Received March 1, 2019, accepted March 23, 2019, date of publication March 29, 2019, date of current version April 11, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2907781

Secrecy Outage Performance for DF Buffer-Aided Relaying Networks With a Multi-Antenna Destination

CHEN WEI[1], WENDONG YANG[1], YUEMING CAI[1], (Senior Member, IEEE), XUANXUAN TANG[1], AND GUOQIN KANG[2]

[1]College of Communications Engineering, Army Engineering University of PLA, Nanjing 210007, China
[2]College of Information and Communication, National University of Defense Technology, Wuhan 430010, China

Corresponding author: Wendong Yang (ywd1110@163.com)

This work was supported in part by the National Science Foundations of China under Grant 61771487 and Grant 61371122, and in part by the Research Program of the National University of Defense Technology under Grant NO.ZS18-02-04.

ABSTRACT In this paper, we investigate the secrecy outage performance of decode-and-forward (DF) buffer-aided relaying networks with a multi-antenna destination in the presence of an eavesdropper. In order to take full advantage of the benefits provided by the multiple antennas at the destination and the available relays, we adopt the max-link relay selection scheme and propose a half-duplex and two full-duplex secure transmission schemes for secrecy improvement, i.e., 1) maximal-ratio combining (MRC), 2) maximal-ratio combining/cooperative jamming (MRC/CJ), and 3) zero-forcing beamforming/cooperative jamming (ZFB/CJ). For all proposed schemes, we present exact and asymptotic closed-form expressions of the secrecy outage probability by modeling the dynamic buffer state transitions as a Markov chain. Moreover, simple and informative asymptotic results are provided under both $L \not\to \infty$ and $L \to \infty$ scenarios (where L denotes the buffer size), from which we can obtain further insights on the secrecy diversity gain and the secrecy coding gain. The highlights of this paper can be summarized as follows: 1) Under $L \not\to \infty$ scenario, the secrecy diversity gains of all proposed schemes both reach M. When $L \to \infty$, the secrecy diversity gains of MRC, MRC/CJ and ZFB/CJ increase to $M(1+N_D)$, MN_D and $2M$ respectively, where M is the number of relays and N_D represents the number of antennas at the destination; 2) The secrecy coding gain of the system differs with different schemes, and it improves with the increase of M and N_D under both the two scenarios; and 3) Under the scenario $L \not\to \infty$, ZFB/CJ outperforms MRC and MRC/CJ across the entire signal-to-noise ratio (SNR) range of interest, however, when $L \to \infty$, ZFB/CJ outperforms MRC/CJ and MRC in the low SNR regime, while the opposite holds in the high SNR regime.

INDEX TERMS Buffer-aided relay, multi-antenna, full-duplex, secrecy outage probability, secrecy diversity gain, secrecy coding gain.

I. INTRODUCTION

Nowadays, cooperative communications through relay nodes has attracted enormous attention due to their abilities of increasing the effective data transmission rates and extending the coverage of wireless networks [1], [2]. For cooperative networks with multiple relay nodes, higher diversity gain and more efficient utilization of the system resources can be achieved by exploiting various relay selection schemes [3], [4]. In conventional relay networks, the selected relay receives data from source in the first time slot, and forwards it to the destination immediately in the next time slot [5]. That is to say, a prefixed schedule for data transmission or reception must be followed at the relays which caused that the best link may be unavailable in a fast-fading environment. In recent years, equipping data buffers at the relays has attracted more and more attention, due to its capacity of providing extra degrees of freedom and offering higher performance gains in terms of throughput and diversity [6]–[8]. Although the buffer-aided relaying introduces an additional delay and higher complexity, it is still a promising approach for delay insensitive cooperative networks.

Currently, buffer-aided relaying schemes have been proposed in numerous works [9]–[12]. In [11], the max-max

The associate editor coordinating the review of this manuscript and approving it for publication was Yongpeng Wu.

relay selection (MMRS) scheme was proposed for decode-and-forward (DF) cooperative networks. In this protocol, the relay with the best source-to-relay link can be chosen for reception in odd time slots, while the relay with the best relay-to-destination link can be chosen for transmission in even time slots, which can achieve the diversity gain of M (M is the number of relays). Although the MMRS protocol improves the throughput or signal-to-noise ratio (SNR) gain compared with conventional relaying protocol, its diversity gain is limited to M. To overcome the above problem, Krikidis *et al.* in [12] proposed the max-link relay selection scheme, which adaptively activates the link with best channel condition at each time slot. That is to say, the best link among all available source-to-relay and relay-to-destination links can be selected for transmission or reception and hence, a diversity gain of $2M$ is achieved.

The broadcast nature of the wireless medium makes the security of data transmission being a vital issue in wireless networks [13]. As such, a number of researches have investigated the security of buffer-aided relaying systems from the physical layer perspective [14]–[16]. In [14], a new max-ratio relay selection scheme was proposed to improve the confidentiality of transmission in the buffer-aided DF cooperative wireless networks. The authors in [15] investigated the secure transmission of buffer-aided cognitive relay networks, and a closed-form expression of secrecy outage probability was derived to evaluate secrecy performance. In [16], a buffer-aided joint transmit antenna and relay selection (JTARS) scheme was proposed to improve the secrecy performance of multi-relay multiple-input multiple-output (MIMO) cooperative systems in the presence of a passive eavesdropper, and closed-form expressions of exact and asymptotic secrecy outage probability were obtained to assess the impact of different parameters on the secrecy performance.

To further prevent information from being intercepted by eavesdropper and strengthen the security of cooperative networks, the destination jamming scheme was investigated in several works [17]–[19]. The authors in [18] proposed a joint source, relay and destination jamming precoding optimization scheme to improve the secrecy performance of the amplify-and-forward (AF) MIMO untrusted relay networks. Furthermore, the idea of introducing the full-duplex technique into the destination jamming scheme was investigated in [19]. Specifically, the joint transmitting and receiving beamforming scheme was utilized at the destination to improve system security where the destination node can receive signals and send a jamming signal to eavesdropper simultaneously. From the above, combining buffer-aided relaying with the destination jamming scheme can not only improve the transmission capacity of the system, but also provide an effective way to improve the system secrecy performance. To the best of our knowledge, the destination jamming scheme has not been examined in buffer-aided relaying networks before.

Inspired by the observations above, we consider a DF buffer-aided relaying network with a multi-antenna destination in the presence of an eavesdropper. To exploit the extra degrees of freedom provided by the multiple antennas at the destination, we propose a half-duplex scheme and two full-duplex destination jamming schemes, i.e., 1) maximal-ratio combining (MRC), 2) maximal-ratio combining/cooperative jamming (MRC/CJ), 3) zero forcing beamforming/cooperative jamming (ZFB/CJ). The contributions of this paper mainly lie in the following:

1) We derive novel exact and asymptotic closed-form expressions for the secrecy outage probability of the considered system with MRC, which provides an efficient means to assess the impact of key parameters on the secrecy performance. To gain more deep insights, simple asymptotic results are also derived in the high SNR regime considering $L \not\to \infty$ and $L \to \infty$ scenarios (where L denotes the buffer size). Based on this, the secrecy diversity gain and the secrecy coding gain are investigated furthermore, and the results suggest that they are affected by the buffer size, the number of relays and the number of destination's antennas.
2) For destination jamming schemes, i.e., MRC/CJ and ZFB/CJ, exact and asymptotic expressions for the secrecy outage probability in closed-form are obtained respectively. Moreover, the secrecy diversity gain and the secrecy coding gain of these two schemes are analyzed based on the derived asymptotic expressions under $L \not\to \infty$ and $L \to \infty$ scenarios. Specifically, the secrecy diversity gains of these two schemes both reach M under the $L \not\to \infty$ scenario. When $L \to \infty$, the secrecy diversity gain of ZFB/CJ is $2M$, while MRC/CJ can achieve MN_D (N_D represents the number of destination's antennas). Moreover, the buffer size, the number of relays and the number of destination's antennas also affect the secrecy coding gain.
3) The results demonstrate that increasing the number of antennas N_D can improve the secrecy performance of all the proposed schemes both under the $L \not\to \infty$ and $L \to \infty$ scenarios. Moreover, ZFB/CJ outperforms MRC and MRC/CJ across the entire SNR range of interest when $L \not\to \infty$, however, under the scenario $L \to \infty$, ZFB/CJ outperforms MRC/CJ and MRC in the low SNR regime, while the opposite holds in the high SNR regime.

The remainder of the paper is organized as follows. In Section II, the system model is introduced. Section III investigates the exact secrecy outage probability of the system. Asymptotic secrecy outage probability in the high SNR regime is provided in Section IV. Section V presents simulation results. Finally, we summarize the conclusions of this paper in Section VI.

Notation: In this paper, lower-case and upper-case boldface symbols are utilized to denote vectors and matrices respectively. $\|\cdot\|$ and $\|\cdot\|_F$ denote the Euclidean or L_2 vector norm and the Frobenius norm. $(\cdot)^T$ and $(\cdot)^\dagger$ represent the transpose operation and the conjugate transpose operation. $F_\gamma(\cdot)$ and $f_\gamma(\cdot)$ denote the cumulative distribution function (CDF) and

the probability density function (PDF) of the random variable γ respectively.

II. SYSTEM MODEL

We consider a dual-hop multi-relay network as shown in Fig. 1, which consists of a source node S, a multi-antenna destination node D, a set of M DF relays $\{R_k\}_{k=1}^{M}$ and an eavesdropper E. All the nodes are equipped with a single antenna except D, which is equipped with N_D ($N_D > 1$) antennas. It is worth noting that the assumed scenario can be considered as an uplink network, which is similar to [20]. In addition, we assume that each relay is equipped with a data buffer B_k of finite size L, and the packets in the buffer follow the ''first-in-first-out'' rule. It is also assumed that all of the relay nodes operate in the half-duplex time-division mode and the direct link between S and D is not available due to severe path loss or shadowing effects caused by some obstacles [14].

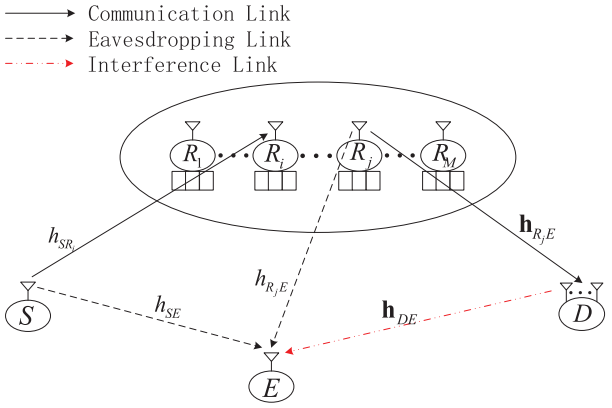

FIGURE 1. System Model.

Without loss of generality, we denote the channel coefficient of link $a \rightarrow b$ as h_{ab}, which is a complex Gaussian random variable with zero mean and variance λ_{ab}. Hence, the channel gain $|h_{ab}|^2$ is an exponentially distributed random variable. Moreover, all the channels are subject to independent and nonidentical quasi-static flat Rayleigh fading so that the channel coefficients remain unchanged during the coherent time of the channels [16], [21].

A. THE TRANSMISSION SCHEME

In this subsection, we present a half-duplex scheme and two destination jamming schemes to fully exploit the advantage of multi-antenna at D. For the reader's convenience, we utilize capital letters A, B and C represent the MRC, MRC/CJ and ZFB/CJ schemes respectively.

1) THE MRC SCHEME

The whole transmission process between S and D is completed within two hops. In the first hop, S sends the signal to the selected relay while intercepted by the eavesdropper E. Hence, the received SNR at the $i-th$ relay and E can be respectively expressed as

$$\gamma_{SR_i}^{A} = \frac{P_S \left|h_{SR_i}\right|^2}{\sigma_{R_i}^2}, \tag{1}$$

$$\gamma_{SE}^{A} = \frac{P_S \left|h_{SE}\right|^2}{\sigma_E^2}, \tag{2}$$

where P_S denotes the transmit power of S, $\left|h_{SR_i}\right|^2$ and $|h_{SE}|^2$ represent the channel gains of link $S \rightarrow R_i$ and $S \rightarrow E$, $\sigma_{R_i}^2$ and σ_E^2 are the variance of the additive white Gaussian noises (AWGNs) at R_i and E.

In the second hop, the destination node D adopts the MRC scheme to strengthen the signal reception. Therefore, the received SNR at D and E are given by

$$\gamma_{R_jD}^{A} = \frac{P_R \left\|h_{R_jD}^{1}\right\|^2}{\sigma_D^2}, \tag{3}$$

$$\gamma_{R_jE}^{A} = \frac{P_R \left|h_{R_jE}\right|^2}{\sigma_E^2}, \tag{4}$$

where P_R represents the transmit power of R_j, $\left|h_{R_jE}\right|^2$ is the channel gain of link $R_j \rightarrow E$ and $h_{R_jD}^{1} = \left[h_{R_jD_1}, h_{R_jD_2} \cdots, h_{R_jD_{N_D}}\right]^T$ denotes the $N_D \times 1$ channel vector between R_j and D. σ_D^2 is the variance of AWGN at D.

2) THE MRC/CJ SCHEME

For the MRC/CJ scheme, the destination D performs in the full-duplex mode, where there are $N_D - 1$ receiving antennas and one jamming antenna. The first hop of MRC/CJ is the same as the MRC scheme. Hence we have $\gamma_{SR_i}^{B} = \gamma_{SR_i}^{A}$, and $\gamma_{SE}^{B} = \gamma_{SE}^{A}$. In the second hop, D receives signal from the selected relay utilizing MRC linear processing scheme and sends jamming signal from the jamming antenna simultaneously. However, it is critical for full-duplex communication to measure and suppress the self-interference (SI) accurately. With advances on antenna design and signal processing, the SI can be significantly canceled or sufficiently suppressed to a very low level and made negligible by using existing SI cancellation (SIC) technologies, such as directional SI suppression, antenna separation, analog cancellation and digital cancellation, and thus the full-duplex mode has attracted a lot of attention from the research community [22], [23]. In order to facilitate the following analysis, we assume that the SI at D can be completely suppressed [24]. Hence the received SNR at D and signal-to-interference-plus-noise ratio (SINR) at E can be respectively expressed as

$$\gamma_{R_jD}^{B} = \frac{P_R \left\|h_{R_jD}^{2}\right\|^2}{\sigma_D^2}, \tag{5}$$

$$\gamma_{R_jE}^{B} = \frac{P_R \left|h_{R_jE}\right|^2}{P_D \left|h_{DE}\right|^2 + \sigma_E^2}, \tag{6}$$

where $h_{R_jD}^2 = \left[h_{R_jD_1}, h_{R_jD_2} \cdots, h_{R_jD_{N_D-1}}\right]^T$ denotes the $(N_D-1)\times 1$ channel vector between the N_D-1 receiving antennas of D and R_j, P_D is the transmit power of D, $|h_{DE}|^2$ represents the channel gain between the jamming antenna of D and E.

3) THE ZFB/CJ SCHEME

For the ZFB/CJ scheme, we assume that the destination D where there is one antenna for receiving signal from the source node and N_D-1 antennas for transmitting jamming signal. In the first hop, S sends the signal to the selected relay while the useful information is intercepted by eavesdropper E and we also have $\gamma_{SR_i}^C = \gamma_{SR_i}^A$. Simultaneously, D transmits a jamming signal to degrade the quality of eavesdropper's channel. The ZFB scheme is applied to null the undesirable interference at the selected receiving relay. Thus, according to the ZFB principles, the problem formulation for finding the optimal weight vector w_{ZF} is given by

$$\begin{aligned} &\max_{w_{ZF}} \left|h_{DE}^{\dagger} w_{ZF}\right| \\ &s.t. : \left|h_{DR_i}^{\dagger} w_{ZF}\right| = 0 \\ &\quad \|w_{ZF}\|_F = 1, \end{aligned} \tag{7}$$

where $h_{DE} = \left[h_{D_1E}, h_{D_2E} \cdots, h_{D_{N_D-1}E}\right]^T$ denotes the $(N_D-1)\times 1$ channel vector between the N_D-1 jamming antennas of D and E. Similarly, h_{DR_i} is the channel vector between the N_D-1 jamming antennas of D and R_i. Then, by utilizing projection matrix theory [25], the optimal weight vector that satisfies the above optimization method can be expressed as

$$w_{ZF} = \frac{T^{\perp} h_{DE}}{\left\|T^{\perp} h_{DE}\right\|}, \tag{8}$$

where $T^{\perp} = \left(I - h_{DR_i}\left(h_{DR_i}^{\dagger} h_{DR_i}\right)^{-1} h_{DR_i}^{\dagger}\right)$ denotes the projection idempotent matrix with rank N_D-2. Thus, the received SINR at E is given by

$$\gamma_{SE}^C = \frac{P_S |h_{SE}|^2}{P_D \left|h_{DE}^{\dagger} w_{ZF}\right|^2 + \sigma_E^2}, \tag{9}$$

In the second hop, the destination D receives the signal from the selected relay while send a jamming signal to the eavesdropper E by using maximal-ratio transmission (MRT) processing approach. The received SNR at D and SINR at E are respectively given by

$$\gamma_{R_jD}^C = \frac{P_R \left|h_{R_jD}\right|^2}{\sigma_D^2}, \tag{10}$$

$$\gamma_{R_jE}^C = \frac{P_R \left|h_{R_jE}\right|^2}{P_D \|h_{DE}\|^2 + \sigma_E^2}, \tag{11}$$

where $\left|h_{R_jD}\right|^2$ represents the channel gain between the receiving antenna of D and R_j.

According to [26], [27], the achievable secrecy rate of the first and second hop can be formulated as

$$C_{SRE}^{\star} = \left[\log_2\left(1+\gamma_{SR_i}^{\star}\right) - \log_2\left(1+\gamma_{SE}^{\star}\right)\right]^+, \tag{12}$$

$$C_{RDE}^{\star} = \left[\log_2\left(1+\gamma_{R_jD}^{\star}\right) - \log_2\left(1+\gamma_{R_jE}^{\star}\right)\right]^+, \tag{13}$$

where $\star \in \{A, B, C\}$, $[x]^+ = \max\{0, x\}$.

B. THE MAX-LINK RELAY SELECTION SCHEME

In this subsection, the max-link relay selection scheme is adopted to strengthen the secrecy performance of the system [12]. Before delving into analyzing the max-link scheme, we first model the number of the data packets in each buffer as a state. Hence $s_n = [\varphi_n(1), \varphi_n(2), \cdots, \varphi_n(M)]^T$ denotes the $n-th$ state of all possible states, where $\varphi_n(k) \in \{0, 1, \cdots, L\}$ $(1 \le k \le M)$ represents the number of data packets in buffer B_k at state s_n.

Then, the number of available links in the first and second hop at state s_n are respectively given by $M_{1,n} = \sum_{k=1}^{M} \phi_{1,n}(k)$ and $M_{2,n} = \sum_{k=1}^{M} \phi_{2,n}(k)$, where $\phi_{1,n}(k) = \begin{cases} 1, & \varphi_n(k) \neq L \\ 0, & \varphi_n(k) = L \end{cases}$ and $\phi_{2,n}(k) = \begin{cases} 1, & \varphi_n(k) \neq 0 \\ 0, & \varphi_n(k) = 0 \end{cases}$. More specifically, when $\varphi_n(k) = L$ or $\varphi_n(k) = 0$, it means that the relay R_k can no longer be selected for reception or transmission. Therefore, $\phi_{1,n}(k) = 0$ and $\phi_{2,n}(k) = 0$ represent the corresponding link is not available at state s_n. On the contrary, $\phi_{1,n}(k) = 1$ and $\phi_{2,n}(k) = 1$ mean that the corresponding link is available, that is to say, the relay R_k can be used for reception or transmission.

Based on the above definition, we will present the expression of the max-link relay selection scheme in the following part. The main idea of the max-link scheme is to select the strongest link for data transmission among all source-to-relay and relay-to-destination available links. It can be mathematically expressed as

$$R^* = \arg\max\left\{\gamma_{SR'_{M_{1,n}}}, \gamma_{R''_{M_{2,n}}D}\right\}, \tag{14}$$

where $\gamma_{SR'_{M_{1,n}}} = P_S \left|h_{SR'_{M_{1,n}}}\right|^2 / \sigma_R^2$ and $\left|h_{SR'_{M_{1,n}}}\right|^2 = \max_{\varphi_n(i)\neq L}\left\{\left|h_{SR_i}\right|^2\right\}$ denote the maximum SNR and the best channel gain of the $M_{1,n}$ available links respectively in the first hop. $\gamma_{R''_{M_{2,n}}D} \in \left\{\gamma_{R''_{M_{2,n}}D}^A, \gamma_{R''_{M_{2,n}}D}^B, \gamma_{R''_{M_{2,n}}D}^C\right\}$, for the MRC or MRC/CJ scheme, $\gamma_{R''_{M_{2,n}}D}^A = P_R \left\|h_{R''_{M_{2,n}}D}^1\right\| / \sigma_D^2$ and $\gamma_{R''_{M_{2,n}}D}^B = P_R \left\|h_{R''_{M_{2,n}}D}^2\right\| / \sigma_D^2$ represent the maximum SNR, $\left\|h_{R''_{M_{2,n}}D}^1\right\| = \max_{\varphi_n(j)\neq 0}\left\{\left\|h_{R_jD}^1\right\|\right\}$ and $\left\|h_{R''_{M_{2,n}}D}^2\right\| = \max_{\varphi_n(j)\neq 0}\left\{\left\|h_{R_jD}^2\right\|\right\}$ denote the strongest channel vector norm

of all available $M_{2,n}$ links. Similarly, for ZFB/CJ scheme, $\gamma^{C}_{R''_{M_{2,n}}D} = P_R \left|h_{R''_{M_{2,n}}D}\right|^2 / \sigma_D^2$ also represents the maximum SNR, and $\left|h_{R''_{M_{2,n}}D}\right|^2 = \max\limits_{\varphi_n(j)\neq 0} \left\{\left|h_{R_jD}\right|^2\right\}$ denotes the best channel gain among $M_{2,n}$ available links in the second hop.

According to the relay selection scheme above, we can easily find that the best relay R^* is always selected for data transmission according to the instantaneous quality of the links and the state of the buffer at the relays. Specifically, if the source-to-relay link is available, i.e., the corresponding buffer is not full, meanwhile, the corresponding channel gain is best among all available links, hence the relay R^* is selected for reception. In that case, S transmits the data packet to the selected relay R^*, R^* receives and decodes the data packet while intercepted by E. At the meantime, the packet can be stored in the buffer B^*, hence, the number of the packets in buffer B^* will be increased by one. Similarly, when R^* is chosen for transmission, D receives and decodes the data packet successfully, buffer B^* discards the packet and the number of the packets correspondingly decreases by one.

III. EXACT SECRECY OUTAGE ANALYSIS

This section investigates the exact secrecy outage analysis for DF buffer-aided relaying networks with a multi-antenna destination. The secrecy outage probability is defined as the probability that the achievable secrecy rate is less than the predefined secrecy rate $R_s\,(bit/s/Hz)$. The secrecy outage probability of this system can be represented as [12]

$$P_{out}\left(\gamma_{th}\right) = \sum_{n=1}^{N} \boldsymbol{\pi}_n P_{out,n}\left(\gamma_{th}\right), \tag{15}$$

where $N = (L+1)^M$ is the total number of states, $\boldsymbol{\pi}_n$ and $P_{out,n}\left(\gamma_{th}\right)$ denote the stationary distribution probability and the secrecy outage probability at state s_n, and $\gamma_{th} \triangleq 2^{2R_s}$ is the secrecy outage threshold. It is worth noting that the exponential term is "$2R_s''$ due to the whole transmission process is divided into two time slots.

Next, we will proceed with the secrecy outage probability of three schemes in the following subsections.

A. PRELIMINARIES

Before delving into analyzing the secrecy outage performance of the proposed transmission schemes, we first define random variables $X = \left|h_{SR'_{M_{1,n}}}\right|^2$ and $Y = \left\|h^1_{R''_{M_{2,n}}D}\right\|^2$. Moreover, for the tractability of analysis, we denote $\bar{\gamma}_{SR} = E\left(\gamma_{SR_i}\right)$, $\bar{\gamma}_{RD} = E\left(\gamma_{R_jD}\right)$, $\bar{\gamma}_{SE} = E\left(\gamma_{SE}\right)$, $\bar{\gamma}_{RE} = E\left(\gamma_{R_jE}\right)$ and $\bar{\gamma}_{DE} = E\left(\gamma_{DE}\right)$ and the noise variance is $\sigma^2 = 1$. Then we present the CDF or PDF of these random variables in the following analysis.

Lemma 1: The CDF of X is given by

$$F_X(x) = \sum_{s=0}^{M_{1,n}-1} \frac{M_1(s)}{N_1(s)} \left(1 - e^{-N_1(s)x}\right) \tag{16}$$

where $M_1(s) = \binom{M_{1,n}-1}{s} \frac{(-1)^s M_{1,n} P_S}{\bar{\gamma}_{SR}}$ and $N_1(s) = \frac{(s+1)P_S}{\bar{\gamma}_{SR}}$.

Proof: The proof can be found in [28]. ■

Lemma 2: The CDF of Y can be expressed as

$$F_Y(y) = \sum_{r_0+r_1+\cdots+r_{N_D}=M_{2,n}} \frac{M_{2,n}!}{r_0! r_1! \cdots r_{N_D}!} \times \frac{(-1)^{M_{2,n}-r_0}}{\prod\limits_{m=1}^{N_D} [\Gamma(m)]^{r_m}} \left(\frac{P_R y}{\bar{\gamma}_{RD}}\right)^{T^1_{RD}} e^{-\frac{(M_{2,n}-r_0)P_R y}{\bar{\gamma}_{RD}}} \tag{17}$$

where $T^1_{RD} = \sum\limits_{m=1}^{N_D} (m-1) r_m$, and $r_0, r_1 \cdots r_{N_D} \in \{0, 1, \cdots M_{2,n}\}$.

Proof: Without loss of generality, we define $Y_1 = \left\|h^1_{R_jD}\right\|^2$. According to [29], we find that Y_1 is a chi-squared random variable with $2N_D$ degrees of freedom if D adopts MRC processing. Hence its CDF is given by

$$F_{Y_1}(y) = 1 - \sum_{m=1}^{N_D} \left(\frac{P_R y}{\bar{\gamma}_{RD}}\right)^{m-1} \frac{1}{\Gamma(m)} e^{-\frac{P_R y}{\bar{\gamma}_{RD}}}, \tag{18}$$

Noticing that there is $M_{2,n}$ available relays for transmission, the CDF of Y can be further expressed as $F_Y(y) = \left[F_{Y_1}(y)\right]^{M_{2,n}}$. Then, utilizing the multinomial theorem, the CDF of Y can be easily derived. ■

B. THE MRC SCHEME

From (15), in order to derive the secrecy outage probability of MRC, we will analysis $P^A_{out,n}\left(\gamma_{th}\right)$ first. For the notation convenience, we define $\gamma^A_{SR'_{M_{1,n}}E} = \left(1 + \gamma^A_{SR'_{M_{1,n}}}\right) / \left(1 + \gamma^A_{SE}\right)$ and $\gamma^A_{R''_{M_{2,n}}DE} = \left(1 + \gamma^A_{R''_{M_{2,n}}D}\right) / \left(1 + \gamma^A_{R''_{M_{2,n}}E}\right)$. According to [16], the secrecy outage probability at state s_n under the MRC scheme is given by

$$P^A_{out,n}\left(\gamma_{th}\right) = F_{\gamma^A_{SR'_{M_{1,n}}E}}\left(\gamma_{th}\right) \cdot F_{\gamma^A_{R''_{M_{2,n}}DE}}\left(\gamma_{th}\right) \tag{19}$$

Theorem 1: The CDF of $\gamma^A_{SR'_{M_{1,n}}E}$ and $\gamma^A_{R''_{M_{2,n}}DE}$ are respectively given by

$$F_{\gamma^A_{SR'_{M_{1,n}}E}}(x) = \sum_{s=0}^{M_{1,n}-1} \frac{M_1(s)}{N_1(s)} \left[1 - \frac{P_S e^{-\frac{N_1(s)(x-1)}{P_S}}}{P_S + N_1(s)\bar{\gamma}_{SE} x}\right] \tag{20}$$

$$F_{\gamma^A_{R''_{M,n}DE}}(x) = \sum_{r_0+r_1+\cdots+r_{N_D}=M_{2,n}} \sum_{s=0}^{T^1_{RD}} \left(T^1_{RD} s\right)$$

$$\times \frac{M_{2,n}!}{r_0!r_1!\cdots r_{N_D}!}\frac{(-1)^{M_{2,n}-r_0}}{\prod_{m=1}^{N_D}[\Gamma(m)]^{r_m}}\left(\frac{P_R}{\bar{\gamma}_{RD}}\right)^{T_{RD}^1}\frac{P_R}{\bar{\gamma}_{RE}}$$
$$\times \left(\frac{x-1}{P_R}\right)^{T_{RD}^1-s}\frac{e^{-\frac{(M_{2,n}-r_0)(x-1)}{\bar{\gamma}_{RD}}}x^s s!}{\left[\frac{P_R}{\bar{\gamma}_{RE}}+\frac{(M_{2,n}-r_0)P_R x}{\bar{\gamma}_{RD}}\right]^{s+1}} \quad (21)$$

Proof: See Appendix A. ■

Furthermore, note that for the MRC scheme, the probabilities of selecting the source-to-relay and relay-to-destination link are not equal, which is different from [12]. To make the following analysis tractable, we denote $P_{RD,n}^A$ as the probabilities to select the relay-to-destination link at state s_n under the MRC scheme. We also divide the sets of states which can be transferred from state s_n within one step into two sets, denoted as Ω_n^1 and Ω_n^2. If the source-to-relay link is selected, the buffer state will transfer from state s_n to a certain state in Ω_n^1. Similarly, if the relay-to-destination link is chosen, the buffer state will transfer to one of states in Ω_n^2.

***Theorem** 2*: The probability to select the relay-to-destination link at state s_n under the MRC scheme is expressed as (22), as shown at the bottom of this page.

Proof: If the buffers are full or empty, i.e., $M_{1,n}=0$ or $M_{2,n}=0$, it is clear that $P_{RD,n}^A=1$ and $P_{RD,n}^A=0$ always holds. When $M_{1,n}M_{2,n}\neq 0$, the relay-to-destination link is selected if the SNR of the second hop is higher than the first hop, which can be expressed as

$$P_{RD,n}^A = \Pr\left(\gamma_{SR'_{M_{1,n}}}^A < \gamma_{R''_{M_{2,n}}D}^A\right) = \int_0^\infty F_X\left(\frac{P_R y}{P_S}\right) f_Y(y)\,dy \quad (23)$$

The PDF of Y can be derived by taking the derivative of $F_Y(y)$ with respect to y. Substituting (16) and the PDF of Y into (23), the desired result can be derived as in (22). ■

Now, we turn our attention to the stationary distribution probability under the MRC scheme $\boldsymbol{\pi}^A$. Firstly, we model the state transition of the buffer as a Markov chain according to [12]. Without loss of generality, we denote $A^A \in^{N\times N}$ as the state transition matrix of the MRC scheme, where the entry $A_{v,n}^A = \Pr[T(t+1)=s_v \,|\, T(t)=s_n]$ is the probability of moving from state s_n at time slot t to state s_v at time slot $t+1$, s_v represents one of the elements in Ω_n^1 or Ω_n^2.

Specifically, if there is no change in buffer state, i.e., $s_v=s_n$, the data packet is not successfully received and decoded, in other words, an outage event occurs. On the other hand, when $s_v\in\Omega_n^1$ or $s_v\in\Omega_n^2$, it means that the current state changes to another state within one step, that is to say, data transmission is completed between the corresponding nodes. From the analysis above, A^A can be further expressed as

$$A_{v,n}^A = \begin{cases} P_{out,n}^A(\gamma_{th}), & s_v = s_n \\ \frac{\left(1-P_{out,n}^A(\gamma_{th})\right)\left(1-P_{RD,n}^A\right)}{M_{1,n}}, & s_v\in\Omega_n^1 \\ \frac{\left(1-P_{out,n}^A(\gamma_{th})\right)P_{RD,n}^A}{M_{2,n}}, & s_v\in\Omega_n^2 \\ 0, & else \end{cases} \quad (24)$$

Then, we can obtain the following key result by utilizing the analysis above.

***Theorem** 3*: The stationary distribution probability vector of the MRC scheme can be represented as

$$\boldsymbol{\pi}^A = \left(A^A - I + Q\right)^{-1} b. \quad (25)$$

where $\boldsymbol{\pi}^A = \left[\boldsymbol{\pi}_1^A, \boldsymbol{\pi}_2^A\cdots,\boldsymbol{\pi}_N^A\right]^T$, $b=(1,1,\cdots,1)^T$, I is the identity matrix and Q is the all-ones matrix.

Proof: The proof can be found in [12]. ■

It is worth noting that the closed-form expression of secrecy outage probability under the MRC scheme can be easily derived by substituting (19) and (25) into (15) and performing some mathematical manipulations, which provides an efficient way to evaluate the system secrecy performance.

C. THE MRC/CJ SCHEME

The secrecy outage probability at state s_n under the MRC/CJ scheme is given by

$$P_{out,n}^B(\gamma_{th}) = F_{\gamma_{SR'_{M_{1,n}}E}^B}(\gamma_{th})\cdot F_{\gamma_{R''_{M_{2,n}}DE}^B}(\gamma_{th}) \quad (26)$$

***Theorem** 4*: The CDF of $\gamma_{SR'_{M_{1,n}}E}^B$ and $\gamma_{R''_{M_{2,n}}DE}^B$ can be respectively expressed as

$$F_{\gamma_{SR'_{M_{1,n}}E}^B}(x) = \sum_{s=0}^{M_{1,n}-1}\frac{M_1(s)}{N_1(s)}\left[1-\frac{P_S e^{-\frac{N_1(s)(x-1)}{P_S}}}{P_S+N_1(s)\bar{\gamma}_{SE}x}\right] \quad (27)$$

$$F_{\gamma_{R''_{M_{2,n}}DE}^B}(x) = \sum_{r_0+r_1+\cdots+r_{N_D-1}=M_{2,n}}\sum_{s=0}^{T_{RD}^2}\binom{T_{RD}^2}{s}$$

$$P_{RD,n}^A = \begin{cases} 1, & M_{1,n}=0 \\ \sum_{s=0}^{M_{1,n}-1}\frac{M_1(s)}{N_1(s)}\left[1-\sum_{r_0+r_1+\cdots+r_{N_D}=M_{2,n}-1}\frac{(M_{2,n}-1)!M_{2,n}(-1)^{M_{2,n}-1-r_0}P_R^{T_{RD}^1}(T_{RD}^1+N_D-1)!}{r_0!r_1!\cdots r_{N_D}!\Gamma(N_D)\prod_{m=1}^{N_D}[(\Gamma(m))]^{r_m}\bar{\gamma}_{RD}^{T_{RD}^1}\left[\frac{P_R N_1(s)}{P_S}+\frac{(M_{2,n}-r_0)P_R}{\bar{\gamma}_{RD}}\right]^{T_{RD}^1+N_D}}\right], & M_{1,n}M_{2,n}\neq 0 \\ 0, & M_{2,n}=0 \end{cases} \quad (22)$$

$$P^B_{RD,n}=\begin{cases}\sum\limits_{s=0}^{M_{1,n}-1}\frac{M_1(s)}{N_1(s)}\left[1-\sum\limits_{\substack{r_0+r_1+\cdots+r_{N_D-1}\\=M_{2,n}-1}}\frac{(M_{2,n}-1)!M_{2,n}(-1)^{M_{2,n}-1-r_0}P_R^{T^2_{RD}}(T^2_{RD}+N_D-2)!}{r_0!r_1!\cdots r_{N_D-1}!\Gamma(N_D-1)\prod\limits_{m=1}^{N_D-1}[(\Gamma(m))]^{r_m}\bar{\gamma}_{RD}^{T^2_{RD}}\left[\frac{P_RN_1(s)}{P_S}+\frac{(M_{2,n}-r_0)P_R}{\bar{\gamma}_{RD}}\right]^{T^2_{RD}+N_D-1}}\right], & M_{1,n}M_{2,n}\neq 0\\ 1, & M_{1,n}=0\\ 0, & M_{2,n}=0\end{cases} \quad (30)$$

$$\times\frac{M_{2,n}!}{r_0!r_1!\cdots r_{N_D-1}!}\frac{(-1)^{M_{2,n}-r_0}}{\prod\limits_{m=1}^{N_D-1}[\Gamma(m)]^{r_m}}\left(\frac{P_R}{\bar{\gamma}_{RD}}\right)^{T^2_{RD}}$$
$$\times\frac{e^{-\frac{(M_{2,n}-r_0)(x-1)}{\bar{\gamma}_{RD}}}x^ss!}{\bar{\gamma}_{DE}}\left(\frac{x-1}{P_R}\right)^{T^2_{RD}-s}\left(\frac{\bar{\gamma}_{RE}}{P_RP_D}\right)^s\times\Lambda \quad (28)$$

where $T^2_{RD}=\sum\limits_{m=1}^{N_D-1}(m-1)r_m$, $r_0, r_1\cdots r_{N_D-1}\in\{0,1,\cdots M_{2,n}\}$ and Λ is given by

$$\Lambda=\begin{cases}e^{\varepsilon\kappa}Ei(-\varepsilon\kappa)(P_D\varepsilon-1)+\frac{P_D}{\kappa}, & s=0\\ e^{\varepsilon\kappa}Ei(-\varepsilon\kappa)(\kappa-P_D-P_D\varepsilon\kappa)+\frac{1}{\varepsilon}-P_D, & s=1\\ (1-P_D\varepsilon)\left[\sum\limits_{k=1}^{s}\frac{(k-1)!(-\kappa)^{s-k}}{s!\varepsilon^k}-\frac{(-\kappa)^se^{\varepsilon\kappa}Ei(-\varepsilon\kappa)}{s!}\right]\\ +P_D\left[\sum\limits_{k=1}^{s-1}\frac{(k-1)!(-\kappa)^{s-k-1}}{(s-1)!\varepsilon^k}-\frac{(-\kappa)^{s-1}e^{\varepsilon\kappa}Ei(-\varepsilon\kappa)}{(s-1)!}\right], & s>1\end{cases} \quad (29)$$

with $\varepsilon=\frac{(M_{2,n}-r_0)x\bar{\gamma}_{RE}}{P_D\bar{\gamma}_{RD}}+\frac{1}{P_D}$, $\kappa=\frac{P_D}{\bar{\gamma}_{DE}}$ and $Ei(\cdot)$ being the exponential integral function [30, eq. (8.211.1)].

Proof: See Appendix B. ■

***Theorem** 5*: The probability to select the relay-to-destination link at state s_n under the MRC/CJ scheme is given by (30), as shown at the top of this page.

Proof: The proof follows similar lines as that of **Theorem 2**, hence is omitted. ■

Following the similar analysis as MRC, we can also obtain the state transition matrix and stationary distribution probability vector of MRC/CJ, and they are expressed as

$$A^B_{v,n}=\begin{cases}P^B_{out,n}(\gamma_{th}), & s_v=s_n\\ \frac{\left(1-P^B_{out,n}(\gamma_{th})\right)\left(1-P^B_{RD,n}\right)}{M_{1,n}}, & s_v\in\Omega^1_n\\ \frac{\left(1-P^B_{out,n}(\gamma_{th})\right)P^B_{RD,n}}{M_{2,n}}, & s_v\in\Omega^2_n\\ 0, & else\end{cases} \quad (31)$$

$$\boldsymbol{\pi}^B=\left(A^B-I+Q\right)^{-1}b. \quad (32)$$

Finally, substituting (26) and (32) into (15) and performing some mathematical manipulations, the secrecy outage probability of the MRC/CJ scheme in closed-form is derived.

D. THE ZFB/CJ SCHEME

The secrecy outage probability at state s_n under the ZFB/CJ scheme is given by

$$P^C_{out,n}(\gamma_{th})=F_{\gamma^C_{SR'_{M_{1,n}}E}}(\gamma_{th})\cdot F_{\gamma^C_{R''_{M_{2,n}}DE}}(\gamma_{th}) \quad (33)$$

***Theorem** 6*: The CDF of $\gamma^C_{SR'_{M_{1,n}}E}$ and $\gamma^C_{R''_{M_{2,n}}DE}$ are given by

$$F_{\gamma^C_{SR'_{M_{1,n}}E}}(x)=\sum_{s=0}^{M_{1,n}-1}\frac{M_1(s)}{N_1(s)}\left[1-\frac{\kappa^{N_D-2}e^{-\frac{N_1(s)(x-1)}{P_S}}\times\Psi_1}{(N_D-3)!P_D}\right] \quad (34)$$

$$F_{\gamma^C_{R''_{M_{2,n}}DE}}(x)=\sum_{s=0}^{M_{2,n}-1}\frac{M_2(s)}{N_2(s)}\left[1-\frac{\kappa^{N_D-1}e^{-\frac{N_2(s)(x-1)}{P_R}}\times\Psi_2}{(N_D-2)!P_D}\right] \quad (35)$$

where $\beta_1(s)=\frac{1}{P_D}+\frac{N_1(s)\bar{\gamma}_{SE}x}{P_SP_D}$, $\beta_2(s)=\frac{1}{P_D}+\frac{N_2(s)\bar{\gamma}_{RE}x}{P_RP_D}$, Ψ_1 and Ψ_2 are given by

$$\Psi_1=\begin{cases}-e^{\beta_1(s)\kappa}Ei(-\beta_1(s)\kappa)\\ +P_D\left(\beta_1(s)e^{\beta_1(s)\kappa}Ei(-\beta_1(s)\kappa)+\frac{1}{\kappa}\right), & N_D=3\\ (-1)^{N_D-4}\beta_1(s)^{N_D-3}e^{\beta_1(s)\kappa}Ei(-\beta_1(s)\kappa)\\ +\sum\limits_{k=1}^{N_D-3}(k-1)!(-\beta_1(s))^{N_D-3-k}\kappa^{-k}\\ +P_D\left[(-1)^{N_D-3}\beta_1(s)^{N_D-2}e^{\beta_1(s)\kappa}Ei(-\beta_1(s)\kappa)\right.\\ \left.+\sum\limits_{k=1}^{N_D-2}(k-1)!(-\beta_1(s))^{N_D-2-k}\kappa^{-k}\right], & N_D>3\end{cases} \quad (36)$$

$$\Psi_2=\begin{cases}-e^{\beta_2(s)\kappa}Ei(-\beta_2(s)\kappa)\\ +P_D\left(\beta_2(s)e^{\beta_2(s)\kappa}Ei(-\beta_2(s)\kappa)+\frac{1}{\kappa}\right), & N_D=2\\ (-1)^{N_D-3}\beta_2(s)^{N_D-2}e^{\beta_2(s)\kappa}Ei(-\beta_2(s)\kappa)\\ +\sum\limits_{k=1}^{N_D-2}(k-1)!(-\beta_2(s))^{N_D-2-k}\kappa^{-k}\\ +P_D\left[(-1)^{N_D-2}\beta_2(s)^{N_D-1}e^{\beta_2(s)\kappa}Ei(-\beta_2(s)\kappa)\right.\\ \left.+\sum\limits_{k=1}^{N_D-1}(k-1)!(-\beta_2(s))^{N_D-1-k}\kappa^{-k}\right], & N_D>2\end{cases} \quad (37)$$

Proof: See Appendix C. ∎

For ZFB/CJ, recalling the i.i.d assumption of the main channel, the probabilities to select the first or second hop are equal, i.e, $1/(M_{1,n}+M_{2,n})$, hence the probability of data packet transmission successfully is equal to $\left(1-P^{C}_{out,n}(\gamma_{th})\right)/\left(M_{1,n}+M_{2,n}\right)$, which is the same as [12]. As such, the state transition matrix of the ZFB/CJ scheme is given by

$$A^{C}_{v,n}=\begin{cases}P^{C}_{out,n}(\gamma_{th}), & s_v=s_n\\ \dfrac{\left(1-P^{C}_{out,n}(\gamma_{th})\right)}{M_{1,n}+M_{2,n}}, & s_v\in\Omega^{1}_{n}\cup\Omega^{2}_{n}\\ 0, & else\end{cases}\tag{38}$$

In addition, the stationary distribution probability vector of ZFB/CJ $\boldsymbol{\pi}^{C}=\left(A^{C}-I+Q\right)^{-1}b$, which can also be obtained by following the similar analysis as in **Theorem 3**. To this end, we can obtain the closed-form expression of the secrecy outage probability under the ZFB/CJ scheme by substituting (33) and $\boldsymbol{\pi}^{C}$ into (15).

IV. ASYMPTOTIC SECRECY OUTAGE ANALYSIS

As can be seen, the form of exact closed-form expression is too complicated, we present the asymptotic secrecy outage analysis at high SNR regime to obtain more insights. Without loss of generality, we denote $\bar{\gamma}$ as the average SNR and we have $\bar{\gamma}=\bar{\gamma}_{SR}=\bar{\gamma}_{RD}$, $\bar{\gamma}_{SE}=\bar{\gamma}_{RE}$. Moreover, we assume that $\bar{\gamma}_{SR}\to\infty$ and $\bar{\gamma}_{SE}$ is fixed, which corresponds the scenario that the main channel is much better than the eavesdropper's channel, that is to say, when the eavesdropper E is located far away from S and D, or the eavesdropper's channel suffers from significant shadowing effect.

A. THE MRC SCHEME

Theorem 7: The asymptotic secrecy outage probability of the MRC scheme can be approximated as

$$P^{A}_{out}(\gamma_{th})\overset{\bar{\gamma}\to\infty}{\approx}\sum_{n=1}^{N}\boldsymbol{\pi}^{A}_{n}\theta^{A}_{1,n}\theta^{A}_{2,n}\left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^{M_{1,n}+N_DM_{2,n}}\tag{39}$$

where

$$\theta^{A}_{1,n}=\sum_{s=0}^{M_{1,n}}\binom{M_{1,n}}{s}\left(\frac{\gamma_{th}-1}{\gamma_{th}}\right)^{M_{1,n}-s}\bar{\gamma}^{s}_{SE}s!\tag{40}$$

and

$$\theta^{A}_{2,n}=\frac{1}{(N_D!)^{M_{2,n}}}\sum_{s=0}^{N_DM_{2,n}}\binom{N_DM_{2,n}}{s}\times\left(\frac{\gamma_{th}-1}{\gamma_{th}}\right)^{N_DM_{2,n}-s}\bar{\gamma}^{s}_{RE}s!\tag{41}$$

Proof: See Appendix D. ∎

From **Theorem 7**, we can gather some insights exactly. Moreover, we can also obtain more insights by analyzing the asymptotic result on the perspective of the buffer states. Specifically, we first denote s_1 and s_N as the states that all the buffers are empty and full respectively. Then we divide the set of the whole buffer states into three parts, i.e., $\Xi=\Xi_1\cup\Xi_2\cup\Xi_3$, where Ξ_1 represents the set of the states in which all the buffers are neither full nor empty, Ξ_2 is the set of the states in which at least one buffer is either full or empty except s_1 and s_N, and $\Xi_3=\{s_1\}\cup\{s_N\}$. The number of elements in Ξ_1 and Ξ_2 are $N_1=(L-1)^M$ and $N_2=N-2-(L-1)^M$.

Then we turn our attention to the asymptotic secrecy outage probability derived from the division of the buffer states and the following key result can be easily obtained.

Corollary 1: The asymptotic secrecy outage probability of the MRC scheme can be further expressed as

$$P^{A}_{out}(\gamma_{th})\overset{\bar{\gamma}\to\infty}{\approx}\Phi^{A}_{1}+\Phi^{A}_{2}+\Phi^{A}_{3},\tag{42}$$

where

$$\Phi^{A}_{1}=\boldsymbol{\pi}^{A}_{1}\theta^{A}_{1}\left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^{M}+\boldsymbol{\pi}^{A}_{N}\theta^{A}_{2}\left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^{N_DM},\tag{43}$$

$$\Phi^{A}_{2}=\sum_{s_n\in\Xi_1}\boldsymbol{\pi}^{A}_{n}\theta^{A}_{1}\theta^{A}_{2}\left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^{M(1+N_D)},\tag{44}$$

$$\Phi^{A}_{3}=\sum_{s_n\in\Xi_2}\boldsymbol{\pi}^{A}_{n}\theta^{A}_{1,n}\theta^{A}_{2,n}\left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^{M_{1,n}+N_DM_{2,n}},\tag{45}$$

where $\boldsymbol{\pi}^{A}_{1}$ and $\boldsymbol{\pi}^{A}_{N}$ represent the corresponding stationary probability at s_1 and s_N under the MRC scheme, θ^{A}_{1} and θ^{A}_{2} can be obtained by substituting $M_{1,n}=M$ and $M_{2,n}=M$ into (40) and (41) respectively.

Proof: Recalling the assumption of state s_1, which means that all the links of the first hop are available and all the links of the second hop are not available, i.e., $M_{1,n}=M$ and $M_{2,n}=0$, hence the corresponding term at s_1 is $\boldsymbol{\pi}^{A}_{1}\theta^{A}_{1}(\gamma_{th}/\bar{\gamma})^{M}$. We can also derive the corresponding term at state s_N by following the similar analysis. For the states which belong to Ξ_1, we have $M_{1,n}=M$ and $M_{2,n}=M$ and the corresponding term Φ^{A}_{2} can be derived as (44). Similarly, Φ^{A}_{3} can be expressed as (45) when the buffer states belong to the set Ξ_2. ∎

Note that **Corollary 1** is derived based on the perspective of the buffer states, thus, in the following analysis, we study two special scenario according to the buffer size to analyze the secrecy diversity gain and the secrecy coding gain: 1) $L\not\to\infty$, which is a scenario that each buffer at the relays can only store finite data packets. 2) $L\to\infty$, which is an extreme scenario that means the whole communication process is not limited by buffer size.

For these two scenarios under the MRC scheme, we have the following result.

Corollary 2: The asymptotic secrecy outage probability of the MRC scheme can be further simplified as

$$P^{A}_{out}(\gamma_{th})\overset{\bar{\gamma}\to\infty}{\approx}\begin{cases}\boldsymbol{\pi}^{A}_{1}\theta^{A}_{1}\left(\dfrac{\gamma_{th}}{\bar{\gamma}}\right)^{M}, & L\not\to\infty\\ \Theta_1\left(\dfrac{\gamma_{th}}{\bar{\gamma}}\right)^{M(1+N_D)}, & L\to\infty\end{cases}\tag{46}$$

where $\Theta_1=\theta^{A}_{1}\theta^{A}_{2}$.

Proof: From **Corollary 1**, for $L \not\to \infty$, we find that the terms corresponding to state s_N, Φ_2^A and Φ_3^A are high order terms compared to the term corresponding to state s_1 when $\bar{\gamma} \to \infty$, hence $P_{out}^A(\gamma_{th}) \overset{\bar{\gamma}\to\infty}{\approx} \boldsymbol{\pi}_1^A \theta_1^A (\gamma_{th}/\bar{\gamma})^M$. Moreover, for $L \to \infty$, the states in Ξ_2 occupy the vast majority of all states due to the fact that $\lim_{L\to\infty}(N_1/N) = 1$, hence the stationary state converges to a uniform distribution and the sum of the stationary state probabilities equals to 1. We also have $\Phi_1^A + \Phi_2^A \approx 0$, thus the asymptotic secrecy outage probability of the MRC scheme can be approximated as (46). ∎

In the following part, we turn our attention to the secrecy diversity gain and the secrecy coding gain and we have the following result.

***Corollary** 3*: The secrecy diversity gain and the secrecy coding gain under the MRC scheme are respectively given by

$$G_d^A = \begin{cases} M, & L \not\to \infty \\ M(1+N_D), & L \to \infty \end{cases} \tag{47}$$

$$G_c^A = \begin{cases} \dfrac{(\boldsymbol{\pi}_1^A \theta_1^A)^{-\frac{1}{M}}}{\gamma_{th}}, & L \not\to \infty \\ \dfrac{\Theta_1^{-\frac{1}{M(1+N_D)}}}{\gamma_{th}}, & L \to \infty \end{cases} \tag{48}$$

Proof: On the basis of [31] and [32], the asymptotic secrecy outage probability under the MRC scheme can be expressed as $P_{out}^A(\gamma_{th}) \overset{\bar{\gamma}\to\infty}{\approx} \left(G_c^A \bar{\gamma}\right)^{-G_d^A}$. Hence the secrecy diversity gain and the secrecy coding gain of the MRC scheme under $L \not\to \infty$ and $L \to \infty$ scenarios can be easily derived by using the expression (46). ∎

B. THE MRC/CJ SCHEME

***Theorem** 8*: The asymptotic secrecy outage probability of the MRC/CJ scheme can be approximated as

$$P_{out}^B(\gamma_{th}) \overset{\bar{\gamma}\to\infty}{\approx} \sum_{n=1}^{N} \boldsymbol{\pi}_n^B \theta_{1,n}^B \theta_{2,n}^B \left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^{M_{1,n}+(N_D-1)M_{2,n}} \tag{49}$$

where

$$\theta_{1,n}^B = \sum_{s=0}^{M_{1,n}} \binom{M_{1,n}}{s} \left(\frac{\gamma_{th}-1}{\gamma_{th}}\right)^{M_{1,n}-s} \bar{\gamma}_{SE}^{s} s! \tag{50}$$

$$\theta_{2,n}^B = \frac{P_D}{[(N_D-1)!]^{M_{2,n}} \bar{\gamma}_{DE}} \sum_{s=0}^{(N_D-1)M_{2,n}} \binom{(N_D-1)M_{2,n}}{s} \times \left(\frac{\gamma_{th}-1}{\gamma_{th}}\right)^{(N_D-1)M_{2,n}-s} \frac{\bar{\gamma}_{RE}^{s} s!}{P_D^s} \Delta_1 \tag{51}$$

with $\Delta_1 = \int_0^\infty \frac{e^{-\kappa u}}{\left(\frac{1}{P_D}+u\right)^s} du$ which is given by

$$\Delta_1 = \begin{cases} \frac{1}{\kappa}, & s = 0 \\ -e^{\frac{\kappa}{P_D}} Ei\left(-\frac{\kappa}{P_D}\right), & s = 1 \\ \dfrac{\sum_{k=1}^{s-1}(k-1)!(-\kappa)^{s-k-1}}{(s-1)!}\left(\frac{1}{P_D}\right)^{-k} - \dfrac{(-\kappa)^{s-1}}{(s-1)!} e^{\frac{\kappa}{P_D}} Ei\left(-\frac{\kappa}{P_D}\right), & s \geq 2 \end{cases} \tag{52}$$

Proof: See Appendix E. ∎

***Corollary** 4*: The asymptotic secrecy outage probability of the MRC/CJ scheme can be further expressed as

$$P_{out}^B(\gamma_{th}) \overset{\bar{\gamma}\to\infty}{\approx} \Phi_1^B + \Phi_2^B + \Phi_3^B \tag{53}$$

where

$$\Phi_1^B = \boldsymbol{\pi}_1^B \theta_1^B \left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^M + \boldsymbol{\pi}_N^B \theta_2^B \left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^{(N_D-1)M}, \tag{54}$$

$$\Phi_2^B = \sum_{s_n \in \Xi_1} \boldsymbol{\pi}_n^B \theta_1^B \theta_2^B \left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^{MN_D}, \tag{55}$$

$$\Phi_3^B = \sum_{s_n \in \Xi_2} \boldsymbol{\pi}_n^B \theta_{1,n}^B \theta_{2,n}^B \left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^{M_{1,n}+(N_D-1)M_{2,n}}, \tag{56}$$

Proof: By following the similar analysis as in **Corollary 1**, we can easily obtain the desired result after some mathematical manipulations. ∎

Similarly, for $L \not\to \infty$ and $L \to \infty$ scenarios under the MRC/CJ scheme, we can also obtain the following result.

***Corollary** 5*: The asymptotic secrecy outage probability of the MRC/CJ scheme can be further simplified as

$$P_{out}^B(\gamma_{th}) \overset{\bar{\gamma}\to\infty}{\approx} \begin{cases} \left(\boldsymbol{\pi}_1^B \theta_1^B + \boldsymbol{\pi}_N^B \theta_2^B\right)\left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^M, & L \not\to \infty, N_D = 2 \\ \boldsymbol{\pi}_1^B \theta_1^B \left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^M, & L \not\to \infty, N_D > 2 \\ \Theta_2 \left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^{MN_D}, & L \to \infty \end{cases} \tag{57}$$

where $\Theta_2 = \theta_1^B \theta_2^B$.

Proof: Following the similar analysis as in **Corollary 2**, the above result can be easily obtained. ∎

***Corollary** 6*: The secrecy diversity gain and the secrecy coding gain under the MRC/CJ scheme are respectively given by

$$G_d^B = \begin{cases} M, & L \not\to \infty \\ MN_D, & L \to \infty \end{cases} \tag{58}$$

$$G_c^B = \begin{cases} \left(\boldsymbol{\pi}_1^B \theta_1^B + \boldsymbol{\pi}_N^B \theta_2^B\right)^{-\frac{1}{M}} / \gamma_{th}, & L \not\to \infty, N_D = 2 \\ \dfrac{\left(\boldsymbol{\pi}_1^B \theta_1^B\right)^{-\frac{1}{M}}}{\gamma_{th}}, & L \not\to \infty, N_D > 2 \\ \dfrac{\Theta_2^{-\frac{1}{MN_D}}}{\gamma_{th}}, & L \to \infty \end{cases} \tag{59}$$

Proof: The proof follows similar lines as that of **Corollary 3**, hence is omitted. ■

C. THE ZFB/CJ SCHEME

***Theorem** 9*: The asymptotic secrecy outage probability of the ZFB/CJ scheme can be approximated as

$$P_{out}^C(\gamma_{th}) \overset{\bar{\gamma}\to\infty}{\approx} \sum_{n=1}^{N} \boldsymbol{\pi}_n^C \theta_{1,n}^C \theta_{2,n}^C \left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^{M_{1,n}+M_{2,n}} \tag{60}$$

where

$$\theta_{1,n}^C = \left(\frac{P_D}{\bar{\gamma}_{DE}}\right)^{N_D-2} \sum_{s=0}^{M_{1,n}} \binom{M_{1,n}}{s} \times \left(\frac{\gamma_{th}-1}{\gamma_{th}}\right)^{M_{1,n}-s} \frac{\bar{\gamma}_{SE}^s s!}{(N_D-3)! P_D^s} \Delta_2 \tag{61}$$

$$\theta_{2,n}^C = \left(\frac{P_D}{\bar{\gamma}_{DE}}\right)^{N_D-1} \sum_{s=0}^{M_{2,n}} \binom{M_{2,n}}{s} \times \left(\frac{\gamma_{th}-1}{\gamma_{th}}\right)^{M_{2,n}-s} \frac{\bar{\gamma}_{RE}^s s!}{(N_D-2)! P_D^s} \Delta_3 \tag{62}$$

with $\Delta_2 = \int_0^\infty \frac{u^{N_D-3} e^{-\kappa u}}{\left(\frac{1}{P_D}+u\right)^s} du$ and $\Delta_3 = \int_0^\infty \frac{u^{N_D-2} e^{-\kappa u}}{\left(\frac{1}{P_D}+u\right)^s} du$, which are respectively given by

$$\Delta_2 \approx \begin{cases} \dfrac{(N_D-3-s)!}{\kappa^{N_D-2-s}}, & N_D-s-3 \geq 0 \\ -e^{\kappa P_D} Ei\left(-\dfrac{\kappa}{P_D}\right), & N_D-s-3 = -1 \\ \dfrac{\sum_{k=1}^{s-N_D+2} (k-1)! (-\kappa)^{s-N_D+2-k} P_D^k}{(s-N_D+2)!} - \dfrac{(-\kappa)^{s-N_D+2} e^{\kappa P_D} Ei\left(-\dfrac{\kappa}{P_D}\right)}{(s-N_D+2)!}, & N_D-s-3 \leq -2 \end{cases} \tag{63}$$

$$\Delta_3 \approx \begin{cases} \dfrac{(N_D-2-s)!}{\kappa^{N_D-1-s}}, & N_D-s-2 \geq 0 \\ -e^{\kappa P_D} Ei\left(-\dfrac{\kappa}{P_D}\right), & N_D-s-2 = -1 \\ \dfrac{\sum_{k=1}^{s-N_D+1} (k-1)! (-\kappa)^{s-N_D+1-k} P_D^k}{(s-N_D+1)!} - \dfrac{(-\kappa)^{s-N_D+1} e^{\kappa P_D} Ei\left(-\dfrac{\kappa}{P_D}\right)}{(s-N_D+1)!}, & N_D-s-2 \leq -2 \end{cases} \tag{64}$$

Proof: See Appendix F. ■

***Corollary** 7*: The asymptotic secrecy outage probability of the ZFB/CJ scheme can be further written as

$$P_{out}^C(\gamma_{th}) \overset{\bar{\gamma}\to\infty}{\approx} \Phi_1^C + \Phi_2^C + \Phi_3^C, \tag{65}$$

where

$$\Phi_1^C = \left(\boldsymbol{\pi}_1^C \theta_1^C + \boldsymbol{\pi}_N^C \theta_2^C\right) \left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^M, \tag{66}$$

$$\Phi_2^C = \sum_{s_n \in \Xi_1} \boldsymbol{\pi}_n^C \theta_1^C \theta_2^C \left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^{2M}, \tag{67}$$

$$\Phi_3^C = \sum_{s_n \in \Xi_2} \boldsymbol{\pi}_n^C \theta_{1,n}^C \theta_{2,n}^C \left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^{M_{1,n}+M_{2,n}}, \tag{68}$$

Proof: By following similar analysis as in **Corollary 1**, we can easily obtain the desired result after some mathematical manipulations. ■

***Corollary** 8*: The asymptotic secrecy outage probability of the ZFB/CJ scheme can be further simplified as

$$P_{out}^C(\gamma_{th}) \overset{\bar{\gamma}\to\infty}{\approx} \begin{cases} \left(\boldsymbol{\pi}_1^C \theta_1^C + \boldsymbol{\pi}_N^C \theta_2^C\right) \left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^M, & L \not\to \infty \\ \Theta_3 \left(\frac{\gamma_{th}}{\bar{\gamma}}\right)^{2M}, & L \to \infty \end{cases} \tag{69}$$

where $\Theta_3 = \theta_1^C \theta_2^C$.

Proof: Following similar analysis as in **Corollary 2**, the above result can be easily obtained. ■

***Corollary** 9*: The secrecy diversity gain and the secrecy coding gain under the ZEB/CJ scheme are given by

$$G_d^C = \begin{cases} M, & L \not\to \infty \\ 2M, & L \to \infty \end{cases} \tag{70}$$

$$G_c^C = \begin{cases} \left(\boldsymbol{\pi}_1^C \theta_1^C + \boldsymbol{\pi}_N^C \theta_2^C\right)^{-\frac{1}{M}} / \gamma_{th}, & L \not\to \infty \\ \dfrac{\Theta_3^{-\frac{1}{2M}}}{\gamma_{th}}, & L \to \infty \end{cases} \tag{71}$$

Proof: The proof follows similar lines as that of **Corollary 3**, hence is omitted. ■

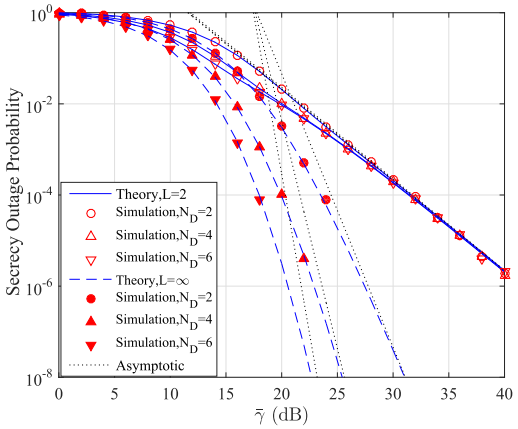

FIGURE 2. Secrecy outage probability of the MRC scheme vs. the average SNR $\bar{\gamma}$ with different destination antenna number N_D when $M = 2$, $\bar{\gamma}_{SE} = 10$dB.

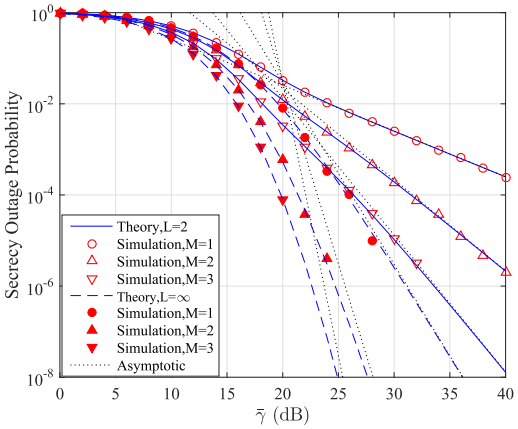

FIGURE 3. Secrecy outage probability of the MRC scheme vs. the average SNR $\bar{\gamma}$ with different number of relays M when $N_D = 3$, $\bar{\gamma}_{SE} = 10$dB.

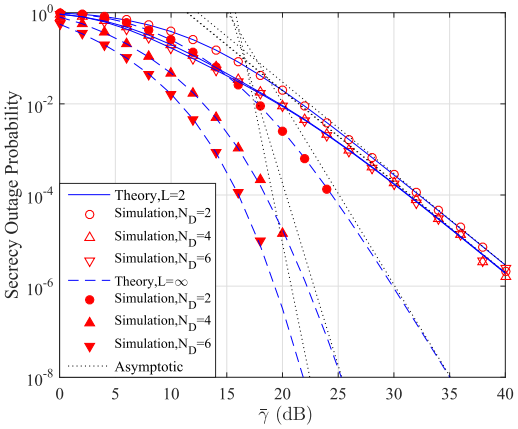

FIGURE 4. Secrecy outage probability of the MRC/CJ scheme vs. the average SNR $\bar{\gamma}$ with different destination antenna number N_D when $M = 2$, $\bar{\gamma}_{SE} = \bar{\gamma}_{DE} = 10$dB.

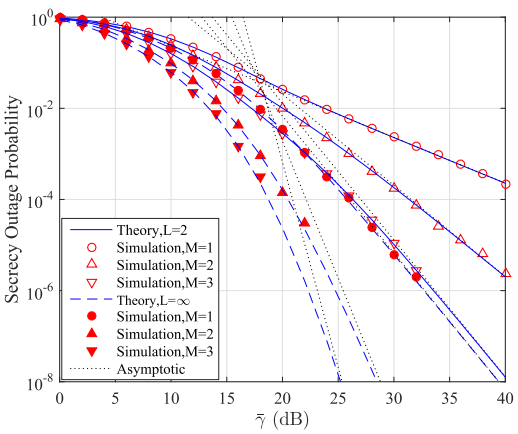

FIGURE 5. Secrecy outage probability of the MRC/CJ scheme vs. the average SNR $\bar{\gamma}$ with different number of relays M and when $N_D = 3$, $\bar{\gamma}_{SE} = \bar{\gamma}_{DE} = 10$dB.

V. SIMULATION ANALYSIS

In this section, we present simulation results to verify the theoretical analysis obtained in the above sections for the three transmission schemes and investigate the impact of different curial parameters on the secrecy outage performance of DF buffer-aided relaying networks with a multi-antenna destination. Without loss of generality, we assume that pre-defined secrecy rate $R_s = 1\ bit/s/Hz$, and all transmission powers are normalized to unity. As indicated in these figures, we find that the analytical results are in exact agreement with the Monte Carlo simulations and the asymptotic curves keep completely tight at high SNR regimes which corroborates the accuracy of the theoretical analysis.

Fig. 2 and 3 illustrate the secrecy outage probability of the considered system with MRC for different number of antennas N_D and different number of relays M under $L \not\to \infty$ and $L \to \infty$ scenarios. It is clear that the secrecy outage probability of the system is degraded as N_D and M increases, both in the case with $L \not\to \infty$ and $L \to \infty$. This is intuitive since increasing N_D or M provides additional secrecy diversity gain or secrecy coding gain. Specifically, from Fig. 2, we can see that when $L \not\to \infty$, the secrecy diversity gains of $N_D = 2, 4, 6$ are both 2, while under the scenario $L \to \infty$ become 6, 10, 14. From Fig. 3, we can also observe that the secrecy diversity gains of $M = 1, 2, 3$ are 1, 2, 3 under the scenario $L \not\to \infty$ while increases to 4, 8, 12 when $L \to \infty$. Moreover, increasing N_D and M can improve the secrecy coding gain of the considered system and all these above observations can be verified by (47) and (48).

Fig. 4 and 5 present the secrecy outage probability of the considered system with MRC/CJ for different number of antennas N_D and different number of relays M under $L \not\to \infty$ and $L \to \infty$ scenarios. We find a similar phenomenon as the above figures in Fig. 4 and 5. As shown in Fig. 4, if the number of relays is fixed, i.e., $M = 2$, the secrecy diversity gain of the MRC/CJ scheme is 2 regardless of the antennas numbers N_D under the scenario $L \not\to \infty$. On the contrary, the secrecy diversity gains of $N_D = 2, 4, 6$ become 4, 8, 12, i.e., MN_D when $L \to \infty$. As can be observed in Fig. 5, when $M = 1, 2$ and 3, the secrecy diversity gains are 1, 2, and 3 under the scenario $L \not\to \infty$ while increase linearly with

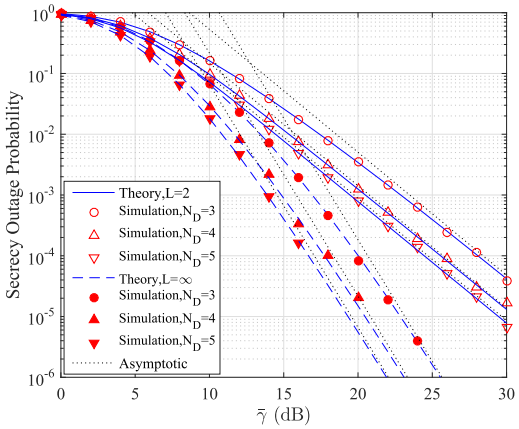

FIGURE 6. Secrecy outage probability of the ZFB/CJ scheme vs. the average SNR $\bar{\gamma}$ with different destination antenna number N_D when $M = 2$, $\bar{\gamma}_{SE} = \bar{\gamma}_{DE} = 10$dB.

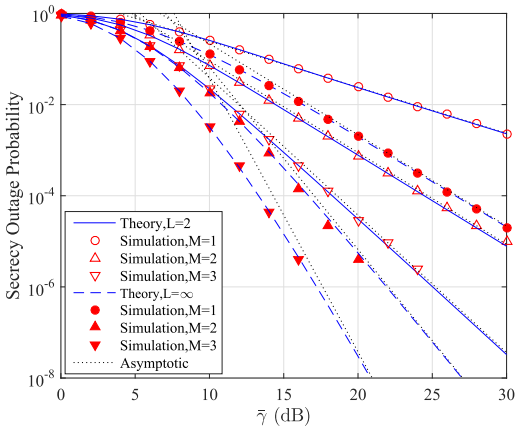

FIGURE 7. Secrecy outage probability of the ZFB/CJ scheme vs. the average SNR $\bar{\gamma}$ with different number of relays M and when $N_D = 5$, $\bar{\gamma}_{SE} = \bar{\gamma}_{DE} = 10$dB.

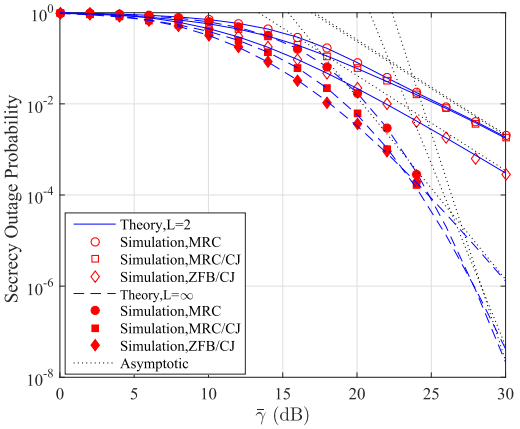

FIGURE 8. Secrecy outage probability of the proposed schemes vs. the average SNR $\bar{\gamma}$ when $M = 2$, $N_D = 4$, $\bar{\gamma}_{SE} = 15$dB, $\bar{\gamma}_{DE} = 5$dB.

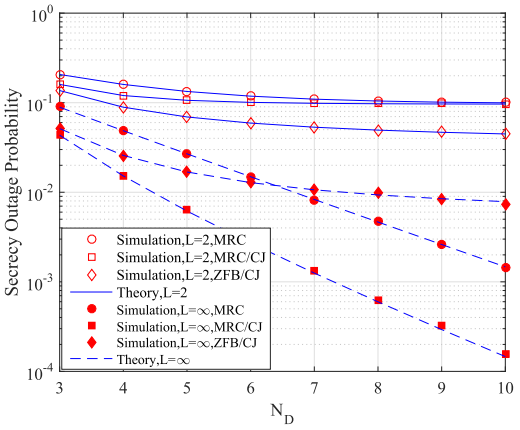

FIGURE 9. Secrecy outage probability of the proposed schemes vs. destination antenna number N_D when $M = 2$, $\bar{\gamma}_{SR} = 10$dB, $\bar{\gamma}_{SE} = \bar{\gamma}_{DE} = 6$dB.

N_D when $L \to \infty$. In addition, it is also observed that the secrecy coding gain improves with the increase of N_D and M, which agrees with the theoretical asymptotic analysis.

Fig. 6 and 7 examine the impacts of different number of antennas N_D at the destination and different number of relays M on the secrecy outage probability of the ZFB/CJ scheme, respectively. As illustrated in Fig. 6, no matter how much N_D is, the secrecy diversity gains remain unchanged, specifically, the secrecy diversity gain achieves M under the scenario $L \not\to \infty$ while achieves $2M$ under the scenario $L \to \infty$. From Fig. 7, we can also find that the secrecy diversity gain increases only with the increase of the number of relays M, which is in accordance with the result in (70). Similar to the other schemes, a secrecy coding gain is observed when N_D and M increase.

Fig. 8 plots the secrecy outage probability versus the average SNR $\bar{\gamma}$ for the three proposed schemes. As illustrated, two destination jamming schemes achieve better performance than the MRC scheme under the scenario $L \not\to \infty$. Specifically, ZFB/CJ outperforms MRC/CJ and MRC across the entire SNR range of interest due to a jamming signal can be transmitted not only in the first hop but also in the second hop, which degrades the quality of eavesdropper ŕs channel significantly. MRC/CJ outperforms MRC in the low SNR regime while attains similar outage performance in the high SNR regime. It is also observed that the larger secrecy coding gain of ZFB/CJ can be obtained than the other schemes and all schemes achieve the same secrecy diversity gain of M when $L \not\to \infty$. On the other hand, under the scenario $L \to \infty$, ZFB/CJ outperforms MRC/CJ and MRC in the low SNR regime, while the opposite holds in the high SNR regime. This is quite intuitive since MRC/CJ and MRC can achieve much larger secrecy diversity gain than ZFB/CJ.

Fig. 9 investigates the impacts of antenna numbers N_D on the secrecy outage probability for the proposed schemes. As can be readily observed, when $L \not\to \infty$, ZFB/CJ always attains better performance than the other two schemes. Moreover, the secrecy outage probability of ZFB/CJ is constantly degraded with increasing of N_D, while an outage performance floor occurs for MRC and MRC/CJ. While under the scenario $L \to \infty$, the secrecy performance of MRC and MRC/CJ

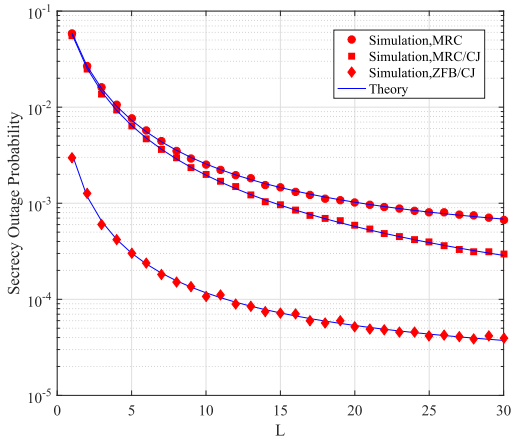

FIGURE 10. Secrecy outage probability of the proposed schemes vs. the buffer size L when $M = 2$, $N_D = 5$, $\bar{\gamma} = 20$dB, $\bar{\gamma}_{SE} = 12$dB, $\bar{\gamma}_{DE} = 10$dB.

are much better than ZFB/CJ with the increase of N_D, due to the fact that when $L \to \infty$, the states of buffer which are neither full nor empty dominate the system, that is to say, all of the links in the first hop and second hop are always available. Meanwhile, the reception performance and the jamming intensity increase with the increase of N_D. It is clearly that the improvement of reception performance makes more contributions to the system secrecy performance. Hence, when $L \to \infty$ and N_D is lager, the MRC/CJ scheme can obtain the best secrecy performance than two other schemes. However, the MRC scheme is the most appropriate scheme of the three proposed schemes after comprehensive consideration about complexity and system performance in practical applications.

Fig. 10 presents the secrecy outage probability versus the buffer size L for the three proposed schemes. As can be seen, the secrecy outage probability degrades with the increase of the buffer size no matter which scheme is adopted. That is to say, the secrecy performance of the considered system can be enhanced by enlarging the buffer size L.

VI. CONCLUSION

In this paper, we investigate the secrecy outage performance of the DF buffer-aided relaying networks with a multi-antenna destination. To fully exploit the advantages of multi-antenna, three transmission schemes with half-duplex and full-duplex operations are proposed. Moreover, we adopt the max-link relay selection scheme to enhance the secrecy performance. By utilizing the Markov chain theory, exact and asymptotic closed-form expressions for the secrecy outage probability of all the proposed schemes are derived. Meanwhile, considering $L \not\to \infty$ and $L \to \infty$ scenarios, simple and informative asymptotic results are also presented, which enables us to obtain further insights into the impact of key parameters on the secrecy performance. Our findings suggest that all of the proposed schemes achieve a secrecy diversity gain of M under the scenario $L \not\to \infty$. On the other hand, when $L \to \infty$, the secrecy diversity gain of ZFB/CJ achieves $2M$ while MRC and MRC/CJ achieve $M(1 + N_D)$ and MN_D respectively. Secrecy coding gain of the system which also differs from different schemes, improves with the increase of the number of relays M and the number of destination's antennas N_D. Furthermore, ZFB/CJ outperforms MRC and MRC/CJ under the scenario $L \not\to \infty$. The same results can be obtained in the low SNR regime, while the opposite holds in the high SNR regime when $L \to \infty$. In this work, we assume that perfect channel state information can be acquired, hence the impact of imperfect channel estimates on the system secrecy performance under three transmission schemes could be investigated in the future work.

APPENDIX A

Without loss of generality, we first define $Z_1 = |h_{SE}|^2$. According to the order statistic, the CDF of $\gamma^A_{SR'_{M_{1,n}}E}$ is calculated as

$$F_{\gamma^A_{SR'_{M_{1,n}}E}}(x) = \Pr\left(\frac{1+P_S X}{1+P_S Z_1} < x\right) = \int_0^\infty F_X\left(\frac{x-1}{P_S} + xz\right) f_{Z_1}(z)\, dz \quad (72)$$

Recalling Z_1 is an exponential random variable, and the PDF of Z_1 is $f_{Z_1}(z) = \frac{P_S}{\bar{\gamma}_{SE}} e^{-\frac{P_S z}{\bar{\gamma}_{SE}}}$, then we substitute it and (16) into (72), and the CDF of $\gamma^A_{SR'_{M_{1,n}}E}$ can be easily derived. By utilizing the formula [30, eq. (3.351.3)] and following the similar operation, we can also obtain the CDF of $\gamma^A_{R''_{M_{2,n}}DE}$. Hence the desired results in **Theorem 1** can be obtained.

APPENDIX B

Due to the fact that $\gamma^B_{SR'_{M_{1,n}}E} = \gamma^A_{SR'_{M_{1,n}}E}$, hence we turn our attention to the proof for the CDF of the $\gamma^B_{R''_{M_{2,n}}DE}$. Let us denote $Y_2 = \left\|h^2_{R''_{M_{2,n}}DE}\right\|^2$, $Z_2 = \left|h_{R_j E}\right|^2$, $U_1 = |h_{DE}|^2$. Considering the receiving antennas are $N_D - 1$, according to **Lemma 2**, we have

$$F_{Y_2}(y) = \sum_{r_0+r_1+\cdots+r_{N_D-1}=M_{2,n}} \frac{M_{2,n}!}{r_0! r_1! \cdots r_{N_D-1}!} \times \frac{(-1)^{M_{2,n}-r_0}}{\prod_{m=1}^{N_D-1}[\Gamma(m)]^{r_m}} \left(\frac{P_R y}{\bar{\gamma}_{RD}}\right)^{T^2_{RD}} e^{-\frac{(M_{2,n}-r_0)P_R y}{\bar{\gamma}_{RD}}} \quad (73)$$

Similarly, by utilizing order statistic, the CDF of $\gamma^B_{R''_{M_{2,n}}DE}$ can be expressed as

$$F_{\gamma^B_{R''_{M_{2,n}}DE}}(x) = \Pr\left(\frac{1+P_R Y_2}{1+\frac{P_R Z_2}{1+P_D U_1}} < x\right) = \int_0^\infty \int_0^\infty F_{Y_2}\left(\frac{x-1}{P_R} + \frac{xz}{1+P_D u}\right) \times f_{Z_2}(z)\, dz f_{U_1}(u)\, du \quad (74)$$

$$F_{\gamma^{B}_{R''_{M,n}DE}}(x)=\sum_{r_0+r_1+\cdots+r_{N_D-1}=M_{2,n}}\sum_{s=0}^{T^2_{RD}}\binom{T^2_{RD}}{s}\times\frac{M_{2,n}!}{r_0!r_1!\cdots r_{N_D-1}!}\frac{(-1)^{M_{2,n}-r_0}}{\prod_{m=1}^{N_D-1}[\Gamma(m)]^{r_m}}\left(\frac{P_R}{\bar{\gamma}_{RD}}\right)^{T^2_{RD}}\frac{e^{-\frac{(M_{2,n}-r_0)(x-1)}{\bar{\gamma}_{RD}}}x^s s!}{\bar{\gamma}_{DE}}$$
$$\times\left(\frac{x-1}{P_R}\right)^{T^2_{RD}-s}\left(\frac{\bar{\gamma}_{RE}}{P_RP_D}\right)^{s}\Bigg\{\underbrace{\int_0^\infty\frac{e^{-\frac{P_Du}{\bar{\gamma}_{DE}}}du}{\left[u+\frac{(M_{2,n}-r_0)x\bar{\gamma}_{RE}}{P_D\bar{\gamma}_{RD}}+\frac{1}{P_D}\right]^{s+1}}}_{\Lambda_1}+P_D\underbrace{\int_0^\infty\frac{ue^{-\frac{P_Du}{\bar{\gamma}_{DE}}}du}{\left[u+\frac{(M_{2,n}-r_0)x\bar{\gamma}_{RE}}{P_D\bar{\gamma}_{RD}}+\frac{1}{P_D}\right]^{s+1}}}_{\Lambda_2}\Bigg\}}_{\Lambda} \tag{75}$$

Substituting the PDF of Z_2 and U_1 and (73) into (74), we can obtain the CDF of $\gamma^{B}_{R''_{M_{2,n}}DE}$ in (75), as shown at the top of this page.

To make the analysis tractable, we define $\varepsilon=\frac{(M_{2,n}-r_0)x\bar{\gamma}_{RE}}{P_D\bar{\gamma}_{RD}}+\frac{1}{P_D}$ and $\kappa=\frac{P_D}{\bar{\gamma}_{DE}}$, hence Λ_1 and Λ_2 can be simplified as $\Lambda_1=\int_0^\infty\frac{e^{-\kappa u}du}{(u+\varepsilon)^{s+1}}$ and $\Lambda_2=\int_0^\infty\frac{ue^{-\kappa u}du}{(u+\varepsilon)^{s+1}}$. For item Λ_1, there are two cases to consider, which are $s=0$ and $s\geq 1$. Utilizing the equalities [30, eq. (3.352.4)] and [30, eq. (3.353.2)], we can derive the corresponding items under two cases respectively. For item Λ_2, we also consider two cases, i.e., $s=0$ and $s\geq 1$. As $s=0$, with the help of [30, eq. (3.353.5)], it yields $\Lambda_2=\varepsilon e^{\varepsilon\kappa}Ei(-\varepsilon\kappa)+\frac{1}{\kappa}$.

In order to calculate Λ_2 as $s\geq 1$, we take a change of integral variable $x+\varepsilon=t$, then the calculation of Λ_2 can be further given by

$$\begin{aligned}\Lambda_2&=\int_\varepsilon^\infty\frac{(t-\varepsilon)e^{-\kappa(t-\varepsilon)}dt}{t^{s+1}}\\&=e^{\varepsilon\kappa}\left(\int_\varepsilon^\infty\frac{e^{-\kappa t}dt}{t^s}-\varepsilon\int_\varepsilon^\infty\frac{e^{-\kappa t}dt}{t^{s+1}}\right),s\geq 1\end{aligned} \tag{76}$$

By utilizing the integral relationship [30, eq. (3.352.2)] and [30, eq. (3.353.1)], the item Λ_2 as $s\geq 1$ can be derived. With the above analysis, the desired results in **Theorem 4** are easily derived after some mathematical manipulations.

APPENDIX C

Assuming $U_2=\left|h^{\dagger}_{DE}w_{ZF}\right|^2$, $U_3=\|h_{DE}\|^2$, the PDF of U_2 is given by [33]

$$f_{U_2}(u)=\left(\frac{P_D}{\bar{\gamma}_{DE}}\right)^{N_D-2}\frac{u^{N_D-3}e^{-\frac{P_Du}{\bar{\gamma}_{DE}}}}{(N_D-3)!},\quad N_D\geq 3 \tag{77}$$

Then, with the help of the order statistic, the CDF of $\gamma^{C}_{SR'_{M_{1,n}}E}$ can be derived as

$$\begin{aligned}&F_{\gamma^{C}_{SR'_{M_{1,n}}E}}(x)\\&=\sum_{s=0}^{M_{1,n}-1}\frac{M_1(s)}{N_1(s)}\Bigg\{1-\frac{\kappa^{N_D-2}e^{-\frac{N_1(s)(x-1)}{P_S}}}{(N_D-3)!P_D}\\&\times\Bigg[\underbrace{\int_0^\infty\frac{u^{N_D-3}e^{-\frac{P_Du}{\bar{\gamma}_{DE}}}}{u+\left(\frac{1}{P_D}+\frac{N_1(s)\bar{\gamma}_{SE}x}{P_SP_D}\right)}+\int_0^\infty\frac{P_Du^{N_D-2}e^{-\frac{P_Du}{\bar{\gamma}_{DE}}}}{u+\left(\frac{1}{P_D}+\frac{N_1(s)\bar{\gamma}_{SE}x}{P_SP_D}\right)}}_{\Psi_1}\Bigg]\Bigg\}\end{aligned} \tag{78}$$

Considering two cases of $N_D=3$ and $N_D>3$, and with the help of [30, eq. (3.352.4)] and [30, eq. (3.353.5)], we can obtain Ψ_1 as in (36) and the CDF of $\gamma^{C}_{SR'_{M_{1,n}}E}$ can be derived.

On the other hand, the CDF of U_3 can be obtained when MRT is applied, then we can obtain the PDF of U_3 by taking the derivative of the CDF of U_3, which is given by

$$f_{U_3}(u)=\left(\frac{P_D}{\bar{\gamma}_{DE}}\right)^{N_D-1}\frac{u^{N_D-2}e^{-\frac{P_Du}{\bar{\gamma}_{DE}}}}{(N_D-2)!} \tag{79}$$

By following similar analysis above, we can also obtain the CDF of $\gamma^{C}_{R''_{M_{2,n}}DE}$, thus the desired results in **Theorem 6** can be derived.

APPENDIX D

When $\bar{\gamma}\to\infty$, with the help of $e^x\approx 1+x$ $(x\to 0)$, the CDF of X can be approximated as $F_X(x)\approx\left(\frac{P_Sx}{\bar{\gamma}_{SR}}\right)^{M_{1,n}}$, then by pulling the approximated CDF of X and the PDF of Z_1 into (72), we have

$$\begin{aligned}F_{\gamma^{A}_{SR'_{M_{1,n}}E}}(x)&\overset{\bar{\gamma}\to\infty}{\approx}\sum_{s=0}^{M_{1,n}}\binom{M_{1,n}}{s}\left(\frac{x-1}{x}\right)^{M_{1,n}-s}\\&\times\bar{\gamma}^s_{SE}s!\left(\frac{x}{\bar{\gamma}}\right)^{M_{1,n}}\end{aligned} \tag{80}$$

On the other hand, utilizing the Maclaurin series expansion of the exponential function and neglecting the higher order terms, the CDF of Y can be approximated as $F_Y(y) \approx \frac{1}{(N_D!)^{M_{2,n}}}\left(\frac{P_R y}{\bar{\gamma}_{RD}}\right)^{N_D M_{2,n}}$, by following the similar analysis above, the CDF of $\gamma^A_{R''_{M_{2,n}}DE}$ can be further approximated as

$$F_{\gamma^A_{R''_{M_{2,n}}DE}}(x) \overset{\bar{\gamma}\to\infty}{\approx} \frac{1}{(N_D!)^{M_{2,n}}} \sum_{s=0}^{N_D M_{2,n}} \binom{N_D M_{2,n}}{s} \times \left(\frac{x-1}{x}\right)^{N_D M_{2,n}-s} \bar{\gamma}_{RE}^s s! \left(\frac{x}{\bar{\gamma}}\right)^{N_D M_{2,n}} \tag{81}$$

Substituting (80) and (81) into (15) yields to the desired results in **Theorem 7**.

APPENDIX E

Recalling that the first hop of MRC/CJ is the same as the MRC scheme, hence we have $F_{\gamma^B_{SR'_{M_{1,n}}E}}(x) = F_{\gamma^A_{SR'_{M_{1,n}}E}}(x)$. Moreover, by following similar analysis of (81), the approximated CDF of $\gamma^B_{R''_{M_{2,n}}DE}$ is given by

$$\begin{aligned} &F_{\gamma^B_{R''_{M_{2,n}}DE}}(x) \\ &\overset{\bar{\gamma}\to\infty}{\approx} \frac{P_D}{[(N_D-1)!]^{M_{2,n}}\bar{\gamma}_{DE}} \sum_{s=0}^{(N_D-1)M_{2,n}} \binom{(N_D-1)M_{2,n}}{s} \\ &\quad\times \left(\frac{x-1}{x}\right)^{(N_D-1)M_{2,n}-s} \frac{\bar{\gamma}_{RE}^s s!}{P_D^s} \underbrace{\int_0^\infty \frac{e^{-\kappa u}du}{\left(\frac{1}{P_D}+u\right)^s}}_{\Delta_1} \\ &\quad\times \left(\frac{x}{\bar{\gamma}}\right)^{(N_D-1)M_{2,n}} \end{aligned} \tag{82}$$

Now, we turn our attention to the inner integral item Δ_1. Considering $s = 0$, $s = 1$ and $s \geq 2$ three cases, with the help of the integral relationships [30, eq. (3.352.4)] and [30, eq. (3.353.2)], we can obtain the closed-form expression of Δ_1 as given in (52). Finally, the desired results in **Theorem 8** can be easily obtained after some mathematical manipulations.

APPENDIX F

Utilizing the asymptotic CDF of X and the order statistic, the asymptotic CDF of $\gamma^C_{SR'_{M_{1,n}}E}$ is given by

$$\begin{aligned} &F_{\gamma^C_{SR'_{M_{1,n}}E}}(x) \\ &\overset{\bar{\gamma}\to\infty}{\approx} \left(\frac{P_D}{\bar{\gamma}_{DE}}\right)^{N_D-2} \sum_{s=0}^{M_{1,n}} \binom{M_{1,n}}{s} \\ &\quad\times\left(\frac{x-1}{x}\right)^{M_{1,n}-s} \frac{\bar{\gamma}_{SE}^s s!}{(N_D-3)!P_D^s} \underbrace{\int_0^\infty \frac{u^{N_D-3}e^{-\kappa u}du}{\left(\frac{1}{P_D}+u\right)^s}}_{\Delta_2} \left(\frac{x}{\bar{\gamma}}\right)^{M_{1,n}} \end{aligned} \tag{83}$$

To obtain a closed-form expression of the asymptotic CDF of $\gamma^C_{SR'_{M_{1,n}}E}$, we need to calculate the integral item Δ_2. There are also three cases to consider, i.e., $N_D - s - 3 \geq 0$, $N_D - s - 3 = -1$ and $N_D - s - 3 \leq -2$. Recalling that the main channel SNR is high enough, meanwhile in order to make the analysis tractable, when $N_D - s - 3 = -1$, the item Δ_2 can be simplified as $\Delta_2 \approx \int_0^\infty \left(\frac{1}{P_D}+u\right)^{N_D-3-s} e^{-\kappa u}du$. According to [30, eq. (3.352.4)], we have $\Delta_2 \approx -e^{\frac{\kappa}{P_D}} Ei\left(-\frac{\kappa}{P_D}\right)$. Similarly, as $N_D - s - 3 \geq 0$ or $N_D - s - 3 \leq -2$, the item Δ_2 can be approximated as $\Delta_2 \approx \int_0^\infty u^{N_D-3-s}e^{-\kappa u}du$, hence the desired result in (63) can be obtained using the integral relationships [30, eq. (3.351.3)] and [30, eq. (3.353.2)]. By following the similar approach, the asymptotic CDF of $\gamma^C_{R''_{M_{2,n}}DE}$ can also be derived, to this end, pulling these two asymptotic CDFs into (15) yields the desired result.

REFERENCES

[1] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[2] A. Host-Madsen and J. Zhang, "Capacity bounds and power allocation for wireless relay channels," *IEEE Trans. Inf. Theory*, vol. 51, no. 6, pp. 2020–2040, Jun. 2005.

[3] M. R. Bhatnagar, "Performance analysis of a path selection scheme in multi-hop decode-and-forward protocol," *IEEE Commun. Lett.*, vol. 16, no. 12, pp. 1980–1983, Dec. 2012.

[4] B. Gui, L. Dai, and L. J. Cimini, "Routing strategies in multihop cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 2, pp. 843–855, Feb. 2009.

[5] D. Michalopoulos and G. Karagiannidis, "Performance analysis of single relay selection in Rayleigh fading," *IEEE Trans. Wireless Commun.*, vol. 7, no. 10, pp. 3718–3724, Oct. 2008.

[6] B. Xia, Y. Fan, J. Thompson, and H. V. Poor, "Buffering in a three-node relay network," *IEEE Trans. Wireless Commun.*, vol. 7, no. 11, pp. 4492–4496, Nov. 2008.

[7] N. Zlatanov, R. Schober, and P. Popovski, "Throughput and diversity gain of buffer-aided relaying," in *Proc. IEEE Global Commun. Conf.*, Dec. 2011, pp. 1–6.

[8] N. Zlatanov, R. Schober, and P. Popovski, "Buffer-aided relaying with adaptive link selection," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 8, pp. 1530–1542, Aug. 2013.

[9] N. Zlatanov and R. Schober, "Buffer-aided relaying with adaptive link selection-fixed and mixed rate transmission," *IEEE Trans. Inf. Theory*, vol. 59, no. 5, pp. 2816–2840, May 2013.

[10] Z. Tian, G. Chen, Y. Gong, Z. Chen, and J. A. Chambers, "Buffer-aided max-link relay selection in amplify-and-forward cooperative networks," *IEEE Trans. Veh. Technol.*, vol. 64, no. 2, pp. 553–565, Feb. 2015.

[11] A. Ikhlef, D. S. Michalopoulos, and R. Schober, "Max-max relay selection for relays with buffers," *IEEE Trans. Wireless Commun.*, vol. 11, no. 3, pp. 1124–1135, Mar. 2012.

[12] I. Krikidis, T. Charalambous, and J. S. Thompson, "Buffer-aided relay selection for cooperative diversity systems without delay constraints," *IEEE Trans. Wireless Commun.*, vol. 11, no. 5, pp. 1957–1967, May 2012.

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

[14] G. Chen, Z. Tian, Y. Gong, Z. Chen, and J. A. Chambers, "Max-ratio relay selection in secure buffer-aided cooperative wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 4, pp. 719–729, Apr. 2014.

[15] A. Sun, T. Liang, and Y. Zhang, "Performance analysis of secure buffer-aided cognitive radio network," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, Nov. 2015, pp. 1–4.

[16] X. Tang, Y. Cai, Y. Huang, T. Q. Duong, W. Yang, and W. Yang, "Secrecy outage analysis of buffer-aided cooperative MIMO relaying systems," *IEEE Trans. Vehi. Technol.*, vol. 67, no. 3, pp. 2035–2048, Mar. 2018.

[17] S. Jia, J. Zhang, H. Zhao, and R. Zhang, "Destination assisted secret transmission in wireless relay networks," in *Proc. IEEE VTC-Fall*, Sep. 2016, pp. 1–5.
[18] J. Xiong, L. Cheng, D. Ma, and J. Wei, "Destination-aided cooperative jamming for dual-hop amplify-and-forward MIMO untrusted relay systems," *IEEE Trans. Veh. Tech.*, vol. 65, no. 9, pp. 7274–7284, Sep. 2016.
[19] G. Zheng, I. Krikidis, J. Li, A. P. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Signal Process.*, vol. 61, no. 20, pp. 4962–4974, Oct. 2013.
[20] M. Najafi, V. Jamali, and R. Schober, "Optimal relay selection for the parallel hybrid RF/FSO relay channel: Non-buffer-aided and buffer-aided designs," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 2794–2810, Jul. 2017.
[21] A. Bletsas, H. Shin, and M. Z. Win, "Cooperative communications with outage-optimal opportunistic relaying," *IEEE Trans. Wireless Commun.*, vol. 6, no. 9, pp. 3450–3460, Sep. 2007.
[22] Z. Zhang, X. Chai, K. Long, A. V. Vasilakos, and L. Hanzo, "Full duplex techniques for 5G networks: Self-interference cancellation, protocol design, and relay selection," *IEEE Commun. Mag.*, vol. 53, no. 5, pp. 128–137, May 2015.
[23] B. Van Nguyen, H. Jung, and K. Kim, "Physical layer security schemes for full-duplex cooperative systems: State of the art and beyond," *IEEE Commun. Mag.*, vol. 56, no. 11, pp. 131–137, Nov. 2018.
[24] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1628–1631, Oct. 2012.
[25] A. Basilevsky, *Applied Matrix Algebra in the Statistical Sciences*. New York, NY, USA: North Holland, 1983.
[26] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
[27] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.
[28] X. Tang, Y. Cai, W. Yang, W. Yang, T. Zhang, and H. Chen, "Outage analysis of buffer-aided underlay cognitive relay networks with outdated CSI," *AEU-Int. J. Electron. Commun.*, vol. 70, no. 3, pp. 359–366, Mar. 2016.
[29] Y. Huang, J. Wang, C. Zhong, T. Q. Duong, and G. K. Karagiannidis, "Secure transmission in cooperative relaying networks with multiple antennas," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6843–6856, Oct. 2016.
[30] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. San Diego, CA, USA: Academic, 2007.
[31] Z. Wang and G. B. Giannakis, "A simple and general parameterization quantifying performance in fading channels," *IEEE Trans. Commun.*, vol. 51, no. 8, pp. 1389–1398, Aug. 2003.
[32] 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.
[33] A. Afana, V. Asghari, A. Ghrayeb, and S. Affes, "Cooperative relaying in spectrum-sharing systems with beamforming and interference constraints," in *Proc. IEEE 13th Int. Workshop Signal Process. Adv. Commun.*, Jun. 2012, pp. 429–433.

CHEN WEI received the B.S. degree in electronic information engineering from the Taiyuan University of Technology, Taiyuan, China, in 2017. He is currently pursuing the M.S. degree with the College of Communication Engineering, Army Engineering University of PLA. His current research interests include cooperative communications, physical layer security, and cognitive radio systems.

WENDONG YANG received the B.S. degree in communications engineering and the Ph.D. degree in communications and information Systems from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2004 and 2009, respectively, where he has been with the College of Communications Engineering, since 2009. His current research interests include MIMO systems, OFDM systems, cooperative communications, and cognitive radio.

YUEMING CAI (M'05–SM'12) received the B.S. degree in physics from Xiamen University, Xiamen, China, in 1982, and the M.S. degree in microelectronics engineering and the Ph.D. degree in communications and information systems from Southeast University, Nanjing, China, in 1988 and 1996, respectively. His current research interests include cooperative communications, signal processing in communications, wireless sensor networks, and physical layer security.

XUANXUAN TANG received the B.S. degree in communication engineering from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2014. He is currently pursuing the Ph.D. degree in information and communications engineering with the College of Communications Engineering, Army Engineering University of PLA, Nanjing. His current research interests include cooperative communications, wireless sensor networks, Internet of Things, physical layer security, energy harvesting, full-duplex, and cognitive radio systems.

GUOQIN KANG received the B.S. degree in communications engineering and the M.S. degree in electronics science and technology from the College of Communication Engineering, PLA University of Science and Technology, Nanjing, China, in 2004 and 2008, respectively, and the Ph.D. degree in campaign from National Defense University, Beijing, China, 2016. He is currently an Associate Professor with the College of Information and Communication, National University of Defense Technology. His current research interests include spectrum management, cognitive radio, IMT systems, and cyberspace security.