On Eavesdropper-Tolerance Capability of Two-Hop Wireless Networks

Yuanyu Zhang, Yulong Shen, Hua Wang and Xiaohong Jiang, Senior Meember, IEEE

Abstract—Two-hop wireless network serves as the basic network model for the study of general wireless networks, while cooperative jamming is a promising scheme to achieve the physical layer security. This paper establishes a theoretical framework for the study of eavesdropper-tolerance capability (i.e., the exact maximum number of eavesdroppers that can be tolerated) in a two-hop wireless network, where the cooperative jamming is adopted to ensure security defined by secrecy outage probability (SOP) and opportunistic relaying is adopted to guarantee reliability defined by transmission outage probability (TOP). For the concerned network, closed form modeling for both SOP and TOP is first conducted based on the Central Limit Theorem. With the help of SOP and TOP models and also the Stochastic Ordering Theory, the model for eavesdropper-tolerance capability analysis is then developed. Finally, extensive simulation and numerical results are provided to illustrate the efficiency of our theoretical framework as well as the eavesdropper-tolerance capability of the concerned network from adopting cooperative jamming and opportunistic relaying.

Index Terms—Security, networking, reliability, eavesdropper-tolerance.

I. INTRODUCTION

TWO-HOP wireless networks, in which a source can communicate with its destination directly or via an intermediate relay, have been a class of basic and attractive network scenarios [11]. More importantly, the performance analysis in such two-hop networks lays the groundwork for the study in general multi-hop wireless networks. Due to the broadcast nature of wireless channels and the increasing demand for exchanging confidential information, ensuring secure and reliable transmission in such wireless networks has become a challenging yet critical task in practice, especially for those applications demanding high security and reliability, such as battle command, emergency treatment and disaster relief.

Traditionally, information is secured above the physical layer by applying cryptography [2] or other approaches [3]. The idea of cryptography is to encrypt the information through a cryptographic algorithm (e.g., RSA and AES) that is hard to break in practice by any eavesdropper with limited computing power and without the secret key. These schemes are therefore termed computationally secure [4], since they are built around the unproven computational hardness assumption.

However, recent advances in computing power (e.g., quantum computing) could make it possible to break such difficult cryptographic algorithms [5] and thus the demand for everlasting security in modern wireless communications becomes more and more urgent. That is why there is an increasing interest recently in physical layer security, behind which the fundamental idea is to exploit the inherent physical characteristics of communication channels to provide information-theoretic security to the legitimate transmissions without the assistance of a secret key [6], [7]. It is more important that no limitations are assumed for the eavesdroppers in terms of the computing power or network parameter knowledge. Moreover, the physical layer security approaches can offer some significant advantages over the traditional cryptographic scheme, like no need to employ complicated cryptographic algorithms and guaranteeing an everlasting security without applying key distribution and management, which is extremely expensive and difficult for large scale decentralized networks. Additionally, physical layer techniques can be used with cryptographic approaches in a complementary way and thus can augment the security achieved by cryptography. Therefore, physical layer approaches have been very promising in guaranteeing a strong form of security in wireless communications.

In the seminal work [8] on the physical layer security, Wyner introduced the wire-tap channel model where the source transmits messages to the intended receiver over a discrete memoryless channel which is wire-tapped by an eavesdropper (wiretapper) through another discrete memoryless channel, called wiretap channel. This work was later generalized to the broadcast model in [9] and to the Gaussian setting in [10]. These works indicated that perfect secrecy can be achieved if the intended receiver has a better channel than the eavesdropper, which however can hardly be satisfied in practice. Thus, many works sought to explore the possibility of secure transmission when the eavesdropper observes a better channel. Maurer [11] showed that perfect secrecy is achievable when the eavesdropper enjoys a better channel by generating a secret key over a public and error-free feedback channel. Nevertheless, this work is treated as a further step in the direction of public-key cryptography. Hero [12] introduced the spacetime coding over multiple antennas for secure communication and artificial noise injection strategy was first proposed by Negi and Goel [13], [14], where the noise generated by the extra antennas of the transmitter such that only the eavesdropper channel is degraded. However, due to the cost of deploying multiple antennas and designing efficient noise, these schemes are not suitable for large scale wireless network with nodes of single antenna. Barros and Rodrigues et al. [15] analyzed
the secrecy outage probability and outage secrecy capacity of a quasi-static Rayleigh fading channel and showed that fading alone can guarantee the information-theoretic security even when the eavesdropper has a better average SNR than the legitimate receiver. Tekin and Yener [16] introduced the cooperative jamming scheme where a nontransmitting user can increase the secrecy capacity by transmitting jamming signal instead of its codewords to confuse the eavesdropper. Since random noise can be generated by helper nodes rather than extra antennas, cooperating jamming has been widely introduced to enhance the physical layer security in wireless networks [17]–[27].

By now, various works have been dedicated to explore the security performances in wireless networks with cooperative jamming. For instance, the per-node secure throughput in large decentralized networks was explored in [17], [18], [28]. The secrecy capacity maximization problem was investigated in [19]–[22] based on cooperative communication, how to design efficient jamming strategies in terms of power or position of jamming was analyzed in [22]–[24]. The opportunistic selection and use of the relays to enhance the physical layer security was studied in [25]–[27]. However, to the best of our knowledge, relatively fewer works consider the performance limits of the eavesdropper-tolerance capability of a network. As shown in [29], [30], the density of the eavesdroppers has a dramatic impact on the connectivity of secrecy graph and the secrecy throughput, which implies that the number of eavesdroppers present in the network is critical in guaranteeing the network security. Knowing the relationship between the eavesdropper-tolerance capability and other network parameters not only plays an important role in the security performance analysis of the network but also serve as the guideline on determining the system parameters to build a secure network for the designers. Therefore, we focus on the eavesdropper-tolerance capability study of a two-hop wireless network in this paper.

The related works regarding eavesdropper-tolerance capability can be classified into two categories according to the network size. For infinite network scenarios, the scaling law of eavesdropper-tolerance capability against the per-node throughput was studied in [28] by constructing a highway system. By cooperative jamming, Goeckel et al. [31] considered one source-destination pair with opportunistic relaying scheme [32], where the best relay is selected among the available relays based on some policy in terms of their channels to the source and destination, and analyzed the asymptotic behavior of eavesdropper-tolerance capability as the number of relays goes to infinity. However, the metrics used in their paper cannot fully reflect the security and reliability of the end-to-end transmission. This work was later generalized to a scenario with multiple source-destination pairs where artificial noises are generated from concurrent transmitters [33]. For finite network scenarios, Shen et al. [24] proposed a flexible relay selection scheme and derived the lower bound on the eavesdropper-tolerance capability. However, it is notable that all the above works have focused on either the order-sense scaling law results for infinite networks, or bounds for finite networks. Such order sense results or bounds are certainly important but cannot reflect the actual eavesdropper-tolerance capability in more practical network scenarios with finite nodes, which is more important for the system designers. In our previous work [35], we considered a random relay selection scheme and derived the exact eavesdropper-tolerance capability, which can exactly tell us how many eavesdroppers a network can tolerate at most for a desired level of security and reliability. However, the results showed that with the random relay selection, the eavesdropper-tolerance performance is not good, especially for small-scale networks and high security/reliability requirement.

In this paper, we establish a theoretical framework to explore the eavesdropper-tolerance capability in a two-hop wireless network, where the cooperative jamming is adopted to ensure security defined by secrecy outage probability (SOP) and opportunistic relaying is adopted to guarantee reliability defined by transmission outage probability (TOP). Different from [31], we use different outage probability metrics that can fully characterize the security and reliability of the end-to-end transmission. More importantly, we consider the inherent channel dependence of the transmissions in two hops, which is critical in determining the exact eavesdropper-tolerance capability. Our contributions can be summarized as follows:

- We first apply the the Central Limit Theorem to develop the closed form models for both SOP and TOP of a source-destination transmission.
- Based on the SOP and TOP models and also the Stochastic Ordering Theory, we then conduct analysis to reveal the monotonicity properties of SOP and TOP. With the help of such properties, the model for eavesdropper-tolerance capability is derived.
- A simulator is developed to validate the efficiency of our theoretical framework and numerical results are also provided to illustrate the eavesdropper-tolerance capability of the concerned network from adopting cooperative jamming and opportunistic relaying.

The reminder of the paper is organized as follows. Section II introduces the system model and problem formulation. In Section III, we conduct the closed form modeling of SOP and TOP of the end-to-end transmission. The model for eavesdropper-tolerance capability analysis is developed in Section IV. Section V presents the simulation and numerical results to validate our theoretical model and Section VI concludes the paper.

II. SYSTEM MODEL AND PROBLEM FORMULATION

A. System Model and Assumptions

As depicted in Fig 1, we consider a two-hop wireless network scenario consisting of a source node $S$, a destination node $D$, $n$ legitimate half-duplex relays $R_1, R_2, \ldots, R_m$ that cannot transmit and receive at the same time and $m$ passive and independently-operating eavesdroppers $E_1, E_2, \ldots, E_m$. We assume that the direct link between $S$ and $D$ does not exist due to the deep fading and thus $S$ needs to transmit messages to $D$ via one of the relays. Each of the eavesdroppers attempts to intercept the messages on its own. Meanwhile, some of the remaining $n - 1$ relays will be selected to generate artificial noise to suppress the eavesdroppers during the transmission.
In order to improve the link condition from $S$ to $D$, an opportunistic relaying scheme is adopted, where the best relay $R_b$ is selected by a timer-based method explained in [32] to forward messages. Here, $b$ is given by

$$ b \triangleq \arg \max_j \min \{|h_{S,R_b}|^2, |h_{R_b,D}|^2\}. $$

The transmission then can be conducted in two phases. In the first phase, $S$ transmits the message to $R_b$. At the same time, relays with indices in $R_1 = \{j|j \neq b, |h_{R_b,R_j}|^2 < \gamma\}$, where $\gamma$ is the noise-generating threshold to control the interference at legitimate receivers, generate artificial noise to suppress the eavesdroppers. Analogous to the first phase, $R_b$ forwards its received message to $D$ with relays whose indices are in $R_2 = \{j|j \neq b, |h_{R_j,D}|^2 < \gamma\}$ generating noise to assist the transmission in the second phase.

### B. Problem Formulation

In this subsection, we first introduce the concepts of TOP and SOP of the concerned network, based on which we then formulate our problem regarding the eavesdropper-tolerance capability in this paper.

To fully characterize the security and reliability performances of the transmission, we adopt the same outage definitions in [17]. Consider the direct link from a transmitter $A$ to a legitimate receiver $B$. We say transmission outage happens if $B$ cannot decode the message (i.e., $SIR_{A,B} < \gamma$) and secrecy outage happens if at least one of the eavesdroppers (say $E_i$) can decode the message (i.e., $SIR_{A,E_i} \geq \gamma_e$). It is shown in [30] that securing each of the individual links is sufficient to secure the end-to-end path. Thus, the secrecy (transmission) outage of the $S \rightarrow R_b \rightarrow D$ link occurs if either $S \rightarrow R_b$ or $R_b \rightarrow D$ suffers from secrecy (transmission) outage. Then we can introduce the following definitions:

- **TOP for opportunistic relaying $P_{bst}^{to}$**: This probability is defined as the probability that the transmission outage of the $S \rightarrow R_b \rightarrow D$ link happens under the opportunistic relaying scheme.

- **SOP for opportunistic relaying $P_{bst}^{so}$**: This probability is defined as the probability that the secrecy outage of the $S \rightarrow R_b \rightarrow D$ link happens under the opportunistic relaying scheme.

Based on the above definitions, $P_{bst}^{to}$ and $P_{bst}^{so}$ can be formulated as

$$ P_{bst}^{to} = P(SIR_{S,R_b} < \gamma \cup SIR_{R_b,D} < \gamma) $$

$$ = 1 - P(SIR_{S,R_b} \geq \gamma, SIR_{R_b,D} \geq \gamma) $$

$$ = 1 - P\left(\frac{|h_{S,R_b}|^2}{\sum_{j \in R_1} |h_{R_j,R_b}|^2} \geq \gamma, \frac{|h_{R_b,D}|^2}{\sum_{j \in R_2} |h_{R_j,D}|^2} \geq \gamma\right) $$

We aim to ensure both the secure and reliable transmission from $S$ to $D$ against these eavesdroppers of unknown channel and location information.

A slow and flat block Rayleigh Fading environment is assumed, where the channel remains static for one coherence interval and varies randomly and independently from interval to interval. Thus, the channel from a transmitter $A$ to a receiver $B$ can be represented by a complex zero-mean Gaussian random variable $h_{A,B}$ and the corresponding channel gain $|h_{A,B}|^2$ is an exponential random variable. Without loss of generality, we assume that $|h_{A,B}|^2 = |h_{B,A}|^2$ and $\mathbb{E}[|h_{A,B}|^2] = 1$, where $\mathbb{E}[,]$ stands for the expectation operator. It is assumed that the source $S$ and the relays transmit with the same power $P_t$. In addition, we assume the network is interference-limited and thus the noise at each receiver is negligible. Therefore, when $A$ is transmitting and relays with indices in $\mathcal{R}$ are generating noise, the received signal-to-interference ratio (SIR) at a receiver $B$ can be formulated as

$$ SIR_{A,B} = \frac{P_t |h_{A,B}|^2}{\sum_{j \in \mathcal{R}} P_t |h_{R_j,B}|^2} = \frac{|h_{A,B}|^2}{\sum_{j \in \mathcal{R}} |h_{R_j,B}|^2}. $$

For the eavesdroppers and legitimate receivers, we use positive $\gamma_e$ and $\gamma$ respectively to denote the minimum SIR required to recover the received message. That is, a legitimate receiver (eavesdropper) is able to decode the transmitted message if and only if its received SIR exceeds $\gamma$ ($\gamma_e$). This SIR threshold scheme can be easily mapped to the Wyner’s encoding scheme where the transmitter chooses two rates, the rate of transmitting codewords $R_t$ and the rate of the confidential message $R_s$ [8, 17]. The rate difference $R_c = R_t - R_s$ reflects the cost of securing the message against the eavesdroppers. The conversions between the thresholds and the code rates are as follows:

$$ \gamma = 2^{R_t} - 1, $$

$$ \gamma_e = 2^{R_c} - 1. $$

Therefore, the results in this paper also applies to the Wyner’s encoding scheme.
and
\[ P_{bst}^{so} = \Pr \left( \bigcup_{i=1}^{m} \{ SIR_{Si,Ei} \geq \gamma_{e} \} \cup \bigcup_{i=1}^{m} \{ SIR_{Rb,Ei} \geq \gamma_{e} \} \right) \]
\[ = 1 - \Pr \left( \bigcap_{i=1}^{m} \{ SIR_{Si,Ei} < \gamma_{e} \} \bigcap_{i=1}^{m} \{ SIR_{Rb,Ei} < \gamma_{e} \} \right) \]
\[ = 1 - \left( \Pr \left( \bigcap_{i=1}^{m} \{ SIR_{Si,Ei} < \gamma_{e} \} \right) \right)^2 \]
\[ = 1 - \left( \Pr \left( \bigcap_{i=1}^{m} \{ h_{Si,Ei}^2 \leq \frac{\gamma_{e}}{\gamma_{e}} \} \right) \right)^2 \]

where \( \Pr(\cdot) \) stands for the probability operator and \( (a) \) follows since the received power of each eavesdropper in two phases are independent and identically distributed. It is notable that the second \( \Pr(\cdot) \) term in (1) cannot be formulated as
\[ \Pr(SIR_{Rb} \geq \gamma) \Pr(SIR_{Rb} \geq \gamma) \]
since \( SIR_{Rb} \) and \( SIR_{Rb,D} \) are dependent, as will be observed in Appendix A.

Since security and reliability are two important metrics in network design, we use the SOP constraint \( \varepsilon_{s} \) and TOP constraint \( \varepsilon_{t} \) to represent the security and reliability requirements of the end-to-end transmission. We say that the transmission from \( S \) to \( D \) is secure if and only if \( P_{bst}^{so} \leq \varepsilon_{s} \) and it is reliable if and only if \( P_{bst}^{so} \leq \varepsilon_{t} \). Notice that larger \( \varepsilon_{s} \) and \( \varepsilon_{t} \) represent less stringent security and reliability requirements. In this paper, we aim to determine the exact \( P_{bst}^{so} \) and \( P_{bst}^{so} \) which can be then used to determine the exact eavesdropper-tolerance capability while ensuring both the reliable and secure end-to-end transmission. We use \( m_{bst}^{*} \) to represent the eavesdropper-tolerance capability for the opportunistic relaying scheme hereafter.

Based on the above observations, we are now ready to formulate our problem. From the definition of \( P_{bst}^{so} \) and \( P_{bst}^{so} \), we can see that when given the number of system relays \( n \), the \( SIR \) thresholds \( \gamma_{s} \), \( \gamma_{c} \), the security requirement \( \varepsilon_{s} \) and reliability requirement \( \varepsilon_{t} \), \( m_{bst}^{*} \) only depends on the noise-generating threshold \( \tau \). Thus, we define the maximum number of eavesdroppers that can be tolerated for a specified \( \tau \) by
\[ M_{bst}(\tau) = \max \{ m : P_{bst}^{so}(n, m, \tau) \leq \varepsilon_{s} \} \]
Now the considered problem can be formulated as
\[ \begin{align*}
\text{maximize} & \quad M_{bst}(\tau) \\
\text{subject to} & \quad P_{bst}^{so}(n, \tau) \leq \varepsilon_{t}, \tau \geq 0 \\
& \quad \varepsilon_{t} \in [0, 1], \varepsilon_{s} \in [0, 1]
\end{align*} \]
where \( P_{bst}^{so} \) and \( P_{bst}^{so} \) are regarded as functions. That is, we want to maximize \( M_{bst}(\tau) \) over \( \tau \). We use \( \tau_{bst}^{b} \) to represent the optimal \( \tau \) that maximizes \( M_{bst}(\tau) \) for opportunistic relaying scheme and thus we have \( m_{bst}^{*} = M_{bst}(\tau_{bst}^{b}) \).

In order to explore the efficiency of the opportunistic relaying scheme, we also give the eavesdropper-tolerance capability of the same network scenario but with a random relay selection scheme as a comparison, which is considered in [55]. Similarly, for random relay selection scheme, we define the TOP by \( P_{bst}^{so} \), the SOP by \( P_{bst}^{so} \), the optimal \( \tau \) by \( \tau_{bst}^{b} \), and the eavesdropper-tolerance capability by \( m_{bst}^{*} \).

### III. Outage Performances

In this section we determine the TOP \( P_{bst}^{so} \) and SOP \( P_{bst}^{so} \) of the network with opportunistic relaying scheme based on some theoretical analysis. Applying the same approach, we also give the outage probabilities of the network with random relay selection scheme.

#### A. SOP and TOP For Opportunistic Relaying

Before determining the TOP of a network with opportunistic relaying, we first define the total interference at the legitimate receiver in two phases by
\[ I_{1} = \sum_{j \in \mathcal{R}_{1}} |h_{R_{j},R_{0}}|^2, \quad I_{2} = \sum_{j \in \mathcal{R}_{2}} |h_{R_{j},D}|^2. \]

Then, we establish the following lemmas regarding the probability distribution of \( I_{1} \) and \( I_{2} \) and an important joint probability of the channel gains in two phases, which is critical in determining \( P_{bst}^{so} \).

**Lemma 1:** For one message transmission from \( S \) to \( D \), the total interference \( I_{1} \) and \( I_{2} \) are independent and identically distributed, and can be approximated by a normal random variable. Thus, the corresponding pdf is given by
\[ f(x) \approx \tilde{f}(x) = \frac{e^{-\frac{(x-\mu)^2}{2\sigma^2}}}{\sigma\sqrt{2\pi}}, \]
where
\[ \mu = (n-1)\left[1 - (1 + \tau)e^{-\tau}\right] \]
is the mean and
\[ \sigma = \sqrt{(n-1)(1 + \tau^2 - e^{-\tau} - 1 + \tau^2 e^{-2\tau})} \]
is the standard derivation of the normal random variable.

**Lemma 2:** For one message transmission from \( S \) to \( D \), the joint probability that \( |h_{S,R_{0}}|^2 \geq x \) and \( |h_{R_{0},D}|^2 \geq y \) can be determined as
\[ \Pr \left( |h_{S,R_{0}}|^2 \geq x, |h_{R_{0},D}|^2 \geq y \right) \]
\[ = 1 - (1 - e^{-2\max \{x,y\}})^n \]
\[ + ne^{-\max \{x,y\}} \left[ \varphi(n, \min \{x,y\}) - \varphi(n, \max \{x,y\}) \right], \]
where
\[ \varphi(n, x) = e^{-x} F_{1} \left( \frac{1}{2}, 1 - n; \frac{3}{2}; e^{-2x} \right) \]
and \( F_{1} \) is the Gaussian hypergeometric function.

**Remark 1:** Since \( S \) and relays transmit with the same power, \( P_{1} \) can be reduced in determining the TOP as shown in (1), and thus it is not considered in Lemma 1. The proofs of the above lemmas can be found in Appendix A.

For a two-hop wireless network with opportunistic relaying scheme, we are now ready to derive its TOP \( P_{bst}^{so} \) and SOP
\( P_{bst}^{io} \) of the end-to-end transmission based on Lemma 1 and Lemma 2.

**Theorem 1:** Consider the network scenario in Fig. 1 with opportunistic relaying scheme. The TOP \( P_{bst}^{io} \) and SOP \( P_{bst}^{so} \) can be given by

\[
P_{bst}^{io} \approx 2 \int_{0}^{(n-1)\tau} g(n, \gamma, x) \hat{f}(x) \left[ \Phi\left(\frac{x - \mu}{\sigma}\right) - \Phi\left(-\frac{\mu}{\sigma}\right) \right] dx
- 2 \int_{0}^{(n-1)\tau} \int_{x}^{\infty} ne^{-\gamma x} \varphi(n, \gamma y) \hat{f}(x) \hat{f}(y) dy dx
\]

(4)

and

\[
P_{bst}^{so} = 1 - \left( \sum_{k=1}^{m} \binom{m}{k} (-1)^k (1 - e^{-\tau})^k + e^{-\tau} \right)^{-1}
\]

(5)

where

\[
c = \frac{1}{1 + \gamma c}, \quad \hat{f}(x) = \frac{e^{\frac{(x-n)^2}{2\sigma^2}}}{\sigma \sqrt{2\pi}},
\]

\[
\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{t^2}{2}} dt,
\]

\[
\mu = (n-1) \left[ 1 - (1 + \tau) e^{-\tau} \right],
\]

\[
\sigma = \sqrt{(n-1) \left[ 1 - \tau^2 e^{-\tau} - (1 + \tau)^2 e^{-2\tau} \right]},
\]

\[
g(n, \gamma, x) = (1 - e^{-2\gamma x})^n + ne^{-\gamma x} \varphi(n, \gamma x),
\]

\[
\varphi(n, x) = e^{-x} \frac{\Gamma(1 + n)}{\Gamma(1 + 3/2)}
\]

and \( _2F_1 \) is the Gaussian hypergeometric function.

**Proof:** 1) We first prove the \( P_{bst}^{io} \) in (4). According to the definition in (4), we have

\[
P_{bst}^{io} = 1 - \mathbb{P} \left( \text{SIR}_{S,R_b} \geq \gamma, \text{SIR}_{R_b,D} \geq \gamma \right)
\]

\[
= 1 - \mathbb{P} \left( |h_{S,R_b}|^2 \geq \gamma I_1, |h_{R_b,D}|^2 \geq \gamma I_2 \right)
\]

Applying the law of total probability, we have

\[
P_{bst}^{io} = 1 - \mathbb{E}_{I_1, I_2} \left[ \mathbb{P} \left( |h_{S,R_b}|^2 \geq \gamma I_1, |h_{R_b,D}|^2 \geq \gamma I_2 \right) \right]
\]

(6)

where (b) is due to Lemma 1 and (c) follows after applying Lemma 2.

2) Now we proceed to prove the \( P_{bst}^{so} \) in (5). According to the definition in (5), we first need to derive the probability

\[
\mathbb{P} \left( \bigcap_{i=1}^{m} \left\{ \sum_{j \in \mathcal{R}_i} |h_{S,E_i}|^2 < \gamma c \right\} \right)
\]

Note that the number of noise-generating relays in the first phase \( |\mathcal{R}_1| \) follows the binomial distribution \( B(n-1, 1 - e^{-\tau}) \).

Now, we define the event that there are \( l \) noise-generating relays in the first phase (i.e., \( |\mathcal{R}_1| = l \)) by \( B_l \) and thus we have

\[
\mathbb{P} \left( \bigcap_{i=1}^{m} \left\{ \sum_{j \in \mathcal{R}_i} |h_{S,E_i}|^2 < \gamma c \right\} \right)
\]

(7)

\[
= \sum_{l=0}^{n-1} \mathbb{P} \left( \bigcap_{i=1}^{m} \left\{ \sum_{j \in \mathcal{R}_i} |h_{S,E_i}|^2 < \gamma c \right\} \big| B_l \right) \mathbb{P}(B_l)
\]

\[
= \sum_{l=0}^{n-1} \mathbb{P} \left( \bigcap_{i=1}^{m} \left\{ \sum_{j \in \mathcal{R}_i} |h_{S,E_i}|^2 < \gamma c \right\} \big| B_l \right) \mathbb{P}(B_l)
\]

(8)

\[
= \sum_{i=1}^{m} \mathbb{P} \left( \bigcap_{j \in \mathcal{R}_i} |h_{S,E_i}|^2 < \gamma c \big| B_l \right) \mathbb{P}(B_l)
\]

(9)

\[
= \sum_{l=0}^{n-1} \left[ 1 - \left( \frac{l}{n} \right)^m \right]^{m} \left( n-1 \right)^{l} (1-e^{-\tau})^{n-1-l}
\]

(10)

where (a) follows since all the \( \{SIR_{S,E_i}, i = 1, \cdots, m\} \) are conditionally independent given event \( B_l \), (e) follows by
applying the law of total probability and the expectation is computed with respect to \( \{ |h_{R_j,E_i}|^2, j \in \mathcal{R}_1 \} \). \( (f) \) follows since all the \( |h_{R_j,E_i}|^2 \) are independent and identically distributed and \( (g) \) follows by applying the binomial theorem. Therefore, \( (5) \) follows after substituting \( (7) \) into \( (2) \).

### B. SOP and TOP For Random Relay Selection

Applying the same approach, we now can establish the following lemma about the TOP and SOP under the random relay selection scheme.

**Lemma 3:** Consider the network scenario in Fig. 2 with random relay selection scheme. The TOP \( P_{\text{ran}}^{\text{so}} \) and SOP \( P_{\text{ran}}^{\text{so}} \) can be given by

\[
P_{\text{ran}}^{\text{so}} = 1 - \left( e^{-\tau} + \frac{1 - e^{-(1+\gamma)\tau}}{1 + \gamma} \right)^{2n-2} \tag{8}
\]

and

\[
P_{\text{ran}}^{\text{so}} = 1 - \left( \sum_{k=1}^{m} \binom{m}{k} (-1)^k \left( 1 - e^{-\tau} \right)^k \right)^{2} \tag{9}
\]

where \( c = \frac{1}{1 + \gamma} \).

**Remark 2:** The distributions of \( I_1 \) and \( I_2 \) are not used in determining the \( P_{\text{ran}}^{\text{so}} \) in \( (8) \), because the channel gains in two hops are independent. Therefore, we can give an exact TOP. The detailed proof can be found in [35]. It is also noticed that the SOP \( P_{\text{ran}}^{\text{so}} \) in \( (9) \) is identical to \( P_{\text{bst}}^{\text{so}} \) in \( (5) \). This is because that the noise-generating schemes are identical in these two schemes and the message relay selection has no impact on the intercepting behavior of the eavesdroppers.

## IV. EAVESDROPPER-TOLERANCE CAPABILITY

Eavesdropper-tolerance capability characterizes how many eavesdroppers that can be tolerated at most by a wireless network with \( n \) relays in order to guarantee the desired security requirement \( \varepsilon_s \) and reliability requirement \( \varepsilon_r \). In this section, we determine the eavesdropper-tolerance capability for opportunistic relaying scheme based on the problem formulation in section II.B. The eavesdropper-tolerance capability for random relay selection scheme is also provided by applying the same approach.

### A. Eavesdropper-Tolerance Capability for Opportunistic Relaying

It can be observed from the transmission scheme in section II-A and the problem formulation in section II-B that the noise-generating threshold \( \tau \) is a critical parameter in determining the eavesdropper-tolerance capability. Too large \( \tau \) will do harm to the end-to-end transmission, while too small \( \tau \) is not enough to interfere the eavesdroppers. Therefore, finding a optimal \( \tau \) is the key to solving our considered problem. Before solving the problem, we establish the following lemma based on the Stochastic Ordering in [32].

**Lemma 4:** Let \( \mathbf{X} \) and \( \mathbf{Y} \) be two N-dimensional random vectors such that

\[
\mathbb{P}(\mathbf{X} \in U) \leq \mathbb{P}(\mathbf{Y} \in U) \quad \text{for all upper sets} \quad U \in \mathbb{R}^N.
\]

Then \( \mathbf{X} \) is said to be *smaller than \( \mathbf{Y} \) in the usual stochastic order* (denoted by \( \mathbf{X} \leq_{st} \mathbf{Y} \)). And for all increasing function \( \phi \), we always have \( \mathbb{E}[\phi(\mathbf{X})] \leq \mathbb{E}[\phi(\mathbf{Y})] \).

Based on the above lemma, we then establish the following lemmas in terms of the monotonicity of SOP and TOP with respect to \( \tau \).

**Lemma 5:** The TOP \( P_{\text{bst}}^{\text{so}} \) for opportunistic relaying scheme increases as \( \tau \) increases.

**Proof:** For any \( 0 < \tau_1 < \tau_2 \), we use random vector \( \mathbf{I}_1 = (I_{11}, I_{12}) \) to represent the interferences in two phases when the noise-generating threshold is \( \tau_1 \) and \( \mathbf{I}_2 = (I_{21}, I_{22}) \) to represent those interferences for \( \tau_2 \). For any upper set \( U = \{ (I_{11}, I_{12}) \mid I_{11} \geq x \geq 0, I_{22} \geq y \geq 0 \} \), we always have

\[
\mathbb{P}(\mathbf{I}_1 \in U) = \mathbb{P}(I_{11} \geq x)\mathbb{P}(I_{12} \geq y)
\]

and

\[
\mathbb{P}(\mathbf{I}_2 \in U) = \mathbb{P}(I_{21} \geq x)\mathbb{P}(I_{22} \geq y).
\]

It is easy to see that \( \mathbb{P}(I_{11} \geq x) < \mathbb{P}(I_{21} \geq x) \) and \( \mathbb{P}(I_{22} \geq y) < \mathbb{P}(I_{22} \geq y) \), since more interference can be generated as \( \tau \) increases. Therefore, we have \( \mathbb{P}(\mathbf{I}_1 \in U) < \mathbb{P}(\mathbf{I}_2 \in U) \) and then \( \mathbf{I}_1 \leq_{st} \mathbf{I}_2 \) according to Lemma 4. Define the term \( \mathbb{P}(|h_{R_1E_1}|^2 \geq \gamma I_1, |h_{R_2E_1}|^2 \geq \gamma I_2) \) in \( (6) \) by \( \Gamma(\mathbf{I}) \) which decreases as \( \mathbf{I} \) increases, where \( \mathbf{I} = (I_{11}, I_{22}) \). Thus, we have \( \mathbb{E}[\Gamma(\mathbf{I}_1)] > \mathbb{E}[\Gamma(\mathbf{I}_2)] \) according to Lemma 4. That is, for any \( 0 < \tau_1 < \tau_2 \), we always have \( P_{\text{bst}}^{\text{so}}(\tau_1) < P_{\text{bst}}^{\text{so}}(\tau_2) \), which indicates the TOP \( P_{\text{bst}}^{\text{so}} \) increases with \( \tau \).

**Lemma 6:** The SOP \( P_{\text{bst}}^{\text{so}} \) for opportunistic relaying scheme decreases as \( \tau \) increases, whereas increases as \( m \) increases.

**Proof:** Notice that the step following \( (f) \) in \( (7) \) can also be written as

\[
\mathbb{E}\left[ 1 - \left( \frac{1}{1 + \gamma_e} \right)^{|\mathcal{R}_1|} \right],
\]

where the expectation is computed with respect to \( |\mathcal{R}_1| \). For any \( 0 \leq \tau_1 < \tau_2 \), we use two random variables \( |\mathcal{R}_1| \) and \( |\mathcal{R}_2| \) to represent the number of noise-generating relays in the first phase, where

\[
|\mathcal{R}_1| \sim B(n - 1, 1 - e^{-\tau_1})
\]

and

\[
|\mathcal{R}_2| \sim B(n - 1, 1 - e^{-\tau_2}).
\]

It is shown in [33] that \( |\mathcal{R}_1| \leq_{st} |\mathcal{R}_2| \). Applying Lemma 4 again, we can see that

\[
\mathbb{E}\left[ 1 - \left( \frac{1}{1 + \gamma_e} \right)^{|\mathcal{R}_1|} \right] < \mathbb{E}\left[ 1 - \left( \frac{1}{1 + \gamma_e} \right)^{|\mathcal{R}_2|} \right].
\]

Therefore, the SOP \( P_{\text{bst}}^{\text{so}} \) decreases as \( \tau \) increases.

Next, we consider the step following \( (f) \) in \( (7) \) again. It is easy to see that the term

\[
1 - \left( \frac{1}{1 + \gamma_e} \right)^m \in [0, 1).
\]

Thus, the term \( \left[ 1 - \left( \frac{1}{1 + \gamma_e} \right)^m \right]^m \) decreases with \( m \). Therefore, the SOP \( P_{\text{bst}}^{\text{so}} \) increases as \( m \) increases.
Define step (g) in (7) by a function $G(m, n, \tau)$. Then we can derive the eavesdropper-tolerance capability $m^*_{bst}$ for opportunistic relaying scheme based on Lemma 5 and Lemma 6.

**Theorem 2:** Consider the network scenario in Fig[1] with opportunistic relaying scheme. The eavesdropper-tolerance capability under the security constraint $\varepsilon_s$ and reliability constraint $\varepsilon_t$ is

$$m^*_{bst} = \max\{m : G(m, n, \tau_{bst}) \geq \sqrt{1 - \varepsilon_s}\},$$

where

$$G(m, n, \tau_{bst}) = \sum_{k=1}^{m} \binom{m}{k} (-1)^k \left[(1 - e^{-\tau_{bst}}) e^k + e^{-\tau_{bst}}\right]^{n-1},$$

c = \frac{1}{1 + \gamma}$ and $\tau^b_{bst}$ is the solution of $P_{bst}^t = \varepsilon_t$.

**Proof:** As shown in (3), we need to find the optimal $\tau$ that maximizes $M_{bst}(\tau)$, where

$$M_{bst}(\tau) = \max\{m : G(m, n, \tau) \geq \sqrt{1 - \varepsilon_s}\},$$

according to its definition. Since the TOP $P_{bst}^t$ increases with $\tau$ according to Lemma 5, in order to guarantee the reliability (i.e., $P_{bst}^t \leq \varepsilon_t$), $\tau$ must take values in the region $[0, \tau_m]$, where $\tau_m$ is the solution of $P_{bst}^t = \varepsilon_t$.

Next, we need to prove that $\tau_m$ is the optimal $\tau$ (i.e., $\tau_{bst}^* = \tau_m$). That is, for any $\tau \in [0, \tau_m)$ we always have $M_{bst}(\tau) \leq M_{bst}(\tau_m)$. Now we prove it by contradiction. Suppose there exists a $\tau' \in [0, \tau_m)$ such that $M_{bst}(\tau') > M_{bst}(\tau_m) + 1$. It is easy to see that

$$G(M_{bst}(\tau_m) + 1, n, \tau_m) < \sqrt{1 - \varepsilon_s},$$

since $M_{bst}(\tau_m)$ is the largest $m$ satisfying $G(m, n, \tau_m) \geq \sqrt{1 - \varepsilon_s}$. By Lemma 6, it can be observed that $G(m, n, \tau)$ increases with $\tau$, whereas decreases with $m$. Thus, we have

$$G(M_{bst}(\tau_m) + 1, n, \tau') < G(M_{bst}(\tau_m) + 1, n, \tau_m) < \sqrt{1 - \varepsilon_s}$$

and

$$G(M_{bst}(\tau_m) + 1, n, \tau') \geq G(M_{bst}(\tau'), n, \tau') \geq \sqrt{1 - \varepsilon_s}.$$
observed that

By comparing these three curves in Fig.3, it can also be

This is because more interferences can be generated at the

receivers to successfully recover the messages.

Theorem used in deriving our theoretical result fails to model

the reason that more interferences will be generated at the

as

increases, which agrees with Lemma 6. This is intuitive since distributing more eavesdroppers by the adversary would post more potential threats to the end-to-end transmission and increasing \( \tau \) would generate more interferences at the eavesdroppers, so it is more difficult for them to successfully decode the messages.

\[ P_{bst}^{\infty} \] as \( \tau \) increases, which agree with Lemma 6. This is intuitive since distributing more eavesdroppers by the adversary would post more potential threats to the end-to-end transmission and increasing \( \tau \) would generate more interferences at the eavesdroppers, so it is more difficult for them to successfully decode the messages.

\[ b_s \] vs. number of relays

\[ I \]

\[ \gamma \]

\[ \epsilon_s \]

\[ \epsilon_t \]

Theorem used in deriving our theoretical result fails to model

the reason that more interferences will be generated at the

as \( \tau \) increases, which agrees with Lemma 6. This is intuitive since distributing more eavesdroppers by the adversary would post more potential threats to the end-to-end transmission and increasing \( \tau \) would generate more interferences at the eavesdroppers, so it is more difficult for them to successfully decode the messages.

\[ P_{bst}^{\infty} \] as \( \tau \) increases, which agree with Lemma 6. This is intuitive since distributing more eavesdroppers by the adversary would post more potential threats to the end-to-end transmission and increasing \( \tau \) would generate more interferences at the eavesdroppers, so it is more difficult for them to successfully decode the messages.

To explore how the number of relays affects the eavesdropper-tolerance capability, we illustrate in Fig.5 the behavior of \( m_{bst}^{\infty} \) vs. \( \epsilon_t \) and \( \epsilon_s \) for different settings of \( \gamma \). This suggests that either the security or reliability requirement has to sacrifice for the other one in order to achieve a certain level of eavesdropper-tolerance capability. For example, \( \epsilon_t \) has to increase from 0.04 to 0.085 as \( \epsilon_s \) decreases from 0.03 to 0.02 for achieving an eavesdropper-tolerance capacity of about 1000. This suggests that either the security or reliability requirement has to sacrifice for the other one in order to achieve a certain eavesdropper-tolerance capability. From the above discussions, we can see that there exists clear tradeoffs between the eavesdropper-tolerance capability and the reliability/security constraint.

To explore how the number of relays affects the eavesdropper-tolerance capability, we illustrate in Fig.5 the behavior of \( m_{bst}^{\infty} \) vs. \( \epsilon_t \) and \( \epsilon_s \) for different settings of \( \gamma \). This suggests that either the security or reliability requirement has to sacrifice for the other one in order to achieve a certain level of eavesdropper-tolerance capability. For example, \( \epsilon_t \) has to increase from 0.04 to 0.085 as \( \epsilon_s \) decreases from 0.03 to 0.02 for achieving an eavesdropper-tolerance capacity of about 1000. This suggests that either the security or reliability requirement has to sacrifice for the other one in order to achieve a certain eavesdropper-tolerance capability. From the above discussions, we can see that there exists clear tradeoffs between the eavesdropper-tolerance capability and the reliability/security constraint.

By comparing these three curves in Fig.3 it can also be observed that \( P_{bst}^{\infty} \) increases as \( m \) increases while decreases

as \( \tau \) increases, which agree with Lemma 6. This is intuitive since distributing more eavesdroppers by the adversary would post more potential threats to the end-to-end transmission and increasing \( \tau \) would generate more interferences at the eavesdroppers, so it is more difficult for them to successfully decode the messages.

Fig. 2. TOP for opportunistic relaying \( P_{bst}^{\infty} \) vs. number of relays \( n \) with different settings of \( \tau \), when \( \gamma = 10 \).

Fig. 3. SOP for opportunistic relaying \( P_{bst}^{\infty} \) vs. number of relays \( n \) with different settings of \( m \) and \( \tau \), when \( \gamma_c = 0.5 \).

Fig. 4. Eavesdropper-tolerance capability \( m_{bst}^{\infty} \) for opportunistic relaying vs. reliability constraint \( \epsilon_t \) and security constraint \( \epsilon_s \) with \( n = 2000, \gamma = 10 \) and \( \gamma_c = 0.5 \).

Based on the SOP and TOP models, we now explore the performance of eavesdropper-tolerance capability for opportunistic relaying scheme. To illustrate the impact of security and reliability constraints on the eavesdropper-tolerance capability, we show in Fig.4 the behavior of \( m_{bst}^{\infty} \) vs. \( \epsilon_t \) and \( \epsilon_s \) for the network scenario of \( n = 2000, \gamma = 10, \gamma_c = 0.5 \), which implies that the eavesdroppers have a much better decoding ability than the legitimate receivers. We can observe from Fig.4 that \( m_{bst}^{\infty} \) increases as \( \epsilon_t \) and \( \epsilon_s \) increase. This reflects that the network can tolerate more eavesdroppers by relaxing either the security or reliability requirement. A careful observation of Fig.4 indicates that \( \epsilon_t \) increases as \( \epsilon_s \) decreases in order to guarantee a certain level of eavesdropper-tolerance capability. For example, \( \epsilon_t \) has to increase from 0.04 to 0.085 as \( \epsilon_s \) decreases from 0.03 to 0.02 for achieving an eavesdropper-tolerance capacity of about 1000. This suggests that either the security or reliability requirement has to sacrifice for the other one in order to achieve a certain eavesdropper-tolerance capability. From the above discussions, we can see that there exists clear tradeoffs between the eavesdropper-tolerance capability and the reliability/security constraint.

To explore how the number of relays affects the eavesdropper-tolerance capability, we illustrate in Fig.5 the behavior of \( m_{bst}^{\infty} \) vs. \( n \) with \( \epsilon_t = 0.01 \) and \( \epsilon_s = 0.01 \) for different settings of \( \gamma \) and \( \gamma_c \). It can be observed from Fig.5 that \( m_{bst}^{\infty} \) increases as \( n \) increases. This is because that although the optimal threshold \( \tau_{bst}^{\infty} \) decreases as \( n \) increase for a specific reliability
Fig. 5. Eavesdropper-tolerance capability \( m_{\text{batt}} \) for opportunistic relaying vs. number of relays \( n \) with \( \varepsilon_t = 0.01 \), and \( \varepsilon_s = 0.01 \).

Fig. 6. Eavesdropper-tolerance capability \( m_{\text{ran}}^* \) for random relay selection vs. number of relays \( n \) with \( \varepsilon_t = 0.1 \), and \( \varepsilon_s = 0.1 \).

For different setting of \( \gamma \) and \( \gamma_e \). Notice that the security and reliability requirements here are much more relaxed and the decoding ability of the legitimate receivers are much more improved than those for opportunistic relaying in Fig[5]. For example, \( \gamma = 0.6 \) is much smaller compared to \( \gamma = 10 \) in Fig[5]. That means we consider a much more conservative scenario for random relay selection scheme and the network can hardly tolerate any eavesdropper if we consider the same scenario as that in Fig[5]. It can be observed from Fig[6] that \( m_{\text{ran}}^* \) also increases as \( \gamma_e \) increases, while decreases as \( \gamma \) increases due to the same reason presented in the discussion of Fig[5]. Even for such a conservative scenario, we still can observe from Fig[6] and Fig[5] that the eavesdropper tolerance capability of random relay selection is orders of magnitude less than that of opportunistic relaying scheme, especially for large values of \( n \). For example, for the case that \( \gamma = 0.7 \) and \( \gamma_e = 0.6 \) in Fig[5] the network can tolerate about 207 eavesdroppers, which is much less than 8959 eavesdroppers for the case that \( \gamma = 11 \) and \( \gamma_e = 0.6 \) in Fig[5] when \( n = 3000 \). As the eavesdropper-tolerance capability for random relay selection scheme decreases with \( \gamma \), it will decreases to 0 if we increases \( \gamma \) to 11. This implies that the opportunistic relaying scheme can achieve a significantly better eavesdropper-tolerance capability than random relay selection.

VI. CONCLUSION

This paper established a theoretical framework to analyze the eavesdropper-tolerance capability of a two-hop wireless network, where cooperative jamming and opportunistic relaying techniques are adopted to provide secure and reliable end-to-end transmission against passive and independently operating eavesdroppers of unknown location and channel information. We first apply the Central Limit Theorem to model the TOP and SOP in closed form, based on which and also the Stochastic Ordering we then develop the model for eavesdropper-tolerance capability analysis. Our results indicate that in general more eavesdroppers can be tolerated in the concerned network if a less stringent requirement on both metrics security and reliability is allowed, but a tradeoff between the requirements on these two metrics does exist to ensure a certain level of eavesdropper-tolerance capability. The results in this paper also reveal that the opportunistic relaying scheme significantly outperforms the random relay selection scheme in terms of the eavesdropper-tolerance capability, and the scheme can guarantee an acceptable eavesdropper-tolerance capability even when a stringent requirement on security and reliability is imposed.

APPENDIX A

PROOF OF LEMMA 1 AND 2

Proof of Lemma 1: From the transmission protocol and the i.i.d fading assumption, we can easily see that \( I_1 \) and \( I_2 \) are the sum of random variables which are smaller than \( \tau \) among \( n-1 \) i.i.d random variables and thus \( I_1 \) and \( I_2 \) are independent and identically distributed.
Now we take $I_1$ for example to determine the distribution of the total interference in both hops. First, we define a function

$$U(x) = 1_{x<\tau}(x) \cdot x,$$

where

$$1_{x<\tau}(x) = \begin{cases} 1, & x < \tau \\ 0, & \text{otherwise} \end{cases}$$

is an indicator function and then $I_1$ can be formulated as

$$I_1 = \sum_{j=1}^{n} U(|h_{R_j,R_0}|^2),$$

which is the sum of $n-1$ i.i.d random variables with pdf given by the following mixed density and mass function

$$f_U(u) = \begin{cases} e^{-\tau} \delta(u) + e^{-u}, & 0 \leq u \leq \tau \\ 0, & \text{otherwise} \end{cases},$$

where $\delta(x)$ is the Dirac delta function. The mean and variance of the mixed-type random variable $U(|h_{R_j,R_0}|^2)$ can be given by

$$\mu_1 = 1 - (1 + \tau)e^{-\tau}$$

and

$$\sigma_1^2 = 1 - \tau^2e^{-\tau} - (1 + \tau)^2e^{-2\tau}.$$

Therefore, the pdf of $I_1$ can be recursively given by the following mixed density and mass function

$$f(x) = \begin{cases} e^{-(n-1)\tau} \delta(x) + p_{n-1}(x)e^{-x}, & 0 \leq x \leq (n-1)\tau \\ 0, & \text{otherwise} \end{cases},$$

where $p_{n-1}(x)$ is a piecewise function and coincides with different polynomial functions of degree at most $n-2$ on each interval $(k\tau, (k+1)\tau]$ for $0 \leq k \leq n-2$. However, it is quite difficult to determine the function $p_{n-1}(x)$, especially for large $n$. Thus, we approximate it by a normal random variable with mean $\mu = (n-1)\mu_1$ and variance $\sigma^2 = (n-1)\sigma_1^2$, according to the Central Limit Theorem and its pdf can be approximated by

$$f(x) \approx \hat{f}(x) = \frac{(x-y)^2}{\sigma^2 \sqrt{2\pi}}$$

where

$$\mu = (n-1)[1 - (1 + \tau)e^{-\tau}]$$

and

$$\sigma = \sqrt{(n-1)[1 - \tau^2e^{-\tau} - (1 + \tau)^2e^{-2\tau}]}.$$

**Proof of Lemma 2:** Before deriving the probability in Lemma 2, we first define the event that relay $R_k$, $k = 1, \cdots, n$ is selected as the message relay by $A_k$ (i.e., $b = k$). Besides, we use a new random variable $S_j$ to define $\min(|h_{S_j,R_j}|^2, |h_{R_j,D}|^2)$ for each relay $R_j$. It is notable that $S_j, j = 1, \cdots, n$ is an exponential random variable with mean $1$. Then, we have

$$A_k \triangleq \bigcap_{j=1, j\neq k}^{n} (S_j \leq S_k).$$

Now, applying the law of total probability, we have

$$\mathbb{P}\left(|h_{S,R_k}|^2 \geq x, |h_{R_j,D}|^2 \geq y \right) \tag{12}$$

$$= \sum_{k=1}^{n} \mathbb{P}\left(|h_{S,R_k}|^2 \geq x, |h_{R_j,D}|^2 \geq y, A_k \right)$$

$$= \sum_{k=1}^{n} \mathbb{P}\left(|h_{S,R_k}|^2 \geq x, |h_{R_j,D}|^2 \geq y, \bigcap_{j=1, j\neq k}^{n} (S_j \leq S_k) \right)$$

$$= \sum_{k=1}^{n} \int_{0}^{\infty} \mathbb{P}\left(|h_{S,R_k}|^2 \geq x, |h_{R_j,D}|^2 \geq y, S_k = s \right) ds$$

$$= \sum_{k=1}^{n} \int_{0}^{\infty} \mathbb{P}\left(|h_{S,R_k}|^2 \geq x, |h_{R_j,D}|^2 \geq y, S_k = s \right) \times \mathbb{P}\left(\bigcap_{j=1, j\neq k}^{n} (S_j \leq s) \right) ds$$

$$= \sum_{k=1}^{n} \int_{0}^{\infty} \mathbb{P}\left(|h_{S,R_k}|^2 \geq x, |h_{R_j,D}|^2 \geq y, S_k = s \right) \times (1 - e^{-2s})^{n-1} ds,$$

where $(h)$ integrates over all the values $S_k$ can take. When $x \geq y \geq 0$, $(12)$ can be reduced to

$$\mathbb{P}\left(|h_{S,R_k}|^2 \geq x, |h_{R_j,D}|^2 \geq y \right) \tag{13}$$

$$= \sum_{k=1}^{n} \left\{ \int_{x}^{\infty} \mathbb{P}\left(|h_{S,R_k}|^2 = s, |h_{R_j,D}|^2 \geq s \right) (1 - e^{-2s})^{n-1} ds \right. + \left. \int_{y}^{\infty} \mathbb{P}\left(|h_{S,R_k}|^2 > x, |h_{R_j,D}|^2 = s \right) (1 - e^{-2s})^{n-1} ds \right\}$$

$$= 2n \int_{x}^{\infty} \frac{(1 - e^{-2s})^{n-1} ds + ne^{-x} \int_{x}^{y} \frac{(1 - e^{-2s})^{n-1} ds}{e^{s}} ds}$$

$$= 1 - (1 - e^{-2x})^{n-1} + ne^{-x} \int_{e^{-x}}^{\infty} (1 - t^2)^{n-1} dt$$

$$= 1 - (1 - e^{-2x})^{n-1} + ne^{-x}[\varphi(n, y) - \varphi(n, x)],$$

where

$$\varphi(n, x) = e^{-x} \sum_{k=0}^{n-1} \frac{n!}{k!} \left(\frac{3}{2} e^{-2x}\right)^k$$

and $\sum_{k=0}^{n-1}$ is the Gaussian hypergeometric function. Similarly, when $0 \leq x < y$, $(12)$ can be reduced to

$$\mathbb{P}\left(|h_{S,R_k}|^2 \geq x, |h_{R_j,D}|^2 \geq y \right) \tag{14}$$

$$= 1 - (1 - e^{-2y})^{n-1} + ne^{-y}[\varphi(n, x) - \varphi(n, y)],$$

Combining $(13)$ and $(14)$, Lemma 2 then follows.