IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 20, 2019, accepted September 6, 2019, date of publication September 30, 2019, date of current version December 26, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2944543

On the Security Analysis of a Cooperative Incremental Relaying Protocol in the Presence of an Active Eavesdropper

SAEED VAHIDIAN[1], SAJAD HATAMNIA[2], AND BENOIT CHAMPAGNE[3], (Senior Member, IEEE)

[1]Department of Electrical and Computer Engineering, University of California San Diego, San Diego, CA 92093, USA
[2]Faculty of Electrical and Computer Engineering, K. N. Toosi University of Technology, Tehran 47231210, Iran
[3]Department of Electrical and Computer Engineering, McGill University, Montreal, QC H3A 0E9, Canada

Corresponding author: Saeed Vahidian (saeed@ucsd.edu)

The work of B. Champagne was supported by the Natural Sciences and Engineering Research Council (NSERC), Canada.

ABSTRACT Physical layer security offers an efficient means to decrease the risk of confidential information leakage through wiretap links. In this paper, we address the physical-layer security in a cooperative wireless subnetwork that includes a source-destination pair and multiple relays, exchanging information in the presence of a malevolent eavesdropper. Specifically, the eavesdropper is active in the network and transmits artificial noise (AN) with a multiple-antenna transmitter to confound both the relays and the destination. We first analyse the secrecy capacity of the direct source-to-destination transmission in terms of intercept probability (IP) and secrecy outage probability (SOP). A decode-and-forward incremental relaying (IR) protocol is then introduced to improve security of communications in the presence of the active eavesdropper. Within this context, and depending on the availability of channel state information, three different schemes (one optimal and two sub-optimal) are proposed to select a trusted relay and improve the achievable secrecy rate. For each one of these schemes, and for both selection and maximum ratio combining at the destination and eavesdropper, we derive new and exact closed-form expressions for the IP and SOP. Our analysis and simulation results demonstrate the superior performance of the proposed IR-based selection schemes for secure communication. They also confirm the existence of a floor phenomenon for the SOP in the absence of AN.

INDEX TERMS Artificial noise, incremental relaying, network, physical-layer security.

I. INTRODUCTION

Wireless communication is naturally susceptible to eavesdropping due to the openness of the wireless medium and its broadcast nature [1]. Hence, confidential information exchanged between legitimate nodes may easily be intercepted by unauthorized users. Due to increasing demand for private communication over wireless channels, security issues in wireless networks have gained considerable interest in recent years. Traditionally, security is implemented via cryptographic protocols using public or private keys at upper layers of the network stack. However, due to vulnerability in secret key distribution and management in dense wireless networks, information could be decrypted readily if the eavesdropper obtains the encryption key.

A. BACKGROUND

Using an information-theoretic approach, Shannon [2] and Wyner [3], and shortly afterwards Csiszár and Körner [4], have argued that it is possible to achieve perfectly secure communications without the use of cryptographic schemes if the channel of the wiretap link is inferior in quality to the legitimate channel. In that case, a confidential message can be encoded such that it can be reliably decoded at its intended destination while revealing almost no information to the eavesdropper. This line of work was extended in [5], where the impact of feedback on a wiretap channel was examined in terms of secrecy capacity, revealing that secure communication is still feasible, even when the

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

wiretap link is superior to the legitimate channel by exploiting feedback information. On such bases, physical (PHY) layer security derived from the information-theoretic perspective has attracted much attention in recent years as a promising approach for protecting against eavesdropping, without significantly increasing computational complexity [6]. The basic idea is to exploit the PHY characteristics of the wireless channels in order to mitigate eavesdropping attacks.

Taking advantage of multi-antenna systems to combat wireless fading as well as increasing the secrecy capacity of the link, there has been a growing interest in extending the basic Gaussian wiretap channel to multiple-input multiple-output (MIMO) terminals [7]. The authors in [8] focused on the achievable secrecy capacity of a multi-input single-output (MISO) configuration, while in [9] the PHY layer security in MIMO relay networks was studied, revealing a significant improvement in terms of secrecy rate through the use of MIMO relays. The secrecy capacity of a broadcast MIMO wiretap channel for an arbitrary number of transmit/receive antennas was studied in [10], which showed that the perfect secrecy capacity is equal to the maximal difference in mutual information between the wiretap and legitimate links. However, considering the hardware cost and size limitations of multiple-antenna systems, cooperative relaying offers a compelling alternative that enables single-antenna nodes to enjoy the benefits of multiple-antenna systems while enhancing end-to-end security and reliability of communications [11].

Depending on the role played by the relay in cooperative schemes, three different generic scenarios can be identified. In the first scenario, the relay nodes aim to assist the eavesdropper by decreasing the secrecy rate [12]. In the second scenario, the relay acts as both a collaborator and an eavesdropper [13]. In the third scenario, which is the focus of this work, the relay collaborates with the source to enhance security of the legitimate link [14]. Most of the existing works on user cooperation for PHY layer security focus on developing the secrecy rate from an information-theoretic viewpoint. In [15], three different types of cooperative schemes are investigated, namely: amplify-and-forward (AF), decode-and-forward (DF) and cooperative-jamming (CJ). In particular, optimal relay weight selection and power allocation strategies are proposed to enhance the achievable secrecy rate for the second hop. The authors in [16] study the four-node (i.e., source, destination, relay and eavesdropper) secure communication system for different relay strategies, including DF and noise-forwarding (NF). In [17], the four-node system is further examined in the context of multi-carrier transmissions, where the aim is to maximize the sum of secrecy rate under a total system power constraint. A novel relay selection strategy with jamming is investigated in [18], where the aim is to improve security at the destination under the assumption that the eavesdropper only overhears the second hop.

Reference [19] analyzes secure relay and jammer selection for the PHY-layer security improvement of a wireless network including multiple intermediate nodes and eavesdroppers. In [6], the authors propose a new multi-hop strategy where the relays add independent randomization in each hop, which leads to significant secrecy improvement for the end-to-end transmission. The PHY layer security is further explored in [20] for the two-way relay channels, where multiple two-way relays are employed to enhance the secrecy rate against eavesdropping attacks. Other related works addressing the problem of PHY layer security in the presence of multiple intermediate nodes or eavesdroppers include [21]–[23].

The aforementioned works are limited to cases where the eavesdropper node can only overhear the source's message or that of the relay but not both. The sub-network models invoked in these and other studies are often afflicted by further restrictions, which may limit their realm of application in practice. This includes the following: consideration of a single eavesdropper equipped with single antenna, as opposed to multiple antennas; legitimate network sending artificial noise to degrade the wiretap link but not the converse; and adoption of conventional cooperation protocols which are not spectrally efficient.

B. TECHNICAL CONTRIBUTIONS

Motivated by these observations, in this paper, we investigate the effects of different relay selection schemes as well as different combining techniques (under the Rayleigh fading model) on the PHY layer security when the eavesdropper has access to both the source and relay messages. Three relay selection schemes are employed based on the availability of the channel state information (CSI), namely: conventional selection, minimum selection, and optimal selection. In conventional selection, the selected relay is the one that results in the highest SNR at the destination. In minimum selection, the selected relay is the one that results in the lowest SNR at the eavesdropper. Finally, in optimal selection, the selected relay is the one that maximizes the secrecy capacity.

For each one of these schemes, we study the performance of a DF-incremental relaying (IR) protocol in the presence of eavesdropper's generated AN at both the relays and the destination. The IR protocol exploits a one-bit feedback from the destination to request DF retransmission of the source message from selected relays. Cooperative schemes based on IR outperform those based on the traditional retransmission of the source message [24], [25]. In effect, they are amongst the best performing schemes, as they preserve the channel resources *i.e.*, bandwidth and energy, while maintaining reliable communication.

By employing IR and due to the presence of direct links, the destination and the eavesdropper may each receive two different versions of the source message. Consequently, diversity signal combining techniques can be employed by these nodes, including: selection combining (SC), which only selects the best signal out of all replicas for further processing; and maximal ratio combining (MRC), which coherently adds the signal replicas together for detection. For convenience, henceforth, we shall use the nomenclature in Table 1 to refer to the various combinations of relay selection and signal combining schemes. In this table each scheme

TABLE 1. Adopted nomenclature for relay selection schemes under study.

Scheme	Signal Combining	Relay Selection
DMC	MRC	Conventional
DSC	SC	Conventional
DMM	MRC	Minimum
DSM	SC	Minimum
DMO	MRC	Optimal
DSO	SC	Optimal
DMA	MRC	All relays
DSA	SC	All relays
DT	-	No relay

is identified by a three-letter label where the first letter stands for the DF strategy, the second letter represents the type of the signal combining technique and the third letter denotes the adopted relay selection scheme. In addition, the scheme labeled "DT" denotes the conventional direct transmission and finally, "All relays" means that all successful relays in decoding cooperate simultaneously in the next phase.

While the literature on PHY layer security is abundant, physical layer security for cooperative IR networks affected by eavesdropper's generated AN has not been previously addressed. In this regard, our main contributions can be

- We consider a cooperative wireless network with multiple relays in the presence of an active eavesdropper and investigate communication security from the perspective of information theory. Unlike previous works, i.e. [26], [27] where the source or relays transmit AN together with information signals to deliberately interfere with the eavesdropper's received signal, both the relays and the destination node in our model are confounded by AN originating from the eavesdropper node, which represents the worst case scenario.
- Cooperative diversity with traditional fixed relaying leads to a notable loss in system capacity and efficiency because it requires two time intervals for half-duplex transmission. In order to prevent such a loss, we consider a novel IR strategy and investigate its performance in the context of secure communications.
- We present and investigate three different relay selection schemes to enhance PHY layer security against eavesdropping attack. In contrast to [28] which assumes conventional relay selection and therefore focuses on the relay-destination links, we herein depending on the availability of CSI examine alternative selection schemes which take into account the quality of both source-relay and relay-destination channels.
- We derive closed-form expressions for the intercept probability (IP) and the secrecy outage probability (SOP) of all the proposed schemes for cooperative IR networks, thereby fully characterizing the associated security trade-offs [29].
- To provide further insight into system behavior, we also derive corresponding asymptotic expressions for the SOP of each scheme in the high SNR regime. These expressions facilitate system design and help better understand the role played by various internal parameters and their interaction.

C. KEY FINDINGS

Based on the IP and SOP analysis analysis provided in this paper for the cooperative IR wireless network with an active eavesdropper, some of our key results include:

- When perfect CSI is available, the optimal relay selection scheme provides the best security performance as compared to the others. This follows because the optimal scheme takes into account the quality of both the source-destination and relay-destination links in its decision metric. In addition, the conventional selection scheme always outperforms minimum selection, which can be justified by invoking the concept of diversity order. Indeed conventional selection provides a diversity gain for the legitimate links when compared to minimum selection.
- The performance of SC is worse than that of MRC, typically exhibiting a few dBs of power penalty. This is the price paid for reduced complexity with SC, which allows a trade-off between complexity and performance. However, there is no significant performance gap between the two combining techniques when the minimum selection scheme is employed.
- Only marginal performance improvements can be obtained by increasing the number of relays for the DMM and DSM schemes.
- In the high SNR regime, all the proposed schemes achieve the same diversity gain, while the difference in their performance can be characterized by their achieved coding gain.

Mathematical Notations: The notation $o(x)$ means an higher order terms in x, (i.e. $\lim_{x\to 0} o(x)/x = 0$); $f(x)$ and $F(x)$ respectively denote the probability distribution function (PDF) and cumulative distribution function (CDF) of random variable (RV) X; $\Gamma(a, x)$ is the upper incomplete gamma function while $\Phi(a, b; x)$ is the confluent hypergeometric function of the second kind.

The rest of the paper is organized as follows. The adopted system and channel model for cooperative relaying with active eavesdropper are exposed in Section II. Section III concisely develops the secrecy analysis of the direct transmission model as a benchmark. Sections IV and V present the proposed IR-based schemes and their secrecy performance analysis, respectively. Section VI analyzes diversity order in the high SNR regime. Section VII presents numerical and simulation results to support the theoretical study. Finally, Section VIII contains concluding remarks.

II. SYSTEM MODEL

Consider the generic topology shown in Fig. 1 for secure communication in a cooperative wireless sub-network consisting of a source S, a destination D, and a cluster of M

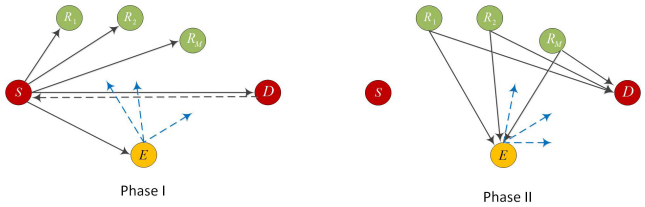

FIGURE 1. A wireless relay network consisting of one source (*S*), one destination (*D*), and *M* relay nodes R_m, exchanging information in the presence of an eavesdropper (*E*). The continuous and dashed black lines correspond to the legitimate forward and backward links of the legitimate network, respectively, while the dashed blue line illustrates the AN propagated by *E*.

DF relays $R_m, m \in \{1, \ldots, M\}$. The purpose of the relays is to assist the data transmission between the source and the destination, in order to protect against the attack of a malicious eavesdropper E. The source, destination and relay nodes, each equipped with single-antenna receiver and/or transmitter, are characterized by the half-duplex constraint and therefore cannot transmit and receive simultaneously; meanwhile, the eavesdropper node, which is equipped with single-antenna receiver and multiple-antenna transmitter, operates in full duplex mode. Specifically, the eavesdropper is active and utilizes a hybrid overhearing and AN generating mechanism. Herein, ''hybrid'' means that during the data exchange, the eavesdropper not only overhears to extract confidential information but also propagates AN to degrade the PHY layer security of the legitimate sub-network. To this end, the eavesdropper can use multiple-antennas or collude with other attackers concealed nearby to generate AN and confound the target receivers.[1]

Unlike traditional cooperation [30], in the considered topology only a subset of the M relays will be activated. Specifically, we consider IR as a cooperation protocol which exploits an one-bit feedback from the destination to the source in the form of Acknowledgement/Negative-Acknowledgement (ACK/NACK) signaling as shown in Fig. 1. Specifically, the proposed IR protocol consists of two main half-duplex transmission phases, where the first phase is further decomposed into two stages, as explained below:

I-a During the first time slot, source S broadcasts its signal to destination D, while all the relays R_m, $m \in \{1, \ldots, M\}$, also attempt to decode it. Let $\mathcal{F}$ denote the random subset of relays that can successfully decode the source message, referred to as the well-informed relay subset (WIRS). Accordingly, the sample space of all possible WIRS outcomes is the power set $\mathcal{P}(\{R_1, \ldots, R_M\})$ with cardinality 2^M. In the sequel, it is convenient to individually represent these subsets by $\mathcal{F}_n$ where the index $n \in \{0, 1, \ldots, 2^M - 1\}$ and $\mathcal{F}_0 = \emptyset$.

I-b Next, let $\mathcal{R}$ be a pre-determined rate which is contingent on the quality of service (QoS) of the source-destination link. On the basis of rate $\mathcal{R}$, destination D decides whether another copy of the source signal is required or not. As previously mentioned, the retransmission process is based on an ACK/NACK mechanism, in which short-length error-free packets are broadcasted by D over a separate channel, to inform S and relays $\{R_m\}$ of the QoS status of its reception.

II During the second phase, if necessary, i.e., if the achievable rate of the source-destination channel falls below $\mathcal{R}$, selected relays R_m from $\mathcal{F}$ process their received signals using the DF protocol [31], whereby a copy of the original source message is generated and transmitted again to D. There is no direct signal from S to D during this phase.

In Phase I, source S transmits a sequence of complex valued digital symbols to destination D, at the rate $\mathcal{R}$ in units of bits per channel use. Here, we assume that quadrature phase-shift keying (QPSK) is employed as the modulation technique, and we let $\mathcal{A}$ with cardinality $Q = |\mathcal{A}|$ denote the normalized symbol constellation. Hence, at a given time instant, S transmits a scaled random symbol $\sqrt{P_s}s$, where $s \in \mathcal{A}$ with $E\{|s|^2\} = 1$ and P_s is the source transmit power. Due the broadcast nature of electromagnetic waves, the radio signal emitted by S will also reach some unintended areas, i.e., information leakage. Consequently, eavesdropper E overhears the transmission of S and attempts to extract its confidential signal. During Phase I, and II if applicable, E emits an AN vector expressed by $[\sqrt{P}x_1, \ldots, \sqrt{P}x_N]$, where N is the number of available transmit antennas, x_i for $i \in \{1, 2, \ldots, N\}$ are independent random variables taken from a complex circular Gaussian distribution [2] with zero mean and variance $E\{|x_i|^2\} = 1$, $P = P_{tot}/N$ is the transmit power allocated to each antenna, and P_{tot} is the total AN power budget [3] of E. Ideally, the AN is generated to be in the null space of E's receiving channel, and hence, does not affect E but degrades the receivers' channels [32].

It is assumed that all wireless links in Fig. 1, including the E's channels, exhibit frequency flat Rayleigh block fading. This means that the fading channel coefficients remain (approximately) static for one coherence interval, but change independently in different coherence intervals according to a zero-mean circularly symmetric complex Gaussian distribution. We let $h_{i,j}$ denote the complex valued channel coefficient characterizing the transmission from node i to node j, where $i, j \in \{s, d, e, r_1, \ldots, r_M\}$. The receivers at nodes S, D, E, and R_m are impaired by additive

[1] Even if the eavesdropper is equipped with a single antenna, by collaborating with helper nodes in its surrounding, it can control the generation of AN that can still be malicious.

[2] While the Gaussian distribution may not be optimal for the eavesdropper, this assumption does not significantly lessen the generality of our analysis since, according to the central limit theorem (CLT), when the independent random variables x_i are superimposed at the receiver, their weighted sum tends toward a Gaussian distribution.

[3] In this work, it is assumed that the eavesdropper has a specific power budget which is uniformly allocated to the available antennas. Nevertheless, our subsequent analysis remains general, since the mean values of all the channel gains between the AN antennas and the other legitimate nodes, as represented by $\bar{\sigma}_{ij}$, can be different.

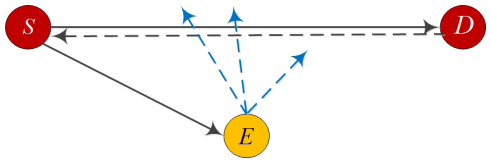

FIGURE 2. A wireless relay network consisting of one source (*S*) and one destination (*D*) exchanging information in the presence of an eavesdropper (*E*). The continuous and dashed black lines correspond to the forward links of the legitimate network, while the dashed blue line shows the AN propagated by *E*.

white Gaussian noise (AWGN). Hence, the signal-to-noise ratio (SNR) with respect to (w.r.t.) link *i*-*j*, i.e., $P_{\rm i}|h_{i,j}|^2/\sigma_n^2$ follows an exponential distribution with mean denoted as $\bar{\sigma}_{ij}$, where P_i is the transmit power at node i and σ_n^2 is the noise variance at all nodes. Likewise, we let $c_{i,j}$ denote the complex channel gain between the $i^{\rm th}$ AN antenna of E and the mth relay R_m or the destination D, where the subscripts $i \in \{1,\ldots,N\}$ and $j \in \{m,d\}$. Hence, $|c_{i,j}|^2$ follows an exponential distribution whose mean is also denoted by $\bar{\sigma}_{ij}$ for convenience.

III. DIRECT TRANSMISSION

In the following and for later reference, we proceed by presenting the security analysis in the special case of direct transmission (i.e., without using relay cooperation) as a benchmark. Subsequently, in Section IV, we will consider the DF-based IR protocol to improve the PHY layer security against eavesdropping attack.

In the case of direct transmission (Fig. 2), which corresponds to Phase I-a, the received signals at D and E are respectively given by

$$r_{s,d} = \sqrt{P_s}h_{s,d}s + \sum_{i=1}^{N}\sqrt{P}c_{i,d}x_i + n_{s,d}, \tag{1}$$

$$r_{s,e} = \sqrt{P_s}h_{s,e}s + n_{s,e}, \tag{2}$$

where $n_{s,d} \sim \mathcal{CN}\left(0,\sigma_n^2\right)$ and $n_{s,e} \sim \mathcal{CN}\left(0,\sigma_n^2\right)$ are the additive noise terms at the destination and eavesdropper nodes, respectively.[4] Then, the channel capacities of the direct $S-D$ and wiretap $S-E$ links are given by

$$C_{sd} = \log_2\left(1+\Psi_{sd}\right), \quad \Psi_{sd} = \frac{P_{\rm s}|h_{s,d}|^2}{\sum\limits_{i=1}^{N}P|c_{i,d}|^2+\sigma_n^2}, \tag{3}$$

$$C_{se} = \log_2\left(1+\Psi_{se}\right), \quad \Psi_{se} = \frac{P_{\rm s}|h_{s,e}|^2}{\sigma_n^2}. \tag{4}$$

According to [28], when the capacity of the wiretap $S-E$ link is lower than the data rate $\mathcal{R}$, E will fail to decode the message from S, while the legitimate $S-D$ link remains secure. However, if the capacity of the wiretap link becomes higher than the data rate $\mathcal{R}$, E may succeed in decoding S's message and hence, an intercept event occurs. Within this context, the intercept probability (IP) defined below is a key metric in evaluating the performance of PHY layer security:

$$\mathcal{P}_{\rm int}^{\rm DT} = \Pr\left(C_{se} > \mathcal{R}\right) = \exp\left(-\frac{\delta}{\bar{\sigma}_{se}}\right) \tag{5}$$

where $\delta = 2^{\mathcal{R}}-1$ and the superscript DT stands for direct transmission. As expected, the IP is contingent on the transmit power of source S and the quality of the wiretap $S-E$ link, through the parameter $\bar{\sigma}_{se}$, as well as the data rate $\mathcal{R}$. Note that increasing the data rate or decreasing the transmit power of the source, causes the IP to decrease. However, this comes at the cost of a deterioration in secrecy, since the SOP of the legitimate link increases (see below) when a higher data rate or lower transmit power is adopted at S.

Let us next investigate the achievable secrecy rate of direct transmission, which is defined as the difference between the information rate of the $S-D$ link and that of the $S-E$ link [30]:

$$C_{sd}^{\rm DT} = \left[C_{sd}-C_{se}\right]^+ = \log_2\left(\frac{1+\Psi_{sd}}{1+\Psi_{se}}\right), \tag{6}$$

where $[x]^+ = \max[x,0]$.[5] Under the security constraint, a secrecy outage event occurs for the legitimate network whenever a transmitted message cannot be received in secrecy i.e., when the secrecy rate falls below the thresholding secure rate $\mathcal{R}$. In this regard, the secrecy outage probability (SOP) provides another key metric in evaluating the performance of PHY layer security. For the traditional direct transmission mode, the SOP can be formulated as

$$\begin{aligned}\mathcal{P}_{\rm out}^{\rm DT} &= \Pr\left(C_{\rm sd}^{\rm DT} \le \mathcal{R}\right) = \Pr\left(\log_2\left(\frac{1+\Psi_{sd}}{1+\Psi_{se}}\right) < \mathcal{R}\right)\\ &= \Pr\left(\Psi_{sd} \le 2^{\mathcal{R}}\Psi_{se}+\delta\right).\end{aligned} \tag{7}$$

In order to obtain the SOP of the traditional direct transmission, we need the CDF of RV Ψ_{sd} and the PDF of RV Ψ_{se}. The PDF of Ψ_{se} can be written as

$$f_{\Psi_{se}}\left(\Psi_{se}\right) = \frac{1}{\bar{\sigma}_{se}}\exp\left(-\frac{1}{\bar{\sigma}_{se}}\Psi_{se}\right), \tag{8}$$

while the CDF of Ψ_{sd} is given by the following Lemma.

Lemma 1: The CDF of Ψ_{sd} can be expressed as

$$F_{\Psi_{sd}}\left(\Psi_{sd}\right) = 1-\sum_{i=1}^{N}\pi_{sd,i}\frac{\kappa_{sd,i}}{\Psi_{sd}+\kappa_{sd,i}}\exp\left(-\frac{\Psi_{sd}}{\bar{\sigma}_{sd}}\right), \tag{9}$$

where $\kappa_{sd,i} = \frac{\bar{\sigma}_{sd}}{\bar{\sigma}_{id}}$ and $\pi_{sd,i} = \prod\limits_{\substack{j=1\\ j\neq i}}^{N}\frac{\bar{\sigma}_{id}}{\bar{\sigma}_{id}-\bar{\sigma}_{jd}}$.

Proof: See Appendix A. ∎

[4] For simplicity, we assume that these noise terms have the same power but the analysis can be extended to the case of different noise powers.

[5] When the secrecy capacity is negative, a SOP event occurs.

Using these expressions, the SOP of the conventional direct transmission is obtained as

$$\begin{aligned}\mathcal{P}_{\text{out}}^{\text{DT}} &= \int_0^{\infty} F_{\Psi_{sd}}\left(2^{\mathcal{R}}\Psi_{se}+\delta\right) f_{\Psi_{se}}(\Psi_{se})\; d\Psi_{se} \\ &= 1-\sum_{i=1}^{N}\bar{\sigma}_{se}^{-1}\pi_{sd,i}\kappa_{sd,i}(\delta+1)^{-1}\exp\left(\frac{(\delta+\kappa_{sd,i})}{\bar{\sigma}_{se}(\delta+1)}+\frac{\kappa_{sd,i}}{\bar{\sigma}_{sd}}\right) \\ &\quad\times\Gamma\left(0,\frac{(\delta+\kappa_{sd,i})}{\bar{\sigma}_{se}(\delta+1)}+\frac{(\delta+\kappa_{sd,i})}{\bar{\sigma}_{sd}}\right). \end{aligned} \tag{10}$$

IV. PROPOSED DF INCREMENTAL RELAYING SCHEME

In this and the next sections, the proposed relay selection scheme is exposed and its secrecy performance analyzed. We here make use of the DF relaying strategy along with IR protocol to augment the spectral efficiency over fixed relaying systems. Based on the model description provided in Section II, the received signal from S at a given relay R_m during Phase I, and the received signal from a selected relay R_m at D and E during Phase II, are respectively given by

$$r_{s,m} = \sqrt{P_s}h_{s,m}s+\sum_{\ell=1}^{N}\sqrt{P}c_{\ell,m}x_{\ell}+n_{s,m}, \tag{11}$$

$$r_{m,d} = \sqrt{P_m}h_{m,d}s+\sum_{i=1}^{N}\sqrt{P}c_{i,d}x_i+n_{m,d}, \tag{12}$$

$$r_{m,e} = \sqrt{P_m}h_{m,e}s+n_{m,e}, \tag{13}$$

where $P_s = P'/2$ and $P_m = P'/2$ are the transmitted power at S and R_m respectively and P' is the total power budget of the network, while $n_{s,m} \sim \mathcal{CN}\left(0,\sigma_n^2\right)$, $n_{m,d} \sim \mathcal{CN}\left(0,\sigma_n^2\right)$ and $n_{m,e} \sim \mathcal{CN}\left(0,\sigma_n^2\right)$ are additive noise terms. There are two possible cases for the data transmission depending on whether the WIRS $\mathcal{F}$ is empty or not. For simplicity, let $\mathcal{F}=\emptyset$ represents the former case and $\mathcal{F}=\mathcal{F}_n$ the latter.

- Case $\mathcal{F}=\emptyset$: This case corresponds to a situation where all the relays fail in perfectly decoding the source signal. From an information theoretic perspective, this condition occurs when the data rate exceeds the capacity of all the links between source S and the relays R_m, which can be expressed based on (11) in the following form,

$$\frac{1}{2}\log_2(1+\Psi_{sm}) < \mathcal{R}, \quad \forall m, \tag{14}$$

where $\Psi_{sm} = \frac{P_s|h_{s,m}|^2}{\sum_{i=1}^{N}P|c_{i,m}|^2+\sigma_n^2}$ is the SNR of the $S-R_m$ link. Based on (14), the occurrence probability of case $\mathcal{F}=\emptyset$ is threfore given by

$$\begin{aligned}\Pr(\mathcal{F}=\emptyset) &= \prod_{m=1}^{M}\Pr\left(\frac{1}{2}\log_2(1+\Psi_{sm})<\mathcal{R}\right) \\ &= \prod_{m=1}^{M}\Pr\left(\Psi_{sm}<2^{2\mathcal{R}}-1\right) = \prod_{m=1}^{M}\mathcal{E}_m, \end{aligned} \tag{15}$$

where $\mathcal{E}_m = 1-\sum_{\ell=1}^{N}\pi_{s,\ell}\frac{\kappa_{s,\ell}}{\varrho+\kappa_s}\exp\left(-\frac{\varrho}{\bar{\sigma}_{sm}}\right)$, $\varrho = 2^{2\mathcal{R}}-1$, $\pi_{s,\ell} = \prod_{\substack{q=1\\q\neq\ell}}^{N}\frac{\bar{\sigma}_{\ell m}}{\bar{\sigma}_{\ell m}-\bar{\sigma}_{qm}}$ and $\kappa_{s,\ell} = \frac{\bar{\sigma}_{sm}}{\bar{\sigma}_{\ell m}}$.

- Case $\mathcal{F}=\mathcal{F}_n$ ($n\neq 0$): This case corresponds to a situation where all the relays in WIRS $\mathcal{F}_n$ can decode the source signal successfully. Hence, invoking the above information theoretic criterion, the event $\mathcal{F}=\mathcal{F}_n$ can be formulated as

$$\frac{1}{2}\log_2(1+\Psi_{sm}) > \mathcal{R} \text{ if and only if } m\in\mathcal{F}_n \tag{16}$$

Based on (16), the occurrence probability of case $\mathcal{F}=\mathcal{F}_n$ can be formulated as

$$\begin{aligned}\Pr(\mathcal{F}=\mathcal{F}_n) &= \prod_{m\in\mathcal{F}_n}\Pr\left(\frac{1}{2}\log_2(1+\Psi_{sm})>\mathcal{R}\right) \\ &\quad\times\prod_{m\in\bar{\mathcal{F}}_n}\Pr\left(\frac{1}{2}\log_2(1+\Psi_{sm})<\mathcal{R}\right) \\ &= \prod_{m\in\mathcal{F}_n}\Pr(\Psi_{sm}>\varrho)\prod_{m\in\bar{\mathcal{F}}_n}\Pr(\Psi_{sm}<\varrho) \\ &= \prod_{m\in\mathcal{F}_n}\mathcal{E}_m\prod_{m\in\bar{\mathcal{F}}_n}(1-\mathcal{E}_m). \end{aligned} \tag{17}$$

During the cooperative Phase II and according to the assumed security protocol, when $\mathcal{F}_n$ is non-empty, the best relay is chosen from $\mathcal{F}_n$ to forward its decoded signal toward the destination, allowing the eavesdropper to intercept the transmission.

V. SECURITY-RELIABILITY ANALYSIS OF IR SCHEMES

Depending on the available CSI knowledge for the different links and the system complexity, different relay selection schemes are presented and analyzed for the following three base cases:

- Case I: When the CSI of the legitimate channels (i.e. $S-R_m, R_m-D$) is available but not that of the R_m-E channel, the conventional relay selection scheme is implemented, in which the selected relay maximizes the SNR at D. The latter scheme only takes into account the capacity of the legitimate channels, without considering the secrecy rate.
- Case II: When only the CSI of the R_m-E link is known, the minimum relay selection scheme is applied, in which the selected relay minimizes the SNR at E. We note that for both Cases I and II, suboptimal relay selection is performed.
- Case III: When the CSI of the R_m-E and R_m-D links is available, an optimal relay selection scheme is implemented, whereby the relay that achieves the maximum secrecy rate is chosen for retransmission.

Compared to conventional relay selection approaches [33]–[35] where only the CSI of the legitimate $S-R_m$ and R_m-D links are required, in the optimal IR scheme,

knowledge of the magnitudes of the eavesdroppers channels is needed for maximizing the secrecy rate [11]). The assumption of known CSI at eavesdropper E can be justified when E is presumed to be a legitimate user waiting to be served by source S, while the latter is attempting to transmit a legitimate message to destination D. In this setup, E has to know and report its CSI to S to be considered for future service. This situation is of particular interest in networks combining multicast and unicast transmissions.

Without loss of generality, assuming that event $\mathcal{F} = \mathcal{F}_n$ occurs and relay "m" is selected as the "best one", the corresponding $R_m - D$ and $R_m - E$ channel capacities are

$$C_{md}^{\mathrm{DF}} = \frac{1}{2}\log_2\left(1+\Psi_{md}\right), \tag{18}$$

$$C_{me}^{\mathrm{DF}} = \frac{1}{2}\log_2\left(1+\Psi_{me}\right), \tag{19}$$

where $\Psi_{md} = \frac{P_m|h_{m,d}|^2}{\sum_{i=1}^{N} P|c_{i,d}|^2+\sigma_n^2}$, $\Psi_{me} = \frac{P_m|h_{m,e}|^2}{\sigma_n^2}$ and the superscript DF refers to decode-and-forward. For the case of unsuccessful direct transmission where the Phase II is necessary, two time slots are required to transmit the data, justifying the factor of 1/2 in (18)-(19). To boost the effective channel gain and thereby enhance communication reliability, the destination then applies either MRC or SC to the signals received during both phases, and generates an estimation of the original signal after maximum likelihood decoding (MLD). The two types of combining solutions are considered for both the destination and eavesdropper nodes, leading to various ramifications in our analysis, as detailed below (see also Table 1).

A. SUBOPTIMAL SELECTION CASE I: DMC

Let us investigate the security performance of the DF IR scheme when a combination of the conventional relay mode and the MRC technique are applied. In this approach, the relay selection does not take into account the eavesdropper's channels, but is based instead on the instantaneous quality of the combined $S-D$ and $R_m - D$ links, with the aim to maximize the achievable rate at the destination node. Specifically, the index of the relay chosen to forward the legitimate signal from S to D is given by

$$m^* = \underset{m\in\mathcal{F}_n}{\operatorname{argmax}}\ C_{sd}^{\mathrm{DM}}, \tag{20}$$

where we define $C_{sd}^{\mathrm{DM}} = \frac{1}{2}\log_2\left(1+\Psi_{md}+\Psi_{sd}\right)$. Notice that for the MRC technique, the effective SNR is given by the sum of two SNRs, i.e., Ψ_{md} and Ψ_{sd}. Then, the secrecy rate is expressed as

$$C_{sd}^{\mathrm{DMC}} = \left[C_d^{\mathrm{DMC}} - C_e^{\mathrm{DM}}\right]^+ = \frac{1}{2}\log_2\left(\frac{1+\max\limits_{m\in\mathcal{F}_n}\Psi_{md}+\Psi_{sd}}{1+\Psi_{m^*e}+\Psi_{se}}\right), \tag{21}$$

where $C_d^{\mathrm{DMC}} = \max\limits_{m\in\mathcal{F}_n} C_{sd}^{\mathrm{DM}}$ and $C_e^{\mathrm{DM}} = \frac{1}{2}\log_2\left(1+\Psi_{me}+\Psi_{se}\right)$.

We now derive an analytical expression for the IP for conventional relaying with MRC. To this end, we first present the following general expression for the IP, which is based on the law of total probability and is applicable to various combinations of signal combining and relay selection schemes,

$$\mathcal{P}_{\mathrm{int}} = \Pr\left(\mathcal{F}=\emptyset\right)\mathcal{P}_{\mathrm{int}}^{\mathrm{DT}} + \sum_{n=1}^{2^M-1}\Pr\left(\mathcal{F}=\mathcal{F}_n\right)\mathcal{P}_{\mathrm{int}}^{\mathrm{Q}}, \tag{22}$$

where superscript $\mathcal{Q} \in$ {DSC, DSM, DMC, DMM, DMA, DSA} refers to the applicable scheme and $\mathcal{P}_{\mathrm{int}}^{\mathrm{Q}} = \Pr\left(C_e^{\mathrm{Q}} > \mathcal{R}\right)$. In the particular case of interest here, i.e. $\mathcal{Q} =$ DMC, the following closed-form expression for the IP can be obtained,

$$\begin{aligned}\mathcal{P}_{\mathrm{int}}^{\mathrm{DMC}} &= \Pr\left(\frac{1}{2}\log_2\left(1+\Psi_{m^*e}+\Psi_{se}\right) > \mathcal{R}\right)\\ &= 1-\Pr(\Psi_{m^*e}+\Psi_{se}<\varrho) = \sum_{l=1}^{5}\tilde{\mathbf{r}}(l)\exp\left(-\tilde{\mathbf{t}}(l)\,\varrho\right),\end{aligned} \tag{23}$$

where $\tilde{\mathbf{r}} = [1, -\rho, \rho, \lambda, -\lambda]$, $\tilde{\mathbf{t}} = \left[0, 0, \frac{1}{\bar{\sigma}_{me}}, 0, \frac{1}{\bar{\sigma}_{se}}\right]$, $\rho = \frac{\bar{\sigma}_{me}}{(\bar{\sigma}_{me}-\bar{\sigma}_{se})}$ and $\lambda = \frac{\bar{\sigma}_{se}}{(\bar{\sigma}_{me}-\bar{\sigma}_{se})}$.

Next, we focus on the derivation of the SOP expression. For a DF IR network using M relays, and based on the law of total probability, the following general expression can be obtained for the SOP,

$$\mathcal{P}_{\mathrm{out}} = \Pr\left(\mathcal{F}=\emptyset\right)\mathcal{P}_{\mathrm{out}}^{\mathrm{DT}} + \sum_{n=1}^{2^M-1}\Pr\left(\mathcal{F}=\mathcal{F}_n\right)\mathcal{P}_{\mathrm{out}}^{\tilde{\mathcal{Q}}}, \tag{24}$$

where $\tilde{\mathcal{Q}} \in$ {DSC,DSM,DSO, DMC, DMM, DMO, DMA, DSA} and $\mathcal{P}_{\mathrm{out}}^{\tilde{\mathcal{Q}}} = \Pr\left(C_{sd}^{\tilde{\mathcal{Q}}} < \mathcal{R}\right)$. Noting that $\mathcal{P}_{\mathrm{out}}^{\mathrm{DT}}$ was derived in (10), we next proceed to obtain $\mathcal{P}_{\mathrm{out}}^{\mathrm{DMC}}$. The following lemma and theorem provide key results towards this end.

Lemma 2: The CDF of RV $Y = \max\limits_{m\in\mathcal{F}_n}\Psi_{md}+\Psi_{sd}$ *can be expressed in closed-form as*

$$\begin{aligned}&F_Y(\varrho)\\ &= 1-\sum_{i=1}^{N}\frac{\pi_{sd,i}}{\bar{\sigma}_{id}\eta}\exp\left(-\frac{\varrho}{\bar{\sigma}_{sd}}\right) - \sum_{m=1}^{|\mathcal{F}_n|}\sum_{i=1}^{N}\frac{(-1)^{m-1}\pi_{sd,i}}{\bar{\sigma}_{sd}\bar{\sigma}_{id}}\\ &\quad\times\binom{|\mathcal{F}_n|}{m}\left[\frac{\exp\left(-\frac{m\varrho}{\bar{\sigma}_{md}}\right)}{\tilde{\eta}\left(\frac{1}{\bar{\sigma}_{id}}+\frac{m\varrho}{\bar{\sigma}_{md}}\right)} + \frac{\exp\left(-\frac{\varrho}{\bar{\sigma}_{sd}}\right)}{(\eta\tilde{\eta})}\right],\end{aligned} \tag{25}$$

where $\tilde{\eta} = \left(\frac{1}{\bar{\sigma}_{sd}} - \frac{m}{\bar{\sigma}_{md}}\right)$ and $\eta = \frac{\varrho}{\bar{\sigma}_{sd}} + \frac{1}{\bar{\sigma}_{id}}$.

Proof: See Appendix B. ■

The following theorem, whose proof relies on lemma 2, quantifies the SOP for the DMC case.

Theorem 1: The SOP for the DMC scheme is given by

$$\mathcal{P}_{\text{out}}^{\text{DMC}} = 1 - \sum_{l=1}^{2}\sum_{i=1}^{N} \frac{\mathbf{h}\,(l)\,\pi_{sd,i}}{\bar{\sigma}_{id}\,(\varrho+1)} \left[\chi_{\bar{\sigma}_{sd}} - \sum_{m=1}^{|\mathcal{F}_n|} (-1)^{m-1} \times \binom{|\mathcal{F}_n|}{m} \frac{\left[\chi_{m^{-1}\bar{\sigma}_{md}} - \chi_{\bar{\sigma}_{sd}}\right]}{\left(1 - \frac{m\bar{\sigma}_{sd}}{\bar{\sigma}_{md}}\right)} \right], \quad (26)$$

where $\chi_{\bar{\sigma}_{sd}} = \bar{\sigma}_{sd} \exp\left(-\frac{\varrho}{\bar{\sigma}_{sd}}\right) \Phi\left(1, 1; \eta + \frac{\eta\bar{\sigma}_{sd}}{\varrho+1}\mathbf{g}\,(l)\right)$ with $\chi_{m^{-1}\bar{\sigma}_{md}}$ obtained by substituting $m^{-1}\bar{\sigma}_{md}$ in place of $\bar{\sigma}_{sd}$ in $\chi_{\bar{\sigma}_{sd}}$, $\mathbf{h} = \left[\frac{1}{\bar{\sigma}_{me}-\bar{\sigma}_{se}}, -\frac{1}{\bar{\sigma}_{me}-\bar{\sigma}_{se}}\right]$ and $\mathbf{g} = \left[\frac{1}{\bar{\sigma}_{me}}, \frac{1}{\bar{\sigma}_{se}}\right]$.

Proof: See Appendix C ∎

B. SUBOPTIMAL SELECTION CASE I: DSC

In this subsection, we analyze the DF-based IR scheme in which the destination and the eavesdropper node employ SC in order to maximize their respective achievable rate. In this case, the relay that gives the maximum capacity at the destination node is selected, i.e.,

$$m^* = \underset{m\in\mathcal{F}_n}{\text{argmax}}\ C_{md}^{\text{DF}}, \quad (27)$$

where C_{md}^{DF} is defined in (18). Then, the secrecy rate for DSC is given by $C_{sd}^{\text{DSC}} = \left[C_s^{\text{DSC}} - C_e^{\text{DS}}\right]^+ = \frac{1}{2}\log_2\left(\frac{1+\max\left\{\max\limits_{m\in\mathcal{F}_n}\Psi_{md}, \Psi_{sd}\right\}}{1+\max\left\{\Psi_{m^*e}, \Psi_{se}\right\}}\right)$, where $C_e^{\text{DS}} = \max\left\{\frac{1}{2}\log_2\left(1+\Psi_{me}\right), \frac{1}{2}\log_2\left(1+\Psi_{se}\right)\right\}$, $C_s^{\text{DSC}} = \max\limits_{m\in\mathcal{F}_n} C_{sd}^{\text{DS}}$ and $C_{sd}^{\text{DS}} = \max\left\{\frac{1}{2}\log_2\left(1+\Psi_{md}\right), \frac{1}{2}\log_2\left(1+\Psi_{sd}\right)\right\}$. Notice that for the SC technique, the instantaneous SNR is given by the maximum of the two SNRs as in C_e^{DS} and C_{sd}^{DS}. In the following, we proceed to derive $\mathcal{P}_{\text{int}}^{\text{DSC}}$, starting with

$$\mathcal{P}_{\text{int}}^{\text{DSC}} = \Pr\left(\max\left\{\Psi_{se}, \Psi_{m^*e}\right\} > \varrho\right) = 1 - F_{\Psi_{m^*e}}(\varrho)F_{\Psi_{se}}(\varrho). \quad (28)$$

Making use of the CDFs of the RVs Ψ_{se} and Ψ_{me}, we obtain

$$\mathcal{P}_{\text{int}}^{\text{DSC}} = \sum_{l=1}^{3} \mathbf{r}\,(l) \exp\left(-\mathbf{b}\,(l)\,\varrho\right), \quad (29)$$

where $\mathbf{r} = [1, 1, -1]$ and $\mathbf{b} = \left[\frac{1}{\bar{\sigma}_{me}}, \frac{1}{\bar{\sigma}_{se}}, \frac{1}{\bar{\sigma}_{se}} + \frac{1}{\bar{\sigma}_{me}}\right]$.

Theorem 2: The SOP for the DSC scheme is given by

$$\mathcal{P}_{\text{out}}^{\text{DSC}} = 1 - \sum_{l=1}^{3}\sum_{m=1}^{|\mathcal{F}_n|}\sum_{i=1}^{N} \frac{\mathbf{a}\,(l)\,\pi_{sd,i}}{\bar{\sigma}_{id}} (-1)^{m-1} \binom{|\mathcal{F}_n|}{m} \times \left[\mathcal{I}_{m^{-1}\bar{\sigma}_{md}} - \mathcal{I}_{\tau^{-1}}\right] - \sum_{l=1}^{3}\sum_{i=1}^{N} \frac{\mathbf{a}\,(l)\,\pi_{sd,i}}{\bar{\sigma}_{id}} \mathcal{I}_{\bar{\sigma}_{sd}}, \quad (30)$$

where $\mathcal{I}_{\bar{\sigma}_{sd}} = \exp\left(-\frac{\varrho}{\bar{\sigma}_{sd}}\right) \frac{\bar{\sigma}_{sd}}{\varrho+1} \Phi\left(1, 1; \eta + \mathbf{b}\,(l)\,\frac{\bar{\sigma}_{sd}\eta}{\varrho+1}\right)$, $\tau = \left(\frac{m}{\bar{\sigma}_{md}} + \frac{1}{\bar{\sigma}_{sd}}\right)$ and $\mathbf{a} = \left[\frac{1}{\bar{\sigma}_{me}}, \frac{1}{\bar{\sigma}_{se}}, -\left(\frac{1}{\bar{\sigma}_{se}} + \frac{1}{\bar{\sigma}_{me}}\right)\right]$.

Proof: The proof follows the same steps as that of Theorem 1. ∎

C. SUBOPTIMAL SELECTION CASE II: DMM

We now investigate the use of MRC with the minimum selection scheme (DMM) under Case II, where CSI information about the $R_m - E$ links is available. The objective is to select the relay in $\mathcal{F}_n$ to minimize the achievable rate at the eavesdropper node. This relay selection scheme considers only the $R_m - E$ link and furthermore, both the destination and eavesdropper nodes employ MRC. In this case, the relay that yields the lowest instantaneous rate at the eavesdropper will be selected, i.e.,

$$m^* = \underset{m\in\mathcal{F}_n}{\text{argmin}}\ C_e^{\text{DM}}. \quad (31)$$

Consequently, the secrecy rate becomes $C_{sd}^{\text{DMM}} = \left[C_{sd}^{\text{DM}} - C_e^{\text{DMM}}\right]^+ = \frac{1}{2}\log_2\left(\frac{1+\Psi_{m^*d}+\Psi_{sd}}{1+\min\limits_{m\in\mathcal{F}_n}\Psi_{me}+\Psi_{se}}\right)$, where $C_e^{\text{DMM}} = \min\limits_{m\in\mathcal{F}_n} C_e^{\text{DM}}$. The IP expression for this case can be obtained as

$$\begin{aligned}\mathcal{P}_{\text{int}}^{\text{DMM}} &= \Pr\left(\frac{1}{2}\log_2\left(1+\min_m\ \Psi_{me}+\Psi_{se}\right) > \mathcal{R}\right)\\ &= 1 - \Pr\left(\min_m\ \Psi_{me}+\Psi_{se} < \varrho\right)\\ &= 1 - \sum_{l=1}^{2} \frac{\tilde{\mathbf{h}}\,(l)}{\tilde{\mathbf{g}}\,(l)}\left[1 - \exp\left(-\tilde{\mathbf{g}}\,(l)\,\varrho\right)\right], \end{aligned} \quad (32)$$

where $\tilde{\mathbf{g}}\,(l) = \left[\frac{1}{\bar{\sigma}_{se}}, \frac{|\mathcal{F}_n|}{\bar{\sigma}_{me}}\right]$ and $\tilde{\mathbf{h}}\,(l) = \left[\frac{|\mathcal{F}_n|}{(|\mathcal{F}_n|\bar{\sigma}_{se}-\bar{\sigma}_{me})}, -\frac{|\mathcal{F}_n|}{(|\mathcal{F}_n|\bar{\sigma}_{se}-\bar{\sigma}_{me})}\right]$.

To proceed with the derivation of the SOP, we first need to obtain a closed-form expression for the CDF of the RV $\tilde{Y} = \Psi_{m^*d} + \Psi_{sd}$, which is presented in the following lemma.

Lemma 3: The CDF of $\tilde{Y}$ *is given by*

$$\begin{aligned}F_{\tilde{Y}}(\gamma) &= 1 - \sum_{i=1}^{N} \frac{\pi_{sd,i}}{1+\frac{\bar{\sigma}_{id}}{\bar{\sigma}_{sd}}\gamma}\left[\exp\left(-\frac{\gamma}{\bar{\sigma}_{sd}}\right) + \frac{\exp\left(-\frac{\gamma}{\bar{\sigma}_{sd}}\right)}{\bar{\sigma}_{sd}\left(\frac{1}{\bar{\sigma}_{sd}} - \frac{1}{\bar{\sigma}_{md}}\right)}\right]\\ &\quad - \frac{\exp\left(-\frac{\gamma}{\bar{\sigma}_{md}}\right)}{\bar{\sigma}_{sd}\left(\frac{1}{\bar{\sigma}_{sd}} - \frac{1}{\bar{\sigma}_{md}}\right)} \sum_{i=1}^{N} \frac{\pi_{sd,i}}{\bar{\sigma}_{id}} \frac{1}{\left(\frac{\gamma}{\bar{\sigma}_{md}} + \frac{1}{\bar{\sigma}_{id}}\right)}. \end{aligned} \quad (33)$$

Proof: The proof of this lemma is analogous to that of Lemma 2. ∎

We are now in a position to derive the desired SOP expression, which is provided in the following theorem.

Theorem 3: The SOP for the DMM scheme is given by

$$\mathcal{P}_{\text{out}}^{\text{DMM}} = 1 - \sum_{l=1}^{2}\sum_{m=1}^{|\mathcal{F}_n|}\sum_{i=1}^{N} \frac{\tilde{\mathbf{h}}(l)\pi_{sd,i}\left[\mathcal{T}_{sd} + \vartheta\mathcal{T}_{md} - \vartheta\mathcal{T}_{sd}\right]}{\bar{\sigma}_{id}\,(\varrho+1)}, \quad (34)$$

where $\mathcal{T}_{sd} = \bar{\sigma}_{sd}\exp\left(-\frac{\varrho}{\bar{\sigma}_{sd}}\right)\Phi\left(1, 1; \eta + \frac{\tilde{\mathbf{g}}(l)\eta\bar{\sigma}_{sd}}{\varrho+1}\right)$ *and* $\vartheta = \left(1 - \frac{\bar{\sigma}_{sd}}{\bar{\sigma}_{md}}\right)$. *Proof: See Appendix* D. ∎

D. SUBOPTIMAL SELECTION CASE II: DSM

For this case, the relay is chosen according to the following rule,

$$m^* = \underset{m \in \mathcal{F}_n}{\operatorname{argmin}}\ C_e^{\mathrm{DS}}, \tag{35}$$

while the secrecy rate is given by $C_{sd}^{\mathrm{DSM}} = \left[C_{sd}^{\mathrm{DS}} - C_e^{\mathrm{DSM}}\right]^+ = \frac{1}{2}\log_2\left(\frac{1+\max\{\Psi_{m^*d}, \Psi_{sd}\}}{1+\max\left\{\min\limits_{m\in\mathcal{F}_n} \Psi_{me}, \Psi_{se}\right\}}\right)$, where $C_e^{\mathrm{DSM}} = \min\limits_{m\in\mathcal{F}_n} C_e^{\mathrm{DS}}$.

Herein we define the variable $u = \min\limits_{m\in\mathcal{F}_n} \Psi_{me}$ with CDF $F_U(\gamma) = 1 - \exp\left(-\frac{|\mathcal{F}_n|\gamma}{\bar{\sigma}_{me}}\right)$, in terms of which the intercept probability for the DSM case can be expressed as

$$\begin{aligned}\mathcal{P}_{\mathrm{int}}^{\mathrm{DSM}} &= \Pr\left(\frac{1}{2}\log_2\left(1+\max\left\{u, \Psi_{se}\right\}\right) > \mathcal{R}\right) \\ &= 1 - F_u(\varrho)F_{\Psi_{se}}(\varrho) = \sum_{l=1}^{3} \mathbf{r}(l)\exp\left(-\tilde{\mathbf{b}}(l)\, w\right), \end{aligned} \tag{36}$$

where $\tilde{\mathbf{b}} = \left[\frac{|\mathcal{F}_n|}{\bar{\sigma}_{me}}, \frac{1}{\bar{\sigma}_{se}}, \left(\frac{1}{\bar{\sigma}_{se}} + \frac{|\mathcal{F}_n|}{\bar{\sigma}_{me}}\right)\right]$.

Besides, the SOP can be obtained in closed-form as given in the following theorem.

Theorem 4: The SOP for the DSM scheme is given by

$$\mathcal{P}_{\mathrm{out}}^{\mathrm{DSM}} = 1 - \sum_{l=1}^{3}\sum_{m=1}^{|\mathcal{F}_n|}\sum_{i=1}^{N} \frac{\tilde{\mathbf{a}}(l)\,\pi_{sd,i}\left[\mathcal{J}_{\bar{\sigma}_{md}} + \mathcal{J}_{\bar{\sigma}_{sd}} - \mathcal{J}_{\tilde{\tau}^{-1}}\right]}{\bar{\sigma}_{id}(\varrho+1)}, \tag{37}$$

where $\mathcal{J}_{\bar{\sigma}_{md}} = \bar{\sigma}_{md}\exp\left(-\frac{\varrho}{\bar{\sigma}_{md}}\right)\Phi\left(1, 1; \mu + \frac{\mu\bar{\sigma}_{md}}{(\varrho+1)}\tilde{\mathbf{b}}(l)\right)$, $\tilde{\mathbf{a}} = \left[\frac{|\mathcal{F}_n|}{\bar{\sigma}_{me}}, \frac{1}{\bar{\sigma}_{se}}, -\left(\frac{1}{\bar{\sigma}_{se}} + \frac{|\mathcal{F}_n|}{\bar{\sigma}_{me}}\right)\right]$ and $\tilde{\tau} = \left(\frac{1}{\bar{\sigma}_{md}} + \frac{1}{\bar{\sigma}_{sd}}\right)$.

Proof: The proof is similar to that of Theorem 3. ■

E. OPTIMAL SELECTION CASE III: DSO

The two previously considered relay selection schemes do not simultaneously involve the relay to destination and relay to eavesdropper channels. In contrast, the optimal relay selection scheme takes into account CSI information for both the mentioned links. This subsection presents the DSO scheme where the relay selected for forwarding the source signal to the destination is the one achieving the maximum secrecy capacity, which by definition takes into account the quality of both links. Specifically, the desired relay is chosen as

$$m^* = \underset{m\in\mathcal{F}_n}{\operatorname{argmax}}\ C_m^{\mathrm{b}}, \tag{38}$$

where $C_m^b = \frac{1}{2}\log_2\left(\frac{1+\Psi_{md}}{1+\Psi_{me}}\right)$. The secrecy rate for this case is given by [28]

$$C_{sd}^{\mathrm{DSO}} = \max\left\{C^a, \max_{m\in\mathcal{F}_n} C_m^b\right\}. \tag{39}$$

where $C^a = \frac{1}{2}\log_2\left(\frac{1+\Psi_{sd}}{1+\Psi_{se}}\right)$. We notice that the derivation of the SOP in this case is quite challenging and it does not seem possible to obtain a closed-form expression. Therefore, we rely on the approximation of the SOP at high SNR in our study, as further developed in Section VI.

F. OPTIMAL SELECTION CASE III: DMO

In the case of DMO, the proposed selection technique selects the optimal relay as in (38), and the secrecy rate will be

$$C_{sd}^{\mathrm{DMO}} = \frac{1}{2}\log_2\left(2^{2C^a} + \max_{m\in\mathcal{F}_n} 2^{2C_m^b}\right). \tag{40}$$

Likewise the DSO case, obtaining a closed-form expression for the SOP in the DMO case is intractable. However, a closed form expression for the SOP in the high SNR regime will be obtained in Section VI. Nevertheless, numerical SOP results for the DSO and DMO cases can be obtained through computer simulations.

G. SUBOPTIMAL SELECTION: DSA

Thus far, emphasis has been placed on the cases in which only the best relay was employed in the cooperation phase. The DSA scheme considers the case where several relays (i.e. more than 1) can assist in forwarding confidential information from S to D. To be specific, all the relays in the WIRS re-encode the information and forward this re-encoded message to the destination (and eavesdropper) using orthogonal channels, either in time or frequency (see [36]).[6] This subsection assumes that both the destination and the eavesdropper use SC technique. Hence, the secrecy rate is defined as

$$\begin{aligned} C_{sd}^{\mathrm{DSA}} &= \left[C_{md}^{\mathrm{DSA}} - C_{me}^{\mathrm{DSA}}\right]^+ \\ &= \frac{1}{(|\mathcal{F}_n|+1)}\log\left(\frac{1+\max\left\{\Psi_{md}^{\mathrm{DSA}}, \Psi_{sd}\right\}}{1+\max\left\{\Psi_{me}^{\mathrm{DSA}}, \Psi_{se}\right\}}\right), \end{aligned} \tag{41}$$

where $P'_m = P'/(|\mathcal{F}_n|+1)$, $\Psi_{md}^{\mathrm{DSA}} = \frac{\max\limits_{m\in\mathcal{F}_n} P'_m|h_{md}|^2}{\sum\limits_{i=1}^{N} P_i|c_{id}|^2+\sigma_n^2}$ and $\Psi_{me}^{\mathrm{DSA}} = \max\limits_{m\in\mathcal{F}_n} \frac{P'_m|h_{m,e}|^2}{\sigma_n^2}$.

With the assumption that both the destination and the eavesdropper node employ SC, the IP of the DSA scheme can be formulated as

$$\begin{aligned}&\mathcal{P}_{\mathrm{int}}^{\mathrm{DSA}} \\ &= \sum_{m=1}^{|\mathcal{F}_n|} \frac{(-1)^{m-1}}{\bar{\sigma}_{se}\hat{\omega}}\binom{|\mathcal{F}_n|}{m}\left[\exp\left(-\frac{m\hat{\varrho}}{\bar{\sigma}_{me}}\right) - \exp\left(-\frac{\hat{\varrho}}{\bar{\sigma}_{se}} - \hat{\omega}\hat{\varrho}\right)\right]. \end{aligned} \tag{42}$$

where $\hat{\omega} = \left(\frac{1}{\bar{\sigma}_{se}} - \frac{m}{\bar{\sigma}_{me}}\right)$ and $\hat{\varrho} = 2^{R(|\mathcal{F}_n|+1)} - 1$. We next develop a closed-form expression of the secrecy outage performance for the DSA scheme. To begin, we first introduce the following key result.

Lemma 4: Let the denominator of the log function in (41) be $1+\gamma_1$. Then, the PDF of γ_1 is derived as

$$f_{\gamma_1}(\gamma) = \sum_{m_1=1}^{|\mathcal{F}_n|}\sum_{l=1}^{4} (-1)^{m_1-1}\binom{|F_n|}{m_1}\tilde{\mathbf{c}}(l)\exp\left(-\mathbf{c}(l)\,\gamma\right) \tag{43}$$

[6]The coordination of retransmission among the relays can easily be handled by a central server using available control channels.

where $\tilde{\mathbf{c}} = \left[\frac{m_1}{\bar{\sigma}_{me}}, -\frac{m_1}{\bar{\sigma}_{me}}, -\frac{1}{\bar{\sigma}_{se}}, \frac{1}{\bar{\sigma}_{se}}\right]$, $\mathbf{c} = \left[\frac{m_1}{\bar{\sigma}_{me}}, \hat{\varpi}, \hat{\varpi}, \frac{1}{\bar{\sigma}_{se}}\right]$ and $\hat{\varpi} = \left(\frac{m_1}{\bar{\sigma}_{me}} + \frac{1}{\bar{\sigma}_{se}}\right)$.

Proof: The CDF of Ψ_{me}^{DSA} and Ψ_{se} is obtained respectively as $F_{\Psi_{me}^{\mathrm{DSA}}}(\gamma) = 1 - \sum_{m=1}^{|\mathcal{F}_n|} (-1)^{m-1} \binom{|\mathcal{F}_n|}{m} \exp\left(-\frac{m\gamma}{\bar{\sigma}_{me}}\right)$ and $F_{\Psi_{se}}(\gamma) = \left[1 - \exp\left(-\frac{\gamma}{\bar{\sigma}_{se}}\right)\right]$. Then, by taking the derivative of $f_{\gamma_1}(\gamma) = \frac{d}{d\gamma}\left[F_{\Psi_{mE}^{\mathrm{DSA}}}(\gamma) \times F_{\Psi_{se}}(\gamma)\right]$ we obtain (43). ∎

Lemma 4 allows us to obtain a closed-form expression for the secrecy rate of the DSA scheme as stated in the following theorem.

Theorem 5: The SOP for the DSA scheme is given by

$$\mathcal{P}_{\mathrm{out}}^{\mathrm{DSA}} = 1 - \left[I_{\bar{\sigma}_{sd}} + \sum_{m=1}^{|F_n|} (-1)^{m-1} \binom{|\mathcal{F}_n|}{m} \left[I_{\bar{\sigma}_{md} m^{-1}} - I_{\tau^{-1}} \right] \right], \tag{44}$$

where

$$I_{\bar{\sigma}_{sd}} = \sum_{i=1}^{N} \sum_{m_1=1}^{|\mathcal{F}_n|} \sum_{l=1}^{4} \frac{\pi_{id}}{\bar{\sigma}_{id}} (-1)^{m_1-1} \tilde{\mathbf{c}}(l) \left(\frac{2^{2R}}{\bar{\sigma}_{sd}}\right)^{-1} \binom{|\mathcal{F}_n|}{m_1} \times \exp\left(-\frac{\hat{\varrho}}{\bar{\sigma}_{sd}}\right) \Phi\left(1, 1; \mathbf{c}(l)\, \eta \frac{\bar{\sigma}_{sd}}{2^{2R}} + \eta\right), \tag{45}$$

and $\eta = \left(\frac{1}{\bar{\sigma}_{id}} + \frac{\hat{\varrho}}{\bar{\sigma}_{sd}}\right)$.

Proof: Let the numerator of the log function in (41) be $1 + \gamma_2$. Using the PDF of RV γ_1 as in (43) as well as the CDF of RV Y in (25), we express the secrecy rate of the DSA scheme as

$$\mathcal{P}_{\mathrm{out}}^{\mathrm{DSA}} = \mathrm{E}_{\gamma_1}\left[\Pr\left(\gamma_2 < 2^{2R}\gamma_1 + \varrho\right)\right] \tag{46}$$

$$= \int_0^{\infty} F_{\gamma_2}\left(2^{2R}\gamma_1 + \hat{\varrho}\right) f_{\gamma_1}(\gamma_1)\, d\gamma_1. \tag{47}$$

The desired result is obtained by substituting (43) into (47) and evaluating the resulting integral. ∎

H. SUBOPTIMAL SELECTION: DMA

This scheme is analogous to the DSA one except that the destination and the eavesdropper both employ the MRC technique. In this case, the secrecy rate is

$$C_{sd}^{\mathrm{DMA}} = \left[C_{md}^{\mathrm{DMA}} - C_{me}^{\mathrm{DMA}}\right]^{+} = \frac{1}{(|\mathcal{F}_n|+1)} \log\left(\frac{1+\Psi_{md}^{\mathrm{DMA}}}{1+\Psi_{me}^{\mathrm{DMA}}}\right), \tag{48}$$

where $\Psi_{md}^{\mathrm{DMA}} = \frac{\sum_{m\in\mathcal{F}_n} P'_m |h_{md}|^2}{\sum_{i=1}^{N} P_{id}|c_{id}|^2 + \sigma_n^2} + \Psi_{sd}$ and $\Psi_{me}^{\mathrm{DMA}} = \sum_{m\in\mathcal{F}_n} \frac{P'_m |h_{m,E}|^2}{\sigma_n^2} + \Psi_{se}$.

In the following, we analyze the IP of the DMA case in which all relays that can successfully decode the source's message simultaneously forward its replicated image to the destination. For this DMA case, the IP can be expressed in closed form as

$$\mathcal{P}_{\mathrm{int}}^{\mathrm{DMA}} = \sum_{k=0}^{|\mathcal{F}_n|-1} \sum_{t=0}^{k} \frac{\hat{\varrho}^{k-t}(-1)^t}{(\bar{\sigma}_{me})^k \bar{\sigma}_{se} k!} \binom{k}{t} \times \left[\frac{t!}{\zeta^{t+1}} - \exp\left(-\hat{\varrho}\zeta\right) \sum_{i=0}^{t} \frac{t!\hat{\varrho}^i}{i!\zeta^{t-i+1}}\right], \tag{49}$$

where $\zeta = \left(\frac{1}{\bar{\sigma}_{se}} - \frac{1}{\bar{\sigma}_{me}}\right)$.

Next, we proceed to obtain the SOP of the DMA scheme which can be expressed as

$$\Pr\left(C_{sd}^{\mathrm{DMA}} < \mathcal{R}\right) = \mathrm{E}_{\Psi_{me}^{\mathrm{DMA}}}\left[F_{\Psi_{md}^{\mathrm{DMA}}}\left(\hat{\varrho} + (\hat{\varrho}+1)\,\Psi_{me}^{\mathrm{DMA}}\right)\right]. \tag{50}$$

In order to proceed with the evaluation of (50), we first need to obtain a closed-from expression for the CDF of Ψ_{md}^{DMA}, which is provided in the following lemma.

Lemma 5: The CDF of Ψ_{md}^{DMA} is derived as

$$F_{\Psi_{md}^{\mathrm{DMA}}}(\hat{\varrho}) = 1 - \sum_{m=1}^{|\mathcal{F}_n|} \sum_{k=0}^{m-1} \sum_{l=0}^{k} \sum_{i=1}^{N} \frac{\upsilon_m \pi_{sd,i} \bar{\sigma}_{md}^{m-k} \hat{\varrho}^k \Gamma(l+1)}{\bar{\sigma}_{id} \Gamma(k+1)} \times \binom{k}{l} \frac{\exp\left(-\frac{\hat{\varrho}}{\bar{\sigma}_{md}}\right)}{\Xi^{l+1}} - \sum_{i=1}^{N} \frac{\omega \bar{\sigma}_{sd} \pi_{sd,i}}{\bar{\sigma}_{id}\eta} \exp\left(-\frac{\hat{\varrho}}{\bar{\sigma}_{sd}}\right), \tag{51}$$

where $\Xi = \left(\frac{\hat{\varrho}}{\bar{\sigma}_{md}} + \frac{1}{\bar{\sigma}_{id}}\right)$, $\omega = \frac{1}{\bar{\sigma}_{sd}\bar{\sigma}_{md}^{|\mathcal{F}_n|}} \frac{1}{\left(\frac{1}{\bar{\sigma}_{md}} - \frac{1}{\bar{\sigma}_{sd}}\right)^{|\mathcal{F}_n|}}$ and $\upsilon_m = \frac{(-1)^{|\mathcal{F}_n|-m}}{\bar{\sigma}_{sd}\bar{\sigma}_{md}^{|\mathcal{F}_n|}} \frac{1}{\left(\frac{1}{\bar{\sigma}_{sd}} - \frac{1}{\bar{\sigma}_{md}}\right)^{|\mathcal{F}_n|-m+1}}$.

Proof: See Appendix E ∎

Now, with the help of Lemma 5, the final SOP expression for the DMA case can be obtained, as stated in the following theorem.

Theorem 6: The SOP for the DMA scheme is given by (52)*, as shown at the bottom of the next page, where* $q' = \frac{1}{\bar{\sigma}_{se}\bar{\sigma}_{me}^{|\mathcal{F}_n|}} \frac{1}{\left(\frac{1}{\bar{\sigma}_{me}} - \frac{1}{\bar{\sigma}_{se}}\right)^{|\mathcal{F}_n|}}$ and $\xi_q' = \frac{(-1)^{|\mathcal{F}_n|-m}}{\bar{\sigma}_{se}\bar{\sigma}_{me}^{|\mathcal{F}_n|}} \frac{1}{\left(\frac{1}{\bar{\sigma}_{se}} - \frac{1}{\bar{\sigma}_{me}}\right)^{|\mathcal{F}_n|-m+1}}$.

Proof: See Appendix F ∎

VI. DIVERSITY ORDER ANALYSIS

In this section, to characterize the impact of key parameters on the secrecy outage performance, the asymptotic SOP in the high SNR regime is investigated. To simplify the developments, we let $\bar{\sigma}_{sd} = \varepsilon\bar{\sigma}_{md}$ and $\bar{\sigma}_{sm} = \hat{\varepsilon}\bar{\sigma}_{md}$, where ε and $\hat{\varepsilon}$ are positive numbers close to 1, which means that the channel quality of the legitimate links is comparable (of the same order). We also let $\bar{\sigma}_{se} = \tilde{\varepsilon}\bar{\sigma}_{me}$ with $\tilde{\varepsilon}$ close to 1, meaning that the channel quality of the wiretap links is similar. We first consider the case $\bar{\sigma}_{sd} \to \infty$, which corresponds to a scenario where S is located much closer to D than E. Subsequently, we also consider the limiting case where $\bar{\sigma}_{se} \to \infty$, for which the intercept probability goes to 1. Below, we first derive SOP expressions in the asymptotic regime for each one

of the following relay selection schemes: DSA, DSM, DSC, DMA, DMC, DMM, DSO and DMO. Using these formulas, we then derive corresponding expressions of the coding gain and diversity.

A. ANALYSIS

Direct Transmission: Using the following Maclaurin series $e^x = 1 + x + o(x^2)$ and $(1-x)^{-1} = 1 + x + o(x^2)$, the asymptotic CDF of RV Ψ_{sd} can be obtained as (53).

$$F_{\Psi_{sd}}(\Psi_{sd}) = \sum_{i=1}^{N} \pi_{sd,i}\,(1+\bar{\sigma}_{id})(\bar{\sigma}_{sd})^{-1}\Psi_{sd} + o\left(\bar{\sigma}_{sd}^{-1}\right). \quad (53)$$

In turn, making use the above CDF, the following expression is obtained for the SOP in the asymptotic regime,

$$\mathcal{P}_{\text{out}}^{\infty,\text{DT}} = \left[\sum_{i=1}^{N} \pi_{sd,i} 2^{R} \bar{\sigma}_{se}\,(1+\bar{\sigma}_{id})\right](\bar{\sigma}_{sd})^{-1}. \quad (54)$$

DMC: We first note that in the asymptotic regime of high SNR, the probability of a WIRS event simplifies as follows,

$$\Pr(\mathcal{F}=\emptyset) = \prod_{m=1}^{M} \mathcal{U}_{\ell m}\bar{\sigma}_{sd}^{-M}, \quad \text{and} \quad \Pr(\mathcal{F}=\mathcal{F}_n) = \prod_{m\in\bar{F}_n} \mathcal{U}_{\ell m}\bar{\sigma}_{sd}^{|\mathcal{F}_n|-M}, \quad (55)$$

where $\mathcal{U}_{\ell m} = \sum_{\ell=1}^{N} \pi_{s,\ell}\hat{\varepsilon}\,(\bar{\sigma}_{\ell m}+1)\,\varrho$. Then, making use of (53) and (55) along with appropriate power series expansion, the asymptotic SOP of the DMC scheme is obtained as

$$\mathcal{P}_{\text{out}}^{\infty,\text{DMC}} = \varepsilon^{|\mathcal{F}_n|}2^{2R(|\mathcal{F}_n|+1)}\sum_{i=1}^{N}\sum_{m=0}^{|\mathcal{F}_n|+1}\sum_{l=1}^{2}\binom{|\mathcal{F}_n|+1}{m} \times \mathbf{g}(l)^{-(|\mathcal{F}_n|+2)}\mathbf{h}(l)\pi_{sd,i}\bar{\sigma}_{id}^{m}\Gamma(|\mathcal{F}_n|+1)\,m!(\bar{\sigma}_{sd})^{-(|\mathcal{F}_n|+1)}. \quad (56)$$

By proceeding in a similar manner, we can obtain the SOP expressions of the other schemes, which are presented below

DSC:

$$\mathcal{P}_{\text{out}}^{\infty,\text{DSC}} = \varepsilon^{|\mathcal{F}_n|}2^{2R(|\mathcal{F}_n|+1)}\sum_{m=0}^{|\mathcal{F}_n|+1}\sum_{i=1}^{N}\sum_{l=1}^{3}\binom{|\mathcal{F}_n|+1}{m}\mathbf{a}(l) \times \mathbf{b}^{-(|\mathcal{F}_n|+2)}(l)\,\pi_{sd,i}m!\bar{\sigma}_{id}^{m}\Gamma(|\mathcal{F}_n|+2)\,(\bar{\sigma}_{sd})^{-(|\mathcal{F}_n|+1)}. \quad (57)$$

DMM:

$$\mathcal{P}_{\text{out}}^{\infty,\text{DMM}} = \sum_{i=1}^{N}\sum_{m=0}^{2}\sum_{l=1}^{2}\binom{2}{m}\frac{\varepsilon\pi_{sd,i}\tilde{\mathbf{h}}\bar{\sigma}_{id}^{m}}{2^{-4R}\tilde{\mathbf{g}}^{3}}\Gamma(m+1)(\bar{\sigma}_{sd})^{-2}. \quad (58)$$

DSM:

$$\mathcal{P}_{\text{out}}^{\infty,\text{DSM}} = \sum_{i=1}^{N}\sum_{m=0}^{2}\sum_{l=1}^{3}\binom{2}{m}\frac{\varepsilon\tilde{\mathbf{a}}(l)\pi_{sd,i}\bar{\sigma}_{id}^{m}\Gamma(m+1)}{2^{-4R-1}\tilde{\mathbf{b}}^{3}(l)}(\bar{\sigma}_{sd})^{-2}. \quad (59)$$

DMA: Shown in 60 at the bottom of the next page.
DSA: Shown in 61 at the bottom of the next page.
DMO:

$$\mathcal{P}_{\text{out}}^{\infty,\text{DMO}} = \left(\frac{\varepsilon}{\tilde{\varepsilon}}\right)^{|\mathcal{F}_n|}\bar{\sigma}_{se}^{|\mathcal{F}_n|+1}\frac{2^{2R(|\mathcal{F}_n|+2)}}{(|\mathcal{F}_n|+1)(|\mathcal{F}_n|+2)} \times\sum_{m=0}^{|\mathcal{F}_n|}\sum_{i=1}^{N}\pi_{sd,i}\bar{\sigma}_{id}^{m}\binom{|\mathcal{F}_n|}{m}(m!+\bar{\sigma}_{id}(m+1)!)\,\bar{\sigma}_{sd}^{-(|\mathcal{F}_n|+1)}. \quad (62)$$

DSO:

$$\mathcal{P}_{\text{out}}^{\infty,\text{DSO}} = \left(\frac{\varepsilon}{\tilde{\varepsilon}}\right)^{|\mathcal{F}_n|}\bar{\sigma}_{se}^{|\mathcal{F}_n|+1}2^{2R(|\mathcal{F}_n|+2)}\sum_{m=0}^{|\mathcal{F}_n|}\sum_{i=1}^{N}\pi_{sd,i}\bar{\sigma}_{id}^{m+1} \times\binom{|\mathcal{F}_n|}{m}\left(m!+\bar{\sigma}_{id}\,(m+1)!\right)\bar{\sigma}_{sd}^{-(|\mathcal{F}_n|+1)}. \quad (63)$$

$$\Pr\left(C_{sd}^{\text{DMA}} < \mathcal{R}\right) = 1 - \sum_{i=1}^{N}\frac{\omega\bar{\sigma}_{sd}^{2}\pi_{sd,i}}{\bar{\sigma}_{id}\left(\hat{\varrho}+1\right)}\exp\left(-\frac{\hat{\varrho}}{\bar{\sigma}_{sd}}\right) \times\left[q'\varphi\left(1,1;\alpha\left(1+\frac{\bar{\sigma}_{sd}}{\bar{\sigma}_{se}\left(\hat{\varrho}+1\right)}\right)\right)+\sum_{q=1}^{|\mathcal{F}_n|}\xi_{q}'\left(\frac{\alpha\bar{\sigma}_{sd}}{\hat{\varrho}+1}\right)^{q-1}\Phi\left(q,q;\alpha'\left(1+\frac{\bar{\sigma}_{sd}}{\bar{\sigma}_{me}\left(\hat{\varrho}+1\right)}\right)\right)\right] -\sum_{m=1}^{|\mathcal{F}_n|}\sum_{k=0}^{i-1}\sum_{L=0}^{k}\sum_{i=1}^{N}\sum_{p=0}^{k}\frac{\upsilon_{m}\pi_{sd,i}\bar{\sigma}_{md}^{L+m-k+1}q'\hat{\varrho}^{k-p}\Gamma(L+1)}{\bar{\sigma}_{id}\left(\hat{\varrho}+1\right)^{L-p+1}\Gamma(k+1)}\binom{k}{p}\binom{k}{L}\exp\left(-\frac{\hat{\varrho}}{\bar{\sigma}_{md}}\right) \times\left[\Gamma(p+1)\left(\frac{\beta\bar{\sigma}_{md}}{\hat{\varrho}+1}\right)^{p-L}\Phi\left(p+1,p-L+1;\beta\left(1+\frac{\bar{\sigma}_{md}}{\bar{\sigma}_{se}\left(\hat{\varrho}+1\right)}\right)\right)\right. +\left.\sum_{q=1}^{|\mathcal{F}_n|}\frac{\xi_{q}'\Gamma(p+q)}{\Gamma(q)}\left(\frac{\bar{\sigma}_{md}\beta}{\hat{\varrho}+1}\right)^{p+q-L-1}\Phi\left(p+q,p+q-L;\beta\left(1+\frac{\bar{\sigma}_{md}}{\bar{\sigma}_{me}\left(\hat{\varrho}+1\right)}\right)\right)\right]. \quad (52)$$

TABLE 2. Diversity order in high SNR regime.

Scheme	Diversity order
DT	1
DMC	$M+1$
DSC	$M+1$
DMM	$M-\lvert\mathcal{F}_n\rvert+2$
DSM	$M-\lvert\mathcal{F}_n\rvert+2$
DMO	$M+1$
DSO	$M+1$
DMA	$M+1$
DSA	$M+1$

B. DIVERSITY ORDER AND CODING GAIN

In the high SNR regime for the legitimate links, the coding gain and diversity order are defined through the obtained asymptotic expression for the SOP, that is: $P_{\text{out}}^{\infty,Q} \approx (C\bar{\sigma}_{sd})^{-D}$, where C and D respectively denote the coding gain and the diversity order of the scheme Q under consideration. For example, in the case of DT, we immediately obtain from (54) that

$$C=\left[\sum_{i=1}^{N}\pi_{sd,i}2^{R}\bar{\sigma}_{se}\left(1+\bar{\sigma}_{id}\right)\right]^{-1},\quad D=1. \tag{64}$$

Proceeding in this manner, we can obtain the coding gain and diversity order for each one of the schemes considered in Subsection A. For reference, the diversity orders of these schemes are listed in Table 2, while the coding gain can easily be computed as

$$C_Q=\frac{\left(\mathcal{P}_{\text{out}}^{\infty,\text{Q}}\right)^{-\frac{1}{D_Q}}}{\bar{\sigma}_{sd}}, \tag{65}$$

with the corresponding expression for $\mathcal{P}_{\text{out}}^{\infty,\text{Q}}$ calculated previously. Based on the above results, the diversity order of the considered schemes are summarized in Table 2.

C. REMARKS

- The maximum diversity order of $M+1$ is achieved for the DMC, DSC, DMA, DSA, DMO and DSO schemes. In contrast, the DMM and DSM scheme achieve a (conditional) diversity order of $M-|\mathcal{F}_n|+2$, which decreases with the cardinality of the WIRS. This stems from the fact that minimum selection works on the basis of the SNR at the eavesdroppper node. Finally, the worst performing scheme is DT with a diversity order of $=1$.
- Since the diversity orders of DMC, DSC, DMA, DSA, DMO, and DSO are identical, the tradeoff among these schemes is solely characterized by their respective coding gains. Hence, their relative performance can be quantified in terms of the simple ratio of their coding gains, which can be interpreted as an SNR gap. For example, the SNR gap between the DMC and DSC schemes is given by
$$\Delta C=\frac{C_{\text{DMC}}}{C_{\text{DSC}}}. \tag{66}$$
Here $C_{\text{DMC}}>C_{\text{DSC}}$ and so $\Delta C>1$, indicating that DMC outperforms DSC by $20\log_{10}\Delta_{\text{C}}$ for the same SOP. We can show that the relative performance of the above schemes can be ordered as $C_{\text{DMO}}>C_{\text{DSO}}>C_{\text{DMC}}>C_{\text{DSC}}>C_{\text{DMA}}>C_{\text{DSA}}$.
- It is observed that when $\mathcal{F}_n=\varnothing$, *i.e.*, no relay can decode the source symbol successfully, the exact SOP for all scenarios is reduced to
$$\mathcal{P}_{\text{out}}=\left[\sum_{i=1}^{N}\pi_{sd,i}2^{R}\bar{\sigma}_{se}\left(1+\bar{\sigma}_{id}\right)\right](\bar{\sigma}_{sd})^{-1}. \tag{67}$$
In the special case when both σ_{sd} and $\sigma_{se}\to\infty$ at the same rate, the above expression results in a constant SOP; in turn, this floor phenomenon leads to a zero diversity gain.

VII. NUMERICAL RESULTS AND DISCUSSIONS

In this section, we present numerical results to validate the derived theoretical expressions of the SOP for the

$$\mathcal{P}_{\text{out}}^{\infty,\text{DMA}}=\varepsilon^{|\mathcal{F}_n|}\frac{2^{2\text{R}(|\mathcal{F}_n|+1)}}{\Gamma\left(|\mathcal{F}_n|+2\right)}\sum_{i=1}^{N}\sum_{m=0}^{|\mathcal{F}_n|+1}\pi_{sd,i}\bar{\sigma}_{id}^{m}\Gamma\left(m+1\right)\binom{|\mathcal{F}_n|+1}{m}$$
$$\times\left[q'\Gamma\left(|\mathcal{F}_n|+2\right)\bar{\sigma}_{se}^{|\mathcal{F}_n|+1}+\sum_{k=1}^{|\mathcal{F}_n|}\frac{\xi'_k\Gamma\left(|\mathcal{F}_n|+k+1\right)}{\Gamma\left(k\right)}\bar{\sigma}_{me}^{|\mathcal{F}_n|+k+1}\right](\bar{\sigma}_{sd})^{-(|\mathcal{F}_n|+1)}. \tag{60}$$

$$\mathcal{P}_{\text{out}}^{\infty,\text{DSA}}=\varepsilon^{|\mathcal{F}_n|}2^{2\text{R}(|\mathcal{F}_n|+1)}\sum_{i=1}^{N}\sum_{m=0}^{|\mathcal{F}_n|+1}\sum_{m_1=1}^{|\mathcal{F}_n|}(-1)^{m_1-1}\frac{m_1\pi_{sd,i}\bar{\sigma}_{id}^{m}\Gamma\left(m+1\right)\Gamma\left(|\mathcal{F}_n|+2\right)\xi}{\bar{\sigma}_{me}\bar{\sigma}_{se}}\times\binom{|\mathcal{F}_n|}{m_1}\binom{|\mathcal{F}_n|+1}{m}$$
$$\times\left[\left(\frac{\bar{\sigma}_{me}}{m_1}\right)^{|\mathcal{F}_n|+2}-\bar{\sigma}_{se}^{|\mathcal{F}_n|+2}\right](\bar{\sigma}_{sd})^{-(|\mathcal{F}_n|+1)}. \tag{61}$$

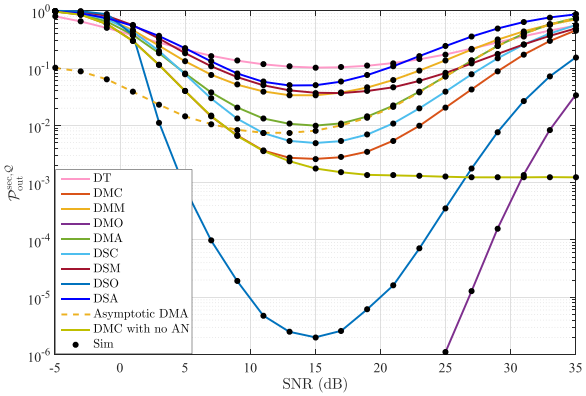

FIGURE 3. SOP performance of proposed relay selection schemes and direct transmission versus average SNR ($M = 4$ and $N = 5$).

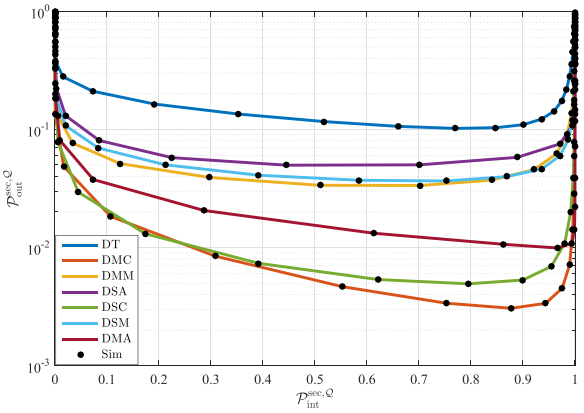

FIGURE 4. SOP performance of proposed relay selection schemes and direct transmission versus IP ($M = 4$ and $N = 5$).

proposed methods. In the simulations, the noise variances are all normalized to unity and the data rate $\mathcal{R} = 0.5$ bits per channel use. The complex channel gains $c_{i,j}$ between the AN antennas of E and the legitimate nodes R_m or D, where $i \in \{1, \ldots, N\}$ and N is the number of colluding antennas, are generated as independent complex circular Gaussian random variables based on the assumed Rayleigh model with parameter $\bar{\sigma}_{i,j}$; the various complex channel gains $h_{i,j}$ are generated in a similar way. The total AN power budget is set to 10 dB throughout the simulations, except for the special case where the E nodes are passive. The simulation results are obtained by averaging over 10^5 independent runs, and the number of transmitted bits is set to 10^4 for each run. All curves are plotted as a function of the average SNR per symbol P_s/σ_n^2. The default values of the parameters M and N, i.e. number of relays and eavesdropper antennas, are set to 4 and 5, respectively, unless otherwise specified.

Fig. 3, compares the SOP performance of the DT, DMC, DSM, DMM, DMA, DSO, DMO, DSC and DSA, by plotting Eqs. (10), (26), (30), (34), (37), (39), (40), (44) and (52), respectively, by varying the SRN. From the various curves in Fig. 3, it is seen that the DMC, DSM, DMM, DMA, DSO, DMO, DSC and DSA schemes (in the low to medium SNR range) all perform better than DT in terms of secrecy performance, demonstrating the security benefits of exploiting cooperative relays to defend against eavesdropping attack.[7] One can also see from Fig. 3 that the SOP performance of the DMO and DSO schemes is better than that of the other schemes, thereby showing the advantage of the optimal relay selection over the other selection schemes and multiple relay selection, as well as the traditional DT. The figure also includes a special curve for the case where the number of transmit antennas of the eavesdropper node $N = 0$ corresponding to the case where E does not send any AN to the legitimate network. From the simulation results, we see that the error floor phenomenon occurs in the absence of AN. This observation confirms that the presence of AN can highly affect the secrecy outage performance of the legitimate network. As can be observed, the analytical results are in perfect agreement with the simulation results, which demonstrates the validity of the derived analytical expressions. We also find that the high SNR approximations are quite accurate (although the asymptotic result is only plotted for DMA to avoid confusion in the figure).

Fig. 4 shows numerical SOP results versus IP for both the conventional DT and the proposed single and multi-relay selection schemes, where the legitimate-to-eavesdropper channel gain ratio is around 11 dB. One can see from Fig. 4 that for a specific IP value, the SOP of the proposed relay selection schemes is strictly lower than that of DT, thereby confirming that the former outperform the conventional DT.[8] It can be observed that the DSC and DMC schemes outperform the DSA approach (i.e., when all successful relays in the WIRS are involved in transmission). This can be explained by noting that in the DSA case, the eavesdropper receives multiple copies of the source signal when multiple relays transmit, which in turn degrades the secrecy performance.

Fig. 5 shows the SOP as a function of the number for relays M of the DMC, DSM, DSA, DMM, DMA, and DSC schemes. It is observed from Fig. 5 that the DMC scheme performs better than the other single and multi-relay selection schemes in terms of SOP, except the DSO and DMO. Again the proposed optimal relay selection schemes, DSO and DMO, outperform the other schemes. Since even with a small increase in M the SOP of DMO and DSO rapidly tends to zero, the corresponding curves are not sketched here. One can also see from Fig. 5 that as the number of relays M increases,

[7] We note that two opposite factors are at play in defining the SOP versus SNR performance characteristic. On the one hand, increasing the transmission power at the source S and the relay R_m (i.e., P_s and P_m) improves the quality of the legitimate links, and therefore tends to decrease the SOP. On the other hand, increasing P_s or P_m is tantamount to additional information leakage to eavesdropper E, and the corresponding increase in the quality of the non-legitimate links tends increase the SOP. The former effect is dominant at low SNR, while the latter is dominant at high SNR, which explains the quasiconvex nature of the curves in Fig. 3.

[8] We note that for the various relaying schemes under study, the limiting case of zero IP, i.e., $\mathcal{P}_{\text{int}} = 0$, is reached when the transmission power of the source and the relay goes to zero. In turn, this implies that the secrecy rate for the legitimate transmission goes to zero (see, e.g., (21)) and consequently, the SOP tends to 1, i.e., $\mathcal{P}_{\text{out}} = 1$.

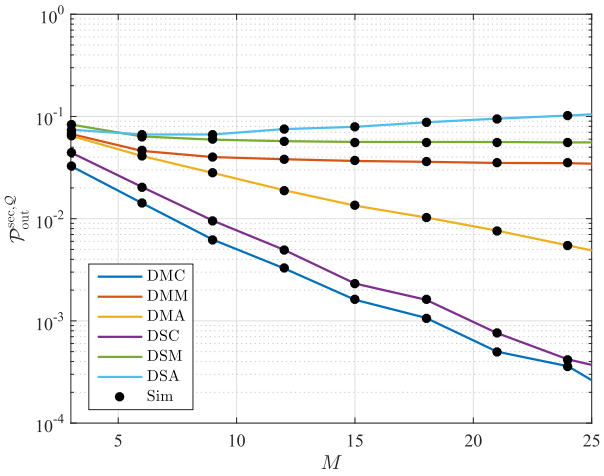

FIGURE 5. SOP performance of proposed relay selection schemes and direct transmission versus number of relays M (SNR = 10 dB, $N = 5$).

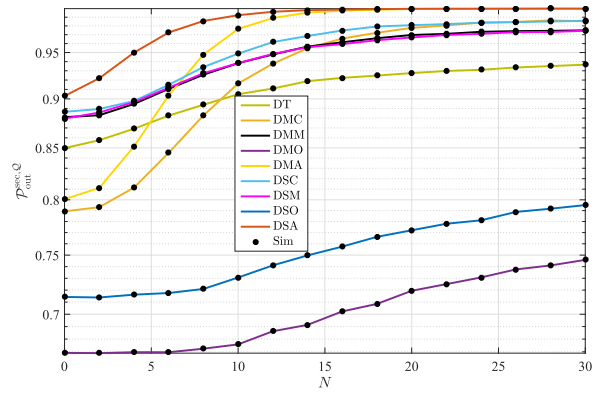

FIGURE 6. SOP performance of proposed relay selection schemes versus number of eavesdropper N ($M = 4$, SNR = 30 dB).

the SOP of the various schemes rapidly decreases, except for the DSA, DSM and DMM schemes. In the case of DSA, this can be explained by noting that for a fair comparison, the total amount of transmit power at the source and relay shall be limited to $P' = 2P_m = 2P_s$. However, using the equal-power allocation for simplicity, the transmit power at the source and relay is given by $P_m = P_s$. Thus, in DSA where all the relays in the WIRS cooperate in the next phase, the power of each relay is reduced to $P'/(|\mathcal{F}_n| + 1)$ which negatively affects the secrecy performance. The same line of thoughts can be applied for DMA; however, in this case with an increasing number of relays, the secrecy performance improves. In addition, as shown in Fig. 5, the SOP improvement of DSC and DMC becomes more significant as M increases.

Fig. 6 examines the impact of the number N of eavesdropper's transmit antennas on the SOP performance when $M = 4$, SNR $= 30$ dB and the legitimate-to-eavesdropper channel gain ratio is around -3 dB. The special case $N = 0$ corresponds to the situation where the eavesdroppers are passive, which has been amply studied in the literature. The results indicate that for all the methods under consideration, the SOP degrades with an increase in the number N of antennas, hence demonstrating the adverse effects of multi-antenna AN on wireless security. Furthermore, for both MRC and SC combining solutions, the proposed optimal relay selection outperforms the other relay selection schemes as well as the DT in terms of SOP. In other words, the DMO and DSO schemes achieves the best SOP performance, further confirming the advantage of the proposed optimal relay selection. That is, no matter which combining solution (*i.e.*, MRC and SC) is considered, the proposed optimal relay selection always performs better than the traditional relay selection and multiple relay combining approaches in terms of secrecy performance. In the case for lower values of SNR, similar trends are observed but the effect of AN on the SOP is lessen, i.e., the curves (not shown due to space limitations) are shifted down slightly.

VIII. CONCLUDING REMARKS

We have studied the PHY-layer security in a cooperative wireless network that includes a source-destination pair, multiple relays, and a malevolent active eavesdropper, which can transmit AN with multiple antennas to degrade the achievable secrecy rate of the legitimate channels. Depending on the availability of the CSI, we considered different relay selection schemes, i.e. conventional, minimum and optimal selection, along with different combining methods at the destination and eavesdropper, i.e. MRC and SC. We first analyzed the secrecy capacity of the direct transmission in terms of IP and SOP. A DF incremental relaying (IR) protocol was then introduced to improve security of communications in the presence of the eavesdropper. For each one of the proposed relay selection schemes, and for both MRC and SC, we derived new closed-form expressions for the IP and SOP under the Rayleigh channel assumption. We also characterized the secrecy performance of the various relay schemes in the asymptotic high SNR regime, which enabled us to obtain the associated coding gains and diversity orders. For both signal combining solutions, the proposed IR schemes (but for DMM and DSM) achieve the maximum diversity order of $M + 1$, where M is the number of relays. Our analysis and simulation results have revealed that the IR-based relaying with optimal selection outperforms the conventional selection, which in turns outperforms minimum selection. Our results also indicate that as M increases, the secrecy performance of the DMO, DSO, DMC, DSC and DMA schemes improves rapidly. An interesting avenue for future work is the additional consideration in our system model of power allocation across the AN antennas by the eavesdropper, in order to maximize the damage to the legitimate network.

APPENDIXES

APPENDIX A

PROOF OF LEMMA 1

By introducing the intermediate random variables (RV) $\gamma_{sd} = \frac{P_s|h_{s,d}|^2}{\sigma_n^2}$, $\gamma_{id} = \sum_{i=1}^{N} \frac{P_i|c_{i,d}|^2}{\sigma_n^2}$ and $z_i = \frac{P_i|c_{i,d}|^2}{\sigma_n^2}$, the CDF of Ψ_{sd}

can be obtained as

$$\Pr\left(\frac{\gamma_{sd}}{\gamma_{id}+1}<\gamma\right)=\Pr\left(\gamma_{sd}<\gamma\left(\gamma_{id}+1\right)\right) \quad (68)$$

$$=\mathrm{E}_{\gamma_{id}}\left[F_{\gamma_{sd}}\left(\gamma\left(\gamma_{id}+1\right)\right)\right] \quad (69)$$

$$=\int_0^{\infty}F_{\gamma_{sd}}\left(\gamma\left(\gamma_{id}+1\right)\right)f_{\gamma_{id}}\left(\gamma\right)d\gamma \quad (70)$$

Next, we should investigate the PDF of γ_{id} and the CDF of γ_{sd}. Since γ_{sd} is an exponential RV, its CDF is $F_{\gamma_{sd}}(\gamma)=1-\exp(-\frac{\gamma}{\bar{\sigma}_{sd}})$. The PDF of γ_{id} can be determined by considering its characteristic function. To begin, the characteristic function of z_i can be expressed as

$$\Phi_{z_i}\left(jw\right)=\mathrm{E}\left(\exp(jwz_i)\right)=\frac{1}{1-jw\bar{\sigma}_{id}} \quad (71)$$

Since γ_{id} is the sum of N statistically independent components z_i, its characteristic function is

$$\Phi_{\gamma_{id}}\left(jw\right)=\prod_{i=1}^{N}\frac{1}{1-jw\bar{\sigma}_{id}}. \quad (72)$$

The inverse Fourier transfrom of the characteristic function in (72) yields the PDF of γ_{id} in the form

$$f_{\gamma_{id}}\left(\gamma\right)=\sum_{i=1}^{N}\frac{\pi_{sd,i}}{\bar{\sigma}_{id}}\exp(-\frac{\gamma}{\bar{\sigma}_{id}}) \quad (73)$$

Finally, substituting (73) and the CDF of γ_{sd} in (70), we can obtain the CDF of Ψ_{sd} as in Lemma 1.

APPENDIX B
PROOF OF LEMMA 2

Let us introduce the following intermediate random variables (RV): $Y=\max_{m\in\mathcal{F}_n}\Psi_{md}+\Psi_{sd}$, $\gamma_{id}=\frac{P_{id}|c_{i,d}|^2}{\sigma_n^2}$, $\gamma_D=\sum_{i=1}^{N}\gamma_{id}$ and $X=\max_{m\in\mathcal{F}_n}\Psi_{md}$. The existence of the common RV γ_D in X and Y leads to a statistical dependence between RVs X and Y. By conditioning on γ_D, we first obtain

$$F_Y(\gamma)=E_{\gamma_D}\left[\Pr\left(X+V\le\gamma\left(\gamma_D+1\right)|\gamma_D\right)\right] \quad (74)$$

$$=E_{\gamma_D}\left[E_V\left[F_X\left(\gamma\left(\gamma_D+1\right)-V\right)|V\right]|\gamma_D\right]. \quad (75)$$

Using of the binomial theorem, we obtain the CDF of X and the PDF of γ_D as

$$F_X(\gamma)=1-\sum_{m=1}^{|\mathcal{F}_n|}(-1)^{m-1}\binom{|\mathcal{F}_n|}{m}\exp(-\frac{m\gamma}{\bar{\sigma}_{md}}),$$

$$f_{\gamma_D}(\gamma)=\sum_{i=1}^{N}\frac{\pi_{sd,i}}{\bar{\sigma}_{id}}\exp\left(-\frac{\gamma}{\bar{\sigma}_{id}}\right). \quad (76)$$

Then, with the help of (3), (75) and (76), and using properties of conditional expectations [37], we finally arrive at the expression of $F_Y(\gamma)$ in (25).

APPENDIX C
PROOF OF THEOREM 1

Introducing $Z=\Psi_{me}+\Psi_{se}$ and according to the definition of SOP, we have

$$\mathcal{P}_{\text{out}}^{\text{DMC}}=\Pr\left(Y<\varrho+(\varrho+1)Z\right)=\mathrm{E}_Z\left[F_Y\left(\varrho+(\varrho+1)Z\right)\right]$$

$$=\Pr\left(C_{sd}^{\text{DMC}}<\mathcal{R}\,|Y>Z\right)\Pr\left(Y>Z\right)$$

$$+\Pr\left(C_{sd}^{\text{DMC}}<\mathcal{R}\,|Y<Z\right)\Pr\left(Y<Z\right). \quad (77)$$

It is straightforward to verify that $\Pr\left(C_{sd}^{\text{DMC}}<\mathcal{R}\,|Y<Z\right)=1$. Then, the first term in (77) can be expressed as

$$\Pr\left(C_{sd}^{\text{DMC}}<\mathcal{R}\,|Y>Z\right)\Pr\left(Y>Z\right)$$

$$=\frac{\Pr\left(C_{sd}^{\text{DMC}}<\mathcal{R},Y>Z\right)}{\Pr\left(Y>Z\right)}$$

$$\times\Pr\left(Y>Z\right)=\Pr\left(Z<Y<2^{2\mathcal{R}}Z+\varrho\right)$$

$$=\Pr\left(Y<2^{2\mathcal{R}}Z+\varrho\right)-\Pr\left(Z<Y\right). \quad (78)$$

Making use of (78) and (77) we can write

$$\mathcal{P}_{\text{out}}^{\text{DMC}}=\Pr\left(Y<\varrho+(\varrho+1)Z\right)=\mathrm{E}_Z[F_Y(\varrho+(\varrho+1)Z)]. \quad (79)$$

To prove the desired result, we call upon (79) and exploit the PDF of the RV Z as

$$f_Z(\gamma)=\sum_{l=1}^{2}\mathbf{h}\left(l\right)\exp\left(-\mathbf{g}\left(l\right)\gamma\right). \quad (80)$$

Then, according to (79), (80) and conjuring the identity [38, Eq. (2.1.3.1)] we arrive at $\mathcal{P}_{\text{out}}^{\text{DMC}}$ as in (26).

APPENDIX D
PROOF OF THEOREM 3

The desired SOP can be first expressed in terms of the CDF of RV $\tilde{Y}$

$$\mathcal{P}_{\text{out}}^{\text{DMM}}=\Pr\left(\tilde{Y}<\varrho+(\varrho+1)\tilde{Z}\right)=\mathrm{E}_{\tilde{Z}}\left[F_{\tilde{Y}}\left(\varrho+(\varrho+1)\tilde{Z}\right)\right]. \quad (81)$$

where $\tilde{Z}=\min_{m\in\mathcal{F}_n}\Psi_{me}+\Psi_{se}$ with its PDF given by

$$f_{\tilde{Z}}(z)=\sum_{l=1}^{2}\tilde{\mathbf{h}}\left(l\right)\exp\left(-\tilde{\mathbf{g}}\left(l\right)z\right). \quad (82)$$

Then, making use of (33), (81), and (82) along with the identity [38, Eq. (2.1.3.1)], we finally obtain (34).

APPENDIX E
PROOF OF LEMMA 5

Introducing the $\Delta=\sum_{m\in\mathcal{F}_n}\gamma_{md}$, $\gamma_{md}=P_m|h_{md}|^2$, $\gamma_d=\sum_{i=1}^{N}\gamma_{id}$ and $\gamma_{id}=\frac{P_{id}|c_{id}|^2}{\sigma_n^2}$ we have

$$F_{\Psi_{md}^{\text{DMA}}}\left(\hat{\varrho}\right)=\mathrm{E}_{\gamma_d}\left[\Pr\left(\Delta<\hat{\varrho}\gamma_d+\hat{\varrho}\,|\gamma_d\right)\right]. \quad (83)$$

Making use of the moment generating function (MGF) of RVs Δ, $F_{\Delta}(x)$ and $f_{\gamma_d}(\gamma_d)$ can be obtained as

$$F_{\Delta}(x) = 1 - \sum_{k=0}^{|\mathcal{F}_n|-1} \left(\frac{x}{\bar{\sigma}_{md}}\right)^k \frac{\exp\left(-\frac{1}{\bar{\sigma}_{md}}x\right)}{k!},$$
$$f_{\gamma_d}(\gamma_d) = \sum_{i=1}^{N} \frac{\pi_{sd,i}}{\bar{\sigma}_{id}} \exp\left(-\frac{\gamma_d}{\bar{\sigma}_{id}}\right). \quad (84)$$

Then, according to (84) we have

$$F_{\Psi_{md}^{\mathrm{DMA}}}\left(\hat{\varrho}\right) = \mathrm{E}_{\gamma_d}\left[F_{\Delta}\left(\hat{\varrho}\gamma_d + \varrho\right)\right] = 1 - \int_0^{\infty} \sum_{k=0}^{|\mathcal{F}_n|-1} \sum_{i=1}^{N} \frac{\pi_{sd,i}}{\bar{\sigma}_{id}} \times \frac{(\gamma_d+1)^k \left(\frac{\hat{\varrho}}{\bar{\sigma}_{md}}\right)^k \exp\left(-\gamma_d\left(\frac{\hat{\varrho}}{\bar{\sigma}_{md}} + \frac{1}{\bar{\sigma}_{id}}\right) - \frac{\hat{\varrho}}{\bar{\sigma}_{md}}\right)}{k!} d\gamma_d. \quad (85)$$

Finally, the desired result is obtained by evaluating the above integral.

APPENDIX F
PROOF OF THEOREM 6

We first use the MGF to compute the PDF of the RV Ψ_{me}^{DMA} as

$$f_{\Psi_{me}^{\mathrm{DMA}}}(\gamma) = q' \exp\left(-\frac{\gamma}{\bar{\sigma}_{se}}\right) + \sum_{q=1}^{|\mathcal{F}_n|} \frac{\xi_q' \gamma^{q-1}}{\Gamma(q)} \exp\left(-\frac{\gamma}{\bar{\sigma}_{me}}\right). \quad (86)$$

Then, based on (51), (50) and (86), we can obtain the following integral expression,

$$\Pr\left(C_{sd}^{\mathrm{DMA}} < R\right) = \int_0^{\infty} F_{\Psi_{md}^{\mathrm{DMA}}}\left(\hat{\varrho} + \left(\hat{\varrho}+1\right)\gamma\right) f_{\Psi_{me}^{\mathrm{DMA}}}(\gamma)\, d\gamma. \quad (87)$$

Finally, by invoking the binomial theorem as well as the identity [38, Eq. (2.1.3.1)], we arrive at (52).

REFERENCES

[1] S. Vahidian, M. Najafi, M. Najafi, and F. S. Al-Qahtani, "Power allocation and cooperative diversity in two-way non-regenerative cognitive radio networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–7.

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

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

[4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[5] K. Khalil, O. O. Koyluoglu, H. E. Gamal, and M. Youssef, "Opportunistic secrecy with a strict delay constraint," *IEEE Trans. Commun.*, vol. 61, no. 11, pp. 4700–4709, Nov. 2013.

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

[7] B. Aygün and A. Soysal, "Capacity bounds on MIMO relay channel with covariance feedback at the transmitters," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2042–2051, Jun. 2013.

[8] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.

[9] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[10] 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.

[11] S. Vahidian, S. Aïssa, and S. Hatamnia, "Relay selection for security-constrained cooperative communication in the presence of eavesdropper's overhearing and interference," *IEEE Wireless Commun. Lett.*, vol. 4, no. 6, pp. 577–580, Dec. 2015.

[12] M. Yuksel, X. Liu, and E. Erkip, "A secure communication game with a relay helping the eavesdropper," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 818–830, Sep. 2011.

[13] Y. Oohama, "Coding for relay channels with confidential messages," in *Proc. CoRR*, Sep. 2006, pp. 87–89.

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

[15] 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.

[16] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4005–4019, Sep. 2008.

[17] C. Jeong and I.-M. Kim, "Optimal power allocation for secure multicarrier relay systems," *IEEE Trans. Signal Process.*, vol. 59, no. 11, pp. 5428–5442, Nov. 2011.

[18] 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.

[19] 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.

[20] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 1, pp. 310–320, Feb. 2012.

[21] Y. Cai and C. Zhang, "Physical layer security in wireless-powered networks with untrusted relays," in *Proc. IEEE 17th Int. Conf. Commun. Technol. (ICCT)*, Oct. 2017, pp. 771–776.

[22] X. Ding, T. Song, Y. Zou, X. Chen, and L. Hanzo, "Security-reliability tradeoff analysis of artificial noise aided two-way opportunistic relay selection," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, pp. 3930–3941, May 2017.

[23] H. Fang, L. Xu, and X. Wang, "Coordinated multiple-relays based physical-layer security improvement: A single-leader multiple-followers Stackelberg game scheme," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 1, pp. 197–209, Jan. 2018.

[24] M. Samavat, A. Morsali, and S. Talebi, "Delay–interleaved cooperative relay networks," *IEEE Commun. Lett.*, vol. 18, no. 12, pp. 2137–2140, Dec. 2014, doi: 10.1109/LCOMM.2014.2361524.

[25] A. Sureshbabu, M. Samavat, X. Li, and C. Tepedelenlioglu, "Outage probability of multi-hop networks with amplify-and-forward full-duplex relaying," *IET Commun.*, vol. 12, no. 13, pp. 1550–1554, Apr. 2018.

[26] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Process. Lett.*, vol. 19, no. 2, pp. 71–74, Feb. 2012.

[27] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2170–2181, Jun. 2013.

[28] Y. Zou, X. Wang, W. Shen, and L. Hanzo, "Security versus reliability analysis of opportunistic relaying," *IEEE Trans. Veh. Technol.*, vol. 63, no. 6, pp. 2653–2661, Jul. 2014.

[29] Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, "Relay-selection improves the security-reliability trade-off in cognitive radio systems," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 215–228, Jan. 2015.

[30] 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.

[31] S. Hatamnia, S. Vahidian, S. Aïssa, B. Champagne, and M. Ahmadian-Attari, "Network-coded two-way relaying in spectrum-sharing systems with quality-of-service requirements," *IEEE Trans. Veh. Technol.*, vol. 66, no. 2, pp. 1299–1312, Feb. 2017.
[32] L. Zhang, H. Zhang, D. Wu, and D. Yuan, "Improving physical layer security for MISO systems via using artificial noise," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2015, pp. 1–6.
[33] A. Bletsas, A. Khisti, D. P. Reed, and A. Lippman, "A simple cooperative diversity method based on network path selection," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 3, pp. 659–672, Mar. 2006.
[34] S. Hataminia, S. Vahidian, M. Mohammadi, and M. Ahmadian-Attari, "Performance analysis of two-way decode-and-forward relaying in the presence of co-channel interferences," *IET Commun.*, vol. 8, no. 18, pp. 3349–3356, 2014.
[35] M. Najafi, M. Ardebilipour, E. Soleimani-Nasab, and S. Vahidian, "Multi-hop cooperative communication technique for cognitive DF and AF relay networks," *Wireless Pers. Commun.*, vol. 83, no. 4, pp. 3209–3221, 2015.
[36] 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.
[37] A. Papoulis, *Probability, Random variables, and Stochastic Processes*. New York, NY, USA: McGraw-Hill, 1991.
[38] Wolfram. (2012). *The Wolfram Functions Site*. [Online]. Available: http://functions.wolfram.com

SAEED VAHIDIAN was born in Ghochan, Iran. He received the B.Sc. degree from the Ferdowsi University of Mashhad, Mashhad, Iran, in 2012, and the M.Sc. degree from the K. N. Toosi University of Technology, Tehran, Iran, in 2014, all in electrical engineering. He is currently pursuing the Ph.D. degree with the University of California San Diego (UCSD), CA, USA. In 2015 and 2016, he worked as an Optimization Specialist with Huawei Company and Ericsson Company, Tehran, Iran. In 2017, he joined to UCSD. Currently, his research interests include the area of machine learning, deep learning, and convex and non-convex optimization.

SAJAD HATAMNIA was born in Iran, in 1988. He received the B.Sc. degree in electrical engineering from Razi University, Kermanshah, Iran, in 2012, and the M.Sc. degree in electrical engineering from K. N. Toosi University of Technology, Tehran, Iran, in 2014. From 2012 to 2013, he was a Research Assistant (RA) with the Spread Spectrum and Wireless Communication Lab. Since 2013, he has been a RA with the Coding and Cryptography Lab (CCL), K. N. Toosi University of Technology. His research interests are in the area of machine learning, statistical signal processing, and optimization.

BENOIT CHAMPAGNE received the B.Ing. degree in engineering physics from the École Polytechnique de Montréal, in 1983, the M.Sc. degree in physics from the Universit de Montral, in 1985, and the Ph.D. degree in electrical engineering from the University of Toronto, in 1990. From 1990 to 1999, he was an Assistant and then an Associate Professor with INRS—Telecommunications, Universit du Quebec, Montréal. In1999, he joined McGill University, Montreal, where he is currently a Full Professor with the Department of Electrical and Computer Engineering; he also served as an Associate Chairman of graduate studies with the Department, from 2004 to 2007. His research focuses on the study of advanced algorithms for the processing of communication signals by digital means. His interests span many areas of statistical signal processing, including detection and estimation, sensor array processing, adaptive filtering, and applications thereof to broadband communications and audio processing, where he has coauthored nearly 250 refereed publications. He has also served on the Technical Committees of several international conferences in the fields of communications and signal processing. His research has been funded by the Natural Sciences and Engineering Research Council (NSERC) of Canada, the Fonds de Recherche sur la Nature et les Technologies from the Government of Quebec, and some major industrial sponsors, including Nortel Networks, Bell Canada, InterDigital, and Microsemi. In particular, he was a Registration Chair of the IEEE ICASSP 2004, a Co-Chair, Antenna and Propagation Track, of IEEE VTCFall 2004, a Co-Chair, Wide Area Cellular Communications Track, of IEEE PIMRC 2011, a Co-Chair, Workshop on D2D Communications, of IEEE ICC 2015, and a Publicity Chair of IEEE VTCFall 2016. He has been an Associate Editor for the *EURASIP Journal on Applied Signal Processing*, from 2005 to 2007, the IEEE SIGNAL PROCESSING LETTERS, from 2006 to 2008, and the IEEE TRANSACTIONS ON SIGNAL PROCESSING, from 2010 to 2012, and a Guest Editor for two special issues of the *EURASIP Journal on Applied Signal Processing* published, in 2007 and 2014, respectively.