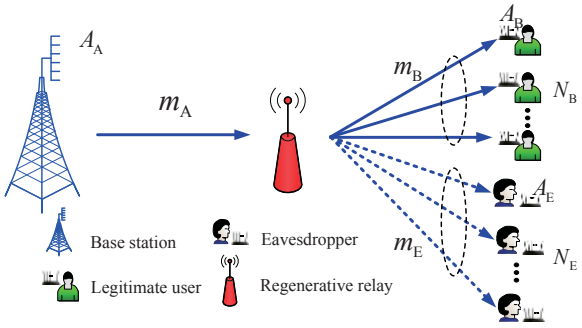

Fig. 1: System model

When the eavesdropper's CSI is unavailable at the relay:

- We derive novel exact closed-form expressions for the secrecy outage probability of both colluding and non-colluding eavesdropping scenarios with arbitrary number of legitimate users and eavesdroppers and number of antennas equipped at BS, legitimate users and eavesdroppers, fading factors of both hops as well as the switching threshold. Based on these expressions, the impact of key system parameters on the secrecy performance of dual-hop regenerative relay multiuser wiretap networks can be characterized.
- In order to achieve more insights, we derive new closed-form approximations for the secrecy outage probability in high SNR regimes for both colluding and non-colluding eavesdropping scenarios. Our results reveal that the secrecy diversity order of the considered system is determined by the worse hop and directly proportional to the number of antennas and channel fading severity associated with the corresponding legitimate link, which is independent of the number of legitimate users $N_{\rm B}$ and eavesdroppers $N_{\rm E}$, the number of antennas at eavesdroppers $A_{\rm E}$ as well as fading factor of the eavesdropper's channel $m_{\rm E}$.

When the eavesdropper's CSI is available at the relay:

- We derive novel exact closed-form expressions for the ergodic secrecy rate, which enable us to accurately examine the impact of the system parameters on the ergodic secrecy rate of the considered networks.
- We further derive new compact approximated expressions for the ergodic secrecy rate in the high SNR regimes. From the asymptotic ergodic secrecy rate, the secrecy multiplexing gain and power cost are quantized for both colluding and non-colluding eavesdropping scenarios.

Notation: The bold lower/upper case letters denote vectors/matrices. † denotes the conjugate transpose operator, $\mathbb{E}[\cdot]$ stands for the expectation operator, $\|\cdot\|_F^2$ accounts for the Frobenius norm, $\mathbf{I}_M$ denotes the $M\times M$ identity matrix, and $n!$ denotes the factorial of integer n. $\Gamma(\cdot)$ is the Gamma function, $\gamma(\cdot,\cdot)$ and $\Gamma(\cdot,\cdot)$ denote the lower and upper incomplete Gamma functions [44, Eqs. (8.350.1) and (8.350.2)], respectively.

II. System and Channel Models

As illustrated in Fig. 1, we consider a dual-hop relaying wiretap network, in which one BS (A) communicates $N_{\rm B}$ legitimate users (B) with the help of a trustful regenerative relay (R), and is overheard by $N_{\rm E}$ eavesdroppers (E). The BS, each legitimate users and each eavesdropper are equipped with $A_{\rm A}$, $A_{\rm B}$ and $A_{\rm E}$ antennas, respectively. It is highlighting that this configuration has numerous practical applications, for instance, in wireless sensor networks (WSN) where the multi-antenna nodes convey information via a mobile relay that is restricted to a single antenna due to cost and size limitations, or in device-to-device (D2D) communications scenarios where the relay assists two multi-antenna devices to exchange messages [36]–[42]. Moreover, we follow the similar scenario in [15], [16], [20], [29]–[33], where both of the direct links $\mathrm{A}\rightarrow\mathrm{B}$ and $\mathrm{A}\rightarrow\mathrm{E}$ are assumed to be nonexistent, due to the direct links may be blocked by an obstruction or suffer from severe shadow fading. By this way, the transmission in the first hop cannot be overheard by Eves.

Throughout this paper, the following assumptions are considered: 1) The CSI of the legitimate link and the eavesdropper's link is available at Bob and Eve, respectively. 2) The links $\mathrm{A}\rightarrow\mathrm{R}$, $\mathrm{R}\rightarrow\mathrm{B}$, and $\mathrm{R}\rightarrow\mathrm{E}$ are subjected to quasi-static fading link with independent non-identically distributed block Nakagami-m fading.

We assume that the relay operates in a half-duplex manner, and thus the transmission between the BS and legitimate users consists of two time slots. At the first time slot, the BS encodes the message block $\mathbf{w}$ into a codeword $\mathbf{x}=[x(1),...,x(j),...x(n)]$ with $\frac{1}{n}\sum_{k=1}^{n}\mathbb{E}\left[|x(k)|^2\right]\leq\mathcal{P}_{\rm A}$ based on capacity achieving codebook for the wiretap channel. Since the BS is equipped with multiple antennas, we adopt maximal ratio transmission scheme to maximize the channel quality of $\mathrm{A}\rightarrow\mathrm{R}$ link. As such, the instantaneous SNRs of the first hop at the relay can be expressed as

$$\gamma_{\rm AR}=\frac{\mathcal{P}_{\rm A}}{\sigma_{\rm R}^2}\|\mathbf{h}_{\rm AR}\|_F^2 \tag{1}$$

where $\mathcal{P}_{\rm A}$ denotes the transmit power at the BS, $\mathbf{h}_{\rm AR}$ represents an $A_{\rm A}\times 1$ vector for the $\mathrm{A}\rightarrow\mathrm{R}$ channel whose entries follow i.i.d. Nakagami-m fading with parameter $m_{\rm A}$, and $\sigma_{\rm R}^2$ denotes the variance of additive white Gaussian noise (AWGN) at the relay.

At the second time slot, the relay re-encodes the messages and re-transmits them to Bob. In addition, since both legitimate users and eavesdroppers are equipped with multiple antennas, maximal ratio combining (MRC) is adopted at Bob and Eve to strengthen the signal detection. Hence, the instantaneous SNR of each legitimate user and eavesdropper are, respectively, given by

$$\gamma_k^{\rm b}=\frac{\mathcal{P}_{\rm R}}{\sigma_{\rm B}^2}\|\mathbf{h}_{\rm RB}(k)\|_F^2,\quad 1\leq k\leq N_{\rm B} \tag{2}$$

and

$$\gamma_j^{\rm e}=\frac{\mathcal{P}_{\rm R}}{\sigma_{\rm E}^2}\|\mathbf{h}_{\rm RE}(j)\|_F^2,\quad 1\leq j\leq N_{\rm E} \tag{3}$$

where $\mathbf{h}_{\mathrm{RB}}(k)$ represents the channel vector between the k-th legitimate user and the relay, and $\mathbf{h}_{\mathrm{RE}}(j)$ represents the channel vector between the j-th eavesdropper and the relay, $\mathcal{P}_{\mathrm{R}}$ denotes the transmit power at the relay, σ_{B}^2 and σ_{E}^2 denote the variance of AWGN at Bob and Eve, respectively.

Different from the high SNR assumption [15], [16] or perfect decoding [17], [18] at the relay, we follow a similar consideration as in [20] and take into account the impact of the quality of the first hop on the secrecy rate. Therefore, the secrecy capacity of dual-hop DF relay system $\mathcal{C}_{\mathrm{s}}$ is given by [20]

$$\mathcal{C}_{\mathrm{s}} = \frac{1}{2}\left[\log_2\left(\frac{1+\gamma_{\mathrm{AB}}}{1+\gamma_{\mathrm{RE}}}\right)\right]^+ \tag{4}$$

where γ_{RE} and γ_{AB} denote the instantaneous SNRs of $\mathrm{R}\to\mathrm{E}$ link and $\mathrm{A}\to\mathrm{R}\to\mathrm{B}$ link, respectively. Additionally, the parameter $1/2$ accounts for the fact that the transmission process completes in two time slots and

$$[x]^+ = \max(x,0) = \begin{cases} x, & x \geq 0 \\ 0, & x < 0 \end{cases} \tag{5}$$

Considering DF scheme at the relay, we have

$$\gamma_{\mathrm{AB}} = \min(\gamma_{\mathrm{AR}}, \gamma_{\mathrm{RB}}) \tag{6}$$

where γ_{RB} denotes the instantaneous SNR of $\mathrm{R}\to\mathrm{B}$ link.

III. Secrecy Performance Analysis

In this section, we provide a comprehensive analysis on the achievable secrecy performance of the considered system with two different eavesdropper's scenarios, i.e., the colluding and non-colluding eavesdropping scenarios.

A. Preliminaries

Before delving into the detail analysis, we first present the basic principle of the multiuser scheduling in this paper, i.e., the SECps scheme [43] as follows:

To relieve the feedback load and estimation complexity, we adopt SECps scheduling scheme to select an acceptable legitimate user for data transmission. To facilitate the analysis, the SECps scheme can be equivalently viewed as selection combining (SC) scheme with an output threshold (OT-SC). Therefore, relying on the analysis of N_{B} users with OT-SC, we first characterize the CDF of γ_{RB}. On account of the events that selecting an acceptable legitimate user are mutually exclusive, thus, according to the total probability theorem, the CDF of γ_{RB} is given by

$$\begin{aligned}\mathcal{F}_{\gamma_{\mathrm{RB}}}(x) &= \Pr[\gamma_{\mathrm{RB}} < x] \\ &= \sum_{n=1}^{N_{\mathrm{B}}} \Pr\left[\gamma_{\mathrm{RB}} = \max\left\{\gamma_1^{\mathrm{b}}, \gamma_2^{\mathrm{b}}, ..., \gamma_n^{\mathrm{b}}\right\} \& \gamma_{\mathrm{RB}} < x\right]\end{aligned} \tag{7}$$

where $\gamma_{\mathrm{RB}} = \max\left\{\gamma_1^{\mathrm{b}}, \gamma_2^{\mathrm{b}}, ..., \gamma_n^{\mathrm{b}}\right\}$ indicates that an n-user SC is employed. Recalling the characterization, we find that

1) An individual user is selected if its channel quality SNR exceeds the threshold, i.e., $\gamma_{\mathrm{RB}} = \gamma_1^{\mathrm{b}} \geq \gamma_{\mathrm{T}}$.

2) An n-user SC scheme ($2 \leq n \leq N_{\mathrm{B}}-1$) is adopted for the legitimate users when the instantaneous SNR of an $n-1$ user SC is smaller than the threshold, while the instantaneous SNR of the n-user exceeds the threshold, i.e., $\gamma_{\mathrm{RB}} = \max\left\{\gamma_1^{\mathrm{b}}, \gamma_2^{\mathrm{b}}, ..., \gamma_{n-1}^{\mathrm{b}}\right\} < \gamma_{\mathrm{T}}$ and $\gamma_{\mathrm{RB}} = \max\left\{\gamma_1^{\mathrm{b}}, \gamma_2^{\mathrm{b}}, ..., \gamma_n^{\mathrm{b}}\right\} = \gamma_n^{\mathrm{b}} > \gamma_{\mathrm{T}}$.

3) An N_{B}-user SC is employed for the legitimate users if the instantaneous SNR of an $(N_{\mathrm{B}}-1)$-user SC is below the threshold, i.e., $\max\left\{\gamma_1^{\mathrm{b}}, \gamma_2^{\mathrm{b}}, ..., \gamma_{N_{\mathrm{B}}-1}^{\mathrm{b}}\right\} < \gamma_{\mathrm{T}}$.

Following the similar steps as developed in [43] and assuming an independent identically distributed Nakagami-m fading for the main channels, we have the following key results.

Lemma 1. *The CDF and PDF of γ_{RB} are, respectively, expressed as*

$$\mathcal{F}_{\gamma_{\mathrm{RB}}}(x) = \begin{cases} 1 - \sum\limits_{n=0}^{N_{\mathrm{B}}-1} \left[\mathcal{F}_{\gamma_k^{\mathrm{b}}}(\gamma_{\mathrm{T}})\right]^n \left[1 - \mathcal{F}_{\gamma_k^{\mathrm{b}}}(x)\right], & x > \gamma_{\mathrm{T}} \\ \left[\mathcal{F}_{\gamma_k^{\mathrm{b}}}(x)\right]^{N_{\mathrm{B}}}, & x < \gamma_{\mathrm{T}} \end{cases} \tag{8}$$

and

$$f_{\gamma_{\mathrm{RB}}}(x) = \begin{cases} \sum\limits_{n=0}^{N_{\mathrm{B}}-1} \left[\mathcal{F}_{\gamma_k^{\mathrm{b}}}(x)\right]^n f_{\gamma_k^{\mathrm{b}}}(x), & x > \gamma_{\mathrm{T}} \\ N_{\mathrm{B}}\left[\mathcal{F}_{\gamma_k^{\mathrm{b}}}(x)\right]^{N_{\mathrm{B}}-1} f_{\gamma_k^{\mathrm{b}}}(x), & x < \gamma_{\mathrm{T}} \end{cases} \tag{9}$$

where

$$\mathcal{F}_{\gamma_k^{\mathrm{b}}}(x) = 1 - \exp\left(-\frac{m_{\mathrm{B}} x}{\overline{\gamma}_{\mathrm{B}}}\right) \sum_{k=0}^{A_{\mathrm{B}} m_{\mathrm{B}}} \frac{(x)^k}{k!} \left(\frac{m_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}}\right)^k \tag{10}$$

and

$$f_{\gamma_k^{\mathrm{b}}}(x) = \left(\frac{m_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}}\right)^{A_{\mathrm{B}} m_{\mathrm{B}}} \frac{x^{A_{\mathrm{B}} m_{\mathrm{B}} - 1}}{\Gamma(A_{\mathrm{B}} m_{\mathrm{B}})} \exp\left(-\frac{m_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}} x\right) \tag{11}$$

represent the CDF and PDF of γ_k^{b}, respectively, $\overline{\gamma}_{\mathrm{B}} = \mathbb{E}\left[\gamma_k^{\mathrm{b}}\right]$ denotes the average SNR of each legitimate channel, m_{B} is the Nakagami-m fading factor of legitimate channel.

Since the MRT scheme is adopted for the $\mathrm{A}\to\mathrm{R}$ link, we have the following key Lemma.

Lemma 2. *The exact CDF and PDF of γ_{AR} are, respectively, provided by*

$$\mathcal{F}_{\gamma_{\mathrm{AR}}}(x) = 1 - \exp\left(-\frac{m_{\mathrm{A}}}{\overline{\gamma}_{\mathrm{A}}} x\right) \sum_{n=0}^{m_{\mathrm{A}} A_{\mathrm{A}} - 1} \frac{x^n}{n!} \left(\frac{m_{\mathrm{A}}}{\overline{\gamma}_{\mathrm{A}}}\right)^n \tag{12}$$

and

$$f_{\gamma_{\mathrm{AR}}}(x) = \left(\frac{m_{\mathrm{A}}}{\overline{\gamma}_{\mathrm{A}}}\right)^{A_{\mathrm{A}} m_{\mathrm{A}}} \frac{x^{A_{\mathrm{A}} m_{\mathrm{A}} - 1}}{\Gamma(A_{\mathrm{A}} m_{\mathrm{A}})} \exp\left(-\frac{m_{\mathrm{A}}}{\overline{\gamma}_{\mathrm{A}}} x\right) \tag{13}$$

where $\overline{\gamma}_{\mathrm{A}} = \mathbb{E}[\gamma_{\mathrm{AR}}]$.

On the other hand, we consider two eavesdropping modes in this paper, i.e., colluding and non-colluding eavesdropping [34], [35]. For non-colluding eavesdropping, the eavesdroppers overhear the confidential message independently without cooperative processing. In other words, secure transmission of main channel can be achieved under the condition that the quality of legitimate channel is better than that of any wiretapper's channel. As such, the end-to-end instantaneous SNR of $\mathrm{R}\to\mathrm{E}$ link is determined by

$$\gamma_{\mathrm{RE}}^{(\mathrm{ncol})} = \max_{1 \leq j \leq N_{\mathrm{E}}} \gamma_j^{\mathrm{e}} \tag{14}$$

While for colluding eavesdropping, the eavesdroppers exchange their observations at a centralized processing module to jointly decode the message, and thus the end-to-end instantaneous SNR of $\mathrm{R} \to \mathrm{E}$ link is given by

$$\gamma_{\mathrm{RE}}^{(\mathrm{col})} = \sum_{j=1}^{N_{\mathrm{E}}} \gamma_j^{\mathrm{e}} \tag{15}$$

To do that, we have the following lemmas.

Lemma 3. *For the colluding eavesdropping scenario, the exact CDF and PDF of $\gamma_{\mathrm{RE}}^{(\mathrm{col})}$ are, respectively, given by*

$$\mathcal{F}_{\gamma_{\mathrm{RE}}}^{(\mathrm{col})}(x) = 1 - \exp\left(-\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}x\right) \sum_{n=0}^{N_{\mathrm{E}} m_{\mathrm{E}} A_{\mathrm{E}} - 1} \frac{x^n}{n!} \left(\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right)^n \tag{16}$$

and

$$f_{\gamma_{\mathrm{RE}}}^{(\mathrm{col})}(x) = \left(\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right)^{N_{\mathrm{E}} A_{\mathrm{E}} m_{\mathrm{E}}} \frac{x^{N_{\mathrm{E}} A_{\mathrm{E}} m_{\mathrm{E}} - 1}}{\Gamma(N_{\mathrm{E}} A_{\mathrm{E}} m_{\mathrm{E}})} \exp\left(-\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}x\right) \tag{17}$$

Lemma 4. *For the non-colluding eavesdropping scenario, the exact CDF and PDF of $\gamma_{\mathrm{RE}}^{(\mathrm{ncol})}$ are, respectively, given by*

$$\mathcal{F}_{\gamma_{\mathrm{RE}}}^{(\mathrm{ncol})}(x) = \sum_{v=0}^{N_{\mathrm{E}}} \binom{N_{\mathrm{E}}}{v} (-1)^v \exp\left(-\frac{m_{\mathrm{E}} v}{\overline{\gamma}_{\mathrm{E}}}x\right) \times \Theta_{\mathrm{E},v} \left(\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}x\right)^{\phi_{\mathrm{E}}} \tag{18}$$

and

$$f_{\gamma_{\mathrm{RE}}}^{(\mathrm{ncol})}(x) = \frac{N_{\mathrm{E}}}{\Gamma(A_{\mathrm{E}} m_{\mathrm{E}})} \sum_{v=0}^{N_{\mathrm{E}}-1} \binom{N_{\mathrm{E}} - 1}{v} (-1)^v \Theta_{\mathrm{E},v} \times \left(\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right)^{\phi_{\mathrm{E}} + A_{\mathrm{E}} m_{\mathrm{E}}} x^{\phi_{\mathrm{E}} + A_{\mathrm{E}} m_{\mathrm{E}} - 1} \exp\left(-\frac{m_{\mathrm{E}}(v+1)}{\overline{\gamma}_{\mathrm{E}}}x\right) \tag{19}$$

where

$$\Theta_{\mathrm{E},v} = \sum_{n_1=0}^{v} \sum_{n_2=0}^{n_1} \cdots \sum_{n_{m_{\mathrm{E}} A_{\mathrm{E}} - 1}=0}^{n_{m_{\mathrm{E}} A_{\mathrm{E}} - 2}} \frac{v!}{n_{m_{\mathrm{E}} A_{\mathrm{E}} - 1}!} \times \prod_{t=1}^{m_{\mathrm{E}} A_{\mathrm{E}} - 1} \frac{(t!)^{n_{t+1} - n_t}}{(n_{t-1} - n_t)!} \tag{20}$$

with $n_0 = v, n_{m_{\mathrm{E}}} = 0, \phi_{\mathrm{E}} = \sum_{q=1}^{m_{\mathrm{E}} A_{\mathrm{E}} - 1} n_q$, $\overline{\gamma}_{\mathrm{E}} = \mathbb{E}\left[\gamma_j^{\mathrm{e}}\right]$ denotes the average SNR of each wiretap channel.

Proof: The proof can be found in [6]. ∎

B. Scenario I: Eavesdropper's CSI is unavailable at the relay

In this subsection, we focus on the scenario where the relay does not have knowledge of the eavesdropper's CSI and therefore the instantaneous capacity of the wiretap channel (i.e., $\mathcal{C}_{\mathrm{E}} = \log_2(1 + \gamma_{\mathrm{E}})$) is not available at the relay. Under this condition, the relay supposes the instantaneous capacity of the eavesdropper's channel as $\tilde{\mathcal{C}}_{\mathrm{E}} = \mathcal{C}_{\mathrm{B}} - \mathcal{R}_{\mathrm{s}}$ to perform secure data transmission [1], where $\mathcal{R}_{\mathrm{s}}$ is a constant secrecy rate selected by the BS and relay. If $\mathcal{C}_{\mathrm{E}} < \tilde{\mathcal{C}}_{\mathrm{E}}$, i.e., the eavesdropper's channel is worse than the estimation, the perfect secrecy can be achieved. Otherwise, if $\mathcal{C}_{\mathrm{E}} > \tilde{\mathcal{C}}_{\mathrm{E}}$, the eavesdropper is capable of overhearing the confidential message and the secrecy is compromised. In doing so, the secrecy outage probability and non-zero secrecy capacity are taken into consideration as primary and well-accepted metrics to evaluate the secrecy performance of the considered system.

1) Secrecy outage probability: The secrecy outage probability is defined as the probability that the achievable secrecy capacity $\mathcal{C}_{\mathrm{s}}$ is lower than a predefined secrecy transmission rate $\mathcal{R}_{\mathrm{s}}$. Mathematically, the secrecy outage probability is formulated as $\mathcal{P}_{\mathrm{out}}(\mathcal{R}_{\mathrm{s}}) = \Pr(\mathcal{C}_{\mathrm{s}} < \mathcal{R}_{\mathrm{s}})$. Following the similar procedures developed in [20], the secrecy outage probability is re-expressed as

$$\begin{aligned} \mathcal{P}_{\mathrm{out}}^{(\kappa)}(\mathcal{R}_{\mathrm{s}}) &= \Pr\left[\min(\gamma_{\mathrm{AR}}, \gamma_{\mathrm{RB}}) < \lambda\right] \\ &= \int_0^{\infty} \Big[\mathcal{F}_{\gamma_{\mathrm{AR}}}(\lambda) + \mathcal{F}_{\gamma_{\mathrm{RB}}}(\lambda) - \mathcal{F}_{\gamma_{\mathrm{AR}}}(\lambda) \\ &\qquad \times \mathcal{F}_{\gamma_{\mathrm{RB}}}(\lambda)\Big] f_{\gamma_{\mathrm{RE}}}^{(\kappa)}(x) dx \end{aligned} \tag{21}$$

where $\kappa \in \{\mathrm{col}, \mathrm{ncol}\}$, $\lambda = \rho(1+x) - 1$ and $\rho = 2^{2\mathcal{R}_{\mathrm{s}}}$. Now, an exact closed-form expression for (21) can be derived in the following theorem.

Theorem 1. *The secrecy outage probability of the considered system is derived as*

$$\mathcal{P}_{\mathrm{out}}^{(\kappa)}(\mathcal{R}_{\mathrm{s}}) = \mathcal{I}_1^{(\kappa)} + \mathcal{I}_2^{(\kappa)} + \mathcal{I}_3^{(\kappa)} \tag{22}$$

where $\kappa \in \{\mathrm{col}, \mathrm{ncol}\}$. For colluding eavesdropping scenario, $\mathcal{I}_1^{(\kappa)}$, $\mathcal{I}_2^{(\kappa)}$ and $\mathcal{I}_3^{(\kappa)}$ are presented in (23)*,* (25) *and* (27)*, respectively, while for non-colluding eavesdropping scenario, $\mathcal{I}_1^{(\kappa)}$, $\mathcal{I}_2^{(\kappa)}$ and $\mathcal{I}_3^{(\kappa)}$ are provided by* (24)*,* (26) *and* (28)*, respectively.*

Proof: See Appendix A. ∎

We remark that the secrecy outage probability of the considered system is separated by three parts for tractable reasons, i.e., $\mathcal{I}_1^{(\kappa)}, \mathcal{I}_2^{(\kappa)}$ and $\mathcal{I}_3^{(\kappa)}$, in which $\mathcal{I}_1^{(\kappa)}$ represents the joint impacts of the parameters related to the $\mathrm{A} \to \mathrm{R}$ and $\mathrm{R} \to \mathrm{E}$ links, $\mathcal{I}_2^{(\kappa)}$ reflects the joint impacts of the parameters related to the $\mathrm{R} \to \mathrm{B}$ and $\mathrm{R} \to \mathrm{E}$ links, and $\mathcal{I}_3^{(\kappa)}$ reflects the joint impacts of the parameters related to the $\mathrm{A} \to \mathrm{R}$, $\mathrm{R} \to \mathrm{B}$ and $\mathrm{R} \to \mathrm{E}$ links on the secrecy performance. Thus, based on the derived closed-form secrecy outage probability expressions, we can readily evaluate the secrecy performance of the considered system.

In addition, we also find that the $\mathrm{A} \to \mathrm{R}$ link is involved in the secrecy outage performance although the $\mathrm{A} \to \mathrm{E}$ link is assumed to be unavailable. This is due to the fact that the imperfect decoding assumption is adopted at the relay, and therefore the transmission rate is limited by the minimum quality of the dual-hop links.

Please note, other secrecy performance metrics can be easily calculated from (22), for instance, the probability of positive secrecy can be evaluated by setting $\mathcal{R}_{\mathrm{s}} = 0$ into (22), and therefore we have the following key result.

$$\mathcal{I}_1^{(\mathrm{col})} = 1 - \frac{\left(\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right)^{N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}}}{\Gamma(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}})} \widetilde{\sum}_{\mathrm{A},k_1} \Gamma\left(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}+k_1\right)\left(\mathcal{S}_{2\mathrm{ae}}\right)^{-(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}+k_1)} \tag{23}$$

$$\begin{aligned}\mathcal{I}_1^{(\mathrm{ncol})} = {} & \frac{N_{\mathrm{E}}}{\Gamma(A_{\mathrm{E}}m_{\mathrm{E}})} \sum_{v=0}^{N_{\mathrm{E}}-1} \binom{N_{\mathrm{E}}-1}{v}(-1)^v \Theta_{\mathrm{E},v}\left(\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right)^{\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}} \Bigg\{\Gamma\left(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}\right)\left(\frac{m_{\mathrm{E}}(v+1)}{\overline{\gamma}_{\mathrm{E}}}\right)^{-(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}})} - \widetilde{\sum}_{\mathrm{A},k_1} \\ & \times\Gamma\left(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}+k_1\right)\left(\mathcal{S}_{2\mathrm{aev}}\right)^{-(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}+k_1)} \Bigg\}\end{aligned} \tag{24}$$

$$\begin{aligned}\mathcal{I}_{2\mathrm{a}}^{(\mathrm{col})} = {} & \frac{\left(\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right)^{N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}}}{\Gamma(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}})} \Bigg[\sum_{l=0}^{N_{\mathrm{B}}} \binom{N_{\mathrm{B}}}{l}(-1)^l \exp\left(-\frac{m_{\mathrm{B}}(\rho-1)l}{\overline{\gamma}_{\mathrm{B}}}\right)\Theta_{\mathrm{B},l}\left(\frac{m_{\mathrm{B}}(\rho-1)}{\overline{\gamma}_{\mathrm{B}}}\right)^{\phi_{\mathrm{B}}} \sum_{s=0}^{\phi_{\mathrm{B}}} \binom{\phi_{\mathrm{B}}}{s}\left(\frac{\rho}{\rho-1}\right)^s \left(\mathcal{S}_{0\mathrm{be}}\right)^{-(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}+s)} \\ & \times\gamma\left(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}+s, \mathcal{S}_{0\mathrm{be}}\aleph_{\gamma_{\mathrm{T}}}\right) + \left(\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right)^{-N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}} \Gamma\left(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}, \frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\aleph_{\gamma_{\mathrm{T}}}\right) - \widetilde{\sum}_{\mathrm{B},n_1}\left(\mathcal{S}_{2\mathrm{be}}\right)^{-(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}+n_1)} \\ & \times\Gamma\left(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}+n_1, \mathcal{S}_{2\mathrm{be}}\aleph_{\gamma_{\mathrm{T}}}\right)\Bigg]\end{aligned} \tag{25a}$$

$$\mathcal{I}_{2\mathrm{b}}^{(\mathrm{col})} = 1 - \frac{\left(\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right)^{N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}}}{\Gamma(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}})} \widetilde{\sum}_{\mathrm{B},n_1} \Gamma\left(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}+n_1\right)\left(\mathcal{S}_{2\mathrm{be}}\right)^{-(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}+n_1)} \tag{25b}$$

$$\begin{aligned}\mathcal{I}_{2\mathrm{a}}^{(\mathrm{ncol})} = {} & \frac{N_{\mathrm{E}}}{\Gamma(A_{\mathrm{E}}m_{\mathrm{E}})} \sum_{v=0}^{N_{\mathrm{E}}-1} \binom{N_{\mathrm{E}}-1}{v}(-1)^v \Theta_{\mathrm{E},v}\left(\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right)^{\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}} \Bigg[\sum_{l=0}^{N_{\mathrm{B}}} \binom{N_{\mathrm{B}}}{l}(-1)^l \exp\left(-\frac{m_{\mathrm{B}}(\rho-1)l}{\overline{\gamma}_{\mathrm{B}}}\right)\Theta_{\mathrm{B},l}\left(\frac{m_{\mathrm{B}}(\rho-1)}{\overline{\gamma}_{\mathrm{B}}}\right)^{\phi_{\mathrm{B}}} \\ & \times \sum_{s=0}^{\phi_{\mathrm{B}}} \binom{\phi_{\mathrm{B}}}{s}\left(\mathcal{S}_{0\mathrm{bev}}\right)^{-(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}+s)} \gamma\left(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}+s, \mathcal{S}_{0\mathrm{bev}}\aleph_{\gamma_{\mathrm{T}}}\right)\left(\frac{\rho}{\rho-1}\right)^s + \Gamma\left(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}, \left(\frac{m_{\mathrm{E}}(v+1)}{\overline{\gamma}_{\mathrm{E}}}\right)\aleph_{\gamma_{\mathrm{T}}}\right) \\ & \times\left(\frac{m_{\mathrm{E}}(v+1)}{\overline{\gamma}_{\mathrm{E}}}\right)^{-(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}})} - \widetilde{\sum}_{\mathrm{B},n_1}\left(\mathcal{S}_{2\mathrm{bev}}\right)^{-(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}+n_1)}\ \Gamma\left(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}+n_1, \mathcal{S}_{2\mathrm{bev}}\aleph_{\gamma_{\mathrm{T}}}\right)\Bigg]\end{aligned} \tag{26a}$$

$$\begin{aligned}\mathcal{I}_{2\mathrm{b}}^{(\mathrm{ncol})} = {} & \frac{N_{\mathrm{E}}}{\Gamma(A_{\mathrm{E}}m_{\mathrm{E}})} \sum_{v=0}^{N_{\mathrm{E}}-1} \binom{N_{\mathrm{E}}-1}{v}(-1)^v \Theta_{\mathrm{E},v}\left(\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right)^{\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}} \Gamma\left(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}\right)\Bigg[\left(\frac{m_{\mathrm{E}}(v+1)}{\overline{\gamma}_{\mathrm{E}}}\right)^{-(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}})} - \widetilde{\sum}_{\mathrm{B},n_1} \\ & \times\Gamma\left(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}+n_1\right)\left(\mathcal{S}_{2\mathrm{bev}}\right)^{-(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}+n_1)}\Bigg]\end{aligned} \tag{26b}$$

$$\begin{aligned}\mathcal{I}_{3\mathrm{a}}^{(\mathrm{col})} = {} & -\frac{\left(\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right)^{N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}}}{\Gamma(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}})} \Bigg\{\sum_{l=0}^{N_{\mathrm{B}}} \binom{N_{\mathrm{B}}}{l}(-1)^l \exp\left(-\frac{m_{\mathrm{B}}(\rho-1)l}{\overline{\gamma}_{\mathrm{B}}}\right)\Theta_{\mathrm{B},l}\left(\frac{m_{\mathrm{B}}(\rho-1)}{\overline{\gamma}_{\mathrm{B}}}\right)^{\phi_{\mathrm{B}}} \sum_{s=0}^{\phi_{\mathrm{B}}} \binom{\phi_{\mathrm{B}}}{s}\left(\frac{\rho}{\rho-1}\right)^s \Bigg[\left(\mathcal{S}_{0\mathrm{be}}\right)^{-(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}+s)} \\ & \times\gamma\left(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}+s, \mathcal{S}_{0\mathrm{be}}\aleph_{\gamma_{\mathrm{T}}}\right) - \widetilde{\sum}_{\mathrm{A},k_1}\left(\mathcal{S}_{0\mathrm{abe}}\right)^{(-N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}+k_1+s)}\gamma\left(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}+k_1+s, \mathcal{S}_{0\mathrm{abe}}\aleph_{\gamma_{\mathrm{T}}}\right)\Bigg] \\ & +\left(\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right)^{-N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}} \Gamma\left(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}, \frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\aleph_{\gamma_{\mathrm{T}}}\right) - \widetilde{\sum}_{\mathrm{A},k_1}\Gamma\left(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}+k_1, \mathcal{S}_{2\mathrm{ae}}\aleph_{\gamma_{\mathrm{T}}}\right)\left(\mathcal{S}_{2\mathrm{ae}}\right)^{-(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}+k_1)} \\ & -\widetilde{\sum}_{\mathrm{B},n_1}\Bigg[\left(\mathcal{S}_{2\mathrm{be}}\right)^{-(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}+n_1)}\Gamma\left(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}+n_1, \mathcal{S}_{2\mathrm{be}}\aleph_{\gamma_{\mathrm{T}}}\right) - \widetilde{\sum}_{\mathrm{A},k_1}\Gamma\left(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}+k_1+n_1, \mathcal{S}_{2\mathrm{abe}}\aleph_{\gamma_{\mathrm{T}}}\right) \\ & \times\left(\mathcal{S}_{2\mathrm{abe}}\right)^{-(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}+k_1+n_1)}\Bigg]\Bigg\}\end{aligned} \tag{27a}$$

$$\begin{aligned}\mathcal{I}_{3\mathrm{b}}^{(\mathrm{col})} = {} & -\frac{\left(\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right)^{N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}}}{\Gamma(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}})} \Bigg\{\Gamma\left(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}\right)\left(\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right)^{-N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}} - \widetilde{\sum}_{\mathrm{A},k_1}\Bigg[\Gamma\left(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}+k_1\right)\left(\mathcal{S}_{2\mathrm{ae}}\right)^{-(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}+k_1)} \\ & -\widetilde{\sum}_{\mathrm{B},n_1}\Gamma\left(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}+n_1+k_1\right)\left(\mathcal{S}_{2\mathrm{abe}}\right)^{-(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}+n_1+k_1)}\Bigg] - \widetilde{\sum}_{\mathrm{B},n_1}\Gamma\left(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}+n_1\right)\mathcal{S}_{2\mathrm{be}}{}^{-(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}+n_1)}\Bigg\}\end{aligned} \tag{27b}$$

Corollary 1. *The probability of positive secrecy of the considered system is quantified by* $\Pr^{(\kappa)}\left(\mathcal{C}_{\mathrm{s}}>0\right) = 1-\mathcal{P}_{\mathrm{out}}^{(\kappa)}(0)$,

$$\mathcal{I}_{3\mathrm{a}}^{(\mathrm{ncol})} = -\tfrac{N_{\mathrm{E}}}{\Gamma(A_{\mathrm{E}}m_{\mathrm{E}})}\sum_{v=0}^{N_{\mathrm{E}}-1}\binom{N_{\mathrm{E}}-1}{v}(-1)^{v}\Theta_{\mathrm{E},v}\Big(\tfrac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\Big)^{\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}}\Bigg\{\sum_{l=0}^{N_{\mathrm{B}}}\binom{N_{\mathrm{B}}}{l}(-1)^{l}\exp\Big(-\tfrac{m_{\mathrm{B}}(\rho-1)l}{\overline{\gamma}_{\mathrm{B}}}\Big)\Theta_{\mathrm{B},l}\Big(\tfrac{m_{\mathrm{B}}(\rho-1)}{\overline{\gamma}_{\mathrm{B}}}\Big)^{\phi_{\mathrm{B}}}$$
$$\times\sum_{s=0}^{\phi_{\mathrm{B}}}\binom{\phi_{\mathrm{B}}}{s}\Big(\tfrac{\rho}{\rho-1}\Big)^{s}\Bigg[(\mathcal{S}_{0\mathrm{bev}})^{-(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}+s)}\gamma\left(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}+s,\mathcal{S}_{0\mathrm{bev}}\aleph_{\gamma_{\mathrm{T}}}\right)-\widetilde{\sum}_{\mathrm{A},k_1}(\mathcal{S}_{0\mathrm{abev}})^{-(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}+k_1+s)}$$
$$\times\,\gamma\left(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}+k_1+s,\mathcal{S}_{0\mathrm{abev}}\aleph_{\gamma_{\mathrm{T}}}\right)\Bigg]+\Bigg[\Gamma\left(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}},\Big(\tfrac{m_{\mathrm{E}}(v+1)}{\overline{\gamma}_{\mathrm{E}}}\Big)\aleph_{\gamma_{\mathrm{T}}}\right)\Big(\tfrac{m_{\mathrm{E}}(v+1)}{\overline{\gamma}_{\mathrm{E}}}\Big)^{-(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}})} \tag{28a}$$
$$-\widetilde{\sum}_{\mathrm{A},k_1}\Gamma\left(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}+k_1,\ \mathcal{S}_{2\mathrm{aev}}\aleph_{\gamma_{\mathrm{T}}}\right)(\mathcal{S}_{2\mathrm{aev}})^{-(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}+k_1)}-\widetilde{\sum}_{\mathrm{B},n_1}(\mathcal{S}_{2\mathrm{bev}})^{-(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}+n_1)}$$
$$\times\Gamma\left(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}+n_1,\mathcal{S}_{2\mathrm{bev}}\aleph_{\gamma_{\mathrm{T}}}\right)+\widetilde{\sum}_{\mathrm{A},k_1}\widetilde{\sum}_{\mathrm{B},n_1}(\mathcal{S}_{2\mathrm{abev}})^{-(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}+k_1+n_1)}\,\Gamma\left(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}+k_1+n_1,\mathcal{S}_{2\mathrm{abev}}\aleph_{\gamma_{\mathrm{T}}}\right)\Bigg]\Bigg\}$$

$$\mathcal{I}_{3\mathrm{b}}^{(\mathrm{ncol})} = -\tfrac{N_{\mathrm{E}}}{\Gamma(A_{\mathrm{E}}m_{\mathrm{E}})}\sum_{v=0}^{N_{\mathrm{E}}-1}\binom{N_{\mathrm{E}}-1}{v}(-1)^{v}\Theta_{\mathrm{E},v}\Big(\tfrac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\Big)^{\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}}\Bigg\{\Gamma\left(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}\right)\Big(\tfrac{m_{\mathrm{E}}(v+1)}{\overline{\gamma}_{\mathrm{E}}}\Big)^{-(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}})}-\widetilde{\sum}_{\mathrm{A},k_1}$$
$$\times\Gamma\left(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}+k_1\right)(\mathcal{S}_{2\mathrm{aev}})^{-(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}+k_1)}-\widetilde{\sum}_{\mathrm{B},n_1}\Bigg[(\mathcal{S}_{2\mathrm{bev}})^{-(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}+n_1)}\Gamma\left(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}+n_1\right)-\widetilde{\sum}_{\mathrm{A},k_1} \tag{28b}$$
$$\times\Gamma\left(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}+k_1+n_1\right)(\mathcal{S}_{2\mathrm{abev}})^{-(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}+k_1+n_1)}\Bigg]\Bigg\}$$

where $\kappa\in\{\mathrm{col},\mathrm{ncol}\}$.

2) Asymptotic secrecy outage probability: Though the exact closed-form expression for secrecy outage probability of multiuser regenerative relay systems has been derived, it is not easy to explore the impact of key system parameters on the secrecy performance from (22). Thus, in order to gain more insights, we turn our attention to the asymptotic secrecy outage probability in high SNR regimes, i.e., $\overline{\gamma}_{\mathrm{B}}\to\infty$. Unless otherwise specified, we assume that the average SNR of the $\mathrm{A}\to\mathrm{R}$ link is equal to that of $\mathrm{R}\to\mathrm{B}$ link, i.e., $\overline{\gamma}_{\mathrm{A}}=\overline{\gamma}_{\mathrm{B}}$, and we have the following important result.

Corollary 2. *Based on* (22)*, the asymptotic secrecy outage probability of the considered system in high SNR regimes is given by*

$$\mathcal{P}_{\mathrm{out}}^{(\kappa)}(\mathcal{R}_{\mathrm{s}})=\Big(\Xi^{(\kappa)}\cdot\overline{\gamma}_{\mathrm{B}}\Big)^{-\Psi}+\mathcal{O}\left(\overline{\gamma}_{\mathrm{B}}{}^{-\Psi}\right) \tag{29}$$

where the secrecy diversity gain Ψ *is*

$$\Psi=\begin{cases}m_{\mathrm{B}}A_{\mathrm{B}}, & m_{\mathrm{A}}A_{\mathrm{A}}=m_{\mathrm{B}}A_{\mathrm{B}}\\ m_{\mathrm{B}}A_{\mathrm{B}}, & m_{\mathrm{A}}A_{\mathrm{A}}>m_{\mathrm{B}}A_{\mathrm{B}}\\ m_{\mathrm{A}}A_{\mathrm{A}}, & m_{\mathrm{A}}A_{\mathrm{A}}<m_{\mathrm{B}}A_{\mathrm{B}}\end{cases} \tag{30}$$

and the secrecy coding gain $\Xi^{(\kappa)}$ *is given by*

$$\Xi^{(\kappa)}=\begin{cases}\Big(\Lambda_1^{(\kappa)}+\Lambda_{\mathrm{g}}^{(\kappa)}\Big)^{-1}, & m_{\mathrm{A}}A_{\mathrm{A}}=m_{\mathrm{B}}A_{\mathrm{B}}\ \&\ \aleph_{\gamma_{\mathrm{T}}}\geq 0\\ \Big(\Lambda_{\mathrm{g}}^{(\kappa)}\Big)^{-1}, & m_{\mathrm{A}}A_{\mathrm{A}}>m_{\mathrm{B}}A_{\mathrm{B}}\ \&\ \aleph_{\gamma_{\mathrm{T}}}\geq 0\\ \Big(\Lambda_1^{(\kappa)}\Big)^{-1}, & m_{\mathrm{A}}A_{\mathrm{A}}<m_{\mathrm{B}}A_{\mathrm{B}}\ \&\ \aleph_{\gamma_{\mathrm{T}}}\geq 0\\ \Big(\Lambda_1^{(\kappa)}+\Lambda_{\mathrm{s}}^{(\kappa)}\Big)^{-1}, & m_{\mathrm{A}}A_{\mathrm{A}}=m_{\mathrm{B}}A_{\mathrm{B}}\ \&\ \aleph_{\gamma_{\mathrm{T}}}<0\\ \Big(\Lambda_{\mathrm{s}}^{(\kappa)}\Big)^{-1}, & m_{\mathrm{A}}A_{\mathrm{A}}>m_{\mathrm{B}}A_{\mathrm{B}}\ \&\ \aleph_{\gamma_{\mathrm{T}}}<0\\ \Big(\Lambda_1^{(\kappa)}\Big)^{-1}, & m_{\mathrm{A}}A_{\mathrm{A}}<m_{\mathrm{B}}A_{\mathrm{B}}\ \&\ \aleph_{\gamma_{\mathrm{T}}}<0\end{cases} \tag{31}$$

where $\kappa\in\{\mathrm{col},\mathrm{ncol}\}$*,* $\mathcal{O}(\cdot)$ *denotes the higher order term,* $\Lambda_1^{(\kappa)}$ *is provided as* (32) *and* (33)*,* $\Lambda_{\mathrm{g}}^{(\kappa)}$ *is provided as* (34) *and* (35)*,* $\Lambda_{\mathrm{s}}^{(\kappa)}$ *is provided as* (36) *and* (37)*, respectively.*

Proof: See Appendix B. ∎

According to the asymptotic expressions of secrecy outage probability in (29), we find that the secrecy diversity order is determined by the worse hop and directly proportional to the number of antennas and channel fading severity associated with the $\mathrm{A}\to\mathrm{R}$ link or $\mathrm{R}\to\mathrm{B}$ link. For instance, if $m_{\mathrm{A}}A_{\mathrm{A}}\geq m_{\mathrm{B}}A_{\mathrm{B}}$, then the secrecy diversity order is equivalent to $m_{\mathrm{B}}A_{\mathrm{B}}$, and vice versa. We remark that the secrecy diversity order is independent of the number of legitimate users N_{B} and eavesdroppers N_{E}, the number of antennas at eavesdroppers A_{E}, the average SNR of eavesdropper's channel $\overline{\gamma}_{\mathrm{E}}$ and the corresponding fading factor m_{E}.

On the other hand, the impacts of the involved parameters on the secrecy outage performance are characterized by the secrecy coding gain in (31), respectively. In addition, we also remark that, the secrecy diversity order remains the same, while they differ in the secrecy coding gain.

C. Scenario II: Eavesdropper's CSI is available at the relay

In this subsection, we focus on the scenario that the relay has the eavesdropper's CSI. Under this condition, the transmitter has an ability to change the coding rate adaptively depending on both CSIs of the legitimate link and eavesdropper's link to achieve the perfect security. Thus, any ergodic transmission rate below the ergodic secrecy rate of the channel is achievable by principle [1]. As such, different from Scenario I, the ergodic secrecy rate is taken here as the principle secrecy performance metric.

$$\Lambda_1^{(\mathrm{col})} = \frac{1}{\Gamma(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}})}\frac{{m_{\mathrm{A}}}^{m_{\mathrm{A}}A_{\mathrm{A}}}}{(m_{\mathrm{A}}A_{\mathrm{A}})!}(\rho-1)^{m_{\mathrm{A}}A_{\mathrm{A}}}\sum_{n=0}^{m_{\mathrm{A}}A_{\mathrm{A}}}\binom{m_{\mathrm{A}}A_{\mathrm{A}}}{n}\left(\frac{\rho}{\rho-1}\right)^{n}\left(\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right)^{-n}\Gamma\left(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}+n\right) \tag{32}$$

$$\Lambda_1^{(\mathrm{ncol})} = \frac{{m_{\mathrm{A}}}^{m_{\mathrm{A}}A_{\mathrm{A}}}}{(m_{\mathrm{A}}A_{\mathrm{A}})!}\frac{N_{\mathrm{E}}}{\Gamma(A_{\mathrm{E}}m_{\mathrm{E}})}\sum_{v=0}^{N_{\mathrm{E}}-1}\binom{N_{\mathrm{E}}-1}{v}(-1)^{v}\Theta_{\mathrm{E},v}\left(\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right)^{\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}}(\rho-1)^{m_{\mathrm{A}}A_{\mathrm{A}}}\sum_{k=0}^{m_{\mathrm{A}}A_{\mathrm{A}}}\binom{m_{\mathrm{A}}A_{\mathrm{A}}}{k}\left(\frac{\rho}{\rho-1}\right)^{k} \times\left(\frac{m_{\mathrm{E}}(v+1)}{\overline{\gamma}_{\mathrm{E}}}\right)^{-(\phi_{\mathrm{E}}+k+A_{\mathrm{E}}m_{\mathrm{E}})}\Gamma\left(\phi_{\mathrm{E}}+k+A_{\mathrm{E}}m_{\mathrm{E}}\right) \tag{33}$$

$$\Lambda_{\mathrm{g}}^{(\mathrm{col})} = \frac{1}{\Gamma(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}})}\frac{{m_{\mathrm{B}}}^{m_{\mathrm{B}}A_{\mathrm{B}}}}{(m_{\mathrm{B}}A_{\mathrm{B}})!}(\gamma_{\mathrm{T}})^{m_{\mathrm{B}}A_{\mathrm{B}}}\left\{-\Gamma\left(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}},\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\aleph_{\gamma_{\mathrm{T}}}\right)+(\rho-1)^{m_{\mathrm{B}}A_{\mathrm{B}}}\sum_{n=0}^{m_{\mathrm{B}}A_{\mathrm{B}}}\binom{m_{\mathrm{B}}A_{\mathrm{B}}}{n}\left(\frac{\rho}{\rho-1}\right)^{n} \times\left(\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right)^{-n}\Gamma\left(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}+n,\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\aleph_{\gamma_{\mathrm{T}}}\right)\right\} \tag{34}$$

$$\Lambda_{\mathrm{g}}^{(\mathrm{ncol})} = \frac{N_{\mathrm{E}}}{\Gamma(A_{\mathrm{E}}m_{\mathrm{E}})}\frac{{m_{\mathrm{B}}}^{m_{\mathrm{B}}A_{\mathrm{B}}}}{(m_{\mathrm{B}}A_{\mathrm{B}})!}\sum_{v=0}^{N_{\mathrm{E}}-1}\binom{N_{\mathrm{E}}-1}{v}(-1)^{v}\Theta_{\mathrm{E},v}(v+1)^{-(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}})}\left\{-(\gamma_{\mathrm{T}})^{m_{\mathrm{B}}A_{\mathrm{B}}}\Gamma\left(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}},\frac{m_{\mathrm{E}}(v+1)}{\overline{\gamma}_{\mathrm{E}}}\aleph_{\gamma_{\mathrm{T}}}\right)\right. \left.+(\rho-1)^{m_{\mathrm{B}}A_{\mathrm{B}}}\sum_{n=0}^{m_{\mathrm{B}}A_{\mathrm{B}}}\binom{m_{\mathrm{B}}A_{\mathrm{B}}}{n}\left(\frac{\rho}{\rho-1}\right)^{n}\left(\frac{m_{\mathrm{E}}(v+1)}{\overline{\gamma}_{\mathrm{E}}}\right)^{-n}\Gamma\left(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}+n,\frac{m_{\mathrm{E}}(v+1)}{\overline{\gamma}_{\mathrm{E}}}\aleph_{\gamma_{\mathrm{T}}}\right)\right\} \tag{35}$$

$$\Lambda_{\mathrm{s}}^{(\mathrm{col})} = \frac{1}{\Gamma(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}})}\frac{{m_{\mathrm{B}}}^{m_{\mathrm{B}}A_{\mathrm{B}}}}{(m_{\mathrm{B}}A_{\mathrm{B}})!}(\gamma_{\mathrm{T}})^{m_{\mathrm{B}}A_{\mathrm{B}}}\left\{-\Gamma\left(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}\right)+(\rho-1)^{m_{\mathrm{B}}A_{\mathrm{B}}}\sum_{n=0}^{m_{\mathrm{B}}A_{\mathrm{B}}}\binom{m_{\mathrm{B}}A_{\mathrm{B}}}{n}\left(\frac{\rho}{\rho-1}\right)^{n}\left(\frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\right)^{-n} \times\Gamma\left(N_{\mathrm{E}}A_{\mathrm{E}}m_{\mathrm{E}}+n\right)\right\} \tag{36}$$

$$\Lambda_{\mathrm{s}}^{(\mathrm{ncol})} = \frac{N_{\mathrm{E}}}{\Gamma(A_{\mathrm{E}}m_{\mathrm{E}})}\frac{{m_{\mathrm{B}}}^{m_{\mathrm{B}}A_{\mathrm{B}}}}{(m_{\mathrm{B}}A_{\mathrm{B}})!}\sum_{v=0}^{N_{\mathrm{E}}-1}\binom{N_{\mathrm{E}}-1}{v}(-1)^{v}\Theta_{\mathrm{E},v}(v+1)^{-(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}})}\left\{-(\gamma_{\mathrm{T}})^{m_{\mathrm{B}}A_{\mathrm{B}}}\Gamma\left(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}\right)\right. \left.+(\rho-1)^{m_{\mathrm{B}}A_{\mathrm{B}}}\sum_{n=0}^{m_{\mathrm{B}}A_{\mathrm{B}}}\binom{m_{\mathrm{B}}A_{\mathrm{B}}}{n}\left(\frac{\rho}{\rho-1}\right)^{n}\left(\frac{m_{\mathrm{E}}(v+1)}{\overline{\gamma}_{\mathrm{E}}}\right)^{-n}\Gamma\left(\phi_{\mathrm{E}}+A_{\mathrm{E}}m_{\mathrm{E}}+n\right)\right\} \tag{37}$$

1) Ergodic Secrecy Rate: According to [6], the ergodic secrecy rate of the considered system is given by

$$\overline{\mathcal{C}}_{\mathrm{s}}^{(\kappa)} = \frac{1}{2}\int_0^{\infty}\int_y^{\infty}\left[\log_2(1+x)-\log_2(1+y)\right] \times f_{\gamma_{\mathrm{AB}}}(x)\, f_{\gamma_{\mathrm{RE}}}^{(\kappa)}(y)\, dxdy \tag{38}$$

Now, a closed-form expression for (38) can be derived in the following theorem.

Theorem 2. *The ergodic secrecy rate of the considered system $\overline{\mathcal{C}}_{\mathrm{s}}^{(\kappa)}$ for colluding eavesdropping and non-colluding eavesdropping scenarios are given by* (39) *and* (40)*, respectively, where $\kappa \in \{\mathrm{col}, \mathrm{ncol}\}$.*

Proof: See Appendix C. ∎

2) Asymptotic Ergodic Secrecy Rate: In order to further characterise the impact of key system parameters on the ergodic secrecy rate, we do a high SNR evaluation on the ergodic secrecy rate of the considered systems. In doing so, two new metrics, i.e., the secrecy multiplexing gain and the power cost are exploited to quantify the asymptotic ergodic secrecy rate, and thus we have the following important results.

Corollary 3. *The asymptotic ergodic secrecy rate of the considered system in the high SNR regime is given by*

$$\overline{\mathcal{C}}_{\mathrm{s\_}\infty}^{(\kappa)} \approx \mathcal{G}_1 - \mathcal{G}_2^{(\kappa)}, \tag{41}$$

where $\kappa \in \{\mathrm{col}, \mathrm{ncol}\}$ is provided by (42) *and $\mathcal{G}_2^{(\kappa)}$ is given by* (43) *and* (44)*, respectively.*

Proof: See Appendix D. ∎

As in the traditional non-secrecy system, we proceed to evaluate the behavior of ergodic secrecy rate in terms of the secrecy multiplexing gain and the power cost. To make the analysis more tractable, a general form to describe the asymptotic ergodic secrecy rate is exploited as

$$\overline{\mathcal{C}}_{\mathrm{s\_}\infty}^{(\kappa)} \approx \ell_{\infty}\left(\log_2\overline{\gamma}_{\mathrm{B}} - \varpi_{\infty}^{(\kappa)}\right), \tag{45}$$

where ℓ_{∞} is the secrecy multiplexing gain in bits/s/Hz(3dB) and $\varpi_{\infty}^{(\kappa)}$ denotes the power cost in 3dB units. According to [6], with the help of (41), the secrecy multiplexing gain can be derived as

$$\ell_{\infty} = \lim_{\overline{\gamma}_{\mathrm{B}}\to\infty}\frac{\overline{\mathcal{C}}_{\mathrm{s\_}\infty}^{(\kappa)}}{\log_2\overline{\gamma}_{\mathrm{B}}} = \frac{1}{2} \tag{46}$$

Building on (46), which shows that under these configurations, the considered multiuser cooperative transmission

$$\overline{\mathcal{C}}_{\mathrm{s}}^{(\mathrm{col})}=\tfrac{1}{2\ln 2}\sum_{k=0}^{A_{\mathrm{A}}m_{\mathrm{A}}-1}\tfrac{1}{k!}\left(\tfrac{m_{\mathrm{A}}}{\overline{\gamma}_{\mathrm{A}}}\right)^{k}\Bigg\{\mathcal{D}\Big(\tfrac{m_{\mathrm{A}}}{\overline{\gamma}_{\mathrm{A}}},k,\gamma_{\mathrm{T}}\Big)-\sum_{l=0}^{N_{\mathrm{B}}}\tbinom{N_{\mathrm{B}}}{l}(-1)^{l}\Theta_{\mathrm{B},l}\Big(\tfrac{m_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}}\Big)^{\phi_{\mathrm{B}}}\mathcal{D}\Big(\tfrac{m_{\mathrm{A}}}{\overline{\gamma}_{\mathrm{A}}}+\tfrac{m_{\mathrm{B}}t}{\overline{\gamma}_{\mathrm{B}}},k+\phi_{\mathrm{B}},\gamma_{\mathrm{T}}\Big)$$
$$-\sum_{n=0}^{N_{\mathrm{E}}m_{\mathrm{E}}A_{\mathrm{E}}-1}\tfrac{1}{n!}\Big(\tfrac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\Big)^{n}\mathcal{D}\Big(\tfrac{m_{\mathrm{A}}}{\overline{\gamma}_{\mathrm{A}}}+\tfrac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}},k+n,\gamma_{\mathrm{T}}\Big)+\sum_{r=0}^{N_{\mathrm{E}}m_{\mathrm{E}}A_{\mathrm{E}}-1}\tfrac{1}{r!}\Big(\tfrac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\Big)^{r}\sum_{l=0}^{N_{\mathrm{B}}}\tbinom{N_{\mathrm{B}}}{l}(-1)^{l}\Theta_{\mathrm{B},l}\Big(\tfrac{m_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}}\Big)^{\phi_{\mathrm{B}}}$$
$$\times\mathcal{D}\Big(\tfrac{m_{\mathrm{A}}}{\overline{\gamma}_{\mathrm{A}}}+\tfrac{m_{\mathrm{B}}t}{\overline{\gamma}_{\mathrm{B}}}+\tfrac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}},r+\phi_{\mathrm{B}}+k,\gamma_{\mathrm{T}}\Big)+\mathcal{S}_1\sum_{n=0}^{m_{\mathrm{B}}A_{\mathrm{B}}-1}\tfrac{1}{n!}\Big(\tfrac{m_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}}\Big)^{n}\Bigg[\mathcal{U}\Big(\tfrac{m_{\mathrm{A}}}{\overline{\gamma}_{\mathrm{A}}}+\tfrac{m_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}},k+n,\gamma_{\mathrm{T}}\Big)-\sum_{t=0}^{N_{\mathrm{E}}m_{\mathrm{E}}A_{\mathrm{E}}-1}\tfrac{1}{t!}$$
$$\times\Big(\tfrac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\Big)^{t}\mathcal{U}\Big(\tfrac{m_{\mathrm{A}}}{\overline{\gamma}_{\mathrm{A}}}+\tfrac{m_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}}+\tfrac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}},t+k+n,\gamma_{\mathrm{T}}\Big)\Bigg]\Bigg\} \tag{39}$$

$$\overline{\mathcal{C}}_{\mathrm{s}}^{(\mathrm{ncol})}=\tfrac{1}{2\ln 2}\sum_{k=0}^{A_{\mathrm{A}}m_{\mathrm{A}}-1}\tfrac{1}{k!}\Big(\tfrac{m_{\mathrm{A}}}{\overline{\gamma}_{\mathrm{A}}}\Big)^{k}\sum_{v=0}^{N_{\mathrm{E}}}\tbinom{N_{\mathrm{E}}}{v}(-1)^{v}\Theta_{\mathrm{E},v}\Big(\tfrac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\Big)^{\phi_{\mathrm{E}}}\Bigg\{\mathcal{D}\Big(\tfrac{m_{\mathrm{A}}}{\overline{\gamma}_{\mathrm{A}}}+\tfrac{m_{\mathrm{E}}v}{\overline{\gamma}_{\mathrm{E}}},\phi_{\mathrm{E}}+k,\gamma_{\mathrm{T}}\Big)-\sum_{t=0}^{N_{\mathrm{B}}}\tbinom{N_{\mathrm{B}}}{t}(-1)^{t}$$
$$\times\Theta_{\mathrm{B},t}\Big(\tfrac{m_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}}\Big)^{\phi_{\mathrm{B}}}\mathcal{D}\Big(\tfrac{m_{\mathrm{A}}}{\overline{\gamma}_{\mathrm{A}}}+\tfrac{m_{\mathrm{B}}t}{\overline{\gamma}_{\mathrm{B}}}+\tfrac{m_{\mathrm{E}}v}{\overline{\gamma}_{\mathrm{E}}},\phi_{\mathrm{E}}+\phi_{\mathrm{B}}+k,\gamma_{\mathrm{T}}\Big)+\sum_{n=0}^{m_{\mathrm{B}}A_{\mathrm{B}}-1}\tfrac{\left(\frac{m_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}}\right)^{n}}{n!}\mathcal{S}_1\,\mathcal{U}\Big(\tfrac{m_{\mathrm{A}}}{\overline{\gamma}_{\mathrm{A}}}+\tfrac{m_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}}+\tfrac{m_{\mathrm{E}}v}{\overline{\gamma}_{\mathrm{E}}},\phi_{\mathrm{B}}+k+n,\gamma_{\mathrm{T}}\Big)\Bigg\} \tag{40}$$

$$\mathcal{G}_1\approx\tfrac{1}{2}\log_2\left(\overline{\gamma}_{\mathrm{B}}\right)+\tfrac{1}{2\ln 2}\Bigg\{\tfrac{(m_{\mathrm{A}})^{A_{\mathrm{A}}m_{\mathrm{A}}}}{\Gamma(A_{\mathrm{A}}m_{\mathrm{A}})}\sum_{n=0}^{m_{\mathrm{B}}A_{\mathrm{B}}-1}\tfrac{(m_{\mathrm{B}})^{n}}{n!}\tfrac{\Gamma(A_{\mathrm{A}}m_{\mathrm{A}}+n)}{(m_{\mathrm{A}}+m_{\mathrm{B}})^{A_{\mathrm{A}}m_{\mathrm{A}}+n}}\Big[\psi\left(A_{\mathrm{A}}m_{\mathrm{A}}+n\right)-\ln\left(m_{\mathrm{A}}+m_{\mathrm{B}}\right)\Big]$$
$$+\tfrac{(m_{\mathrm{B}})^{A_{\mathrm{B}}m_{\mathrm{B}}}}{\Gamma(A_{\mathrm{B}}m_{\mathrm{B}})}\sum_{k=0}^{A_{\mathrm{A}}m_{\mathrm{A}}-1}\tfrac{(m_{\mathrm{A}})^{k}}{k!}\tfrac{\Gamma(A_{\mathrm{B}}m_{\mathrm{B}}+k)}{(m_{\mathrm{A}}+m_{\mathrm{B}})^{A_{\mathrm{B}}m_{\mathrm{B}}+k}}\Big[\psi\left(A_{\mathrm{B}}m_{\mathrm{B}}+k\right)-\ln\left(m_{\mathrm{A}}+m_{\mathrm{B}}\right)\Big]\Bigg\} \tag{42}$$

$$\mathcal{G}_2^{(\mathrm{col})}\approx\tfrac{1}{2\ln 2}\sum_{l=0}^{N_{\mathrm{E}}m_{\mathrm{E}}A_{\mathrm{E}}-1}\tfrac{1}{l!}\Big(\tfrac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\Big)^{l}\Big[(-1)^{l-1}\exp\Big(\tfrac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\Big)\mathrm{Ei}\Big(-\tfrac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\Big)+\sum_{t=1}^{l}(t-1)!(-1)^{l-t}\Big(\tfrac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\Big)^{-t}\Big] \tag{43}$$

$$\mathcal{G}_2^{(\mathrm{ncol})}\approx\tfrac{1}{2\ln 2}\sum_{v=1}^{N_{\mathrm{E}}}\tbinom{N_{\mathrm{E}}}{v}(-1)^{v}\Theta_{\mathrm{E},v}\Big(\tfrac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}\Big)^{\phi_{\mathrm{E}}}\Big[(-1)^{\phi_{\mathrm{E}}-1}\exp\Big(\tfrac{m_{\mathrm{E}}v}{\overline{\gamma}_{\mathrm{E}}}\Big)\mathrm{Ei}\Big(-\tfrac{m_{\mathrm{E}}v}{\overline{\gamma}_{\mathrm{E}}}\Big)+\sum_{t=1}^{\phi_{\mathrm{E}}}(t-1)!(-1)^{\phi_{\mathrm{E}}-t}\Big(\tfrac{m_{\mathrm{E}}v}{\overline{\gamma}_{\mathrm{E}}}\Big)^{-t}\Big] \tag{44}$$

obtains the same spectral efficiency as the scenarios without wiretappers.

Then, we focus on the power cost $\varpi_{\infty}^{(\kappa)}$. Mathematically, it can be written as

$$\varpi_{\infty}^{(\kappa)}=\lim_{\overline{\gamma}_{\mathrm{B}}\to\infty}\left(\log_2\overline{\gamma}_{\mathrm{B}}-\frac{\overline{\mathcal{C}}_{\mathrm{s}\_\infty}^{(\kappa)}}{\ell_{\infty}}\right) \tag{47}$$

It is worth noting that (47) definitely evaluates the impact of the BS to relay channel, legitimate channel and the wiretap channel on the ergodic secrecy rate. Therefore, by inserting (41) and (46) into (47), we obtain

$$\varpi_{\infty}^{(\kappa)}=\varpi_{\infty}\left(A_{\mathrm{A}},m_{\mathrm{A}},A_{\mathrm{B}},m_{\mathrm{B}}\right)+\varpi_{\infty}^{(\kappa)}\left(N_{\mathrm{E}},A_{\mathrm{E}},m_{\mathrm{E}}\right) \tag{48}$$

where

$$\varpi_{\infty}\left(A_{\mathrm{A}},m_{\mathrm{A}},A_{\mathrm{B}},m_{\mathrm{B}}\right)=-\frac{1}{\ln 2}\Bigg\{\frac{(m_{\mathrm{A}})^{A_{\mathrm{A}}m_{\mathrm{A}}}}{\Gamma\left(A_{\mathrm{A}}m_{\mathrm{A}}\right)}\sum_{n=0}^{m_{\mathrm{B}}A_{\mathrm{B}}-1}\frac{(m_{\mathrm{B}})^{n}}{n!}$$
$$\times\frac{\Gamma\left(A_{\mathrm{A}}m_{\mathrm{A}}+n\right)}{\left(m_{\mathrm{A}}+m_{\mathrm{B}}\right)^{A_{\mathrm{A}}m_{\mathrm{A}}+n}}\Big[\psi\left(A_{\mathrm{A}}m_{\mathrm{A}}+n\right)-\ln\left(m_{\mathrm{A}}+m_{\mathrm{B}}\right)\Big]$$
$$+\frac{(m_{\mathrm{B}})^{A_{\mathrm{B}}m_{\mathrm{B}}}}{\Gamma\left(A_{\mathrm{B}}m_{\mathrm{B}}\right)}\sum_{k=0}^{A_{\mathrm{A}}m_{\mathrm{A}}-1}\frac{(m_{\mathrm{A}})^{k}}{k!}\frac{\Gamma\left(A_{\mathrm{B}}m_{\mathrm{B}}+k\right)}{\left(m_{\mathrm{A}}+m_{\mathrm{B}}\right)^{A_{\mathrm{B}}m_{\mathrm{B}}+k}}$$
$$\times\Big[\psi\left(A_{\mathrm{B}}m_{\mathrm{B}}+k\right)-\ln\left(m_{\mathrm{A}}+m_{\mathrm{B}}\right)\Big]\Bigg\} \tag{49}$$

and

$$\varpi_{\infty}^{(\kappa)}\left(N_{\mathrm{B}},N_{\mathrm{E}},A_{\mathrm{E}},m_{\mathrm{E}}\right)=2\mathcal{G}_2^{(\kappa)} \tag{50}$$

Based on the description above, we drawn a conclusion that the positive impact of main channel is characterized by $\varpi_{\infty}^{(\kappa)}\left(A_{\mathrm{A}},m_{\mathrm{A}},A_{\mathrm{B}},m_{\mathrm{B}}\right)$, and the negative impact of eavesdropper's channel is characterized by $\varpi_{\infty}^{(\kappa)}\left(N_{\mathrm{E}},A_{\mathrm{E}},m_{\mathrm{E}}\right)$. In addition, $\varpi_{\infty}^{(\kappa)}\left(N_{\mathrm{E}},A_{\mathrm{E}},m_{\mathrm{E}}\right)$ also explicitly quantifies the loss of ergodic secrecy rate due to the behavior of the wiretapping at Eves.

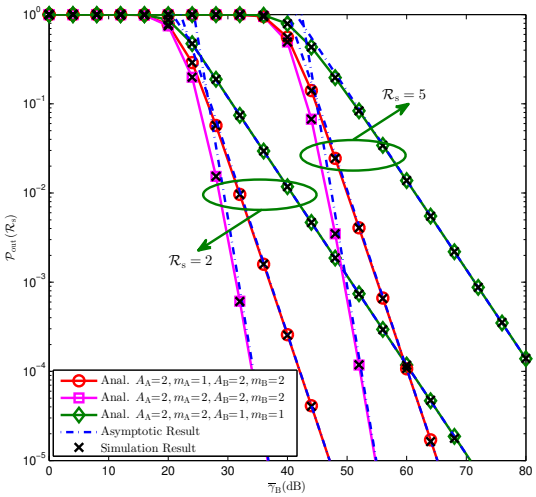

Fig. 2: Secrecy outage probability versus $\overline{\gamma}_{\rm B}$ for colluding eavesdropping with $N_{\rm B}$=2, $N_{\rm E}$=$A_{\rm E}$=$m_{\rm E}$=2, $\gamma_{\rm T}$=20dB and $\overline{\gamma}_{\rm E}$=5dB.

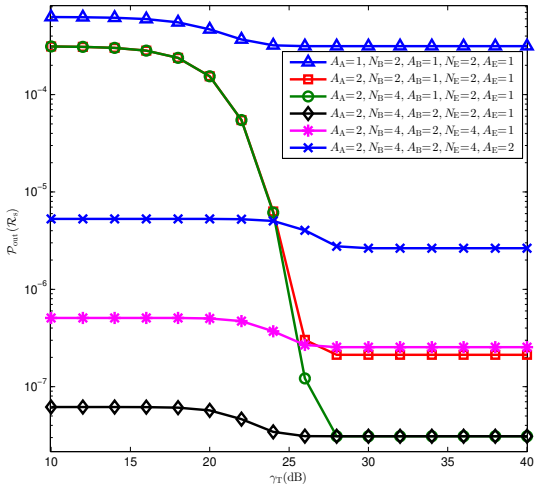

Fig. 3: Secrecy outage probability versus $\gamma_{\rm T}$ for colluding eavesdropping with $m_{\rm A}$=$m_{\rm B}$=$m_{\rm E}$=2, $\mathcal{R}_{\rm s}$=2, $\overline{\gamma}_{\rm E}$=5dB and $\overline{\gamma}_{\rm B}$=40dB.

Once again, it is observed that for both eavesdropping modes, the secrecy multiplexing gain remains the same, while they differ in the power cost.

IV. Simulations and Discussion

In this section, numerical results are presented to validate the aforementioned analysis and investigate the joint impact of key system parameters on the secrecy performance of the considered system.

Fig. 2 illustrates the secrecy outage probability of the dual-hop multiuser regenerative relay system versus different SNR $\overline{\gamma}_{\rm B}$ for colluding eavesdropping scenario. As observed in this figure, we can see that the exact analytical results $\mathcal{P}_{\rm out}^{\rm (col)}(\mathcal{R}_{\rm s})$ in (22) match precisely with the Monte Carlo simulations, and the asymptotic curves $\mathcal{P}_{\rm out}^{\infty\text{-}\rm (col)}(\mathcal{R}_{\rm s})$ in (29) approximate the exact ones quite well in the high SNR regime, which demonstrates the correctness of the theoretical analysis. Furthermore, as expected, increasing the predetermined secrecy rate $\mathcal{R}_{\rm s}$ degrades the secrecy performance, while the asymptotic curves keep parallel for each secrecy rate $\mathcal{R}_{\rm s}$. We also find that our asymptotes accurately predict the secrecy diversity order and secrecy array gain. As indicated in this figure, the secrecy diversity order is equal to $A_{\rm A}m_{\rm A}$ when $A_{\rm A}m_{\rm A} < A_{\rm B}m_{\rm B}$, e.g., $(A_{\rm A}=2, m_{\rm A}=1, A_{\rm B}=2, m_{\rm B}=2)$, while the secrecy diversity order is $A_{\rm B}m_{\rm B}$ when $A_{\rm A}m_{\rm A} \geq A_{\rm B}m_{\rm B}$, e.g., $(A_{\rm A}=2, m_{\rm A}=2, A_{\rm B}=1, m_{\rm B}=1)$ and $(A_{\rm A}=2, m_{\rm A}=2, A_{\rm B}=2, m_{\rm B}=2)$, respectively.

Fig. 3 investigates the secrecy outage probability against switching threshold $\gamma_{\rm T}$ for colluding eavesdropping scenario. It is observed that, the secrecy performance improves as the switching threshold $\gamma_{\rm T}$ grows up. Increasing the number of antennas equipped at the BS and the number of legitimate users or the number of legitimate users have a positive impact on the secrecy performance. As can be seen, it is favorable to put more antennas at legitimate users, which brings about the improvement of secrecy performance especially in low switching threshold regime. However, increasing the number of colluding eavesdroppers or antennas equipped at the eavesdroppers results in more powerful wiretapping capability, which inevitably deteriorates the secrecy performance of the considered system.

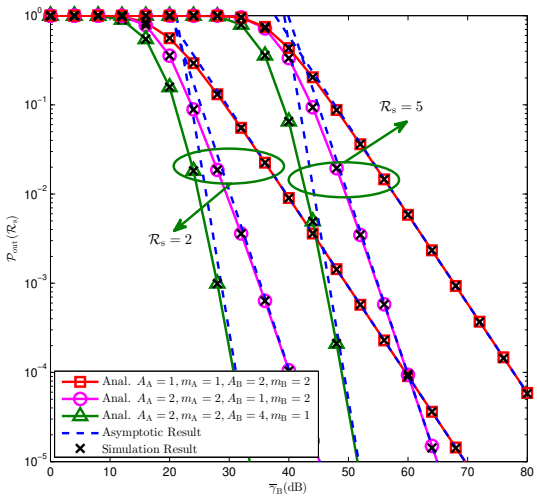

Fig. 4: Secrecy outage probability versus $\overline{\gamma}_{\rm B}$ for non-colluding eavesdropping with $A_{\rm A}$=$m_{\rm A}$=2, $N_{\rm B}$=$N_{\rm E}$=2, $A_{\rm E}$=$m_{\rm E}$=1, $\gamma_{\rm T}$=20dB and $\overline{\gamma}_{\rm E}$=5dB.

Fig. 4 depicts the secrecy outage probability versus different $\overline{\gamma}_{\rm B}$ for non-colluding eavesdropping scenario of the considered system. It is illustrated in this figure that the theoretical results $\mathcal{P}_{\rm out}^{\rm (ncol)}(\mathcal{R}_{\rm s})$ in (22) are in exact agreement with the Monte Carlo simulations, and the asymptotic curves well approximate the exact ones at the high SNR regimes. Similar to the colluding eavesdropping scenario, the asymptotic curves

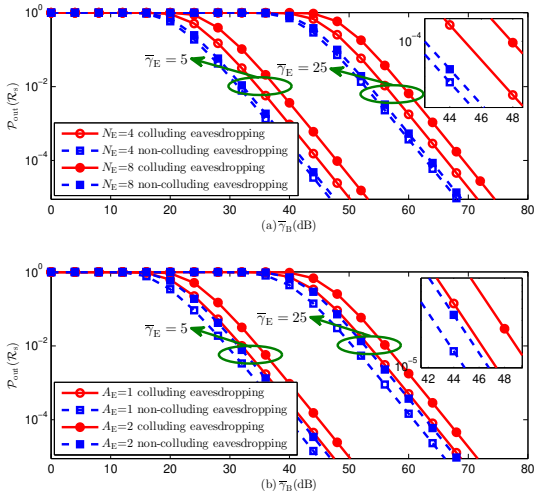

Fig. 5: Secrecy outage probability comparison between colluding eavesdropping and non-colluding eavesdropping with $A_{\rm A}$=2, $m_{\rm A}$=1, $N_{\rm B}$=4, $A_{\rm B}$= 2, $m_{\rm B}$=1, $\mathcal{R}_{\rm s}$=2 and $\gamma_{\rm T}$=30dB. For (a) $A_{\rm E}$=2, $m_{\rm E}$=1; For (b) $N_{\rm E}$=4, $m_{\rm E}$=1.

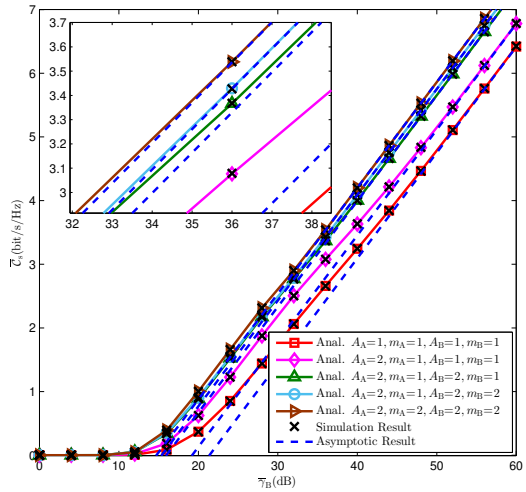

Fig. 6: Ergodic secrecy rate versus $\overline{\gamma}_{\rm B}$ for colluding eavesdropping with $N_{\rm B}=2, N_{\rm E}=m_{\rm E}=A_{\rm E}=2, \gamma_{\rm T}=30$dB and $\overline{\gamma}_{\rm E}=10$dB.

$\mathcal{P}_{\rm out}^{\infty\_(\rm ncol)}(\mathcal{R}_{\rm s})$ in (29) precisely predict the secrecy diversity order and secrecy array gain. As indicated in this figure, the secrecy diversity order also can be divided into three types as characterized in colluding eavesdropping scenario.

Fig. 5 illustrates a comparison of the secrecy outage probability between colluding eavesdropping and non-colluding eavesdropping of the considered system. We mainly evaluate the impact of eavesdropping parameters on the secrecy performance. It is observed that the secrecy outage performance deteriorates profoundly as the ratio of $\overline{\gamma}_{\rm B}/\overline{\gamma}_{\rm E}$ decreases. Furthermore, colluding eavesdropping results in larger secrecy outage than non-colluding eavesdropping since the colluding eavesdroppers are capable of sharing their observations and decoding the messages jointly. Specifically, in Fig. 5 (a) and (b), we can see that increasing the number of eavesdroppers or the number of antennas at eavesdroppers in colluding eavesdropping leads to a poorer secrecy performance than that of non-colluding eavesdropping.

Fig. 6 depicts the ergodic secrecy rate of the considered system versus different $\overline{\gamma}_{\rm B}$ for colluding eavesdropping. We observe that the analytical results for ergodic secrecy rate $\overline{\mathcal{C}}_{\rm s}^{(\rm col)}$ in (39) well match with the Monte Carlo simulations, and the asymptotic curves $\overline{\mathcal{C}}_{\rm s}^{(\rm ncol)}$ in (41) approximate the theoretical ones very well in the high SNR regime, which demonstrates the correctness of our derived expressions. It is shown that increasing the number of antennas equipped at the BS and at legitimate user contributes to larger secrecy capacity improvement than increasing the channel quality of first hop and that of legitimate channel in the second hop. Fig. 7 shows that the ergodic secrecy rate improves with the increase of the switching threshold $\gamma_{\rm T}$. More legitimate users are examined as the switching threshold increases, which results in a preferable performance at the cost of higher estimation complexity. It is worth noting that when $\gamma_{\rm T}$ comes close to infinity, the

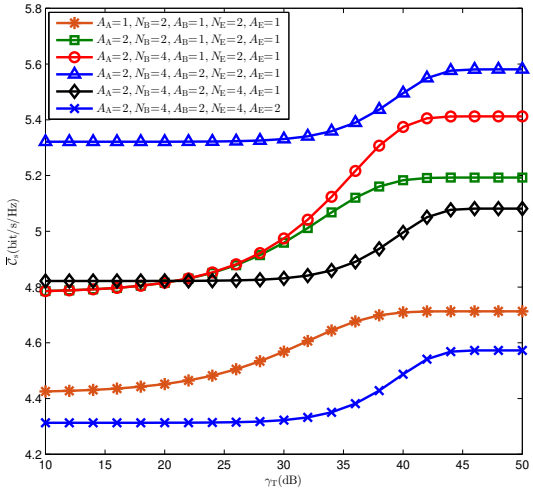

Fig. 7: Ergodic secrecy rate versus $\gamma_{\rm T}$ for colluding eavesdropping with $A_{\rm A}$=$m_{\rm A}$=2, $A_{\rm E}=m_{\rm E}=2$, $\overline{\gamma}_{\rm B}$=40dB, and $\overline{\gamma}_{\rm E}=5$dB.

secrecy performance floor occurs. As demonstrated in the figure, the number of legitimate users and antennas at them in high $\gamma_{\rm T}$ regime leave a positive impact on the ergodic secrecy performance, while increasing the number of eavesdroppers and the antennas equipped at them will deteriorate secrecy performance.

Fig. 8 examines the ergodic secrecy rate against different $\overline{\gamma}_{\rm B}$ for non-colluding eavesdropping scenario. As can be readily observed, the analytical results $\overline{\mathcal{C}}_{\rm s}^{(\rm ncol)}$ in (40) are in exact agreement with the Monte Carlo simulations, and the approximated expression $\overline{\mathcal{C}}_{\rm s\_\infty}^{(\rm ncol)}$ in (41) operates quite well with the analytical ones at high SNR regime. It is noted that the ergodic secrecy rate increases with the antennas equipped at the BS or

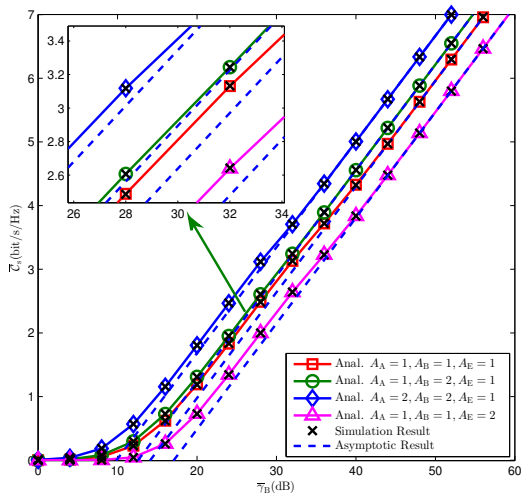

Fig. 8: Ergodic secrecy rate versus $\overline{\gamma}_{\rm B}$ for non-colluding eavesdropping with $N_{\rm B}=N_{\rm E}=2, m_{\rm A}=m_{\rm B}=2, m_{\rm E}=1, \gamma_{\rm T}=30$dB and $\overline{\gamma}_{\rm E}=10$dB.

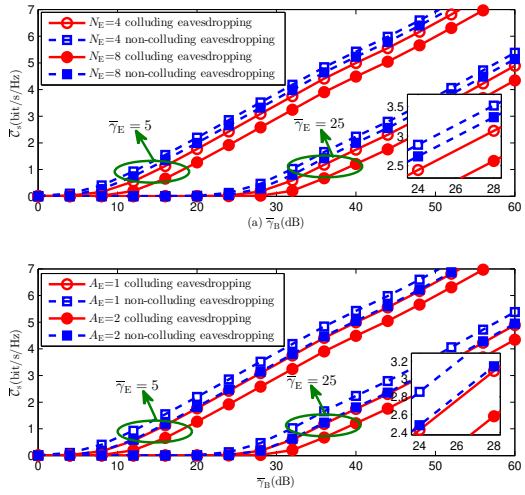

Fig. 9: Ergodic secrecy rate comparison between colluding eavesdropping and non-colluding eavesdropping with $A_{\rm A}$=2, $m_{\rm A}$=1, $N_{\rm B}$=4, $A_{\rm B}$= 2, $m_{\rm B}$=1, $\mathcal{R}_{\rm s}$=2, and $\gamma_{\rm T}$=40dB. For (a) $A_{\rm E}$=2, $m_{\rm E}$=1; For (b) $N_{\rm E}$=4, $m_{\rm E}$=1.

at the legitimate users. Besides, as can be expected, increasing the numbers of antennas at the eavesdroppers improves the quality of wiretap channel, which results in the increment of the power cost $\varpi_{\infty}^{(\rm col)}$, and therefore deteriorates the ergodic secrecy rate of the considered networks.

Fig. 9 presents the ergodic secrecy rate comparison between colluding eavesdropping and non-colluding eavesdropping. As can be seen that, when the ratio of $\overline{\gamma}_{\rm B}/\overline{\gamma}_{\rm E}$ reduces, the ergodic secrecy rate will greatly lower the secrecy performance. For Fig. 9 (a) and (b), the secrecy performance degrades with increasing the number of eavesdroppers or the antennas at eavesdroppers for both scenarios. From an intuitive perspective, more eavesdroppers or more antennas at the eavesdroppers can strengthen wiretapping capability. Furthermore, we discover that colluding eavesdropping imposes more hazardous effect on the secrecy performance of the considered system particularly for medium and high $\overline{\gamma}_{\rm B}$ settings.

V. Conclusions

In this paper, we have presented a comprehensive secrecy performance analysis for multiuser regenerative relay wiretap networks. Specifically, the imperfect decoding at the relay was considered and threshold-based multiuser scheduling scheme was adopted to acquire a good tradeoff between the system complexity and secrecy performance. To quantify the secrecy performance of the considered system, two practical situations were addressed. i.e., Scenario I: the eavesdropper's CSI is not available at the relay and Scenario II: the eavesdropper's CSI is available at the relay. For both scenarios, we further considered both colluding and non-colluding eavesdropping situations. For Scenario I, we have derived exact closed-form expressions of the secrecy outage probability for both two eavesdropping modes, which presents an efficient and convenient approach to characterize the secrecy performance. Besides, conducive high SNR approximations for the secrecy outage probability was provided, which enables further insights into the impact of key system parameters on secrecy performance. For Scenario II, we have concentrated on the analysis of the ergodic secrecy rate achieved by the system. Specifically, new exact and asymptotic closed-form expressions of ergodic secrecy rate were derived for both two eavesdropping modes. With the help of the analytical results, we also examined the secrecy multiplexing gain and the power cost to explicitly evaluate the influence of the legitimate channel and wiretap channel on the ergodic secrecy rate. Our findings reveal that increasing the switching threshold has a positive impact on secrecy performance and it is preferable to put more antennas at BS or legitimate users. In addition, compared with non-colluding eavesdropping, colluding eavesdropping is more detrimental to the considered system.

Appendix A
Proof of Theorem 1

The secrecy outage probability in (21) can be separated in three parts and the first one is given by

$$\mathcal{I}_1^{(\kappa)}=\int_0^{\infty}\mathcal{F}_{\gamma_{\rm AR}}(\lambda)\,f_{\gamma_{\rm RE}}^{(\kappa)}(x)dx \tag{51}$$

For colluding eavesdropping scenario, by inserting (12) and (17) into (51), resorting to [44, Eq. (3.326.2)] and binomial theory, $\mathcal{I}_1^{(\rm col)}$ is provided in (23), where $\mathcal{S}_{\rm 2ae}=\frac{m_{\rm E}}{\overline{\gamma}_{\rm E}}+\frac{m_{\rm A}\rho}{\overline{\gamma}_{\rm A}}$ and

$$\widetilde{\sum}_{{\rm A},k_1}=\exp\left(-\frac{m_{\rm A}(\rho-1)}{\overline{\gamma}_{\rm A}}\right)\sum_{k=0}^{A_{\rm A}m_{\rm A}-1}\frac{(\rho-1)^k}{k!}\times\left(\frac{m_{\rm A}}{\overline{\gamma}_{\rm A}}\right)^k\sum_{k_1=0}^{k}\binom{k}{k_1}\left(\frac{\rho}{\rho-1}\right)^{k_1} \tag{52}$$

Similarly, for the non-colluding eavesdropping scenario, we have $\mathcal{I}_1^{(\mathrm{ncol})}$ as given in (24), where $\mathcal{S}_{2\mathrm{aev}} = \frac{m_{\mathrm{E}}(v+1)}{\overline{\gamma}_{\mathrm{E}}} + \frac{m_{\mathrm{A}}\rho}{\overline{\gamma}_{\mathrm{A}}}$.

The second part for the secrecy outage probability of the considered system is given by

$$\mathcal{I}_2^{(\kappa)} = \int_0^{\infty} \mathcal{F}_{\gamma_{\mathrm{RB}}}(\lambda) f_{\gamma_{\mathrm{RE}}}^{(\kappa)}(x) dx \tag{53}$$

To make the analysis more tractable, here we introduce a new bound point as $\aleph_{\gamma_{\mathrm{T}}} = \rho^{-1}(1+\gamma_{\mathrm{T}}) - 1$. Therefore, $\mathcal{I}_2^{(\kappa)}$ can be converted in a piecewise form with the bound point as

$$\begin{aligned}\mathcal{I}_2^{(\kappa)} &= \begin{cases} \int_0^{\aleph_{\gamma_{\mathrm{T}}}} \mathcal{F}_{\gamma_{\mathrm{RB}}}(\lambda) f_{\gamma_{\mathrm{RE}}}^{(\kappa)}(x)\, dx \\ \quad + \int_{\aleph_{\gamma_{\mathrm{T}}}}^{\infty} \mathcal{F}_{\gamma_{\mathrm{RB}}}(\lambda) f_{\gamma_{\mathrm{RE}}}^{(\kappa)}(x)\, dx, & \aleph_{\gamma_{\mathrm{T}}} \geq 0 \\ \int_0^{\infty} \mathcal{F}_{\gamma_{\mathrm{RB}}}(\lambda) f_{\gamma_{\mathrm{RE}}}^{(\kappa)}(x)\, dx, & \aleph_{\gamma_{\mathrm{T}}} < 0 \end{cases} \\ &= \begin{cases} \mathcal{I}_{2\mathrm{a}}^{(\kappa)}, & \aleph_{\gamma_{\mathrm{T}}} \geq 0 \\ \mathcal{I}_{2\mathrm{b}}^{(\kappa)}, & \aleph_{\gamma_{\mathrm{T}}} < 0 \end{cases} \end{aligned} \tag{54}$$

For colluding eavesdropping scenario, by inserting (8) and (17) into (54), with the assistance of [44, Eqs. (3.351.1), (3.351.2) and (3.351.3)], $\mathcal{I}_2^{(\mathrm{col})}$ is given as (25) after some mathematical manipulations, where $\mathcal{S}_{0\mathrm{be}} = \frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}} + \frac{m_{\mathrm{B}}\rho l}{\overline{\gamma}_{\mathrm{B}}}$, $\mathcal{S}_{2\mathrm{be}} = \frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}} + \frac{m_{\mathrm{B}}\rho}{\overline{\gamma}_{\mathrm{B}}}$,

$$\begin{aligned}\widetilde{\sum}_{\mathrm{B},n_1} = \mathcal{S}_1 \exp\left(-\frac{m_{\mathrm{B}}(\rho-1)}{\overline{\gamma}_{\mathrm{B}}}\right) \sum_{n=0}^{m_{\mathrm{B}}A_{\mathrm{B}}-1} \frac{(\rho-1)^n}{n!} \\ \times \left(\frac{m_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}}\right)^n \sum_{n_1=0}^{n} \binom{n}{n_1} \left(\frac{\rho}{\rho-1}\right)^{n_1}\end{aligned} \tag{55}$$

and $\mathcal{S}_1 = \sum_{k=0}^{N_{\mathrm{B}}-1} \left[1 - \exp\left(-\frac{m_{\mathrm{B}}\gamma_{\mathrm{T}}}{\overline{\gamma}_{\mathrm{B}}}\right) \sum_{n=0}^{m_{\mathrm{B}}A_{\mathrm{B}}-1} \frac{(\gamma_{\mathrm{T}})^n}{n!} \left(\frac{m_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}}\right)^n\right]^k$.
Similarly, for the non-colluding eavesdropping scenario, $\mathcal{I}_2^{(\mathrm{ncol})}$ is given by (26), where $\mathcal{S}_{0\mathrm{bev}} = \frac{m_{\mathrm{E}}(v+1)}{\overline{\gamma}_{\mathrm{E}}} + \frac{m_{\mathrm{B}}\rho l}{\overline{\gamma}_{\mathrm{B}}}$,

$$\begin{aligned}\Theta_{\mathrm{B},l} = \sum_{n_1=0}^{l} \sum_{n_2=0}^{n_1} \cdots \sum_{n_{m_{\mathrm{B}}A_{\mathrm{B}}-1}=0}^{n_{m_{\mathrm{B}}A_{\mathrm{B}}-2}} \frac{l!}{n_{m_{\mathrm{B}}A_{\mathrm{B}}-1}!} \\ \times \prod_{t=1}^{m_{\mathrm{B}}A_{\mathrm{B}}-1} \frac{(t!)^{n_{t+1}-n_t}}{(n_{t-1}-n_t)!}\end{aligned} \tag{56}$$

$\phi_{\mathrm{B}} = \sum_{q=1}^{m_{\mathrm{B}}A_{\mathrm{B}}-1} n_q, n_0 = l, n_{A_{\mathrm{B}}m_{\mathrm{B}}} = 0$, and $\mathcal{S}_{2\mathrm{bev}} = \frac{m_{\mathrm{E}}(v+1)}{\overline{\gamma}_{\mathrm{E}}} + \frac{m_{\mathrm{B}}\rho}{\overline{\gamma}_{\mathrm{B}}}$.

The third part for the secrecy outage probability of the considered system is given by

$$\mathcal{I}_3^{(\kappa)} = -\int_0^{\infty} \mathcal{F}_{\gamma_{\mathrm{AR}}}(\lambda) \mathcal{F}_{\gamma_{\mathrm{RB}}}(\lambda) f_{\gamma_{\mathrm{RE}}}^{(\kappa)}(x) dx \tag{57}$$

Similar to the piecewise form with the bound point in (54), $\mathcal{I}_3^{(\kappa)}$ can be further expressed as

$$\begin{aligned}\mathcal{I}_3^{(\kappa)} &= \begin{cases} \int_0^{\aleph_{\gamma_{\mathrm{T}}}} \mathcal{F}_{\gamma_{\mathrm{AR}}}(\lambda) \mathcal{F}_{\gamma_{\mathrm{RB}}}(\lambda) f_{\gamma_{\mathrm{RE}}}^{(\kappa)}(x) dx + \int_{\aleph_{\gamma_{\mathrm{T}}}}^{\infty} \mathcal{F}_{\gamma_{\mathrm{AR}}}(\lambda) \\ \qquad \times \mathcal{F}_{\gamma_{\mathrm{RB}}}(\lambda) f_{\gamma_{\mathrm{RE}}}^{(\kappa)}(x) dx, & \aleph_{\gamma_{\mathrm{T}}} \geq 0 \\ \int_0^{\infty} \mathcal{F}_{\gamma_{\mathrm{AR}}}(\lambda) \mathcal{F}_{\gamma_{\mathrm{RB}}}(\lambda) f_{\gamma_{\mathrm{RE}}}^{(\kappa)}(x) dx, & \aleph_{\gamma_{\mathrm{T}}} < 0 \end{cases} \\ &= \begin{cases} \mathcal{I}_{3\mathrm{a}}^{(\kappa)}, & \aleph_{\gamma_{\mathrm{T}}} \geq 0 \\ \mathcal{I}_{3\mathrm{b}}^{(\kappa)}, & \aleph_{\gamma_{\mathrm{T}}} < 0 \end{cases} \end{aligned} \tag{58}$$

Thus, for colluding scenario, by inserting (8), (12), and (17) into (58), resorting to [44, Eqs. (3.351.1), (3.351.2) and (3.351.3)] and performing some mathematical operations, $\mathcal{I}_3^{(\mathrm{col})}$ is provided as (27), where $\mathcal{S}_{0\mathrm{abe}} = \frac{m_{\mathrm{A}}\rho}{\overline{\gamma}_{\mathrm{A}}} + \frac{m_{\mathrm{B}}\rho l}{\overline{\gamma}_{\mathrm{B}}} + \frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}, \mathcal{S}_{2\mathrm{ae}} = \frac{m_{\mathrm{A}}\rho}{\overline{\gamma}_{\mathrm{A}}} + \frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}, \mathcal{S}_{2\mathrm{be}} = \frac{m_{\mathrm{B}}\rho}{\overline{\gamma}_{\mathrm{B}}} + \frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}$, and $\mathcal{S}_{2\mathrm{abe}} = \frac{m_{\mathrm{A}}\rho}{\overline{\gamma}_{\mathrm{A}}} + \frac{m_{\mathrm{B}}\rho}{\overline{\gamma}_{\mathrm{B}}} + \frac{m_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}$.

Similarly, for the non-colluding eavesdropping scenario, $\mathcal{I}_3^{(\mathrm{ncol})}$ is provided by (28), where $\mathcal{S}_{0\mathrm{bev}} = \frac{m_{\mathrm{E}}(v+1)}{\overline{\gamma}_{\mathrm{E}}} + \frac{m_{\mathrm{B}}\rho l}{\overline{\gamma}_{\mathrm{B}}}, \mathcal{S}_{0\mathrm{abev}} = \frac{m_{\mathrm{A}}\rho}{\overline{\gamma}_{\mathrm{A}}} + \frac{m_{\mathrm{B}}\rho l}{\overline{\gamma}_{\mathrm{B}}} + \frac{m_{\mathrm{E}}(v+1)}{\overline{\gamma}_{\mathrm{E}}}, \mathcal{S}_{2\mathrm{aev}} = \frac{m_{\mathrm{A}}\rho}{\overline{\gamma}_{\mathrm{A}}} + \frac{m_{\mathrm{E}}(v+1)}{\overline{\gamma}_{\mathrm{E}}}$, $\mathcal{S}_{2\mathrm{bev}} = \frac{m_{\mathrm{B}}\rho}{\overline{\gamma}_{\mathrm{B}}} + \frac{m_{\mathrm{E}}(v+1)}{\overline{\gamma}_{\mathrm{E}}}$, and $\mathcal{S}_{2\mathrm{abev}} = \frac{m_{\mathrm{A}}\rho}{\overline{\gamma}_{\mathrm{A}}} + \frac{m_{\mathrm{B}}\rho}{\overline{\gamma}_{\mathrm{B}}} + \frac{m_{\mathrm{E}}(v+1)}{\overline{\gamma}_{\mathrm{E}}}$.

Hence, by summing up (23), (25) and (27) for colluding eavesdropping scenario, the exact closed-form expression of secrecy probability can be derived as (22) by following a similar analysis for the non-colluding scenario.

Appendix B
Proof of Corollary 2

In the high SNR regime, i.e., $\overline{\gamma}_{\mathrm{B}} \to \infty$, from (10), the CDF of γ_k^{b} can be easily approximated as

$$\mathcal{F}_{\gamma_k^{\mathrm{b}}}(x) \approx \frac{{m_{\mathrm{B}}}^{m_{\mathrm{B}}A_{\mathrm{B}}}}{(m_{\mathrm{B}}A_{\mathrm{B}})!} \left(\frac{x}{\overline{\gamma}_{\mathrm{B}}}\right)^{m_{\mathrm{B}}A_{\mathrm{B}}} \tag{59}$$

By substituting (59) into (8), we have

$$\mathcal{F}_{\gamma_{\mathrm{RB}}}(x) \approx \begin{cases} 1 - \sum_{k=0}^{N_{\mathrm{B}}-1} \left[\frac{{m_{\mathrm{B}}}^{m_{\mathrm{B}}A_{\mathrm{B}}}}{(m_{\mathrm{B}}A_{\mathrm{B}})!} \left(\frac{\gamma_{\mathrm{T}}}{\overline{\gamma}_{\mathrm{B}}}\right)^{m_{\mathrm{B}}A_{\mathrm{B}}}\right]^k \\ \qquad \times \left[1 - \frac{{m_{\mathrm{B}}}^{m_{\mathrm{B}}A_{\mathrm{B}}}}{(m_{\mathrm{B}}A_{\mathrm{B}})!} \left(\frac{x}{\overline{\gamma}_{\mathrm{B}}}\right)^{m_{\mathrm{B}}A_{\mathrm{B}}}\right], & x \geq \gamma_{\mathrm{T}} \\ \left[\frac{{m_{\mathrm{B}}}^{m_{\mathrm{B}}A_{\mathrm{B}}}}{(m_{\mathrm{B}}A_{\mathrm{B}})!} \left(\frac{x}{\overline{\gamma}_{\mathrm{B}}}\right)^{m_{\mathrm{B}}A_{\mathrm{B}}}\right]^{N_{\mathrm{B}}}, & x < \gamma_{\mathrm{T}} \end{cases} \tag{60}$$

On the other hand, the CDF of γ_{AR} is easily approximated as

$$\mathcal{F}_{\gamma_{\mathrm{AR}}}(x) \approx \frac{{m_{\mathrm{A}}}^{m_{\mathrm{A}}A_{\mathrm{A}}}}{(m_{\mathrm{A}}A_{\mathrm{A}})!} \left(\frac{x}{\overline{\gamma}_{\mathrm{A}}}\right)^{m_{\mathrm{A}}A_{\mathrm{A}}} \tag{61}$$

To this end, by pulling everything together in (21) and neglecting the higher order terms, resorting to [44, Eqs. (3.351.1) and (3.351.2)], the desired expressions can be easily obtained as in (29) for both eavesdropping modes.

Appendix C
Proof of Theorem 2

To handle the double integrals in (38), we adopt the similar approach as developed in [5]. To begin with, we evaluate the inner integral by adopting integral by parts, and after performing some mathematical operations, the ergodic secrecy rate can be characterized as follows:

$$\begin{aligned}\overline{\mathcal{C}}_{\mathrm{s}}^{(\kappa)} &= \frac{1}{2\ln 2} \int_0^{\infty} \frac{\mathcal{F}_{\gamma_{\mathrm{RE}}}^{(\kappa)}(y)}{(1+y)} \left(\int_y^{\infty} f_{\gamma_{\mathrm{AB}}}(x) dx\right) dy \\ &= \frac{1}{2\ln 2} \int_0^{\infty} \frac{\mathcal{F}_{\gamma_{\mathrm{RE}}}^{(\kappa)}(y)}{(1+y)} \left(1 - \mathcal{F}_{\gamma_{\mathrm{AB}}}(y)\right) dy\end{aligned} \tag{62}$$

where

$$\mathcal{F}_{\gamma_{\mathrm{AB}}}(y) = \mathcal{F}_{\gamma_{\mathrm{AR}}}(y) + \mathcal{F}_{\gamma_{\mathrm{RB}}}(y) - \mathcal{F}_{\gamma_{\mathrm{AR}}}(y) \mathcal{F}_{\gamma_{\mathrm{RB}}}(y) \tag{63}$$

Taking the threshold $\gamma_{\rm T}$ into account, we have

$$\overline{\mathcal{C}}_{\rm s}^{(\kappa)} = \frac{1}{2\ln 2}\Bigg[\int_0^{\gamma_{\rm T}} \frac{\mathcal{F}_{\gamma_{\rm RE}}^{(\kappa)}(y)}{(1+y)}\left(1-\mathcal{F}_{\gamma_{\rm AB}}(y)\right)dy + \int_{\gamma_{\rm T}}^{\infty} \frac{\mathcal{F}_{\gamma_{\rm RE}}^{(\kappa)}(y)}{(1+y)}\left(1-\mathcal{F}_{\gamma_{\rm AB}}(y)\right)dy\Bigg] \tag{64}$$

By inserting (12) and (8) into (63) and resorting to binomial theorem [44, Eq. (1.111)], after some simple mathematical operations, the CDF of $\gamma_{\rm AB}$ is provided as (65).

In proceeding, we plug (65) and (16) into (64) for colluding eavesdropping scenario, (65) and (18) into (64) for non-colluding eavesdropping scenario. With the help of [44, Eqs. (1.111) and (8.350.2)], after performing some algebraic manipulations, the ergodic secrecy rate of the considered system can be derived as (39) and (40), where

$$\mathcal{D}(\varsigma,\mu,\upsilon) = \exp(\varsigma)\sum_{\mu_1=0}^{\mu}\binom{\mu}{\mu_1}(-1)^{\mu-\mu_1}\varsigma^{-\mu_1} \times\left[\Gamma(\mu_1,\varsigma)-\Gamma(\mu_1,\varsigma(\upsilon+1))\right] \tag{66}$$

and

$$\mathcal{U}(\varsigma,\mu,\upsilon) = \exp(\varsigma)\sum_{\mu_1=0}^{\mu}\binom{\mu}{\mu_1}(-1)^{\mu-\mu_1}\varsigma^{-\mu_1} \times\Gamma(\mu_1,\varsigma(\upsilon+1)) \tag{67}$$

Appendix D
Proof of corollary 3

To facilitate the analysis, we modify the CDF of $\gamma_{\rm E}$ as $\mathcal{F}_{\gamma_{\rm RE}}^{(\kappa)}(y) = 1+\varphi_{\gamma_{\rm RE}}^{(\kappa)}(y)$, thus, we have

$$\varphi_{\gamma_{\rm RE}}^{(\rm col)}(y) = -\exp\left(-\frac{m_{\rm E}y}{\overline{\gamma}_{\rm E}}\right)\sum_{n=0}^{N_{\rm E}m_{\rm E}A_{\rm E}-1}\frac{y^n}{n!}\left(\frac{m_{\rm E}}{\overline{\gamma}_{\rm E}}\right)^n \tag{68}$$

and

$$\varphi_{\gamma_{\rm RE}}^{(\rm ncol)}(y) = \sum_{v=1}^{N_{\rm E}}\binom{N_{\rm E}}{v}(-1)^v\exp\left(-\frac{m_{\rm E}v}{\overline{\gamma}_{\rm E}}y\right)\Theta_{{\rm E},v} \times\left(\frac{m_{\rm E}}{\overline{\gamma}_{\rm E}}\right)^{\phi_{\rm E}} y^{\phi_{\rm E}} \tag{69}$$

Hence, by changing the order of integral, the ergodic secrecy rate can be re-expressed as

$$\overline{\mathcal{C}}_{\rm s\_\infty}^{(\kappa)} = \frac{1}{2\ln 2}\int_0^{\infty}\int_0^{x}\frac{1+\varphi_{\gamma_{\rm RE}}^{(\kappa)}(y)}{1+y}dy\,f_{\gamma_{\rm B}}(x)\,dx = \mathcal{G}_1+\mathcal{G}_2^{(\kappa)} \tag{70}$$

where

$$\mathcal{G}_1 = \frac{1}{2\ln 2}\int_0^{\infty}\ln(1+x)f_{\gamma_{\rm B}}(x)\,dx \tag{71}$$

and

$$\mathcal{G}_2^{(\kappa)} = \frac{1}{2\ln 2}\int_0^{\infty}\int_0^{x}\frac{\varphi_{\gamma_{\rm RE}}^{(\kappa)}(y)}{1+y}f_{\gamma_{\rm B}}(x)\,dydx \tag{72}$$

Now, in the following, we concentrate on the evaluations of $\mathcal{G}_1$ and $\mathcal{G}_2^{(\kappa)}$ in the high SNR regime, respectively. To begin with, taking derivative of (63), the PDF for $\gamma_{\rm B}$ can be derived as follows:

$$f_{\gamma_{\rm B}}(x) = f_{\gamma_{\rm AR}}(x)\left(1-\mathcal{F}_{\gamma_{\rm RB}}(x)\right)+f_{\gamma_{\rm RB}}(x)\left(1-\mathcal{F}_{\gamma_{\rm AR}}(x)\right) \tag{73}$$

On the other hand, when $\overline{\gamma}_{\rm B}\to\infty$, the PDF and CDF of $\overline{\gamma}_{\rm B}$ can be approximated respectively as

$$f_{\gamma_{\rm RB}}(x) \approx \left(\frac{m_{\rm B}}{\overline{\gamma}_{\rm B}}\right)^{A_{\rm B}m_{\rm B}}\frac{x^{A_{\rm B}m_{\rm B}-1}}{\Gamma(A_{\rm B}m_{\rm B})}\exp\left(-\frac{m_{\rm B}}{\overline{\gamma}_{\rm B}}x\right) \tag{74}$$

and

$$\mathcal{F}_{\gamma_{\rm RB}}(x) \approx 1-\exp\left(-\frac{m_{\rm B}x}{\overline{\gamma}_{\rm B}}\right)\sum_{n=0}^{m_{\rm B}A_{\rm B}-1}\frac{x^n}{n!}\left(\frac{m_{\rm B}}{\overline{\gamma}_{\rm B}}\right)^n \tag{75}$$

Thus, by pulling (12), (13), (74) and (75) into (73), then the PDF of $\overline{\gamma}_{\rm B}$ can be approximated as (76) with some mathematical operations.

Besides, when $\overline{\gamma}_{\rm B}\to\infty$, we have $\ln(1+\gamma_{\rm B})\approx\ln(\gamma_{\rm B})$. Finally, by inserting (76) and invoking [44, Eq.(4.352.1)], $\mathcal{G}_1$ is derived as (42), where $\psi(\cdot)$ is the digamma function [45].

Similarly, according to [46, Eq. (19)], $\mathcal{G}_2^{(\kappa)}$ is converted to

$$\mathcal{G}_2^{(\kappa)} \approx \frac{1}{2\ln 2}\int_0^{\infty}\frac{\varphi_{\gamma_{\rm E}}^{(\kappa)}(y)}{1+y}dy \tag{77}$$

Now, by substituting (68) to (77) for colluding eavesdropping, (69) to (77) for the non-colluding eavesdropping, resorting to [44, Eq. (3.353.5)] and performing some mathematical manipulations, we have the corresponding results as provided in (43) and (44). Eventually, by plugging $\mathcal{G}_1$ and $\mathcal{G}_2^{(\kappa)}$ into (70), the proof is completed.

References

[1] 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.

[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] 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.

[5] L. Wang, M. Elkashlan, J. Huang, R. chober, 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] 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.

[7] N. S. Ferdinand, D. B. da Costa, A. L. F. d. Almeida, and M. Latva-aho, "Secrecy outage performance of MISO wiretap channels with outdated CSI," in *Proc. IEEE International Commun. Conf. Workshops*, Sydney, Australia, Jun. 2014, pp. 789-793.

[8] X. Jiang, C. Zhong, X. Chen, T. Q. Duong, T. A. Tsiftsis, and Z. Zhang, "Secrecy performance of wirelessly powered wiretap channels," *IEEE Trans. Commu.*, accepted for publication, in 2016.

[9] T.-X. Zheng, H.-M. Wang, F. Liu, and M. H. Lee, "Outage constrained secrecy throughput maximization for DF relay networks, " *IEEE Trans. Commu.*, vol. 63, no. 5, pp. 1741-1755, May 2015.

$$\mathcal{F}_{\gamma_{\mathrm{AB}}}(x)=\begin{cases}1-\mathcal{S}_1\exp\left(-\left(\frac{m_{\mathrm{A}}}{\overline{\gamma}_{\mathrm{A}}}+\frac{m_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}}\right)x\right)\sum\limits_{k=0}^{A_{\mathrm{A}}m_{\mathrm{A}}-1}\frac{x^k}{k!}\left(\frac{m_{\mathrm{A}}}{\overline{\gamma}_{\mathrm{A}}}\right)^k\sum\limits_{n=0}^{m_{\mathrm{B}}A_{\mathrm{B}}-1}\frac{x^n}{n!}\left(\frac{m_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}}\right)^n, & x>\gamma_{\mathrm{T}}\\ 1-\exp\left(-\frac{m_{\mathrm{A}}x}{\overline{\gamma}_{\mathrm{A}}}\right)\sum\limits_{k=0}^{A_{\mathrm{A}}m_{\mathrm{A}}-1}\frac{x^k}{k!}\left(\frac{m_{\mathrm{A}}}{\overline{\gamma}_{\mathrm{A}}}\right)^k\left[1-\sum\limits_{t=0}^{N_{\mathrm{B}}}\binom{N_{\mathrm{B}}}{t}(-1)^t\exp\left(-\frac{m_{\mathrm{B}}t}{\overline{\gamma}_{\mathrm{B}}}x\right)\left(\sum\limits_{n=0}^{m_{\mathrm{B}}A_{\mathrm{B}}-1}\frac{x^n}{n!}\left(\frac{m_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}}\right)^n\right)^t\right], & x<\gamma_{\mathrm{T}}\end{cases} \tag{65}$$

$$f_{\gamma_{\mathrm{AB}}}(x)\approx\left(\frac{m_{\mathrm{A}}}{\overline{\gamma}_{\mathrm{B}}}\right)^{A_{\mathrm{A}}m_{\mathrm{A}}}\frac{x^{A_{\mathrm{A}}m_{\mathrm{A}}-1}}{\Gamma(A_{\mathrm{A}}m_{\mathrm{A}})}\exp\left(-\left(\frac{m_{\mathrm{A}}}{\overline{\gamma}_{\mathrm{A}}}+\frac{m_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}}\right)x\right)\sum_{n=0}^{m_{\mathrm{B}}A_{\mathrm{B}}-1}\frac{x^n}{n!}\left(\frac{m_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}}\right)^n+\left(\frac{m_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}}\right)^{A_{\mathrm{B}}m_{\mathrm{B}}}\frac{x^{A_{\mathrm{B}}m_{\mathrm{B}}-1}}{\Gamma(A_{\mathrm{B}}m_{\mathrm{B}})}\times\exp\left(-\left(\frac{m_{\mathrm{A}}}{\overline{\gamma}_{\mathrm{A}}}+\frac{m_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}}\right)x\right)\sum_{k=0}^{A_{\mathrm{A}}m_{\mathrm{A}}-1}\frac{x^k}{k!}\left(\frac{m_{\mathrm{A}}}{\overline{\gamma}_{\mathrm{B}}}\right)^k \tag{76}$$

[10] L. Fan, X. Lei, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, "Secure multiuser communications in multiple amplify-and-forward relay networks," *IEEE Trans. Commun.*, vol. 62, no. 9, pp. 3299-3310, Sep. 2014.

[11] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: State of the art and beyond," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 32-39, Dec. 2015.

[12] H.-M. Wang, M. Luo, X.-G. Xia, and Q. Yin, "Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI," *IEEE Signal Process. Lett.*, vol. 20, no.1, pp.39-42, Jan. 2013

[13] H.-M. Wang, M. Luo, Q. Yin, and X.-G. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Trans. Inf. Forensics and Security*, vol. 8, no. 12, pp. 2007-2020, Dec. 2013.

[14] C. Wang, H.-M. Wang, and X.-G. Xia, "Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks," in *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 589-605, Feb. 2015.

[15] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003-5011, Oct. 2009.

[16] I. Krikidis, "Opportunistic relay selection for cooperative networks with secrecy constraints," *IET Commun.*, vol. 4, no. 15, pp. 1787-1791, Oct. 2010.

[17] 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.

[18] H. Hui, A. L. Swindlehurst, G. Li, and J. Liang, "Secure relay and jammer selection for physical layer security," *IEEE Signal Process. Lett.*, vol. 22, no. 8, pp. 1147-1151, Aug. 2015.

[19] F. S. Al-Qahtani, C. Zhong, and H. Alnuweiri, "Opportunistic relay selection for secrecy enhancement in cooperative networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1756-1770, May. 2015.

[20] C. Kundu, S. Ghose, and R. Bose, "Secrecy outage of dual-hop regenerative multi-relay system with relay selection," *IEEE Trans. Wireless Commun.*, vol. 14, no. 8, pp. 4614-4625, Aug. 2015.

[21] T.-X. Zheng, H.-M. Wang, F. Liu, and M. H. Lee, "Outage constrained secrecy throughput maximization for DF relay networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1741-1755, May. 2015.

[22] 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.

[23] 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.

[24] 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 2015.

[25] 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, Canada, Sep. 2014, pp. 1-5.

[26] 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," *IET Electron. Lett.*, vol. 52, no. 9, pp. 720-722, Apr. 2016.

[27] 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.

[28] 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.*, accepted for publication, in 2016.

[29] 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 and Security*, vol. 10, no. 1, pp. 90-103, Jan. 2015.

[30] C. Wang and H.-M. Wang, "Robust joint beamforming and jamming for secure AF networks: Low-complexity design," *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 2192-2198, May. 2015.

[31] H. Hui, A. L. Swindlehurst, G. Li, and J. Liang, "Secure relay and jammer selection for physical layer security," *IEEE Signal Process. Lett.*, vol. 22, no. 8, pp. 1147-1151, Aug. 2015.

[32] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099-2111, Oct. 2013.

[33] V. N. Q. Bao, N. Linh-Trung, and M. Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 12, pp. 6076-6085, Dec. 2013.

[34] 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.*, vol. 13, no. 3, pp. 1281 - 1293, Jul. 2016.

[35] Y. Chen, W. Li, and H. Shu, "Wireless physical-layer security with multiple receivers and eavesdroppers: Outage probability and average secrecy capacity," in *Proc. IEEE Personal, Indoor, and Mobile Radio Commu. Conf.*, Hong Kong, China, Aug. 2015, pp. 662-667.

[36] D. B. da Costa and S. Aissa, "Cooperative dual-hop relaying systems with beamforming over Nakagami-m fading channels," *IEEE Trans. Wireless Commun.*, vol. 8, no. 8, pp. 3950-3954, Aug. 2009.

[37] N. Yang, M. Elkashlan, J. Yuan, and T. Shen, "On the SER of fixed gain amplify-and-forward relaying with beamforming in Nakagami-m fading," *IEEE Commun. Lett.*, vol. 14, no. 10, pp. 942-944, Oct. 2010.

[38] H. Phan, T. Q. Duong, M. Elkashlan, and H. J. Zepernick, "Beamforming amplify-and-forward relay networks with feedback delay and interference," *IEEE Signal Process. Lett.*, vol. 19, no. 1, pp. 16-19, Jan. 2012.

[39] N. Yang, P. L. Yeoh, M. Elkashlan, I. B. Collings, and Z. Chen, "Two-way relaying with multi-antenna sources: Beamforming and antenna selection," *IEEE Trans. Veh. Technol.*, vol. 61, no. 9, pp. 3996-4008, Nov. 2012.

[40] Y. Huang, F. Al-Qahtani, C. Zhong, Q. Wu, J. Wang, and H. Alnuweiri, "Performance analysis of multiuser multiple antenna relaying networks with co-channel interference and feedback delay," *IEEE Trans. Commun.*, vol. 62, no. 1, pp. 59-73, Jan. 2014.

[41] X. Wang, N. Yang, H. Zhang, T. M. Hoang, and T. A. Gulliver, "Generalised selection at multi-antenna sources in two-way relay networks," *IET Commun.*, vol. 10, no. 7, pp. 824-831, Apr. 2016.

[42] S. Modem and S. Prakriya, "Performance of analog network coding

based two-way EH relay with beamforming," in *Proc. IEEE Veh. Technol. Conf.*, Nanjing, China, May. 2016, pp. 1-5.
[43] 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.
[44] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. San Diego, CA, USA: Academic Press, 2007.
[45] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tables*, 9th ed. New York, NY, USA: Dover, 1972.
[46] 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.

Maoqiang Yang (S'15) 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. He has served as a TPC Member for IEEE WCSP 2016 and IEEE SigTelCom 2017.

Daoxing Guo (M'15) 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 (S'12-M'14) 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. Since 2016, he has been a Post-Doctoral Research Associate with the School of Information and Communication, Beijing University of Posts and Telecommunications, Beijing. His research interests focus on channel coding, MIMO communications systems, cooperative communications, physical layer security, and cognitive radio systems. He currently serves as an Associate Editor of KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS. 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 (107 articles) and presented at international conferences (105 papers).

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 ACCESS, 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 also a Ph.D. Supervisor with PLA University of Science and Technology. 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.