MITSUBISHI ELECTRIC RESEARCH LABORATORIES
http://www.merl.com

Secrecy Outage Probability of Selective Relaying Wiretap Channels with Collaborative Eavesdropping

Yeoh, P.L.; Yang, N.; Kim, K.J.

TR2015-128 December 2015

Abstract

We analyze the secrecy outage probability of selective relaying wiretap channels with K decode-and-forward (DF) relays and N collaborative eavesdroppers. In the main channel, we consider a two-hop relay network where the best relay is selected to transmit and the relay link is combined with the direct source-to-destination link at the destination. In the eavesdropper channel, we consider that the eavesdroppers can collaborate to exchange the information obtained from the source and relays. Different from previous works, we introduce an eavesdropping probability measure to model different intercepting capabilities of the malicious nodes. For this network, we derive new closed form expressions for the secrecy outage probability in Rayleigh fading channels. The impact of the number of eavesdroppers and the eavesdropping probabilities are accurately reflected in the array gain of the asymptotic secrecy outage probability.

IEEE Global Communications Conference (GLOBECOM)

Secrecy Outage Probability of Selective Relaying Wiretap Channels with Collaborative Eavesdropping

Phee Lep Yeoh*, Nan Yang†, and Kyeong Jin Kim‡
* Department of Electrical and Electronic Engineering, University of Melbourne, Australia
† College of Engineering and Computer Science, Australian National University, Australia
‡ Mitsubishi Electric Research Laboratories, Cambridge, MA, USA
Email: phee.yeoh@unimelb.edu.au, nan.yang@anu.edu.au, kkim@merl.com,

***Abstract*—We analyze the secrecy outage probability of selective relaying wiretap channels with K decode-and-forward (DF) relays and N collaborative eavesdroppers. In the main channel, we consider a two-hop relay network where the best relay is selected to transmit and the relay link is combined with the direct source-to-destination link at the destination. In the eavesdropper channel, we consider that the eavesdroppers can collaborate to exchange the information obtained from the source and relays. Different from previous works, we introduce an eavesdropping probability measure to model different intercepting capabilities of the malicious nodes. For this network, we derive new closed-form expressions for the secrecy outage probability in Rayleigh fading channels. The impact of the number of eavesdroppers and the eavesdropping probabilities are accurately reflected in the array gain of the asymptotic secrecy outage probability.**

I. Introduction

The world of wireless communications has experienced unprecedented growth in recent years, spurred by the popularity of intelligent devices and the exuberant demand for multimedia content [1]. Given the convenience and ubiquity of wireless connections, it is anticipated that large volumes of private and user-sensitive information will be transmitted over the air. Indeed, designing a robust security service will be a top priority in next generation wireless networks.

As a complement to traditional cryptographic techniques, physical layer security has been developed to promote secure data transmission by exploiting channel characteristics of the wireless medium [2, 3]. In seminal studies [4], the wiretap channel was introduced as the fundamental model for physical layer security and the secrecy capacity was defined as the maximum rate at which messages are reliably transmitted to the legitimate receiver without being intercepted by unintended parties. Inspired by these studies, various secure transmission strategies based on multi-input multi-output (MIMO) techniques have been investigated such as beamforming (e.g., [5]), artificial noise (e.g., [6]), and antenna selection (e.g., [7, 8]).

Recently, relay-aided physical layer security has attracted considerable attention as an alternative paradigm to MIMO techniques. Specifically, due to its low complexity nature, the advantages of selective relaying in wiretap channels have been investigated in [9–12]. Considering the network with a single legitimate destination and a single eavesdropper, [9] and [10] evaluated the intercept probability and security-reliability tradeoff, respectively. Considering the network with multiple legitimate destinations and multiple eavesdroppers without a direct link, [11] proposed a number of relay selection criteria and derived the secrecy outage probability. Most recently, [12] characterized the benefits of selective relaying for security improvement in cognitive radio networks. While [9–12] have uncovered key insights into relay selection in wiretap channels, a common assumption in these studies is that the eavesdropper(s) are always listening to the main channel. However, in practical wireless applications with multiple distributed users, the eavesdroppers may not always be perfectly synchronized with the source and/or relays to successfully eavesdrop on their transmissions [13]. Furthermore, when considering collaborative eavesdropping, some communication resources used for information exchange between the eavesdroppers may prevent them from always listening to the main channel.

In this paper, we analyze the secrecy performance of relay selection in K-relay network with N eavesdroppers. In this network, we assume that the eavesdroppers can collaborate to share information obtained from the source and the relay with each other. Importantly, we describe the cost of this collaboration using an eavesdropping probability which is modeled as a Bernoulli random variable. The use of the eavesdropping probability makes this work particularly suitable for the scenario where eavesdroppers do not always overhear the legitimate communication. We assume that relay selection is adopted among K decode-and-forward (DF) relays such that a single relay is selected to retransmit the source signal to the destination. To quantitatively assess the impact of the eavesdropping probability on the secrecy performance, we derive new exact and asymptotic closed-form expressions for the secrecy outage probability in Rayleigh fading channels. Aided by our analysis together with numerical results, an important conclusion is reached that the asymptotic diversity order and array gain increases with the number of relays K. Furthermore, the asymptotic array gain clearly demonstrates the negative impact of increasing number of eavesdroppers N and eavesdropping probabilities on the secrecy outage probability.

II. Protocol Description

We consider a wiretap relay channel, as shown in Fig. 1, where the eavesdropper channel consists of N colluding eavesdroppers, E_n ($n = 1, \ldots, N$), and the main channel consists of a source node, S, a destination node, D, and K decode-and-forward relays, R_k ($k = 1, \ldots, K$).

In the main channel, we assume that there is a direct link between the source and the destination and selection combining (SC) is implemented at the destination to select a single link between the direct link and the K relay links. Selective

relaying can be implemented using a centralized approach where the best relay with the highest end-to-end SNR, $\tilde{R}$, is selected to transmit based on channel state information (CSI) of the main channel [14].

The instantaneous received signal-to-noise ratio (SNR) of the direct $S \rightarrow D$ link is given by

$$\gamma_{SD} = \frac{P}{\mathcal{N}_0}|h_{SD}|^2 \tag{1}$$

where P is the transmit power, $\mathcal{N}_0$ is the variance of the additive white Gaussian noise, and $|h_{SD}|^2$ is the Rayleigh fading channel gain of the direct link. For DF relaying, the instantaneous end-to-end SNR of the $S \rightarrow R_k \rightarrow D$ relay link is given by

$$\gamma_{SR_kD} = \min\left(\gamma_{SR_k}, \gamma_{R_kD}\right), \tag{2}$$

where $\gamma_{SR_k} = \frac{P}{\mathcal{N}_0}|h_{SR_k}|^2$ is the instantaneous SNR of the $S \rightarrow R_k$ link with Rayleigh fading channel gain $|h_{SR_k}|^2$, and $\gamma_{R_kD} = \frac{P}{\mathcal{N}_0}|h_{SR_k}|^2$ is the instantaneous SNR of the $R_k \rightarrow D$ link with Rayleigh fading channel gain $|h_{R_kD}|^2$.

Based on (1) and (2), the instantaneous received SNR with SC at the destination is given by

$$\gamma_D = \max(\gamma_{SD}, \gamma_{SR_1D}, \ldots, \gamma_{SR_KD}). \tag{3}$$

The corresponding achievable rate of the main channel can be written as

$$\mathcal{C}_D = \log_2\left(1 + \gamma_D\right). \tag{4}$$

In the eavesdropper channel, we consider that the eavesdroppers attempt to eavesdrop on both the source and relay transmissions. We assume that the eavesdroppers collaborate to maximize the total received SNR by applying maximum-ratio combining (MRC) across all the received signals from the source S and the best relay $\tilde{R}$. Furthermore, we assign eavesdropping probabilities to each eavesdropper to model the probability of successfully obtaining information from the source or relay links. These probabilities apply to collaborative eavesdroppers where constraints on signalling synchronization, transmission bandwidth, and channel capacity of the eavesdropper links may prevent them from always listening to the main channel.

The instantaneous received SNR of the $S \rightarrow E_n$ link is defined as

$$\gamma_{SE_n} = I_n \times \frac{P}{\mathcal{N}_0}|h_{SE_n}|^2, \tag{5}$$

where $|h_{SE_n}|^2$ is the Rayleigh fading channel gain of the $S \rightarrow E_n$ link, and I_n is a Bernoulli random variable representing the probability p_n that the eavesdropper is listening in the same time interval as the source transmission, i.e., $\Pr(I_n = 1) = p_n$ and $\Pr(I_n = 0) = 1 - p_n$ with $0 \leq p_n \leq 1$. Similarly, the instantaneous received SNR of the $\tilde{R} \rightarrow E_n$ link is given by

$$\gamma_{\tilde{R}E_n} = I_n \times \frac{P}{\mathcal{N}}|h_{\tilde{R}E_n}|^2, \tag{6}$$

where $|h_{\tilde{R}E}|^2$ is the Rayleigh fading channel gain of the $\tilde{R} \rightarrow E_n$ link and I_n is a Bernoulli random variable representing the probability p_n that the eavesdropper is listening in the same time interval as the relay transmission.

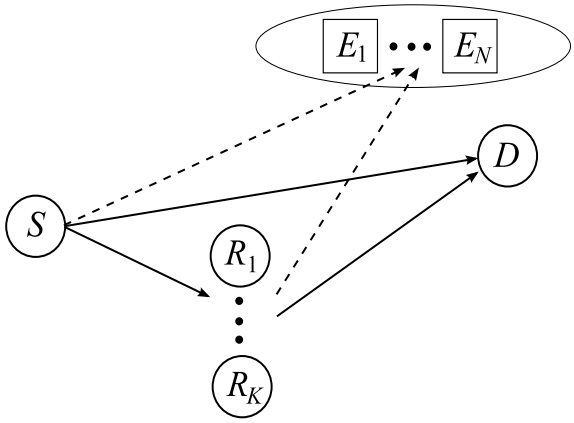

Fig. 1. A cooperative wiretap channel with selective decode-and-forward relaying in the presence of N collaborative eavesdroppers.

Based on (5) and (6), the instantaneous received SNR with MRC across all N eavesdroppers is given by

$$\gamma_E = \sum_{n=1}^{N}(\gamma_{SE_n} + \gamma_{\tilde{R}E_n}). \tag{7}$$

The corresponding achievable rate of the eavesdropper channel is given by

$$\mathcal{C}_E = \log_2\left(1 + \gamma_E\right). \tag{8}$$

The achievable secrecy rate, $\mathcal{C}$, is the difference between the achievable rate of the main channel and the eavesdropper channel, which is given by [14]

$$\mathcal{C} \triangleq \left[\log_2\left(\frac{1+\gamma_D}{1+\gamma_E}\right)\right]^+, \tag{9}$$

where

$$[x]^+ = \max(x, 0) = \begin{cases} x, & x \geq 0 \\ 0 & x < 0. \end{cases} \tag{10}$$

Based on (9), the secrecy outage probability is defined as the probability that the achievable secrecy rate falls below a specified target rate. Accordingly, the secrecy outage probability can be written as

$$\Pr(\mathcal{C} < R) = \Pr\left(\frac{1+\gamma_D}{1+\gamma_E} < 2^R\right), \tag{11}$$

where R is the target secrecy rate. We note that the secrecy outage probability applies to the passive eavesdropping scenario where the source and relays do not know the CSI of the eavesdropper channel.

III. Statistical Distributions for Selective Relaying Wiretap Channels

In this section, we present the statistical distributions of γ_D and γ_E for Rayleigh fading channels which will be used in the derivation of the secrecy outage probability in Section IV. We first present the cumulative distribution function (CDF) and probability density function (PDF) of γ_D based on [15]. Next, we derive new closed-form expressions for the moment generating function (MGF) of γ_E from which the corresponding PDF and CDF are derived.

In the main channel, the CDF of γ_D is given by [15]

$$F_{\gamma_D}(\gamma) = F_{\gamma_{SD}} \prod_{k=1}^{K} F_{\gamma_{SR_kD}}$$
$$= 1 - e^{-\frac{\gamma}{\overline{\gamma}_{SD}}} + \widetilde{\sum}(-1)^k e^{-\gamma\left(\sum_{j=1}^{k}\left(\frac{1}{\overline{\gamma}_{SR_{\ell_j}}}+\frac{1}{\overline{\gamma}_{R_{\ell_j}D}}\right)\right)}$$
$$- \widetilde{\sum}(-1)^k e^{-\gamma\left(\frac{1}{\overline{\gamma}_{SD}}+\sum_{j=1}^{k}\left(\frac{1}{\overline{\gamma}_{SR_{\ell_j}}}+\frac{1}{\overline{\gamma}_{R_{\ell_j}D}}\right)\right)}, \quad (12)$$

where $F_{\gamma_{SD}}(\gamma)$ is the CDF of γ_{SD} given by

$$F_{\gamma_{SD}}(\gamma) = 1 - e^{-\frac{\gamma}{\overline{\gamma}_{SD}}}, \quad (13)$$

and $F_{\gamma_{SR_kD}}(\gamma)$ is the CDF of γ_{SR_kD} given by

$$F_{\gamma_{SR_kD}}(\gamma) = 1 - e^{-\gamma\left(\frac{1}{\overline{\gamma}_{SR_k}}+\frac{1}{\overline{\gamma}_{R_kD}}\right)}. \quad (14)$$

In (12), the average received SNRs are defined as $\overline{\gamma}_{SD} = \mathbb{E}[\gamma_{SD}]$, $\overline{\gamma}_{SR_k} = \mathbb{E}[\gamma_{SR_k}]$, $\overline{\gamma}_{R_kD} = \mathbb{E}[\gamma_{R_kD}]$, where $\mathbb{E}[\cdot]$ denotes the expectation, and the summation over all combinations of the relay links is

$$\widetilde{\sum} = \sum_{k=1}^{K}\sum_{\ell_1=1}^{K-k+1}\sum_{\ell_2=\ell_1+1}^{K-k+2}\cdots\sum_{\ell_k=\ell_{k-1}+1}^{K}. \quad (15)$$

Based on (12), the PDF of γ_D can be derived as

$$f_{\gamma_D}(\gamma) = \frac{1}{\overline{\gamma}_{SD}}e^{-\frac{\gamma}{\overline{\gamma}_{SD}}} - \widetilde{\sum}(-1)^k \sum_{j=1}^{k}\left(\frac{1}{\overline{\gamma}_{SR_{\ell_j}}}+\frac{1}{\overline{\gamma}_{R_{\ell_j}D}}\right)$$
$$\times e^{-\gamma\sum_{j=1}^{k}\left(\frac{1}{\overline{\gamma}_{SR_{\ell_j}}}+\frac{1}{\overline{\gamma}_{R_{\ell_j}D}}\right)}$$
$$+ \widetilde{\sum}(-1)^k \left(\frac{1}{\overline{\gamma}_{SD}}+\sum_{j=1}^{k}\left(\frac{1}{\overline{\gamma}_{SR_{\ell_j}}}+\frac{1}{\overline{\gamma}_{R_{\ell_j}D}}\right)\right)$$
$$\times e^{-\gamma\left(\frac{1}{\overline{\gamma}_{SD}}+\sum_{j=1}^{k}\left(\frac{1}{\overline{\gamma}_{SR_{\ell_j}}}+\frac{1}{\overline{\gamma}_{R_{\ell_j}D}}\right)\right)}. \quad (16)$$

In the eavesdropper channel, the MGF of γ_E is

$$M_{\gamma_E}(s) = \prod_{n=1}^{N} M_{\gamma_{SE_n}}(s) M_{\gamma_{\tilde{R}E_n}}(s), \quad (17)$$

where $M_{\gamma_{SE_n}}(s)$ is the MGF of γ_{SE_n} and $M_{\gamma_{\tilde{R}E_n}}(s)$ is the MGF of $\gamma_{\tilde{R}E_n}$. We derive MGFs of γ_{SE_n} and $\gamma_{\tilde{R}E_n}$ based on their respective PDFs given by [16]

$$f_{\gamma_{SE_n}}(\gamma) = (1-p_n)\delta(\gamma) + \frac{p_n}{\overline{\gamma}_{SE_n}}e^{-\frac{\gamma}{\overline{\gamma}_{SE_n}}}u(\gamma), \quad (18)$$

and

$$f_{\gamma_{\tilde{R}E_n}}(\gamma) = (1-p_n)\delta(\gamma) + \frac{p_n}{\overline{\gamma}_{\tilde{R}E_n}}e^{-\frac{\gamma}{\overline{\gamma}_{\tilde{R}E_n}}}u(\gamma), \quad (19)$$

where p_n is the eavesdropping probability of the nth eavesdropper, $\delta(\gamma)$ is the delta function, $u(\gamma)$ is the unit step function, and $\overline{\gamma}_{SE_n} = \mathbb{E}[\gamma_{SE_n}]$, $\overline{\gamma}_{\tilde{R}E_n} = \mathbb{E}[\gamma_{\tilde{R}E_n}]$ are the average received SNRs. The corresponding MGFs are given by

$$M_{\gamma_{SE_n}}(s) = \int_0^\infty e^{s\gamma} f_{\gamma_{SE_n}}(\gamma)d\gamma = 1 - p_n + \frac{p_n}{1-s\overline{\gamma}_{SE_n}}, \quad (20)$$

and

$$M_{\gamma_{\tilde{R}E_n}}(s) = \int_0^\infty e^{s\gamma} f_{\gamma_{\tilde{R}E_n}}(\gamma)d\gamma = 1 - p_n + \frac{p_n}{1-s\overline{\gamma}_{\tilde{R}E_n}}. \quad (21)$$

We proceed to expand the MGF of γ_E using partial fraction decomposition which results in

$$M_{\gamma_E}(s) = \prod_{n=1}^{N}(1-p_n+\frac{p_n}{1-s\overline{\gamma}_{SE_n}})(1-p_n+\frac{p_n}{1-s\overline{\gamma}_{\tilde{R}E_n}})$$
$$= \prod_{n=1}^{N}\frac{(1-s\overline{\gamma}_{SE_n}(1-p_n))(1-s\overline{\gamma}_{\tilde{R}E_n}(1-p_n))}{(1-s\overline{\gamma}_{SE_n})(1-s\overline{\gamma}_{\tilde{R}E_n})}$$
$$= \prod_{n=1}^{N}(1-p_n)^2 + \sum_{n=1}^{N}\left(\frac{\epsilon_{p_n}}{1-s\overline{\gamma}_{SE_n}} + \frac{\varepsilon_{p_n}}{1-s\overline{\gamma}_{\tilde{R}E_n}}\right), \quad (22)$$

where we define the variables

$$\epsilon_{p_n} = p_n \prod_{i=1}^{N}\frac{\overline{\gamma}_{SE_n}-(1-p_i)\overline{\gamma}_{\tilde{R}E_i}}{\overline{\gamma}_{SE_n}-\overline{\gamma}_{\tilde{R}E_i}}\prod_{\substack{i=1\\i\neq n}}^{N}\frac{\overline{\gamma}_{SE_n}-(1-p_i)\overline{\gamma}_{SE_i}}{\overline{\gamma}_{SE_n}-\overline{\gamma}_{SE_i}}, \quad (23)$$

and

$$\varepsilon_{p_n} = p_n \prod_{i=1}^{N}\frac{\overline{\gamma}_{\tilde{R}E_n}-(1-p_i)\overline{\gamma}_{SE_i}}{\overline{\gamma}_{\tilde{R}E_n}-\overline{\gamma}_{SE_i}}\prod_{\substack{i=1\\i\neq n}}^{N}\frac{\overline{\gamma}_{\tilde{R}E_n}-(1-p_i)\overline{\gamma}_{\tilde{R}E_i}}{\overline{\gamma}_{\tilde{R}E_n}-\overline{\gamma}_{\tilde{R}E_i}}. \quad (24)$$

The pdf of γ_E can be derived by taking the inverse Laplace transform of (22) which results in

$$f_{\gamma_E}(\gamma) = \delta(\gamma)\prod_{n=1}^{N}(1-p_n)^2$$
$$+ \sum_{n=1}^{N}\left(\frac{\epsilon_{p_n}}{\overline{\gamma}_{SE_n}}e^{-\frac{\gamma}{\overline{\gamma}_{SE_n}}} + \frac{\varepsilon_{p_n}}{\overline{\gamma}_{\tilde{R}E_n}}e^{-\frac{\gamma}{\overline{\gamma}_{\tilde{R}E_n}}}\right)u(\gamma), \quad (25)$$

and the corresponding CDF is calculated as

$$F_{\gamma_E}(\gamma) = \int_0^\gamma f_{\gamma_E}(x)dx = \prod_{n=1}^{N}(1-p_n)^2$$
$$+ \sum_{n=1}^{N}\left(\epsilon_{p_n}\left(1-e^{-\frac{\gamma}{\overline{\gamma}_{SE_n}}}\right) + \varepsilon_{p_n}\left(1-e^{-\frac{\gamma}{\overline{\gamma}_{\tilde{R}E_n}}}\right)\right). \quad (26)$$

We note that our statistical expressions for γ_D and γ_E are given in simple closed-form which is advantageous in deriving a range of performance measures for selective relaying wiretap channels.

IV. Secrecy Outage Probability

In this section, we derive new closed-form expressions for the secrecy outage probability of selective relaying wiretap channels. We derive the exact secrecy outage probability which characterizes the impacts of the number of relays K, the number of eavesdroppers N, and the eavesdropping probabilities p_n. Our exact expression is further analyzed in the high SNR regime to explicitly identify the impacts of K, N, and p_n on the secrecy outage probability.

A. Exact Secrecy Outage Probability

Based on (11), the secrecy outage probability can be further evaluated as

$$\begin{aligned}\Pr(\mathcal{C}<R) &= \Pr(\mathcal{C}<R|\gamma_E\geq\gamma_D)\Pr(\gamma_E\geq\gamma_D)\\ &\quad+\Pr(\mathcal{C}<R|\gamma_E<\gamma_D)\Pr(\gamma_E<\gamma_D)\\ &=\int_0^\infty F_{\gamma_D}(2^R(1+\gamma_E)-1)f_{\gamma_E}(\gamma_E)d\gamma_E. \quad (27)\end{aligned}$$

Substituting the CDF of γ_D in (12) and the PDF of γ_E in (25) into (27), the secrecy outage probability is derived as

$$\Pr(\mathcal{C}<R)=\mathcal{I}_1+\mathcal{I}_2-\mathcal{I}_3, \quad (28)$$

where the first term in (28) is solved as

$$\begin{aligned}\mathcal{I}_1 &= \int_0^\infty\left(1-e^{-\frac{(2^R-1)}{\overline{\gamma}_{SD}}}e^{-\gamma_E\frac{2^R}{\overline{\gamma}_{SD}}}\right)\times\left(\delta(\gamma_E)\prod_{n=1}^{N}(1-p_n)^2\right.\\ &\left.+\sum_{n=1}^{N}\left(\frac{\epsilon_{p_n}}{\overline{\gamma}_{SE_n}}e^{-\frac{\gamma_E}{\overline{\gamma}_{SE_n}}}+\frac{\varepsilon_{p_n}}{\overline{\gamma}_{\tilde{R}E_n}}e^{-\frac{\gamma_E}{\overline{\gamma}_{\tilde{R}E_n}}}\right)u(\gamma_E)\right)d\gamma_E\\ &=1-e^{-\frac{(2^R-1)}{\overline{\gamma}_{SD}}}\prod_{n=1}^{N}(1-p_n)^2\\ &-\sum_{n=1}^{N}\left(\frac{\epsilon_{p_n}e^{-\frac{(2^R-1)}{\overline{\gamma}_{SD}}}}{\left(1+\frac{2^R\overline{\gamma}_{SE_n}}{\overline{\gamma}_{SD}}\right)}+\frac{\varepsilon_{p_n}e^{-\frac{(2^R-1)}{\overline{\gamma}_{SD}}}}{\left(1+\frac{2^R\overline{\gamma}_{\tilde{R}E_n}}{\overline{\gamma}_{SD}}\right)}\right)u(\gamma_E), \quad (29)\end{aligned}$$

by utilizing the identity of

$$\int_0^\infty e^{-x\frac{2^R}{\overline{\gamma}_{SD}}}e^{-\frac{x}{\overline{\gamma}_{SE_n}}}dx=\frac{\overline{\gamma}_{SE_n}}{1+\frac{2^R\overline{\gamma}_{SE_n}}{\overline{\gamma}_{SD}}}. \quad (30)$$

Similarly, we can derive the second term in (28) as

$$\begin{aligned}\mathcal{I}_2 &= \int_0^\infty\left(\widetilde{\sum}(-1)^k e^{-\sum_{j=1}^{k}\left(\frac{2^R-1}{\overline{\gamma}_{SR_{\ell_j}}}+\frac{2^R-1}{\overline{\gamma}_{R_{\ell_j}D}}\right)}\right.\\ &\left.e^{-\gamma_E\left(\sum_{j=1}^{k}\left(\frac{2^R}{\overline{\gamma}_{SR_{\ell_j}}}+\frac{2^R}{\overline{\gamma}_{R_{\ell_j}D}}\right)\right)}\right)\times\left(\delta(\gamma_E)\prod_{n=1}^{N}(1-p_n)^2\right.\\ &\left.+\sum_{n=1}^{N}\left(\frac{\epsilon_{p_n}}{\overline{\gamma}_{SE_n}}e^{-\frac{\gamma_E}{\overline{\gamma}_{SE_n}}}+\frac{\varepsilon_{p_n}}{\overline{\gamma}_{\tilde{R}E_n}}e^{-\frac{\gamma_E}{\overline{\gamma}_{\tilde{R}E_n}}}\right)u(\gamma_E)\right)d\gamma_E\\ &=\prod_{n=1}^{N}(1-p_n)^2\widetilde{\sum}(-1)^k e^{-\sum_{j=1}^{k}\left(\frac{2^R-1}{\overline{\gamma}_{SR_{\ell_j}}}+\frac{2^R-1}{\overline{\gamma}_{R_{\ell_j}D}}\right)}\\ &+\widetilde{\sum}(-1)^k\sum_{n=1}^{N}\left(\frac{\epsilon_{p_n}e^{-\sum_{j=1}^{k}\left(\frac{2^R-1}{\overline{\gamma}_{SR_{\ell_j}}}+\frac{2^R-1}{\overline{\gamma}_{R_{\ell_j}D}}\right)}}{\left(1+\sum_{j=1}^{k}\left(\frac{2^R\overline{\gamma}_{SE_n}}{\overline{\gamma}_{SR_{\ell_j}}}+\frac{2^R\overline{\gamma}_{SE_n}}{\overline{\gamma}_{R_{\ell_j}D}}\right)\right)}\right.\\ &\left.+\frac{\varepsilon_{p_n}e^{-\sum_{j=1}^{k}\left(\frac{2^R-1}{\overline{\gamma}_{SR_{\ell_j}}}+\frac{2^R-1}{\overline{\gamma}_{R_{\ell_j}D}}\right)}}{\left(1+\sum_{j=1}^{k}\left(\frac{2^R\overline{\gamma}_{\tilde{R}E_n}}{\overline{\gamma}_{SR_{\ell_j}}}+\frac{2^R\overline{\gamma}_{\tilde{R}E_n}}{\overline{\gamma}_{R_{\ell_j}D}}\right)\right)}\right) \quad (31)\end{aligned}$$

and the third term is given by

$$\begin{aligned}\mathcal{I}_3 &= \prod_{n=1}^{N}(1-p_n)^2\widetilde{\sum}(-1)^k e^{-\left(\frac{2^R-1}{\overline{\gamma}_{SD}}+\sum_{j=1}^{k}\left(\frac{2^R-1}{\overline{\gamma}_{SR_{\ell_j}}}+\frac{2^R-1}{\overline{\gamma}_{R_{\ell_j}D}}\right)\right)}\\ &+\widetilde{\sum}\sum_{n=1}^{N}\left(\frac{(-1)^k\epsilon_{p_n}e^{-\left(\frac{2^R-1}{\overline{\gamma}_{SD}}+\sum_{j=1}^{k}\left(\frac{2^R-1}{\overline{\gamma}_{SR_{\ell_j}}}+\frac{2^R-1}{\overline{\gamma}_{R_{\ell_j}D}}\right)\right)}}{\left(1+\frac{2^R\overline{\gamma}_{SE_n}}{\overline{\gamma}_{SD}}+\sum_{j=1}^{k}\left(\frac{2^R\overline{\gamma}_{SE_n}}{\overline{\gamma}_{SR_{\ell_j}}}+\frac{2^R\overline{\gamma}_{SE_n}}{\overline{\gamma}_{R_{\ell_j}D}}\right)\right)}\right.\\ &\left.+\frac{(-1)^k\varepsilon_{p_n}e^{-\left(\frac{2^R-1}{\overline{\gamma}_{SD}}+\sum_{j=1}^{k}\left(\frac{2^R-1}{\overline{\gamma}_{SR_{\ell_j}}}+\frac{2^R-1}{\overline{\gamma}_{R_{\ell_j}D}}\right)\right)}}{\left(1+\frac{2^R\overline{\gamma}_{\tilde{R}E_n}}{\overline{\gamma}_{SD}}+\sum_{j=1}^{k}\left(\frac{2^R\overline{\gamma}_{\tilde{R}E_n}}{\overline{\gamma}_{SR_{\ell_j}}}+\frac{2^R\overline{\gamma}_{\tilde{R}E_n}}{\overline{\gamma}_{R_{\ell_j}D}}\right)\right)}\right) \quad (32)\end{aligned}$$

We note that the per-hop SNRs in (31) and (32) can be re-expressed in terms of the direct link SNR as $\overline{\gamma}_{SR_{\ell_j}}=\kappa_{SR_{\ell_j}}\overline{\gamma}_{SD}$, $\overline{\gamma}_{R_{\ell_j}D}=\kappa_{R_{\ell_j}D}\overline{\gamma}_{SD}$, where $\kappa_{SR_{\ell_j}},\kappa_{R_{\ell_j}D}\in\mathbb{R}^+$. As such, we present our new closed-form expression for the exact secrecy outage probability in (33) where $\Sigma_k=\sum_{j=1}^{k}(\frac{1}{\kappa_{SR_{\ell_j}}}+\frac{1}{\kappa_{R_{\ell_j}D}})$. The exact expression in (33) is easy to evaluate since it contains finite sums of simple expressions and accurately provides the secrecy outage probability across the whole SNR range.

B. Asymptotic Secrecy Outage Probability

Next, we proceed to derive the asymptotic secrecy outage probability by evaluating the first order Taylor series expansion of (33) as $\overline{\gamma}_{SD}\to\infty$. We note that our asymptotic results can be re-expressed as [15]

$$\Pr(\mathcal{C}<R)\overset{\overline{\gamma}_{SD}\to\infty}{\approx}(\mathcal{G}_a\overline{\gamma}_{SD})^{-\mathcal{G}_d} \quad (34)$$

to clearly identify the diversity order $\mathcal{G}_d$ which represents the slope of the asymptotic curve, and the array gain $\mathcal{G}_a$ which represents the shift of the asymptotic curve from the reference curve of $\overline{\gamma}_{SD}^{-\mathcal{G}_d}$.

For the special case of $K=1$ and general N, the asymptotic secrecy outage probability is derived as

$$\begin{aligned}\Pr(\mathcal{C}<R)&\overset{\overline{\gamma}_{SD}\to\infty}{\approx}\frac{(2^R-1)^2}{\overline{\gamma}_{SD}^2}\left(\frac{1}{\kappa_{SR_1}}+\frac{1}{\kappa_{R_1D}}\right)\\ &\times\left[1+\frac{2.2^R}{(2^R-1)}\sum_{n=1}^{N}\left(\epsilon_{p_n}\overline{\gamma}_{SE_n}+\varepsilon_{p_n}\overline{\gamma}_{\tilde{R}E_n}\right)\right.\\ &\left.+\frac{2.2^{2R}}{(2^R-1)^2}\sum_{n=1}^{N}\left(\epsilon_{p_n}\overline{\gamma}_{SE_n}^2+\varepsilon_{p_n}\overline{\gamma}_{\tilde{R}E_n}^2\right)\right] \quad (35)\end{aligned}$$

From (35), we observe that the diversity order reflected in the negative power of $\overline{\gamma}_{SD}$ is a constant value of 2. This indicates that the diversity order is independent of the number of eavesdroppers N and the eavesdropping probabilities p_n. Our result in (35) also clearly identifies that, for a fixed diversity order, the array gain decreases with increasing N and p_n. This is expected given that the secrecy outage probability worsens as the number of collaborative eavesdroppers increases and the probability of successful eavesdropping increases.

$$\Pr(\mathcal{C}<R)=1-e^{-\frac{(2^R-1)}{\overline{\gamma}_{SD}}}\left(\prod_{n=1}^{N}(1-p_n)^2+\sum_{n=1}^{N}\left(\frac{\epsilon_{p_n}}{\left(1+\frac{2^R\overline{\gamma}_{SE_n}}{\overline{\gamma}_{SD}}\right)}+\frac{\varepsilon_{p_n}}{\left(1+\frac{2^R\overline{\gamma}_{\tilde{R}E_n}}{\overline{\gamma}_{SD}}\right)}\right)u(\gamma_E)\right)$$
$$+\widetilde{\sum}(-1)^k e^{-\frac{(2^R-1)\Sigma_\kappa}{\overline{\gamma}_{SD}}}\left(\prod_{n=1}^{N}(1-p_n)^2+\sum_{n=1}^{N}\left(\frac{\epsilon_{p_n}}{\left(1+\frac{2^R\overline{\gamma}_{SE_n}\Sigma_\kappa}{\overline{\gamma}_{SD}}\right)}+\frac{\varepsilon_{p_n}}{\left(1+\frac{2^R\overline{\gamma}_{\tilde{R}E_n}\Sigma_\kappa}{\overline{\gamma}_{SD}}\right)}\right)u(\gamma_E)\right)$$
$$-\widetilde{\sum}(-1)^k e^{-\frac{(2^R-1)(1+\Sigma_\kappa)}{\overline{\gamma}_{SD}}}\left(\prod_{n=1}^{N}(1-p_n)^2+\sum_{n=1}^{N}\left(\frac{\epsilon_{p_n}}{\left(1+\frac{2^R\overline{\gamma}_{SE_n}(1+\Sigma_\kappa)}{\overline{\gamma}_{SD}}\right)}+\frac{\varepsilon_{p_n}}{\left(1+\frac{2^R\overline{\gamma}_{\tilde{R}E_n}(1+\Sigma_\kappa)}{\overline{\gamma}_{SD}}\right)}\right)u(\gamma_E)\right) \quad (33)$$

For the special case of general K and $N=1$, the asymptotic secrecy outage probability is derived as

$$\Pr(\mathcal{C}<R)\overset{\overline{\gamma}_{SD}\to\infty}{\approx}\frac{(2^R-1)^{K+1}}{\overline{\gamma}_{SD}^{K+1}}\prod_{k=1}^{K}\left(\frac{1}{\kappa_{SR_k}}+\frac{1}{\kappa_{R_kD}}\right)$$
$$\times\left[1+\sum_{k=1}^{K+1}\frac{2^{kR}(K+1)!}{(2^R-1)^k(K+1-k)!}\right.$$
$$\times\left(\frac{p_1(\overline{\gamma}_{SE_1}-(1-p_1)\overline{\gamma}_{\tilde{R}E_1})\overline{\gamma}_{SE_1}^k}{\overline{\gamma}_{SE_1}-\overline{\gamma}_{\tilde{R}E_1}}\right.$$
$$\left.\left.+\frac{p_1(\overline{\gamma}_{\tilde{R}E_1}-(1-p_1)\overline{\gamma}_{SE_1})\overline{\gamma}_{\tilde{R}E_1}^k}{\overline{\gamma}_{\tilde{R}E_1}-\overline{\gamma}_{SE_1}}\right)\right] \quad (36)$$

From (36), we can see that the diversity order increases with of the number of relays K. This means that the secrecy outage probability decays more rapidly as K increases which highlights the significant security advantage of selective relaying in wiretap channels.

Finally, for general K and N, we derive the asymptotic secrecy outage probability given in (37). From (37), we can conclude that the diversity order is in fact $\mathcal{G}_d = K+1$ which increases with K and is independent of N and p_n. For a fixed diversity order, we also confirm that the array gain decreases with increasing N and p_n. Our asymptotic result in (37) accurately characterizes the relative contributions of K, N, and p_n in the diversity order and array gain.

V. Numerical Results

In this section, we present illustrative examples to highlight the impact of the numbers of relays, number of eavesdroppers, and eavesdropper probability on the secrecy outage probability of selective relaying wiretap channels. We plot the exact secrecy outage probability derived in (33), the asymptotic secrecy outage probability derived in (37), and the simulation points using Monte Carlo simulation. We note that our analytical closed-form expressions accurately predict the simulation points in all the examples. In the main channel, we set the target secrecy rate to $R=5$ dB and randomly vary the relay link SNRs as $\overline{\gamma}_{SR_k}=\kappa_{SR_k}\overline{\gamma}_{SD}$, and $\overline{\gamma}_{R_kD}=\kappa_{R_kD}\overline{\gamma}_{SD}$, where $\overline{\gamma}_{SD}$ is the direct link SNR. In the eavesdropper channel, we also randomly vary the eavesdropper link SNRs as $\overline{\gamma}_{SE_n}=\kappa_{SE_n}\overline{\gamma}_E$, and $\overline{\gamma}_{\tilde{R}E_n}=\kappa_{\tilde{R}E_n}\overline{\gamma}_E$, where $\overline{\gamma}_E=3$ dB.

In Fig. 2, we plot the secrecy outage probability versus $\overline{\gamma}_{SD}$ for $K=1$ relay and $N=1,2,3$ eavesdroppers. In the main channel, we set $\{\kappa_{SR},\kappa_{RD}\}=\{1.5,1.3\}$ to model the common scenario where the relay links are stronger than the direct link. In the eavesdropper channel, we set the eavesdropping probabilities to $p_1=0.1$, $p_2=0.3$, and $p_3=0.5$ which models the scenario where the probability of successful eavesdropping increases from $N=1$ to 3. The eavesdropper link SNRs are varied randomly as $\{\kappa_{SE_1},\kappa_{\tilde{R}E_1},\kappa_{SE_2},\kappa_{\tilde{R}E_2},\kappa_{SE_3},\kappa_{\tilde{R}E_3}\}=\{0.1,0.3,1.8,1.3,0.6,0.5\}$. We observe in the plot that the asymptotic diversity order remains unchanged with increasing N. We also note that the asymptotic array gain decreases with increasing N as predicted in (35).

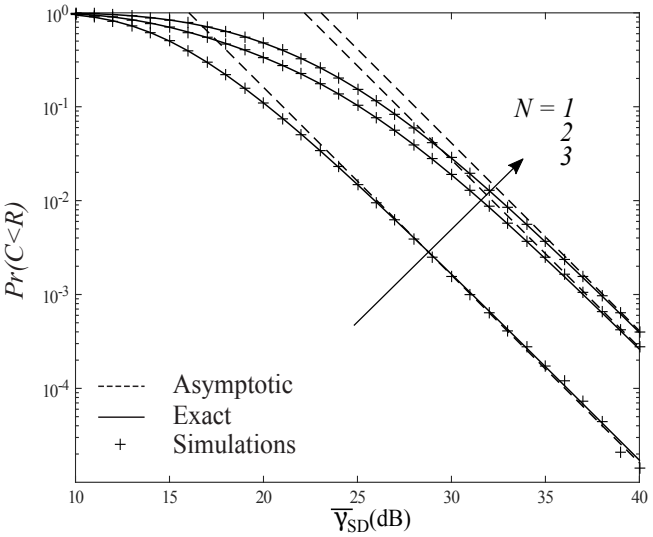

Fig. 2. Secrecy outage probability for $K=1$, $N=1$, 2, 3, and $\{p_1,p_2,p_3\}=\{0.1,0.3,0.5\}$.

In Fig. 3, we plot the secrecy outage probability versus $\overline{\gamma}_{SD}$ for $N=1$ eavesdropper and $K=1,2,3$ relays. In the main channel, the relay link SNRs are varied randomly as $\{\kappa_{SR_1},\kappa_{R_1D},\kappa_{SR_2},\kappa_{R_2D},\kappa_{SR_3},\kappa_{R_3D}\}=\{1.5,1.3,1.8,1.5,2.6,2.5\}$. In the eavesdropper channel, we set $p_1=0.1$ and $\{\kappa_{SE_1},\kappa_{\tilde{R}E_1}\}=\{0.1,0.3\}$. The plot clearly shows that the asymptotic diversity order increases with increasing K as predicted in (36).

In Fig. 4, we plot the secrecy outage probability versus $\overline{\gamma}_{SD}$ for $N=2$ eavesdroppers, $K=2$ relays, and eavesdropper probabilities $\{p_1,p_2\}=\{0,0\},\{0.1,0.3\},\{1,1\}$. The relay and eavesdropper link SNRs are random varied as $\{\kappa_{SR_1},\kappa_{R_1D},\kappa_{SR_2},\kappa_{R_2D}\}=\{1.5,1.3,1.8,1.5\}$ and

$$\Pr(\mathcal{C} < R) \overset{\overline{\gamma}_{SD}\to\infty}{\approx} \frac{(2^R-1)^{K+1}}{\overline{\gamma}_{SD}^{K+1}} \prod_{k=1}^{K} \left(\frac{1}{\kappa_{SR_k}} + \frac{1}{\kappa_{R_k D}} \right) \left[1 + \sum_{k=1}^{K+1} \frac{2^{kR}(K+1)!}{(2^R-1)^k (K+1-k)!} \sum_{n=1}^{N} \left(\epsilon_{p_n} \overline{\gamma}_{SE_n}^{k} + \varepsilon_{p_n} \overline{\gamma}_{\tilde{R}E_n}^{k} \right) \right] \tag{37}$$

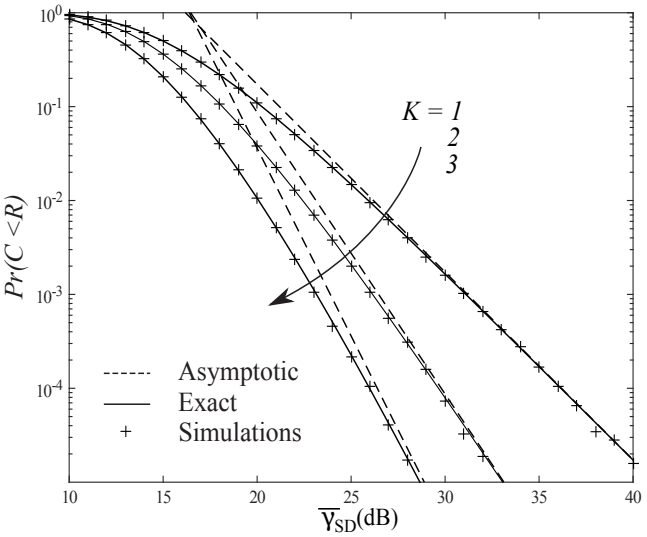

Fig. 3. Secrecy outage probability for $N = 1$, $K = 1$, 2, 3, and $p_1 = 0.1$.

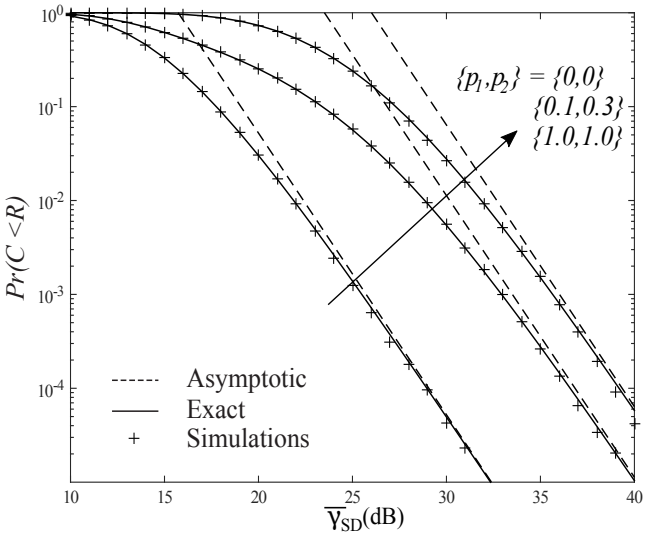

Fig. 4. Secrecy outage probability for $N = 2$, $K = 2$, and $\{p_1, p_2\} = \{0, 0\}, \{0.1, 0.3\}, \{1, 1\}$

$\{\kappa_{SE_1}, \kappa_{\tilde{R}E_1}, \kappa_{SE_2}, \kappa_{\tilde{R}E_2}\} = \{0.1, 0.3, 1.8, 1.3\}$. We can see in the plot that increasing the asymptotic diversity order is independent of $\{p_1, p_2\}$ whereas the asymptotic array gain decreases with increasing $\{p_1, p_2\}$, which corroborates our analytical results in (37). We note that $\{p_1, p_2\} = \{1, 1\}$ corresponds to the ideal scenario where the eavesdropper is always listening to the main channel.

VI. Conclusion

We analyzed the secrecy outage probability of a selective decode-and-forward (DF) relaying link with K relays and N eavesdroppers. We considered that the eavesdroppers can collaborate to share information obtained from the source and the relay amongst themselves. The cost of the collaboration is described by an activity probability which is modeled as a Bernoulli random variable. For this network, we derived new exact and asymptotic closed-form expressions for the secrecy outage probability in Rayleigh fading channels. An interesting extension of this work is to consider a secure transmission region around the nodes in the main channel where the eavesdroppers may not receive any information.

References

[1] D. Raychaudhuri and N. B. Mandayam, "Frontiers of wireless and mobile communications," *Proc. IEEE*, vol. 100, pp. 824–840, Apr. 2012.

[2] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Signal Process. Mag.*, vol. 30, pp. 29–40, Sep. 2013.

[3] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, Apr. 2014.

[4] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, pp. 451–456, Jul. 1978.

[5] C. Liu, N. Yang, G. Geraci, J. Yuan, and R. Malaney, "Secrecy in MIMOME wiretap channels: Beamforming with imperfect CSI," in *Proc. IEEE ICC 2014*, Sydney, Australia, Jun. 2014, pp. 4722–4727.

[6] 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, pp. 2170–2181, Jun. 2013.

[7] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in MIMO wiretap channels," *IEEE Trans. Commun.*, vol. 61, pp. 144–154, Jan. 2013.

[8] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and J. Yuan, "MIMO wiretap channels: A secure transmission using transmit antenna selection and receive generalized selection combining," *IEEE Commun. Lett.*, vol. 17, pp. 1754–1757, Sep. 2013.

[9] 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, pp. 2099–2111, Oct. 2013.

[10] Y. Zou, X. Wang, W. Shen, and L. Hanzo, "Security versus reliability analysis of opportunistic relaying," *IEEE Trans. Veh. Technol.*, vol. 63, pp. 2653–2661, Jul. 2014.

[11] L. Fan, X. Lei, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, "Secure multiuser communications in multiple amplify-and-forward relay networks," *IEEE Trans. Commun.*, vol. 62, pp. 3299–3310, Sep. 2014.

[12] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Q. Duong, "Relay selection for security enhancement in cognitive relay networks," *IEEE Wireless Commun. Lett.*, vol. 4, pp. 46–49, Feb. 2015.

[13] N. Marina and A. Hjørungnes, "Characterization of the secrecy region of a single relay cooperative system," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC '10)*, Sydney, Australia, Apr. 2010, pp. 1–6.

[14] 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, pp. 6076–6085, Dec. 2013.

[15] P. L. Yeoh, M. Elkashlan, Z. Chen, and I. B. Collings, "SER of multiple amplify-and-forward relays with selection diversity," *IEEE Trans. Commun.*, vol. 59, pp. 2078 – 2083, Aug. 2011.

[16] D. Torrieri and M. C. Valenti, "The outage probability of a finite ad hoc network in Nakagami fading," *IEEE Trans. Commun.*, vol. 60, pp. 3509–3518, Nov. 2012.