Physical Layer Security in Multi-hop Cooperative Wireless Relaying

Sajad Hatamnia, Mahdi Morafah, and Bill Lin

Abstract

In the last decade, multi-hop cooperation has evolved bringing several advantages including coverage improvement, more reliability of wireless links, and power consumption reduction. Still, its application has raised several challenges, such as the need for secure transmission at each hop, algorithms to perform relay selection and the accurate models to facilitate performance analysis. This paper addresses the problem of physical layer (PHY) security in a multi-hop wireless cooperative network, where communication at each hop is assisted by multiple relays forming a cluster, each cluster being surrounded by multiple eavesdroppers which together may tap transmissions from both the source and the relays. The main focus of the study is on analyzing the benefits of various relay selection schemes for protecting the source-destination transmission against the eavesdroppers, which can collude and combine information via diversity combining techniques. To be specific, four relay selection schemes, which differ in the way they employ available measures link quality, are considered to deliver the source information to the destination via a decode-and-forward (DF) strategy. To evaluate the security performance of the multi-hop cooperative link in the presence of colluding eavesdroppers, we derive novel closed-form analytical expressions for the secrecy outage probability (SOP) with consideration of special cases of practical interest. These analytical expressions provide considerable insight into the inherent trade-offs between the secrecy performance and key system parameters, such as: number of hops, number of relays within a cluster, and signal-to-noise ratio. Computer simulation results are presented to validate the correctness and accuracy of the derived analytical results.

I. INTRODUCTION

Nowadays, wireless communication networks are heavily relied upon the world over to connect people, facilitate economies, and ensure public safety [1]. They are being increasingly used for the transmission of highly confidential information which, due to the open nature of the wireless channels and network densification, poses security threats at various level, ranging from personal loss of information to major nation wide security issues. Within this demanding context, the study of physical layer security from an information-theoretic perspective, as an alternative or complement to cryptographic techniques to defend against eavesdroppers and security threats, has attracted considerable attention within the last decade [2]. The fundamental aim of physical layer

M. Morafah, and B. Lin are with the Dept. of Electrical and Computer Engineering, University of California San Diego (UCSD), CA, USA (e-mail: mmorafah@eng.ucsd.edu; billlin@eng.ucsd.edu). S. Hatamnia is with the Dept. of Electrical and Computer Engineering, K. N. Toosi University of Technology, Tehran, Iran (e-mail: sajad.hatamnia@gmail.com).
security is to enhance the immunity of communications by exploiting the physical characteristics of the wireless channels. Specifically, inspired by Shannon’s work, it is possible to characterize the amount of data that can be privately transmitted to an expected recipient and exploit this information so as to make it more difficult for unauthorized users to decode the received signal [3–5].

A. Background

From an information-theoretic perspective, the rate at which a source can send information to an expected destination safely without being wiretapped by an eavesdropper is referred to as the achievable secrecy rate [6], while the maximum achievable secrecy rate is referred to as the secrecy capacity. It has been proven that when the wiretap channel is a degraded version of the legitimate channel, the private message can be confidentiality sent from the source to the destination without the requirement of sharing a secret key [7, 8].

To realize positive secrecy rates of wireless communications, even when the source destination channel is inferior to the source eavesdropper channel, cooperative relays have been investigated in the context of physical layer security for which several relaying strategies are developed including distributed beamforming [9, 10], cooperative jamming [11] and relay selection [12–16]. Notably, given the availability of multiple relays, properly designed relay/jammer selection is able to achieve a substantial security improvement for cooperative relaying networks, which is arising as a promising research topic. For example, hybrid relaying and jamming selection schemes are explored in [12–15]. The intercept probabilities have also been analyzed in the context of both amplify and forward (AF) and decode and forward (DF) based relaying systems, where an eavesdropper is only capable of wiretapping the transmissions of the relays. Recently, there has been some work on PHY security in two-hop full-deplex (FD) relaying with focus on the secrecy rate performance and the advantages of FD over half-duplex (HD) [17]. In [18], a cooperative non-orthogonal multiple access (NOMA) system with a single relay is analyzed assuming that NOMA users are affected by an eavesdropper. The work in [19] studies the secrecy performance of a downlink of multiple-input multiple-output (MIMO) scenario, focusing on the impact of a max-min transmit antenna selection strategy. In [20], a cross-layer optimization approach is used to maximize the secrecy rate in multi-hop networks. [21] considers relay selection for a FD two-hop relay network with multiple users under the attack of colluding eavesdroppers.

One of the important things that require meticulous attention is that most of the above mentioned node cooperation approaches address two-hop relay networks. While, for applications like sensor networks where the distance between the source and the central node is large, it is suitable to hand over the signal via multi-hop setup to the intended destination [22, 23]. Moreover, the previous works of the outage-based physical layer secure transmission design are limited to single-antenna-assisted single hop systems and have not been considered for cooperative relaying systems. Hence, the issues of secure transmissions over cooperative relaying channels expressed
in terms of the secrecy outage probability (SOP) and secrecy throughput constitute an open problem. Additionally, considering the security in all hops, it is still unclear how many relay nodes should be selected and also how the relay should be selected in order to achieve the best performance, which motivates this work.

B. Technical Contributions

In light of the foregoing discussion, our work differs from the existing literature in the following senses.

- Multi-hop relaying is a cooperative technique that splits the communication path between the source and the destination into some, possibly shorter, hops for extended coverage, ameliorated reliability, and less power consumption. In this work, we focus our attention on an comprehensive scenario of a wireless multi-hop DF relay network, where the communication from the legitimate source, $S$, to the legitimate destination, $D$, is aided by $T$ trustworthy relaying hops. We assume that each hop equipped with a cluster of multiple relay nodes. We also assume that at each hop there is a cluster of multiple colluding eavesdroppers, jointly perform signal processing to eavesdrop the confidential information. We first propose a general framework for the secure transmission in the legitimate network, we then consider different secure relay selection modes at each hop to improve physical layer security and protect the source message against multiple clusters of multiple eavesdroppers.

- Motivated by the principal question that given the availability of multiple relays at each hop, how to select the relay nodes at each hop appropriately for achieving a significant security improvement and protect the source message against eavesdropper, four different relay selection strategies are invoked by our cooperative network operating under secrecy constraints, referred as maximum selection (MS), maximum selection with decoding Set (MSDS), maxmin selection with decoding set (MMSDS), and minimum selection with decoding set (MiSDS). In particular, in MS mode, the relay that achieves the maximum signal-to-noise ratio (SNR) in its cluster is selected as the forwarding relay to retransmit the confidential signal to the next hop, while MSDS mode, among all successful relays in decoding the received signal, the one that gives maximum instantaneous SNR to the next hop; further, in MMSDS mode, among all relays succeeding in decoding the received signal, the relay that does have the best channel out of the ones that have worst channel quality is selected; finally, in MiSDS, out of all successful relays in decoding, the one that gives minimum instantaneous SNR to the next eavesdropper cluster is chosen to perform forwarding the packet to the next hop.

- Furthermore, we develop an outage-based characterization for quantifying the security performance of a multi-hop DF relaying system and in contrast to [14], [24] and [25], the security in all hops are considered in this paper. We also thoroughly compare the secrecy performance of the proposed schemes from different perspectives.
Extensive numerical examples are used to simulate the SOP, illustrating the accuracy of our analytical derivations. Moreover, since the eavesdropper nodes at each cluster collude with other eavesdroppers at other clusters they employ diversity signal combining techniques 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. Furthermore, the performance of proposed four relay selection modes is compared against two special case of interests as benchmarks.

With the aid of analytical and numerical results, we show that the proposed MMSDS scheme significantly outperforms the other schemes for the whole range of SNR regime. Moreover, we show that increasing the transmit power cannot always improve the secrecy performance of the proposed schemes and an error floor phenomenon occurs. This phenomenon is caused by the fact that after a specific amount of power the higher the transmitted power, the higher the chance of being overheard by eavesdroppers node. Further, we show that the advantage of adding more relay nodes in each cluster is benefited more by the MSDS, MMSDS schemes. Furthermore, it will be illustrated that increasing the number of hops is detrimental for the legitimate network. That’s due to the fact that the amount of information leakage increases as the eavesdropper clusters overhear during all hops to extract information. The remainder of this paper is organized as follows. Section II introduces our system model and scheme description. In Sections III and IV, we present the mathematical framework of our performance analysis both for four relay selection strategies and for two special cases of interests. Our numerical results and discussions are provided in Section IV. Finally, Section VI presents our concluding remarks.

II. SYSTEM MODEL AND SCHEME DESCRIPTION

A. System Model

Consider a wireless \((T + 1)\)-hop relaying network for secure communication in a cooperative wireless sub-network consisting of a source \(S\), a destination \(D\) and \(T\) clusters of DF relays each of which consists of \(N_t\) relay nodes \((N_t \geq 1)\), where \(t\) is the hop number. We also assume that in the vicinity of the source, destinations and each cluster of relay nodes a cluster of eavesdropper node is located each of which comprised of \(M_t\) nodes \((M_t \geq 1)\), i.e., \(T + 1\) clusters of eavesdropper nodes in total. Furthermore, there exists no line-of-sight (LOS) link between \(S\) and \(D\) due to the long distance or blockages between them. As such, the sources can only transmit to the destination via the intermediate relays, and the eavesdropper can overhear the messages from both the source and the relays. Fig. 1 schematically shows the system model under consideration. We assume that all nodes are equipped with a single antenna. We also assume a half-duplex mode for all nodes in the network, where either reception or transmission of a packet is possible in each time slot. All the channels are modeled as quasi-static block fading channels, i.e. channels remain constant within one transmission and vary independently from one block to another, following a Rayleigh distribution. The noise at any receiver is presented by a
zero-mean complex Gaussian variable. We also presume that the total transmit power budget of the system is limited by $P$. Time-division multiple-access is adopted and the communications of the proposed schemes are divided into two phases, i.e. the broadcast phase and the cooperative phase. It is assumed that a data symbol $s$ is transferred from the source to the destination through $N_t$, $t \in \{1, 2, ..., T\}$ DF relays at each cluster, during $T + 1$ time slots. In the meantime, $M_t$, $t \in \{1, 2, ..., T + 1\}$ eavesdropper in each cluster try to decode the received signal to extract source or relay information for its own sake. To exploit the diversity potential of multiple relay nodes over independently fading channels, DF relay selection is employed. The two phases of the proposed cooperative schemes are discussed in detail as follows.

B. Scheme Description

In this subsection, we detail the procedure of the data transmission. The data transmission is performed in two phases. More particularly, during the broadcast phase, the source node transmits its packet to the first cluster of relays; meanwhile, the first cluster of eavesdropper passively overhears the source’s signal. In the next coherence time (slot) a selected relay from the first cluster is invoked for forwarding the signal received from $S$ to the next hop. Then, the second cluster manner in the same fashion and also the second cluster of the eavesdropper wiretaps the message information which is sent by the selected relay from the second cluster. This process iterates in order to deliver the data to the destination via the last hop. We now formulate the received signals in the $t$th time slot with $t = 1, 2, ..., T + 1$ in the presence of eavesdropping as follows. The received signal at time slot $t$, $t \in \{1, 2, ..., T + 1\}$, at $t$th relay cluster and $t$th eavesdropper cluster can be written respectively as

$$x_{t,i,j} = \sqrt{P_{t-1}}h_{t,i,j}s + n_{t,j}$$

$$y_{t,i,j} = \sqrt{P_{t-1}}f_{t,i,j}s + n_{E,t,j}$$

where $P_{t-1}$ denotes the power of the transmitter in time slot $t$, $s$ is the unit-energy symbol transmitted from $i$th transmitter in time slot $t$, $n_{t,j} \sim \mathcal{CN}(0, \sigma_n^2)$ and $n_{E,t,j} \sim \mathcal{CN}(0, \sigma_n^2)$ are the additive white Gaussian noise (AWGN) at the $j$th receiver and eavesdropper at time slot $t$, respectively. Throughout the paper $h_{t,i,j} \sim \mathcal{CN}(0, \Omega_{h,t})$ stands for the Rayleigh flat fading channel coefficient between transmitter $i$ and receiver $j$ in time slot $t$ where $\Omega_{h,t} = \mathbb{E}\{|h_{t,i,j}|^2\}$, $i \in \{1, 2, ..., N_t\}$, $j \in \{1, 2, ..., N_t\}$ and also $f_{t,i,j} \sim \mathcal{CN}(0, \Omega_{f,t})$ follows a complex Gaussian distribution flat fading channel gain between the $i$th transmitter and $j$th eavesdropper node in time slot $t$ where $\Omega_{f,t} = \mathbb{E}\{|f_{t,i,j}|^2\}$, $i \in \{1, 2, ..., N_t-1\}$ and $j \in \{1, 2, ..., M_t\}$.

To exploit the diversity potential of multiple relay nodes over independently fading channels, during the cooperative phase, DF relay selection is performed before data transmission commences. In particular, each hop of the legitimate network selects the best relay based on four relay selection schemes to transmit the signal toward the next hop. We denote the four relay
selection schemes as MS, MSDS, MMSDS, and MiSDS, where in MS scheme the best relay is the one that has the maximum instantaneous SNR within the cluster, while MSDS represents the selection scheme, in which the relay that is successful in decoding of the received message and gives maximum instantaneous SNR to the next cluster. In contrast, MMSDS symbolizes the scheme in which among all the relays that are successful in decoding of the received signal the best relay is selected to retransmit the next hop via max–min criterion. To delineate, the relay that has the maximum instantaneous SNR among the minimum to the next cluster is choose to send its information. Finally, MiSDS stands for the scheme where among all relays that decoded the received message successfully, the relay selection is performed based on the lowest instantaneous SNR of the eavesdropper cluster.

Herein, we consider the worst case scenario in which the eavesdropper can know the systems’ channels. Strictly speaking, in this case the eavesdropper can perform any technique with the signals received in each phases in order to maximize its overall SNR. In this paper, in order to study comprehensively the efficiency of the proposed schemes, we study the impact of both cases in which the eavesdroppers adopt either the MRC or SC with its received signals during \((T + 1)\) time slots. According to the above-mentioned explanations we compute the channel capacity at the receiver node in time slot \(t\) and at the eavesdropper, respectively as [26]

\[
\begin{align*}
C_{D,z} &= \frac{1}{T+1} \log_2 (1 + \Psi_{D,z}), \\
C_{E,t,z}^{w} &= \frac{1}{T+1} \log_2 (1 + \Psi_{E,t,z}^{w}),
\end{align*}
\]

where \(\Psi_{D,z}\) is the received SNR at the destination and \(\Psi_{E,t,z}^{w}\) denotes the SNR at eavesdropper in time slot \(t\) and since \(\Psi_{D,z}\) and \(\Psi_{E,t,z}^{w}\) are determined based on the selection criterion, they will be detailed later in the next section; \(z \in \{\text{MS, MSDS, MMSDS, MiSDS}\}\) and \(w \in \{\text{SC, MRC}\}\). To measure the security level of a wireless system, the secrecy capacity, is usually considered which is in fact defined by the maximum difference between the mutual information of the main
and eavesdropper channels. The secrecy capacity can be defined as

\[ C_{sec,z}^w = [C_{D,z} - C_{E,t,z}^w]^+ = \left[ \frac{1}{T+1} \log_2 \left( \frac{1 + \Psi_{D,z}}{1 + \Psi_{E,t,z}^w} \right) \right]^+ , \]

(5)

where \([x]^+ = \max\{0, x\}\). In the following section secrecy performance of the proposed schemes will be provided.

III. SECRECY PERFORMANCE ANALYSIS

We endeavor in this section to characterize the security performance comprehensively for the proposed scenarios. We commence our analysis by first defining the SOP event. The SOP is defined as the probability that the instantaneous secrecy capacity is less than a target secrecy rate \(R\) [27]. The following gives the definition of SOP followed by derivation of a closed-form expressions for the SOP of the considered network.

**Definition 1:** Let \(\beta_t, t \in \{1, 2, ..., T\}\) be the probability that the transmission be successful up to time slot \(t-1\) and fails in time slot \(t\) and let \(\beta_{T+1}\) denote the probability of successful transmission. Then, the SOP of the system under study can be defined as

\[ P_{sec,z}^w = \Pr(C_{sec,z}^w \leq R) = \sum_{t=1}^{T} \beta_t \Pr\left( \frac{1}{T+1} \log_2 \left( \frac{1 + \Psi_{D,z}}{1 + \Psi_{E,t,z}^w} \right) \leq R \right) + \beta_{T+1} \Pr\left( \frac{1}{T+1} \log_2 \left( \frac{1 + \Psi_{D,z}}{1 + \Psi_{E,T+1,z}^w} \right) \leq R \right) \]

(6)

**Remark 1:** The SOP of all schemes will be obtained based on Eq. (6), however, \(\beta_t\) will be different for the four relay selection schemes which will be discussed later in this section.

**Remark 2:** Notice that in Eq. (6), the first term accounts for the probability at which the transmission is successful up to time slot \(t-1\) (The transmission fails in time slot \(t\)). Therefore, the SNR of the corresponding receiver node (the relay cluster) in that time slot is zero. Thus, the probability in the first term will be 1 which ends up with the simplified term of \(\sum_{t=1}^{T} \beta_t\). The second term in Eq. (6) elucidates the probability of failure in transmission in the last time slot.

**Remark 3:** From cooperative physical layer security point of view, there are two principal concerns: first, how to maximize the capacity of the main link and how to minimize the capacity of the malicious wiretap link. For example, the cooperative relay node which has a perfect channel to the destination may also have perfect channels to the wiretap nodes or, the relay nodes which have low quality channels to the eavesdroppers may also have low quality channels to the destination. Therefore, different relay selection methods and optimization of these criterion can highly contribute to the improvement of a cooperative system’s performance which is the main purpose of this paper. To facilitate the relay selection process, we assume perfect knowledge of channel state information (CSI).
Remark 4: We note the proposed schemes (i.e., selecting one relay among multiple relays as the active relay) can be potentially employed in many practical application scenarios. For example, these users or relays can be vehicles in vehicular networks, while the destination can be a road side center. For instance, thanks to a blockages, the transmission from a user-vehicle may request the assistance from a relay-vehicle, where our proposed schemes can be employed. In general, user selection can be applied in a multiuser LTE-Advanced cellular system to improve the system throughput [28, 29], whereas relay selection is feasible in IEEE 802.12j vehicular networks to improve the system capacity [30, 31].

In what follows, the four relay selection modes will be presented in detail and their corresponding SOP will be derived based on Eq. (6).

A. Maximum Selection (MS)

The first category of selection works based on the maximum SNR. Hence, in this scheme, the relay that has the maximum SNR amongst all in each cluster is selected to forward the received message information. Therefore, the best relay selection criterion is expressed as

$$i_t^* = \arg\max_{i \in \{1, 2, \ldots, N_t\}} \left\{ C_{DF}^t \right\},$$

where $C_{DF}^t = \frac{P_t - 1}{\sigma_n^2} \left| h_{t,i_t^*,t-1,i_t^*} \right|^2$. We note that the selected relay should not be in outage. To avoid this case, we define the parameter $\eta_t$ as the probability that the chosen relay in time slot $t$ is in outage. We formulate this as in the following

$$\eta_t = \left[ 1 - \exp \left( -\frac{\kappa}{\bar{\gamma}_{h,t}} \right) \right]^{N_t},$$

where $\bar{\gamma}_{h,t} = \frac{P_t - 1}{\sigma_n^2} \Omega_{h,t}$ and $\kappa = 2^{(T+1)R} - 1$. Next, we obtain the capacity of the the source to destination and also the source to the eavesdropper channel in time slot $t$ in bit/sec/Hz as

$$C_{D,a} = \frac{1}{T + 1} \log_2 \left( 1 + \Psi_{D,a} \right),$$

$$C_{E,t,a}^{SC} = \frac{1}{T + 1} \log_2 \left( 1 + \Psi_{E,t,a}^{SC} \right),$$

where $\Psi_{D,a} = \frac{P_t - 1}{\sigma_n^2} \left| h_{T+1,i^*_{t,D}} \right|^2$ and $\Psi_{E,t,a}^{SC} = \max_{u=1,\ldots,t} \left\{ \max_{j=1,\ldots,M_u} \left\{ \frac{P_{u-1} - 1}{\sigma_n^2} \left| f_{u,i^*_u,j} \right|^2 \right\} \right\}$. To obtain the system achievable secrecy rate, we first introduce the following lemma.
Lemma 1: The CDF and PDF of the RVs $\Psi_{D,a}$ and $\Psi_{SC}^{E,t,a}$ are given by

\[
F_{\Psi_{D,a}}(y) = 1 - \exp\left(-\frac{y}{\bar{\gamma}_{h,T+1}}\right),
\]

\[
f_{\Psi_{SC}^{E,t,a}}(x) = \sum_{u=1}^{t} \frac{(-1)^{u+1}}{\Gamma(u+1)} \sum_{n_1=1}^{t} \cdots \sum_{n_u=1}^{t} \sum_{k_{n_1}=1}^{M_{n_1}} \cdots \sum_{k_{n_u}=1}^{M_{n_u}} \pi_{ME,u} \Delta_{ME,u} \exp\left(-\Delta_{ME,u} x\right),
\]

respectively, where $\bar{\gamma}_{h,T+1} = P_T \sigma_n^2 n_\Omega$ and $\bar{\gamma}_{E,t} = P_t - 1 \sigma_n^2 n_\Omega$.

Proof: See Appendix A-A. ■

Now, we are in position to derive the exact closed-form expression of the SOP for this scheme where the eavesdropper clusters adopt SC for the received signal in each time slot.

Proposition 1: The achievable secrecy rate of DF relay networks for the MS scheme is

\[
P_{sec,a}^{SC} = 1 - \sum_{u=1}^{T+1} \sum_{n_1=1}^{T+1} \cdots \sum_{n_u=1}^{T+1} \sum_{k_{n_1}=1}^{M_{n_1}} \cdots \sum_{k_{n_u}=1}^{M_{n_u}} \frac{(-1)^{u+1} \pi_{ME,u} \Theta_{T+1}}{\Gamma(u+1) \left(1 + \frac{\partial_{ME,u} \bar{\gamma}_{h,T+1}}{\bar{\gamma}_{h,T+1}}\right)} \exp\left(-\frac{\kappa}{\bar{\gamma}_{h,T+1}}\right).
\]

where $\Theta_t$ is the probability that the transmission fails in time slot $t$ which can be expressed as

\[
\Theta_t = \begin{cases} 
\eta t \prod_{q=1}^{t-1} \bar{\eta}_q & , t = 1, 2, ..., T \\
\prod_{q=1}^{T} \bar{\eta}_q & , t = T + 1 
\end{cases}
\]

To be more concrete, $\Theta_t$ for $t \in 1, 2, ..., T$ denotes the probability that transmission fails in time slot $t$. Failing in time slot $t$ means that the the transmission must be successful up to time slot $t - 1$. Therefore, for obtaining $\Theta_t$ we should multiply the probability of failure in transmission in time slot $t$ with the probabilities of successful transmissions in prior time slots. Besides, $\Theta_{T+1}$ shows the probability that the transmission be successful in all time slots. It is noteworthy that in this scheme $\beta_t = \Theta_t$.

Proof: See Appendix A-A. ■

In case where the eavesdroppers employ MRC to their received signals the source and the eavesdropper channel capacity in time slot $t$ can be written as

\[
C_{E,t,a}^{MRC} = \frac{1}{T+1} \log_2 \left(1 + \Psi_{E,t,a}^{MRC}\right),
\]

where $\Psi_{E,t,a}^{MRC} = \sum_{u=1}^{t} \sum_{j=1}^{M_a} \frac{P_{u-1}}{\sigma_n^2} |f_{u,i_{u-1,j}}|^2$. In the following proposition, we derive exact close-form expression for the case where the eavesdroppers use MRC.
Proposition 2: The secrecy OP for the MS scheme can be derived as
\[ P_{\text{sec,a}}^{MRC} = 1 - \sum_{m=1}^{T+1} \sum_{k=1}^{M_m} \left( \Theta_{T+1}^{\alpha_{m,k}} \exp \left( - \frac{K}{\tilde{\gamma}_{h,T+1}} \right) \right) . \] (16)

Proof: See Appendix A-B.

B. Maximum Selection with Decoding Set (MSDS)

This subsection presents the MSDS scheme, in which the best relay is the one that amongst all relays that decode the received signal correctly gives highest instantaneous SNR to the next cluster. Therefore, the relay selection rule can be written as
\[ \hat{i}_t = \arg\max_{i \in D_t} \left\{ \arg\max_{j \in \{1,2,\ldots,N_t+1\}} \{ C_{ij}^{DF} \} \right\} , \] (17)
where \( C_{ij}^{DF} = \frac{P_u}{\sigma_n^2} |h_{t+1,i,j}|^2 \), \( D_t \) denotes the random subset of relays that can successfully decode the source message in time slot \( t \), referred to as decoding set, and let \( p_t = |D_t| \) denote the cardinality of the decoding set. Herein, for this scheme the probability that \( i \) number of relays be successful in decoding in time slot \( t > 1 \) can be defined as \( \mu_{t,i} \) as in the following
\[ \mu_{t,0} = \sum_{p_{t-1}=0}^{N_{t-1}} \mu_{t-1,p_{t-1}} \left[ 1 - \exp \left( - \frac{\kappa}{\tilde{\gamma}_{h,t}} \right) \right]^{p_{t-1}N_t} , \] (18)
\[ \mu_{t,i} = \sum_{p_{t-1}=1}^{N_{t-1}} \sum_{q=0}^{i-1} \mu_{t-1,p_{t-1}} \prod_{m=0}^{i-1} \left( N_t - m \right) \Gamma(i) \left( q \right) \left[ 1 - \exp \left( - \frac{\kappa}{\tilde{\gamma}_{h,t}} \right) \right]^{N_t+q-i} \times \left( 1 - \left[ 1 - \exp \left( - \frac{\kappa}{\tilde{\gamma}_{h,t}} \right) \right]^{i+N_t(p_{t-1}-1)-q} \right) , \] (19)
where \( \mu_{1,i} = \binom{N_i}{i} \exp \left( - \frac{i\kappa}{\tilde{\gamma}_{h,1}} \right) \left[ 1 - \exp \left( - \frac{\kappa}{\tilde{\gamma}_{h,1}} \right) \right]^{N_1-i} , i \in \{0,1,\ldots,N_1\} .

With that in mind, the capacity of the the source to destination and also the source to the eavesdropper channel in time slot \( t \) can be defined in bit/sec/Hz as
\[ C_{D,b} = \frac{1}{T+1} \log_2 \left( 1 + \Psi_{D,b} \right) , \] (20)
\[ C_{E,t,b}^{SC} = \frac{1}{T+1} \log_2 \left( 1 + \Psi_{E,t,b}^{SC} \right) , \] (21)
where \( \Psi_{D,b} = \max_{i \in D_t} \left\{ \frac{P_u}{\sigma_n^2} |h_{T+1,i,D}|^2 \right\} \) and \( \Psi_{E,t,b}^{SC} = \max_{u=1,\ldots,t} \left\{ \max_{j=1,\ldots,M_u} \left\{ \frac{P_u}{\sigma_n^2} |f_{u,i+1,j}|^2 \right\} \right\} . \) To obtain the SOP of the proposed selection scheme, the CDF expression of the random variable \( \Psi_D^{\text{DSC}} \) is required. In the following, we derive the results.
Lemma 2: The CDF of the RVs $\Psi_{D,b}$ is given by
\[
F_{\Psi_{D,b}}(y|p_T) = \left[1 - \exp\left(-\frac{y}{\bar{\gamma}_{h,T+1}}\right)\right]^{p_T}.
\] (22)

In the following proposition exact close-form expression for the secrecy SOP of the MS scheme will be provided.

**Proposition 3:** This proposition derives a closed-form SOP expression of MS scheme as
\[
P_{SC_{sec,b}} = 1 - \sum_{p_T=1}^{N_T} \sum_{z=1}^{T+1} \sum_{m=1}^{M_m} \sum_{k=1}^{M_n} \left(-1\right)^{k+1} \left(\frac{p_T}{z}\right)^{\mu T,p_T} \frac{\alpha_{m,k} \mu T,p_T}{\bar{\gamma}_{h,T+1}} \exp\left(-\frac{z \kappa}{\bar{\gamma}_{h,T+1}}\right).
\] (23)

**Proof:** See Appendix B-B.

It is noteworthy that in this scheme $\beta_t$ is $\mu T,p_T$.

Next, We derive SOP for case where the eavesdroppers employ MRC.

**Proposition 4:** The SOP for the MS case where the eavesdroppers use MRC is derived as
\[
P_{MRC_{sec,b}} = 1 - \sum_{p_T=1}^{N_T} \sum_{z=1}^{T+1} \sum_{m=1}^{M_m} \sum_{k=1}^{M_n} \left(-1\right)^{k+1} \left(\frac{p_T}{z}\right)^{\mu T,p_T} \frac{\alpha_{m,k} \mu T,p_T}{\bar{\gamma}_{h,T+1}} \exp\left(-\frac{z \kappa}{\bar{\gamma}_{h,T+1}}\right).
\] (24)

**Proof:** See Appendix B-C.

**C. MaxMin Selection with Decoding Set (MMSDS)**

In this category of selection, among all relays that decode the received signal correctly, best relay is the one that its worse channel to the next relay cluster is the best channel. Thus, the DF based MMSDS relay selection criterion can be obtained from Eq. (25) as
\[
\tilde{i}_t = \arg\max_{i \in D_t} \left\{ \arg\min_{j \in \{1,2,...,N_{t+1}\}} \left\{ C_{i,j}^{DF} \right\} \right\},
\] (25)

where $C_{i,j}^{DF} = \frac{P_t}{\sigma_n^2} |h_{t+1,i,j}|^2$. Then, we derive the probability that $i$ number of relay nodes decode the received signal correctly, as follows
\[
\eta_{t,0} = \begin{cases} 
\sum_{p_T=1}^{N_T} \sum_{l=1}^{N_T} \sum_{r=0}^{N_{t-1}} \sum_{k=1}^{N_{t}} \left(-1\right)^{r+1} \frac{N_{t-1} \left(p_T \right)^{r+1}}{\bar{\gamma}_{h,t}} \exp\left(-\frac{r \gamma}{\bar{\gamma}_{h,t}}\right) \left(1 - \exp\left(-\frac{\gamma}{\bar{\gamma}_{h,t}}\right)\right) \left(1 + \frac{\bar{\gamma}_{h,t} \gamma}{\tilde{\gamma}_{h,t+1}}\right), & p_{t-1} \neq 1 \\
\eta_{t-1,1} \left(1 - \exp\left(-\frac{\gamma}{\bar{\gamma}_{h,t}}\right)\right) N_t, & p_{t-1} = 1
\end{cases}
\] (26)
$$\eta_{t,i} = \begin{cases} \sum_{p_{t-1}=1}^{N_t-1} \sum_{l=1}^{N_t-1} \sum_{r=0}^{p_{t-1}-1} \frac{(-1)^{i-r+1}(N_t-m)N_{t-l}}{N_{t-r+1}N_{t-i}N_{t-r+1}} \frac{N_t}{N_{t-i}+N_{t-r+1}} \times \\ \exp \left( -\frac{r+i}{\gamma_{h,t}} \right) \left( 1 - \exp \left( -\frac{N_{t-r+1}}{\gamma_{h,t}} \right) \right) \right), & p_{t-1} \neq 1 \\ \frac{1}{\Gamma(N_{t-r+1})} \exp \left( -\frac{r}{\gamma_{h,t}} \right) \left( 1 - \exp \left( -\frac{\gamma_{h,t}}{\gamma_{h,t}} \right) \right)^{N_{t-r+1}}, & p_{t-1} = 1 \end{cases} \right.,$$

(27)

where $\eta_{1,i} = \mu_{1,i}, i \in \{1, 2, ..., N_1\}$. In this scheme, the received signals at the destination and at the eavesdropper nodes are the same as that of MSDS scheme. Thus, by replacing $\eta_{T,p_T}$ with $\mu_{T,p_T}$ in 23 and 24, we can achieve the SOP of SC and MRC cases for this scheme, respectively.

### D. Minimum Selection with Decoding Set (MiSDS)

We now present the DF based MiSDS relay selection scheme in which the relay that minimizes instantaneous SNR to the eavesdropper is selected as the optimal relay. Thus, the MiSDS relay selection criterion is obtained from

$$\tilde{i}_t = \operatorname{argmin}_{i \in D_t} \left\{ \max_{u=1,2,...,M_{t+1}} \left\{ C_{DF}^{DF,E,t,i,u} \right\} \right\},$$

(29)

where $C_{DF}^{DF,E,t,i,u} = \frac{P_t}{\sigma_n^2} \left| f_{t+1,i,u} \right|^2$. First, we investigate the probability that a relay can succeed in decoding.

$$\xi_{t,i} = \left( \frac{N_t}{i} \right) \left[ \exp \left( -\frac{x}{\tilde{\gamma}_{h,t}} \right) \right]^i \left[ 1 - \exp \left( -\frac{x}{\tilde{\gamma}_{h,t}} \right) \right]^{N_t-i}, t \in \{1, ..., T\}, i \in \{0, ..., N_t\}.$$

(30)

Next, in what follows, we derive exact closed form expression for the secrecy outage probability, where the eavesdropper employs MRC to all received signals in each time slot.

The channel capacity at destination and at eavesdropper node at time slot $t$ in bit/sec/Hz are given respectively by

$$C_{D,d} = \frac{1}{2} \log_2 \left( 1 + \Psi_{D,d} \right),$$

(31)

$$C_{SC,E,t,d}^{SC} = \frac{1}{2} \log_2 \left( 1 + \Psi_{E,t,d}^{SC} \right),$$

(32)

where $\Psi_{D,d} = \Psi_{D,a}$ and $\Psi_{E,t,d}^{SC} = \max_{u=1,...,t} \left\{ \max_{j=1,...,M_u} \left\{ \frac{P_{t-1}}{\sigma_n^2} \left| f_{u,j,i_u-1,j} \right|^2 \right\} \right\}$. Notice the CDF of RVs
\( \Psi_{D,c} \) was given in (11). The following lemma is of important when it provides the closed-form expression of the PDF of \( \Psi_{E,t,c}^{SC} \).

**Lemma 3:** The PDF of the RV \( \Psi_{E,t,c}^{SC} \) can be is obtained as

\[
f_{\Psi_{E,t,c}^{SC}}(x) = 1 - \sum_{k_1=1}^{M_1} (-1)^{k_1+1} \left( \frac{M_1}{k_1} \right) \exp \left( -\frac{k_1 x}{\gamma_{E,1}} \right) - \sum_{u=2}^{T+1} \sum_{n_2=2}^{T+1} \sum_{n_u=2}^{T+1} \sum_{p,k_2}^{T+1} \sum_{p,k_1}^{N,M_2} \sum_{p,k,u}^{N,M_u} \frac{N \exp (-Kx)}{\Gamma(u)} \left( \frac{M_1}{k_1} \right) \times \exp \left( -\left( K + \frac{k_1}{\gamma_{E,1}} \right) x \right),
\]

where \( \sum_{p,k,u}^{N,M} = \sum_{n_u=2}^{M_{nu}} \sum_{k_{nu}=1}^{M_{nu}} \sum_{p_{nu}=1}^{\lambda} N \exp (-Kx) \left( \frac{M_1}{k_1} \right) \times \exp \left( -\left( K + \frac{k_1}{\gamma_{E,1}} \right) x \right) \), and

\[
K = \sum_{q=1}^{u} \sum_{m=1}^{p_{q-1}} \frac{k_{nq,m}}{\gamma_{E,nq}^{+1}}.
\]

**Proof:** See Appendix D-A

**Proposition 5:** The SOP of the MiSDS scheme is computed as

\[
\begin{align*}
P_{sec,d}^{SC} &= 1 - \sum_{k_1=1}^{M_1-1} \frac{(-1)^{k_1+1} \Gamma}{1 + \frac{\gamma_{E,1}(\kappa+1)}{k_1\gamma_{h,T+1}}} \left( \frac{M_1}{k_1} \right) \exp \left( -\frac{\kappa}{\gamma_{h,T+1}} \right) - \sum_{u=2}^{T+1} \sum_{n_2=2}^{T+1} \sum_{n_u=2}^{T+1} \sum_{p,k_2}^{T+1} \sum_{p,k_1}^{N,M_2} \sum_{p,k,u}^{N,M_u} \frac{(-1)^u N \lambda_{p_n}}{\Gamma(u)} \left( \frac{\kappa+1}{\gamma_{h,T+1}} \right) \exp \left( -\frac{\kappa}{\gamma_{h,T+1}} \right) \\
&+ \sum_{k_1=1}^{M_1-1} \sum_{u=2}^{T+1} \sum_{n_2=2}^{T+1} \sum_{n_u=2}^{T+1} \sum_{p,k_2}^{T+1} \sum_{p,k_1}^{N,M_2} \sum_{p,k,u}^{N,M_u} \frac{(-1)^{k_1+u-1} N \lambda_{p_n}}{\Gamma(u)} \left( \frac{\kappa+1}{\gamma_{h,T+1}} \right) \exp \left( -\frac{\kappa}{\gamma_{h,T+1}} \right),
\end{align*}
\]

where \( \lambda_{p_n} = \prod_{l=2}^{u} \xi_{n_{l-1},p_{l-1}} \prod_{m=2}^{T+1} n_{m-1,0} \tilde{\xi}_{m-1,0}, \gamma = \prod_{l=2}^{T+1} \xi_{l-1,0}. \)

**Proof:** See Appendix D-A

In the sequel, we will present secrecy outage probability for the MiSDS scheme where eavesdroppers use MRS to all received signal.

\[
\tilde{i}_t = \arg\min_{i \in D_t} \left\{ \sum_{u=1}^{M_i} C_{E,t,i,u}^{DF} \right\},
\]

(35)
where \( C_{E,t,c}^{DF} = \frac{P_t}{\sigma_n^2} |f_{t+1,i,u}|^2 \).

**Proposition 6:** The channel capacity of eavesdropper at time slot \( t \) and at destination in bit/sec/Hz are given by

\[
C_{E,t,c}^{MRC} = \frac{1}{2} \log_2 \left( 1 + \Psi_{E,t,d}^{MRC} \right),
\]

where \( \Psi_{E,t,d}^{MRC} = \sum_{u=1}^{t} \sum_{j=1}^{M_u} \frac{P_{u-1,j}}{\sigma_n^2} |f_{u+1,i,j}|^2 \). The PDF of RVs \( \Psi_{E,t,c}^{MRC} \) for \( t = 1 \) is

\[
f_{\Psi_{E,1,d}^{MRC}}(x) = \frac{x^{M_1-1}}{\Gamma(M_1)} \exp \left( -\frac{x}{\gamma_{E,1}} \right),
\]

and for \( t > 1 \)

\[
f_{\Psi_{E,t,d}^{MRC}}(x) = \frac{x^{M_1-1}}{\Gamma(M_1)} \exp \left( -\frac{x}{\gamma_{E,1}} \right) + \sum_{r=2}^{T+1} \frac{\zeta_{r,v}^{E,t}}{\Gamma(v)} x^{v-1} \exp \left( -\frac{x}{\gamma_{E,r}} \right),
\]

where \( \sum_{p,k,t} \sum_{p,k,t} \cdots \sum_{p,k,t} \frac{\zeta_{0,v}^{E,t}}{\Gamma(v)} x^{v-1} \exp \left( -\frac{x}{\gamma_{E,1}} \right) + \sum_{r=2}^{T+1} \frac{\zeta_{r,v}^{E,t}}{\Gamma(v)} x^{v-1} \exp \left( -\frac{x}{\gamma_{E,r}} \right) \),

substituting of (37), (38) and (11) into (6), the secrecy outage probability can be expressed as

\[
P_{sec,d}^{MRC} = 1 - \sum_{p_1=1}^{N_1} \sum_{p_2=1}^{N_2} \cdots \sum_{p_T=1}^{N_T} \sum_{p_1=1}^{N_1} \sum_{p_2=1}^{N_2} \sum_{p_T=1}^{N_T} \lambda_p \left( \sum_{v=1}^{M_1} \frac{\zeta_{0,v}^{E,t} \exp \left( -\frac{\kappa}{\gamma_{h,T+1}} \right)}{\gamma_{h,T+1}} + \sum_{r=2}^{T+1} \frac{\zeta_{r,v}^{E,t} \exp \left( -\frac{\kappa}{\gamma_{h,T+1}} \right)}{\gamma_{h,T+1}} \right),
\]

where, \( \lambda_p = \prod_{l=1}^{T} \xi_{l,p} \).

**Proof:** See Appendix D-B.

**E. Special Cases of Interest**

Next, we particularize the above results of the secrecy OP to the one-hop scenario as generally assumed in related works. In addition, we study the special case where the scenario is multi-hop but there is only one relay and a single eavesdropper in each hop. Therefore, in this special case we have no relay selection. For comprehensiveness purposes as before we assume that the eavesdropper node is able to employ either MRC or SC.
1) One Way: The channel capacity at eavesdropper and at the destination in bit/sec/Hz are given by

\[
C_{D,one} = \frac{1}{2} \log_2 (1 + \Psi_{D,one}) ,
\]

\[
C^{SC}_{E,one} = \frac{1}{2} \log_2 (1 + \Psi^{SC}_{E,one}) ,
\]

where \( \Psi_{D,one} = \frac{P_0}{\sigma^2_n} |h_{1,S,D}|^2 \) and \( \Psi^{SC}_{E,one} = \max_{j=1,...,M_1} \left\{ \frac{P_0}{\sigma^2_n} |f_{1,S,j}|^2 \right\} \). Then the CDF and PDF of the RVs \( \Psi_{D,one} \) and \( \Psi^{SC}_{E,one} \) are given by

\[
F_{\Psi_{D,one}} (y) = 1 - \exp \left( - \frac{y}{\gamma_{h,1}} \right) ,
\]

\[
f_{\Psi^{SC}_{E,one}} (x) = \sum_{k=1}^{M_1} (-1)^{k-1} \binom{M_1}{k} \exp \left( - \frac{k}{\gamma_{E,1}} x \right) ,
\]

Then, a closed form expression for the SOP of this case where the eavesdroppers employ MRC of all received signal in each time slot can be obtained as

\[
P^{SC}_{sec,one} = 1 - \sum_{k=1}^{M_1} (-1)^{k-1} \binom{M_1}{k} \exp \left( - \frac{k}{\gamma_{h,1}} \right) \left( 1 + \frac{(\kappa+1)\gamma_{E,1}}{\gamma_{h,1}} \right)^{M_1} .
\]

Herein, we derive exact close-form expression for the first special case where the eavesdropper nodes use MRC. The eavesdropper channel capacity in bit/sec/Hz is

\[
C^{MRC}_{E,one} = \frac{1}{2} \log_2 (1 + \Psi^{MRC}_{E,one}) ,
\]

where \( \Psi^{MRC}_{E,one} = \sum_{j=1}^{M_1} \frac{P_0}{\sigma^2_n} |f_{1,S,j}|^2 \). Then, the PDF of the RV \( \Psi^{MRC}_{E,one} \) is computed as

\[
f_{\Psi^{MRC}_{E,one}} (x) = \frac{1}{\gamma_{E,1}^{M_1}} \Gamma (M_1) x^{M_1-1} \exp \left( - \frac{x}{\gamma_{E,1}} \right) .
\]

Finally, the \( P^{MRC}_{sec,one} \) for this case can be expressed as

\[
P^{MRC}_{sec,one} = 1 - \frac{\exp \left( - \frac{\kappa}{\gamma_{h,1}} \right)}{\left( 1 + \left( \kappa + 1 \right) \frac{\gamma_{E,1}}{\gamma_{h,1}} \right)^{M_1}} .
\]

F. Multi-hop with One Relay at Each Hop and One Eavesdropper at Each Hop

In order to demonstrate the secrecy performance advantage achieved by our proposed cooperative diversity schemes, in this section we examine the secrecy performance of the case where each cluster includes only one relay and one eavesdropper node. To this end, we first derive the
expression for the exact SOP of the case where the eavesdroppers apply SC. We then derive the SOP of the MRC case. To begin, for SC case, the channel capacity at eavesdropper and at the destination in bit/sec/Hz can be expressed as

\[ C_{D,ore} = \frac{1}{2} \log_2 \left( 1 + \Psi_{D,ore} \right), \]

\[ C_{SC}^{E,ore} = \frac{1}{2} \log_2 \left( 1 + \Psi_{SC}^{E,ore} \right), \]

where \( \Psi_{D,ore} = \frac{P_T}{\sigma_n^2} |h_{T+1,1}|^2 \) and \( \Psi_{SC}^{E,ore} = \max_{u=1,...,t} \left\{ \frac{P_{u-1}}{\sigma_n^2} |f_{u,1,1}|^2 \right\} \). Then the CDF of the RV \( \Psi_{D,ore} \) and the PDF of the RV \( \Psi_{SC}^{E,ore} \) can be respectively obtained as

\[ F_{\Psi_{D,ore}} (y) = 1 - \exp \left( -\frac{y}{\gamma_{h,T+1}} \right), \]

\[ f_{\Psi_{SC}^{E,ore}} (x) = 1 - \sum_{u=1}^{t} \frac{(-1)^{u+1}}{(u+1)!} \sum_{n_1=1}^{T+1} \sum_{n_u=1}^{T+1} \left( \frac{\Delta_{E,u} \Theta_{T+1}}{\gamma_{E,m}} + \Delta_{E,u} \right) \exp \left( -\frac{\kappa}{\gamma_{h,T+1}} \right). \]

where \( \Delta_{E,u} = \sum_{p=1}^{u} \frac{1}{\gamma_{E,n_p}} \). Finally, we can write the SOP of this scheme as

\[ P_{SC}^{sec,ore} = 1 - \sum_{u=1}^{t} \frac{(-1)^{u+1}}{(u+1)!} \sum_{n_1=1}^{T+1} \sum_{n_u=1}^{T+1} \left( \frac{\Delta_{E,u} \Theta_{T+1}}{\gamma_{E,m}} + \Delta_{E,u} \right) \exp \left( -\frac{\kappa}{\gamma_{h,T+1}} \right). \]

Next, we derive closed form expression for the case where eavesdropper uses MRC. The eavesdropper channel capacity in bit/sec/Hz can be expressed as

\[ C_{MRC}^{E,ore} = \frac{1}{2} \log_2 \left( 1 + \Psi_{E,ore}^{MRC} \right), \]

where \( \Psi_{E,ore}^{MRC} = \sum_{u=1}^{t} \frac{P_{u-1}}{\sigma_n^2} |f_{u,1,1}|^2 \). The PDF of the RVs \( \Psi_{E,ore}^{MRC} \) can be obtained as

\[ f_{\Psi_{E,ore}^{MRC}} (x) = \sum_{m=1}^{t} \alpha_{m,1} \exp \left( -\frac{\gamma}{\gamma_{E,m}} \right), \]

where \( \alpha_{m,1} = \prod_{j=1}^{t} \frac{1}{\gamma_{E,f}^{j} - \gamma_{E,m}^{j}} \). Then, the SOP for this case, \( P_{MRC}^{sec,ore} \) can be expressed as

\[ P_{MRC}^{sec,ore} = 1 - \sum_{m=1}^{T+1} \frac{\alpha_{m,1} \Theta_{T+1} \exp \left( -\frac{\kappa}{\gamma_{h,T+1}} \right)}{\gamma_{h,T+1} + \gamma_{E,m}}. \]
IV. Numerical Results and Discussions

In this section, we provided numerical results to compare our analysis in section III with Monte Carlo simulation. Herein, we assume the all links obey the Rayleigh distribution. For notational convenience, let $N_i$ denotes the number of relays at $i$th hop, $M_k$ represent the number of eavesdroppers at $k$th hop and finally, $T$ show the number of time slots. In addition, in our analysis, we set $\kappa = 3dB$. All curves are plotted as a function of the average SNR per symbol $P/\sigma_n^2$.

Fig. 2 presents the SOP versus the SNR for four relay selection schemes, namely, MS, MSDS, MMSDS, and MiSDS where we refer as ”Scenario, a”, ”Scenario, b”, ”Scenario, c”, and ”Scenario, d” in our figures. In this figure, we also sketched the SOP for the two so-called signal combining solutions, i.e., MRC and SC. Obviously, the derived results are aligned with the simulation results, which validate the correctness of the aforementioned derivation. From the figure, we observe that the SOP performance increases by increasing SNR for middle SNR and have a floor for high SNR (it appears to be quasiconvex). It’s due to the fact that with increasing the power transmission in source and relay clusters, the received SNR at eavesdropper clusters also increases and that’s why no further improvement occurs at high SNR regime. In addition, we can see that the SOP performance of the MMSDS outperforms that of the other schemes. As the figure shows, we can achieve better SOP when eavesdropper uses SC in comparison with the case where eavesdropper employs MRC.

Fig. 2. SOP performance of proposed relay selection schemes versus the SNR, with $T = 3$, $N_i = [2, 4, 3]$, and $M_k = [2, 1, 3, 2]$.

Fig. 3 depicts the SOP comparison among the four relay selection schemes and for the two special cases of interest presented above as a function of $M_k$, $k \in \{1, 2, ..., T + 1\}$ for different values of relay number. As expected, the SOP of the aforementioned schemes reduce dramatically when $M_k$ increases. Concretely, when the number of eavesdroppers number increases, since the eavesdropper nodes collude with each other, the chance of data extraction and the chance of correctness of the received symbols from the main network increases. Moreover, as can be
seen when the number of eavesdroppers at each hop become more than 10, the SOP of all the schemes converge to 1, implying a fully unsecured system. Additionally, with all the values of $N$ in Fig. 3, the performance of the MMSDS and MSDS schemes outperform that of the other schemes dramatically. Also it needs to be pointed out that once the eavesdroppers employ MRC a performance degradation will occur for all schemes.

Fig. 3. SOP performance of proposed relay selection schemes versus $M_k$, with $T = 3$, $P_t = 15dB$, $N_t = 2$, $t \in \{1, 2, ..., T\}$.

Fig. 4 illustrates the SOP comparison versus $N_i$, $i \in \{1, 2, ..., T\}$ for all relay selection schemes and also for the two special cases of interests. As can be easily found in Fig. 4, the theory curves of the SOP of the selection schemes agree excellently to the simulation ones. As is evident from this figure, by increasing the number of relays, the secrecy performance enhances from $N = 1$ to $N = 10$. However, for the MS and MiSDS selection schemes, the performance floor occurs for small number of relays, implying that employing more relays is not efficient for these two schemes. For the other selection schemes, the larger the number of relays is, the more relays may decode the source signal successfully, and more relays are employed simultaneously in the transmission, resulting in a better performance.

Fig. 4. SOP performance of proposed relay selection schemes versus $N_i$, with $T = 3$, $P_t = 15dB$, $M_t = 2$, $t \in \{1, 2, ..., T\}$.

In Fig. 5 we plot the SOP as a function of $T$ for different relay selection schemes and for the special cases. In this figure, we first observe that the SOPs results obtained from the formulas match precisely the corresponding simulated ones. The figure also indicates that increasing the
number of hops can significantly degrade the physical layer security of the considered system model which shows that taking the number of hops into account in the design of the network is vital. In this figure, we also observe that amongst the proposed schemes the MMSDS is more robust to the change of the system parameters which in turn illustrates the security benefits of exploiting this scheme. Furthermore, as is evident from the figure, the SOP gap between the proposed schemes becomes marginal as $T$ increases (i.e., from $T = 1$ to $T = 7$). This is due to the fact that by increasing the number of hops the chance of data leakage increases which dominates the benefit of employing relay selection. This observation indicates that after a certain value of $T$ the secrecy performance of all schemes converge to 1.

![Graph showing SOP performance](image)

**Fig. 5.** SOP performance of proposed relay selection schemes versus $T$, with $T = 3$, $P_t = 15dB$, $N_t = 2$, $M_t = 2$, and $t \in \{1, 2, ..., T\}$.

### V. Conclusion

In this paper, we dedicate to seek insights into an efficient secure information transmission based on a physical layer security framework over a collaborative multi-hop multi-DF-relay network, coexisting with multiple clusters of passive eavesdroppers. Four relay selection schemes, namely, MS, MSDS, MMSDS, and MiSDS schemes, were proposed to further improve the secrecy performance of the considered scenario. Additionally, to get more insights and for the comparison purposes we studied the performance analysis of two special cases of interest. We have derived the closed-form expression of the SOP of the proposed network under different relay selection schemes. Our analysis revealed that, the secrecy outage performance of the considered system can significantly benefit from increasing the number of cooperative relays at each cluster. Besides, more number of eavesdroppers will pose greater threats to the security of the considered system. In addition, the secrecy performance of the system under study significantly reduces by increasing the number of the wiretap nodes. Moreover, the number of hops also have great effects on the secrecy performance of the network.
**APPENDIX A**

**PROOF OF SCENARIO A**

A. **SC 1**

For calculating $P_{sec,a}^{SC}$, we need to derive the CDF and PDF of the RVs $\Psi_{D,a}$ and $\Psi_{E,t,a}^{SC}$, respectively. The received SNR in destination and its CDF are given by

$$\Psi_{D,a} = \frac{P_T}{\sigma_n^2} |h_{T+1,i_{T,D}}|^2 \tag{56}$$

$$F_{\Psi_{D,a}}(x) = 1 - \exp \left(-\frac{x}{\bar{\gamma}_{h,T+1}}\right). \tag{57}$$

The received SNR at the eavesdropper is

$$\Psi_{E,t,a}^{SC} = \max_{u=1,2,...,t} \left\{ \max_{j=1,2,...,M_u} \left\{ \frac{P_{u-1}}{\sigma_0^2} |f_{E,i_{u-1,j}}|^2 \right\} \right\}. \tag{58}$$

For calculating the PDF of $\Psi_{E,t,a}^{SC}$, we do the following change of variable $w_{u,j} = \frac{P_{u-1}}{\sigma_0^2} |f_{E,i_{u-1,j}}|^2$.

The PDF of received signal at $j$th eavesdropper in relay cluster $u$ is given by

$$f_{W_{u,j}}(y) = 1 - \exp \left(-\frac{y}{\bar{\gamma}_{E,u}}\right). \tag{59}$$

The received signal at eavesdropper cluster $u$ and its CDF are given by

$$\gamma_u = \max_{j=1,2,...,M_u} w_{u,j}, \tag{60}$$

$$F_{\gamma_u}(y) = \prod_{j=1}^{M_u} \left[ 1 - \exp \left(-\frac{x}{\bar{\gamma}_{E,u}}\right) \right] = 1 - \sum_{k_u=1}^{M_u} (-1)^{k_u-1} \binom{M_u}{k_u} \exp \left(-\frac{k_u}{\bar{\gamma}_{E,u}} y\right), \tag{61}$$

respectively. The final received signal at eavesdropper and its CDF are expressed as

$$\Psi_{E,t,a}^{SC} = \max_{u=1,2,...,t} \gamma_u, \tag{62}$$

$$F_{\Psi_{E,t,a}^{SC}}(y) = \prod_{u=1}^{t} \left[ 1 - \sum_{k_u=1}^{M_u} (-1)^{k_u-1} \binom{M_u}{k_u} \exp \left(-\frac{k_u}{\bar{\gamma}_{E,u}} y\right) \right]. \tag{63}$$

respectively. With help of the identity product as in the following

$$\prod_{u=1}^{t} (1 - x_u) = 1 - \sum_{u=1}^{t} \sum_{n_1=1}^{t} \sum_{n_u=1}^{t} \prod_{p=1}^{t} x_{n_p}, \tag{64}$$

and by substituting (63) into (64) and taking the derivative w.r.t. $y$ the equation (12) can be obtained. Finally by replacing (11) and (12) in (6), and after some algebraic manipulations, we get $P_{sec,a}^{MAX}$. 
B. MRC 2

The received SNR at the eavesdropper is given by

$$\Psi_{E,t,a}^{\text{MRC}} = \sum_{u=1}^{t} \sum_{j=1}^{M_u} \frac{P_{u-1}}{\sigma_0^2} |f_{E,i}^u| f_{E,i}^u |f_{E,i}^u|^2.$$  \hspace{1cm} (65)

To compute the PDF of $\Psi_{E,t,a}^{\text{MRC}}$ we use the following change of variables $\gamma_u = \sum_{j=1}^{M_u} w_{u,j}$. Then the CDF of $\gamma_u$ can be written as

$$F_{\gamma_u}(y) = 1 - \sum_{n_u=0}^{M_u} \frac{y^{n_u}}{\Gamma(n_u + 1)} \gamma_u^{n_u} \exp \left( -\frac{y}{\gamma_u} \right).$$  \hspace{1cm} (66)

The MGF of RV $\gamma_u$ is computed as

$$f_{\gamma_u}(s) = \prod_{i=1}^{u} \frac{1}{\gamma_i^{M_i} \left( s + \frac{1}{\gamma_i} \right)^{M_i}}.$$  \hspace{1cm} (67)

Making use of MGF of $\Psi_{E,t,a}^{\text{MRC}}$ we can obtain its PDF. The MGF of $\Psi_{E,t,a}^{\text{MRC}}$ is given by

$$f_{\Psi_{E,t,a}^{\text{MRC}}}(s) = \prod_{u=1}^{t} f_{\gamma_u}(s),$$  \hspace{1cm} (68)

and the PDF of the RVs $\Psi_{E,t,a}^{\text{MRC}}$ is given by

$$f_{\Psi_{E,t,a}^{\text{MRC}}}(x) = \sum_{m=1}^{t} \sum_{k=1}^{M_m} \frac{\alpha_{m,k}}{\Gamma(t-k+1)} y^{k-1} \exp \left( -\frac{y}{\gamma_{E,m}} \right),$$  \hspace{1cm} (69)

where $\alpha_{m,k} = \frac{\varphi_m^{(t-k)} (-\gamma_{E,k}^{-1})}{\Gamma(t-k+1)}$ and $1/\varphi_m(s) = \prod_{f=1}^{t} \gamma_{E,f}^{M_f} \prod_{f \neq m}^{t} \left( s + \gamma_{E,f}^{-1} \right)$. Finally by replacing (11) and (69) in (6), and after some algebraic manipulations, we achieve the $P_{\text{sec},a}^{\text{MRC}}$.

**APPENDIX B**

**MAXIMUM SELECTION WITH DECODING SET**

A. Relay Selection

We need to compute the probability that a relay successfully decode a signal in each cluster. For scenario $b$, we have

$$\hat{\iota}_t = \arg\max_{i \in D_t} \left\{ \arg\max_{j \in \{1,2,\ldots,t+1\}} \{ C_{i,j}^{DF} \} \right\}.$$  \hspace{1cm} (70)
Then, the probability that none of the relays can decode the received signal correctly, is given by

$$\mu_{t,0} = \sum_{p_{t-1}=0}^{N_{t-1}} \mu_{t-1,p_{t-1}} \omega_{t,0},$$  \hspace{1cm} (71)$$

where $\omega_{t,0}$ is the probability that all relays in cluster $t$ can’t decode the receive signal correctly while, $p_{t-1}$ relays in the previous cluster could decode the received signal correctly, and it is given as

$$\omega_{t,0} = \Pr \left( u \in \max_{u \in \mathcal{D}_{t-1}} \left\{ \max_{j=1,\ldots,N_t} \left\{ \frac{P_{t-1}}{\sigma_0^2} |h_{t,u,j}|^2 \right\} \right\} \leq \kappa \right).$$  \hspace{1cm} (72)$$

With the following change of variables and obtaining their corresponding CDFs, we are able to compute $\omega_{t,0}$ as

$$w_{u,j} = \frac{P_{t-1}}{\sigma_0^2} |h_{t,u,j}|^2 \rightarrow F_{w_{u,j}}(x) = 1 - \exp \left( -\frac{x}{\gamma_{h,t}} \right)$$  \hspace{1cm} (73)$$

$$w_u = \max_{j=1,\ldots,N_t} \{w_{u,j}\} \rightarrow F_{w_u}(x) = \left[ 1 - \exp \left( -\frac{x}{\gamma_{h,t}} \right) \right]^{N_t}$$  \hspace{1cm} (74)$$

$$\omega_{t,0} = \max_{u \in \mathcal{D}_{t-1}} \{w_u\} \rightarrow F_{\omega_{t,0}}(x) = \prod_{k=1}^{p_{t-1}} \left[ 1 - \exp \left( -\frac{x}{\gamma_{h,t}} \right) \right]^{N_t} = \left[ 1 - \exp \left( -\frac{x}{\gamma_{h,t}} \right) \right]^{p_{t-1}N_t}$$  \hspace{1cm} (75)$$

Then, we can achieve the probability that relays are not successful in decoding as in 18. In addition, the probability that $i$th relay in the cluster $t$ where $t > 1$ can decode the received signal correctly is

$$\mu_{t,i} = \sum_{p_{t-1}=1}^{N_{t-1}} \mu_{t-1,p_{t-1}} \omega_{t,i},$$  \hspace{1cm} (76)$$

where $\omega_{t,i}$ is defined as the probability that $i$ relays in cluster $t$ were successful in decoding conditioned upon we have $p_{t-1}$ successful relays in time slot $t-1$. It can be written as

$$\omega_{t,i} = \Pr \left( \max_{u \in \mathcal{D}_{t-1}} \left\{ \max_{j=1,\ldots,N_t} \{x_{u,j}\} \right\} \geq \kappa, \ldots, \max_{k_i=1,\ldots,N_t} \{x_{u^*,k_i} \} \geq \kappa, \max_{k_i=1,\ldots,N_t} \{x_{u^*,k_i} \} \leq \kappa \right).$$  \hspace{1cm} (77)$$

Considering the i.i.d-ness of channels, we simplify the previous equation as

$$\omega_{t,i} = p_{t-1} \prod_{m=0}^{i-1} \left( N_t - m \right) \Pr \left( x_{u^*,1} \geq \kappa, \ldots, x_{u^*,i-1} \geq \kappa, x \leq \kappa | x_{u^*,1} \geq \ldots \geq x_{u^*,i-1} \geq x \right)$$  \hspace{1cm} (78)$$
where $x$ and $y$ and their CDF are derived as

$$x = \max_{k^t=1,\ldots,N_t \atop k^t \neq i-1 \neq \ldots \neq 1} \{x_{u^*k^t}\} \rightarrow F(x) = \left[1 - \exp \left(-\frac{x}{\tilde{\gamma}_{h,t}}\right)\right]^{N_t-i},$$

(79)

$$y = \max_{u \in D_{t-1} \atop u \neq u^*} \left\{\max_{j=1,\ldots,N_t} \{x_{u,j}\}\right\} \rightarrow F(y) = \left[1 - \exp \left(-\frac{y}{\tilde{\gamma}_{h,t}}\right)\right]^{N_t(p_{t-1}-1)},$$

(80)

respectively. Then, we derive the following probability

$$\omega = \Pr \left(x_{u^*,1} \geq \kappa, x_{u^*,2} \geq \kappa, \ldots, x_{u^*,i-1} \geq \kappa, x \leq \kappa \mid x_{u^*,1} \geq \ldots \geq x_{u^*,i-1} \geq x, x_{u^*,1} \geq y\right)$$

$$= \int_\kappa^\infty f(x_{u^*,1}) \int_\kappa^{x_{u^*,1}} f(x_{u^*,2}) \ldots \int_\kappa^{x_{u^*,i-2}} f(x_{u^*,i-1}) F_x(\kappa) F_y(x_{u^*,1}) \, dx_{u^*,i-1} \ldots dx_{u^*,1}$$  

(81)

For calculating $\omega$ we first derive the following part

$$\int_\kappa^{x_{u^*,1}} f(x_{u^*,2}) \ldots \int_\kappa^{x_{u^*,i-2}} f(x_{u^*,i-1}) \, dx_{u^*,i-1} \ldots dx_{u^*,2} = \frac{1}{\Gamma(i)} \left(\exp \left(-\frac{\kappa}{\tilde{\gamma}_{h,t}}\right) - \exp \left(-\frac{x_{u^*,1}}{\tilde{\gamma}_{h,t}}\right)\right)^i$$

(82)

Then,

$$\omega = \int_\kappa^\infty \frac{1}{\Gamma(i)} \left(\exp \left(-\frac{\kappa}{\tilde{\gamma}_{h,t}}\right) - \exp \left(-\frac{x_{u^*,1}}{\tilde{\gamma}_{h,t}}\right)\right)^i \, f(x_{u^*,1}) F_x(\kappa) F_y(x_{u^*,1}) \, dx_{u^*,1}$$

(83)

After some algebraic manipulation and substituting $\omega$ in $\omega_{t,i}, \mu_{t,i}$ in hand, $P_{sec,b}^{SC}$ can be obtained as in (23).

B. SC 3

The PDF of the RVs $\Psi_{E_{t,b}}^{SC}$ derived in (12). By substituting (22) and (12) into (6) and having $\mu_{t,i}$ in hand, $P_{sec,b}^{SC}$ can be obtained as in (23).

C. MRC 4

By plugging (22) and (69) into (6) and having $\mu_{t,i}$ in hand, $P_{sec,b}^{MRC}$ can be obtained as in (24).

APPENDIX C

MAXMIN WITH DECODING SET

For scenario $c$, the relay selection scheme is

$$\tilde{i}_t = \arg\max_{i \in D_t} \left\{\arg\min_{j \in \{1,2,\ldots,N_{t+1}\}} \{C_{i,j}^{DF}\}\right\}.$$  

(84)

Then, the probability that none of the relays can decode the received signal correctly is

$$\mu_{t,0} = \sum_{p_{t-1}=0}^{N_{t-1}} \mu_{t-1,p_{t-1}} \omega_{t,0},$$

(85)
where \( \omega_{t,0} \) is
\[
\omega_{t,0} = \Pr \left( \max_{u \in D_{t-1}} \min_{j=1,\ldots,N_t} \left\{ \frac{P_{t-1}}{\sigma_0^2} |h_{t,u,j}|^2 \right\} \leq \kappa \right). \tag{86}
\]

With change of variables as \( x_{u,j} = \frac{P_{t-1}}{\sigma_0^2} |h_{t,u,j}|^2 \) we can write
\[
\omega_{t,0} = \Pr \left( \max_{u \in D_{t-1}} \min_{j=1,\ldots,N_t} \{ x_{u,j} \} \leq \kappa \right) = \min_{k^1=1,\ldots,N_t} \min_{k^{\bar{j}} \neq j^*} \min_{k^1=N_t-1=1,\ldots,N_t} \min_{k^{\bar{j}} \neq j^*} \{ x_{u^*,k^1} \} \leq \kappa \}
\tag{87}
\]

Since channels are i.i.d., we can simplify the equation as
\[
\omega_{t,0} = p_{t-1}\Gamma (N_t + 1) \Pr \left( x_{u^*,1} \leq \kappa, x_{u^*,2} \leq \kappa, \ldots, x_{u^*,N_t} \leq \kappa | x_{u^*,1} \leq \ldots \leq x_{u^*,N_t}, x_{u^*,1} \geq y \right) \tag{88}
\]

where \( y \), its CDF, and PDF are defined as follows
\[
y = \max_{u \in D_{t-1}} \min_{j=1,\ldots,N_t} \{ x_{u,j} \} \tag{89}
\]
\[
F(y) = \left[ 1 - \exp \left( -\frac{N_t}{\gamma_{h,t}} y \right) \right]^{p_{t-1}-1} \tag{90}
\]
\[
f(y) = \sum_{l=1}^{p_{t-1}-1} (-1)^l N_l \frac{N_l l}{\gamma_{h,t}} \left( \frac{p_{t-1} - 1}{l} \right) \exp \left( -\frac{N_l l}{\gamma_{h,t}} y \right) \tag{91}
\]

Then, we can compute the probability part as
\[
\Pr \left( x_{u^*,1} \leq \gamma, x_{u^*,2} \leq \gamma, \ldots, x_{u^*,N_t} \leq \gamma | x_{u^*,1} \leq \ldots \leq x_{u^*,N_t}, x_{u^*,1} \geq y \right)
= \int_0^\gamma f(y) \int_0^\gamma f(x_{u^*,1}) \int_{x_{u^*,1}}^\gamma f(x_{u^*,2}) \ldots \int_{x_{u^*,N_t-1}}^\gamma f(x_{u^*,N_t}) \, dx_{u^*,N_t} \ldots dx_{u^*,1} \, dy \tag{92}
\]

First, we calculate the following part
\[
\int_y^\kappa f(x_{u^*,1}) \int_{x_{u^*,1}}^\kappa f(x_{u^*,2}) \ldots \int_{x_{u^*,N_t-1}}^\kappa f(x_{u^*,N_t}) \, dx_{u^*,N_t} \ldots dx_{u^*,1} = \frac{\left( \exp \left( -\frac{y}{\gamma_{h,t}} \right) - \exp \left( -\frac{\kappa}{\gamma_{h,t}} \right) \right)^{N_t}}{\Gamma (N_t + 1)} \tag{93}
\]

Then, by having (93), we can write
\[
\omega_{t,0} = p_{t-1}\Gamma (N_t + 1) \int_0^\kappa \left( \frac{\exp \left( -\frac{y}{\gamma_{h,t}} \right) - \exp \left( -\frac{\kappa}{\gamma_{h,t}} \right) }{\Gamma (N_t + 1)} \right)^{N_t} f(y) \, dy \tag{94}
\]

After some algebraic manipulations \( \eta_{t,0} \) can be achieved as in (26). For the case of \( p_{t-1} = 1 \)
we can write
\[
\omega_{t,0} = \Pr\left( \min_{j=1,...,N_t} \{x_{1,j}\} \leq \kappa, \min_{k^i \neq j^*} \{x_{1,k^i}\} \leq \kappa, ..., \min_{k^{N_t-1} \neq j^*} \{x_{1,k^{N_t-1}}\} \leq \kappa \right)
\]
\[
= \Pr\left( \max_{j=1,...,N_t} \{x_{1,j}\} \leq \kappa \right) = \left(1 - \exp\left(-\frac{\kappa}{\bar{\gamma}_{h,t}}\right)\right)^{N_t}. \tag{95}
\]

Also, the probability that \( i \) number of relays can decode the received signal correctly and \( i \in \{1, 2, ..., N_t - 1\} \) is given by
\[
\mu_{t,i} = \sum_{p_{t-1}=1}^{N_t-1} \mu_{t-1,p_{t-1}} \omega_{t,i}, \tag{96}
\]

where \( \omega_{t,i} \) is
\[
\omega_{t,i} = \Pr\left( \max_{u \in \mathcal{D}_{t-1}} \left\{ \min_{j=1,...,N_t} \{x_{u,j}\} \right\} \leq \kappa, ..., \min_{k^{N_t-1} \neq j^*, k^{N_t-2} \neq j^*, ..., k^1 \neq j^*} \{x_{u,k^{N_t-1}}\} \leq \kappa, \min_{k^{N_t-1} \neq j^*, k^{N_t-2} \neq j^*, ..., k^1 \neq j^*} \{x_{u,k^{N_t-2}}\} \geq \kappa \right) \tag{97}
\]

We can simplify the equation as
\[
\omega_{t,i} = p_{t-1} \prod_{m=0}^{N_t-1-m} (N_t - m) \Pr \left( x_{u^*,1} \leq \kappa, ..., x_{u^*,N_t-i-1} \leq \kappa, x \geq \kappa | x_{u^*,1} \leq ... \leq x_{u^*,i-1} \leq x, x_{u^*,1} \geq y \right) \tag{98}
\]

where \( x \) and \( y \) and their CDF and PDF are given by
\[
x = \min_{k^{N_t-1} = 1,...,N_t, k^{N_t-2} \neq j^*, ..., k^1 \neq j^*} \{x_{u^*,k^{N_t-1}}\}
\]
\[
F(x) = 1 - \exp\left(-\frac{i}{\bar{\gamma}_{h,t}}x\right), \tag{99}
\]
\[
y = \max_{u \in \mathcal{D}_{t-1}} \left\{ \min_{j=1,...,N_t} \{x_{u,j}\} \right\}
\]
\[
f(y) = \sum_{l=1}^{p_{t-1}-1} (-1)^{l+1} \frac{N_t}{\bar{\gamma}_{h,t}} \left( p_{t-1} - 1 \right) \exp\left(-\frac{N_t y}{\bar{\gamma}_{h,t}}\right) \tag{100}
\]

Then, we need to derive the following probability:
\[
= \Pr \left( x_{u^*,1} \leq \gamma, x_{u^*,2} \leq \gamma, ..., x_{u^*,i-1} \leq \gamma, x \geq \gamma | x_{u^*,1} \leq ... \leq x_{u^*,i-1} \leq x, x_{u^*,1} \geq y \right)
\]
\[
= \int_0^\gamma f(y) \int_y^\gamma f(x_{u^*,1}) \int_{x_{u^*,1}}^\gamma f(x_{u^*,2}) ... \int_{x_{u^*,N_t-i-2}}^\gamma f(x_{u^*,N_t-i-1}) \left[1 - F(x)\right] dx_{u^*,N_t-i-1} ... dx_{u^*,1} dy \tag{101}
\]
First, we calculate the following part
\[
\int_y^\kappa f(x_u^*,1)\int_{x_u^*,1}^{\kappa} f(x_u^*,2)\ldots\int_{x_u^*,N_t-i-1}^{\kappa} f(x_u^*,N_t-i-1)dx_u^*,N_t-i-1\ldots dx_u^*,1 = \\
\left(\exp\left(-\frac{y}{\gamma_{h,t}}\right) - \exp\left(-\frac{\kappa}{\gamma_{h,t}}\right)\right)^{N_t-i} \\
\frac{\Gamma(N_t - i + 1)}{(N_t - i + 1)}
\]

Then,
\[
\omega_{t,i} = \frac{p_{t-1} \prod_{m=0}^{N_t-i-1} (N_t - m)}{\Gamma(N_t - i + 1)} \int_0^\kappa \left(\exp\left(-\frac{y}{\gamma_{h,t}}\right) - \exp\left(-\frac{\kappa}{\gamma_{h,t}}\right)\right)^{N_t-i} \exp\left(-\frac{i\kappa}{\gamma_{h,t}}\right)f(y) \, dy
\]

After some algebraic manipulations, \(\eta_{t,i}\) in (27) is obtained. For the case of \(p_{t-1} = 1\), following similar steps, we can obtain (26).

The probability that \(N_t\)-th relay can decode the received signal successfully is given by
\[
\mu_{t,N_t} = \sum_{p_{t-1}=1}^{N_t-1} \mu_{t-1,p_{t-1}} \omega_{t,N_t},
\]
where \(\omega_{t,N_t}\) is
\[
\omega_{t,N_t} = \Pr\left(\max_{u \in D_{t-1}} \left\{ \min_{j=1,\ldots,N_t} \{x_{u,j}\}\right\} \geq \kappa\right) = p_{t-1} \times \Pr\left(\min_{j=1,\ldots,N_t} \{x_{u^*,j}\} \geq \gamma \right) \min_{u \neq u^*} \left\{ \min_{j=1,\ldots,N_t} \{x_{u,j}\}\right\}
\]

where \(x\) and \(y\) and their corresponding PDF and CDF are
\[
x = \min_{j=1,\ldots,N_t} \{x_{u^*,j}\} \\
f(x) = \frac{N_t}{\gamma_{h,t}} \exp\left(-\frac{N_t}{\gamma_{h,t}} x\right),
\]
\[
y = \max_{u \in D_{t-1}} \left\{ \min_{j=1,\ldots,N_t} \{x_{u,j}\}\right\}
\]
\[
F(y) = \left[1 - \exp\left(-\frac{N_t}{\gamma_{h,t}} y\right)\right]^{p_{t-1}-1}
\]

After some algebraic manipulations we can obtain \(\mu_{t,N_t}\) as in (28).
APPENDIX D
MINIMUM SELECTION WITH DECODING SET

A. SC 5

For calculating $P_{secd}$, first we should calculate the PDF of $\Psi_{E,t,d}$. With help of the following change of variable $w_{1,j} = \gamma_{E,1,j}$, the CDF of received signal in the first time slot at eavesdropper is

$$F_{w_1}(w) = \left[1 - \exp\left(-\frac{w}{\gamma_{E,1}}\right)\right]^{M_1} = 1 - \sum_{k_1=1}^{M_1} (-1)^{k_1-1} \left(\frac{M_1}{k_1}\right) \exp\left(-\frac{k_1}{\gamma_{E,1}}w\right). \quad (108)$$

where $w_{1,j} = \gamma_{E,1,j} = \frac{P_0}{\sigma_0^2}|f_{E,1,j}|^2$, $w_1 = \max_{j=1,...,M_1} w_{1,j}$, and

$$F_{w_{1,j}}(x) = 1 - \exp\left(-\frac{x}{\gamma_{E,1}}\right) \quad (109)$$

For time slot $t > 1$, the received signal at eavesdropper in time slot $t$ is

$$w_t = \min_{u \in D_{t-1}} \left\{ \max_{j=1,...,M_t} \left\{ \frac{P_{t-1}}{\sigma_0^2} |f_{E,u,j}|^2 \right\} \right\} \quad (110)$$

with change of variable $w_u = \max_{j=1,...,M_t} \left\{ \frac{P_{t-1}}{\sigma_0^2} |f_{E,u,j}|^2 \right\}$ the CDF of $w_u$ is obtained as

$$F_{w_u}(x) = 1 - \sum_{k_t=1}^{M_t} \left(\frac{M_t}{k_t}\right) \exp\left(-\frac{k_t}{\gamma_{E,t}}x\right) \quad (111)$$

Then, the $w_t$ and its CDF can be written as

$$w_t = \min_{u \in D_{t-1}} w_u F_{w_t}(x) = 1 - \prod_{m_t=1}^{p_{t-1}} \left(1 - F_{w_u}(x)\right) = 1 - \sum_{k_{t,1}=1}^{M_t} \sum_{k_{t,p_{t-1}}=1}^{M_t} \prod_{q=1}^{p_{t-1}} (-1)^{k_{t,q}+1} \left(\frac{M_t}{k_{t,q}}\right) \exp\left(-\sum_{q=1}^{p_{t-1}} \frac{k_{t,q}}{\gamma_{E,t}}x\right) \quad (112)$$

respectively, where $p_t$ denotes the number of relays that are successful in decoding the received signal in time slot $t$. Then, the final equation for the received SNR at eavesdropper and its CDF can be written as

$$\Psi_{E,t,d}^{SC} = \max\left\{w_1, \max_{u=2,...,t} \{w_u\}\right\}, \quad (113)$$

$$F_{\Psi_{E,t,d}^{SC}}(x) = F_{w_1}(x) \prod_{u=2}^{t} F_{w_u}(x). \quad (114)$$

With the help of (64) and after some algebraic manipulations, we obtain (33). By substituting (33) and (11) into (6) and having $\xi_{t,i}$ in hand, we can achieve the secrecy outage probability as
in (34).

B. SC 6

To compute $P_{sec,d}^\text{MRC}$, first, we need to calculate the PDF of $\Psi_{E,t,d}^\text{MRC}$. With the following change of variable $w_{1,j} = \frac{\gamma_{E,1,j}}{\gamma_{E,1}} = \frac{P_t}{\sigma_0^2} |f_{E,1,k}|^2$, the PDF and the MGF of the received signal in the first time slot at the eavesdropper can be written as

$$f_{w_{1,j}}(x) = \frac{1}{\bar{\gamma}_{E,1}} \exp \left( -\frac{x}{\bar{\gamma}_{E,1}} \right)$$

$$f_{w_{1,j}}(s) = \frac{1}{\bar{\gamma}_{E,1}} \frac{1}{s + \frac{1}{\bar{\gamma}_{E,1}}}$$  \hspace{1cm} (115)

As we know $w_1 = \sum_{j=1}^{M_t} w_{1,j}$. The PDF of $w_1$ can be obtained as

$$f_{w_1}(s) = \prod_{k_1=1}^{M_t} \left[ \frac{1}{\bar{\gamma}_{E,1}} \frac{1}{s + \frac{1}{\bar{\gamma}_{E,1}}} \right] = \frac{1}{\bar{\gamma}_{E,1}^{M_t}} \left( \frac{1}{s + \frac{1}{\bar{\gamma}_{E,1}}} \right)^{M_t}. \hspace{1cm} (116)$$

And for time slot $t > 1$, the received SNR at the eavesdropper is

$$w_t = \min_{u \in D_{t-1}} \left\{ \sum_{j=1}^{M_t} \frac{P_{t-1}}{\sigma_0^2} |f_{E,u,j}|^2 \right\}$$  \hspace{1cm} (117)

With change of variable $w_u = \sum_{j=1}^{M_t} \frac{P_{t-1}}{\sigma_0^2} |f_{E,u,j}|^2$, the CDF of $w_u$ is obtained as

$$F_{w_u}(x) = 1 - \sum_{k=0}^{M_t-1} \frac{x^k}{\Gamma(k+1) \bar{\gamma}_{E,t}^k} \exp \left( -\frac{x}{\bar{\gamma}_{E,t}} \right) \hspace{1cm} (118)$$

Then the CDF, PDF and MGF of $w_t$ can be written as

$$F_{w_t}(x) = 1 - \prod_{m_t=1}^{p_{t-1}} (1 - F_{w_u}(x))$$ \hspace{1cm} (119)

$$f_{w_t}(x) = \frac{P_{t-1}}{\Gamma(M_t) \bar{\gamma}_{E,t}^{M_t}} x^{M_t-1} \exp \left( -\frac{x}{\bar{\gamma}_{E,t}} \right) \left( \sum_{k=0}^{M_t-1} \frac{x^k}{\Gamma(k+1) \bar{\gamma}_{E,t}^k} \exp \left( -\frac{x}{\bar{\gamma}_{E,t}} \right) \right)$$ \hspace{1cm} (120)

$$f_{w_1}(s) = \sum_{k_t,1=0}^{M_t-1} \cdots \sum_{k_t,p_{t-1}=0}^{M_t-1} \frac{\rho_t \Gamma(\vartheta_t+1)}{s + \frac{p_{t-1}}{\bar{\gamma}_{E,t}})^{\vartheta_t+1}}$$ \hspace{1cm} (121)
where $\rho_t$ and $\vartheta_t$ were defined after equation (38). The final received signal and its PDF at eavesdropper can be written as

$$\Psi_{E,t,d}^{MRC} = w_1 + \sum_{u=2}^{t} w_u$$

(122)

$$F_{\Psi_{E,t,d}^{MRC}}(s) = F_{w_1}(s) \prod_{u=2}^{t} F_{w_u}(s).$$

(123)

Then with the help of the MGF we can obtain the PDF of $f_{\Psi_{E,t,d}^{MRC}}(x)$. Finally, by substituting $f_{\Psi_{E,t,d}^{MRC}}(x)$ and (11) into (6) and having $\xi_{t,i}$ in hand, the equation (39) can be obtained.

REFERENCES

[1] S. Vahidian, E. Soleimani-Nasab, S. Aïssa, and M. Ahmadian-Attari, “Bidirectional AF relaying with underlay spectrum sharing in cognitive radio networks,” IEEE Trans. Veh. Technol., vol. 66, no. 3, pp. 2367–2381, 2017.

[2] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, “Safeguarding 5G wireless communication networks using physical layer security,” IEEE Communications Magazine, vol. 53, no. 4, pp. 20–27, April 2015.

[3] I. Csiszar and J. Korner, “Broadcast channels with confidential messages,” IEEE Transactions on Information Theory, vol. 24, no. 3, pp. 339–348, May 1978.

[4] A. D. Wyner, “The wire-tap channel,” The Bell System Technical Journal, vol. 54, no. 8, pp. 1355–1387, Oct 1975.

[5] 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, 2017.

[6] S. Vahidian, S. Aïssa, and S. Hatamnia, “Relay selection for security-constrained cooperative communication in the presence of eavesdropper’s overhearing and interference,” IEEE Wirel. Commun. Lett., vol. 4, no. 6, pp. 577–580, 2015.

[7] Y. Liang, H. V. Poor, and S. Shamai, “Secure communication over fading channels,” IEEE Transactions on Information Theory, vol. 54, no. 6, pp. 2470–2492, June 2008.

[8] P. K. Gopala, L. Lai, and H. E. Gamal, “On the secrecy capacity of fading channels,” IEEE Transactions on Information Theory, vol. 54, no. 10, pp. 4687–4698, Oct 2008.

[9] H. M. Wang, M. Luo, Q. Yin, and X. G. Xia, “Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks,” IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, pp. 2007–2020, Dec 2013.

[10] X. Wang, K. Wang, and X. D. Zhang, “Secure relay beamforming with imperfect channel side information,” IEEE Transactions on Vehicular Technology, vol. 62, no. 5, pp. 2140–2155, Jun 2013.

[11] H. M. Wang, M. Luo, X. G. Xia, and Q. Yin, “Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper’s CSI,” IEEE Signal Processing Letters, vol. 20, no. 1, pp. 39–42, Jan 2013.

[12] C. Wang, H. M. Wang, and X. G. Xia, “Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks,” IEEE Transactions on Wireless Communications, vol. 14, no. 2, pp. 589–605, Feb 2015.
[13] N. E. Wu and H. J. Li, “Effect of feedback delay on secure cooperative networks with joint relay and jammer selection,” *IEEE Wireless Communications Letters*, vol. 2, no. 4, pp. 415–418, August 2013.

[14] I. Krikidis, J. S. Thompson, and S. Mclaughlin, “Relay selection for secure cooperative networks with jamming,” *IEEE Transactions on Wireless Communications*, vol. 8, no. 10, pp. 5003–5011, October 2009.

[15] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, “Opportunistic relaying for secrecy communications: Cooperative jamming vs. relay chatting,” *IEEE Transactions on Wireless Communications*, vol. 10, no. 6, pp. 1725–1729, June 2011.

[16] Y. Zou, X. Wang, W. Shen, and L. Hanzo, “Security versus reliability analysis of opportunistic relaying,” *IEEE Transactions on Vehicular Technology*, vol. 63, no. 6, pp. 2653–2661, July 2014.

[17] S. Y. N. Y. Y. Feng, Z. Yang and B. Lv, “Physical layer security enhancement in multi-user multi-full-duplex-relay networks,” *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017.

[18] L. Y. J. Chen and M.-S. Alouini, “Physical layer security for cooperative noma systems,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 4645–4649, May 2018.

[19] K. H. P. P. X. Z. Z. G. P. H. Lei, J. Zhang and M. S. Alouini, “Secrecy outage of max–min tas scheme in mimo-noma systems,” *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 6981–6990, Aug 2018.

[20] Y. Zou, B. Champagne, W. P. Zhu, and L. Hanzo, “Relay-selection improves the security-reliability trade-off in cognitive radio systems,” *IEEE Transactions on Communications*, vol. 63, no. 1, pp. 215–228, Jan 2015.

[21] H. Hui, A. L. Swindlehurst, G. Li, and J. Liang, “Secure relay and jammer selection for physical layer security,” *IEEE Signal Processing Letters*, vol. 22, no. 8, pp. 1147–1151, Aug 2015.

[22] S. Hataminia, S. Vahidian, M. Mohammadi, and M. Ahmadian-Attari, “Performance analysis of two-way decode-and-forward relaying in the presence of channel interferences,” *IET Commun.*, vol. 8, no. 18, pp. 3349–3356, 2014.

[23] S. Vahidian, S. Hataminia, and B. Champagne, “On the security analysis of a cooperative incremental relaying protocol in the presence of an active eavesdropper,” *IEEE Access*, vol. 7, pp. 181812–181828, 2019.

[24] Y. Zou, B. Champagne, W. P. Zhu, and L. Hanzo, “Relay-selection improves the security-reliability trade-off in cognitive radio systems,” *IEEE Transactions on Communications*, vol. 63, no. 1, pp. 215–228, Jan 2015.

[25] L. Fan, N. Yang, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, “Exploiting direct links for physical layer security in multiuser multirelay networks,” *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 3856–3867, June 2016.

[26] Y. Ge, S. Wen, Y. Ang, and Y. Liang, “Optimal relay selection in ieee 802.16j multihop relay vehicular networks,” *IEEE Transactions on Vehicular Technology*, vol. 59, no. 5, pp. 2198–2206, Jun 2010.

[27] M. S. Alam, J. W. Mark, and X. Shen, “Relay selection and resource allocation for multi-user cooperative lte-a uplink,” in *2012 IEEE International Conference on Communications (ICC)*, June 2012, pp. 5092–5096.