On Eavesdropper-Tolerance Capability of Two-Hop Wireless Networks

On Eavesdropper-Tolerance Capability of Two-Hop Wireless Networks

Yuanyu Zhang, Yulong Shen, Hua Wang and Xiaohong Jiang, *Senior Memeber, 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 a intermediate relay, have been a class of basic and attractive network scenarios [1]. 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 main 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 cryptology. 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

Y. Zhang and Y. Shen are with the School of Computer Science and Technology, Xidian University, China. E-mail:yy90zhang@gmail.com; ylshen@mail.xidian.edu.cn

H. Wang is with the Department of Maths and Computing, University of Southern Queensland, Australia. Email: Hua.Wang@usq.edu.au

X. Jiang is with the School of Systems Information Science, Future University Hakodate, 116-2, Kameda Nakano-Cho, Hakodate, Hokkaido, 041-8655, Japan. E-mail:jiang@fun.ac.jp.

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]–[21] 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.* [34] 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 $R_1, R_2, \cdots, R_n$ that cannot transmit and receive at the same time and m passive and independently-operating eavesdroppers $E_1, E_2, \cdots, E_m$. 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.

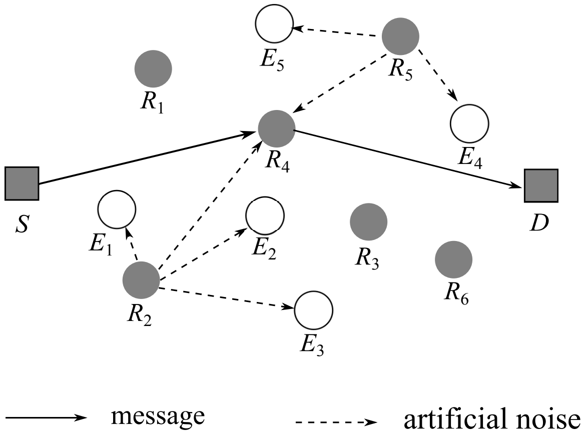

Fig. 1. System scenario: Source S is transmitting message to the destination D with the help of relays $R_1, R_2, \cdots, R_n$ ($n = 6$ in this figure) while eavesdroppers $E_1, E_2, \cdots, E_m$ ($m = 5$ in this figure) are attempting to intercept the message. In this figure, R_4 is the message relay and R_2, R_5 are noise-generating relays.

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 $\mathbb{E}\big[|h_{A,B}|^2\big] = 1$, where $\mathbb{E}\big[\cdot\big]$ 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

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

For the eavesdroppers and legitimate receivers, we use positive γ_e and γ 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 γ (γ_e). This *SIR* threshold scheme can be easily mapped to the Wyner's encoding scheme where the transmitter chooses two rates, the rate of transmitted codewords R_t and the rate of the confidential message R_s [8], [17]. The rate difference $R_e = R_t - R_s$ reflects the cost of securing the message against the eavesdroppers. The conversions between the thresholds and the code rates are as follows:

$$\begin{aligned}\gamma &= 2^{R_t} - 1,\\ \gamma_e &= 2^{R_e} - 1.\end{aligned}$$

Therefore, the results in this paper also applies to the Wyner's encoding scheme.

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

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

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 $\mathcal{R}_1 = \big\{j\big|j \neq b, |h_{R_j,R_b}|^2 < \tau\big\}$, where τ 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 $\mathcal{R}_2 = \big\{j\big|j \neq b, |h_{R_j,D}|^2 < \tau\big\}$ 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 [36] that securing each of the individual links is sufficient to secure the end-to-end path. Thus, the secrecy (transmission) outage of the $S \to R_b \to D$ link occurs if either $S \to R_b$ or $R_b \to D$ 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 $S \to R_b \to D$ 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 $S \to R_b \to D$ link happens under the opportunistic relaying scheme.

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

$$\begin{aligned}P_{bst}^{to} &= \mathbb{P}\left(SIR_{S,R_b} < \gamma \cup SIR_{R_b,D} < \gamma\right) \qquad (1)\\ &= 1 - \mathbb{P}\left(SIR_{S,R_b} \geq \gamma, SIR_{R_b,D} \geq \gamma\right)\\ &= 1 - \mathbb{P}\left(\frac{|h_{S,R_b}|^2}{\sum_{j\in\mathcal{R}_1} |h_{R_j,R_b}|^2} \geq \gamma, \frac{|h_{R_b,D}|^2}{\sum_{j\in\mathcal{R}_2} |h_{R_j,D}|^2} \geq \gamma\right)\end{aligned}$$

and

$$\begin{aligned}
P_{bst}^{so} &= \mathbb{P}\left(\bigcup_{i=1}^{m}\{SIR_{S,E_i} \geq \gamma_e\} \cup \bigcup_{i=1}^{m}\{SIR_{R_b,E_i} \geq \gamma_e\}\right) \quad (2)\\
&= 1 - \mathbb{P}\left(\bigcap_{i=1}^{m}\{SIR_{S,E_i} < \gamma_e\}, \bigcap_{i=1}^{m}\{SIR_{R_b,E_i} < \gamma_e\}\right)\\
&\overset{(a)}{=} 1 - \left[\mathbb{P}\Big(\bigcap_{i=1}^{m}\{SIR_{S,E_i} < \gamma_e\}\Big)\right]^2\\
&= 1 - \left[\mathbb{P}\Big(\bigcap_{i=1}^{m}\Big\{\frac{|h_{S,E_i}|^2}{\sum_{j\in\mathcal{R}_1}|h_{R_j,E_i}|^2} < \gamma_e\Big\}\Big)\right]^2
\end{aligned}$$

where $\mathbb{P}(\cdot)$ 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 $\mathbb{P}(\cdot)$ term in (1) cannot be formulated as

$$\mathbb{P}\left(SIR_{S,R_b} \geq \gamma\right)\mathbb{P}\left(SIR_{R_b,D} \geq \gamma\right),$$

since SIR_{S,R_b} and $SIR_{R_b,D}$ 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 ε_s and TOP constraint ε_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* $P_{bst}^{to} \leq \varepsilon_t$. Notice that larger ε_s and ε_t represent less stringent security and reliability requirements. In this paper, we aim to determine the *exact* P_{bst}^{to} 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}^{to} and P_{bst}^{so}, we can see that when given the number of system relays n, the *SIR* thresholds γ, γ_e, the security requirement ε_s and reliability requirement ε_t, m_{bst}^{*} only depends on the noise-generating threshold τ. Thus, we define the maximum number of eavesdroppers that can be tolerated *for a specified* τ by

$$M_{bst}(\tau) = max\{m : P_{bst}^{so}(n,m,\tau) \leq \varepsilon_s\}.$$

Now the considered problem can be formulated as

$$\begin{aligned}
\underset{\tau}{\text{maximize}} \quad & M_{bst}(\tau)\\
\text{subject to} \quad & P_{bst}^{to}(n,\tau) \leq \varepsilon_t, \tau \geq 0 \qquad (3)\\
& \varepsilon_t \in [0,1], \varepsilon_s \in [0,1]
\end{aligned}$$

where P_{bst}^{to} and P_{bst}^{so} are regarded as functions. That is, we want to maximize $M_{bst}(\tau)$ over τ. We use τ_{bst}^{b} to represent the optimal τ 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 [35]. Similarly, for random relay selection scheme, we define the TOP by P_{ran}^{to}, the SOP by P_{ran}^{so}, the optimal τ by τ_{ran}^{b} and the eavesdropper-tolerance capability by m_{ran}^{*}.

III. Outage Performances

In this section we determine the TOP P_{bst}^{to} 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

$$I_1 = \sum_{j\in\mathcal{R}_1}|h_{R_j,R_b}|^2, I_2 = \sum_{j\in\mathcal{R}_2}|h_{R_j,D}|^2.$$

Then, we establish the following lemmas regarding the probability distribution of I_1, I_2 and an important joint probability of the channel gains in two phases, which is critical in determining P_{bst}^{to}.

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

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

where

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

is the mean and

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

is the standard derivation of the normal random variable.

Lemma 2: For one message transmission from *S* to *D*, the joint probability that $|h_{S,R_b}|^2$ is greater than some constant $x \geq 0$ and $|h_{R_b,D}|^2$ is greater than some constant $y \geq 0$ can be determined as

$$\begin{aligned}
&\mathbb{P}\Big(|h_{S,R_b}|^2 \geq x, |h_{R_b,D}|^2 \geq y\Big)\\
&= 1-(1-e^{-2max\{x,y\}})^n\\
&\quad + ne^{-max\{x,y\}}\Big[\varphi(n,min\{x,y\}) - \varphi(n,max\{x,y\})\Big],
\end{aligned}$$

where

$$\varphi(n,x) = e^{-x}{}_2F_1\left(\frac{1}{2},1-n;\frac{3}{2};e^{-2x}\right)$$

and ${}_2F_1$ is the Gaussian hypergeometric function.

Remark 1: Since S and relays transmit with the same power, P_t 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}^{to} and SOP

P_{bst}^{so} 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}^{to} and SOP P_{bst}^{so} can be given by

$$P_{bst}^{to} \approx 2\int_0^{(n-1)\tau} g(n,\gamma,x)\hat{f}(x)\left[\Phi(\frac{x-\mu}{\sigma})-\Phi(-\frac{\mu}{\sigma})\right]dx \\ -2\int_0^{(n-1)\tau}\int_0^x ne^{-\gamma x}\varphi(n,\gamma y)\hat{f}(x)\hat{f}(y)dydx \quad (4)$$

and

$$P_{bst}^{so} = 1-\left(\sum_{k=1}^{m}\binom{m}{k}(-1)^k\left[(1-e^{-\tau})c^k+e^{-\tau}\right]^{n-1}\right)^2 \quad (5)$$

where

$$c=\frac{1}{1+\gamma_e},\ \hat{f}(x)=\frac{e^{\frac{(x-\mu)^2}{2\sigma^2}}}{\sigma\sqrt{2\pi}},$$

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

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

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

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

$$\varphi(n,x)=e^{-x}{}_2F_1\left(\frac{1}{2},1-n;\frac{3}{2};e^{-2x}\right)$$

and ${}_2F_1$ is the Gaussian hypergeometric function.

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

$$P_{bst}^{to}=1-\mathbb{P}\Big(SIR_{S,R_b}\ge\gamma, SIR_{R_b,D}\ge\gamma\Big) \\ =1-\mathbb{P}\left(|h_{S,R_b}|^2\ge\gamma I_1, |h_{R_b,D}|^2\ge\gamma I_2\right)$$

Applying the law of total probability, we have

$$P_{bst}^{to}=1-\mathbb{E}_{I_1,I_2}\Big[\mathbb{P}\left(|h_{S,R_b}|^2\ge\gamma I_1, |h_{R_b,D}|^2\ge\gamma I_2\right)\Big] \quad (6)$$
$$\overset{(b)}{\approx} 1-\int_0^{(n-1)\tau}\int_0^{(n-1)\tau}\mathbb{P}\Big(|h_{S,R_b}|^2\ge\gamma x, |h_{R_b,D}|^2\ge\gamma y\Big) \\ \times\hat{f}(x)\hat{f}(y)dydx$$
$$\overset{(c)}{=} 2\int_0^{(n-1)\tau}\int_0^x\bigg\{(1-e^{-2\gamma x})^n \\ -ne^{-\gamma x}\Big[\varphi(n,\gamma y)-\varphi(n,\gamma x)\Big]\bigg\}\hat{f}(x)\hat{f}(y)dydx$$
$$=2\int_0^{(n-1)\tau}\int_0^x g(n,\gamma,x)\hat{f}(x)\hat{f}(y)dydx \\ -2\int_0^{(n-1)\tau}\int_0^x ne^{-\gamma x}\varphi(n,\gamma y)\hat{f}(x)\hat{f}(y)dydx$$
$$=2\int_0^{(n-1)\tau}g(n,\gamma,x)\hat{f}(x)\left[\Phi(\frac{x-\mu}{\sigma})-\Phi(-\frac{\mu}{\sigma})\right]dx \\ -2\int_0^{(n-1)\tau}\int_0^x ne^{-\gamma x}\varphi(n,\gamma y)\hat{f}(x)\hat{f}(y)dydx,$$

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 (2), we first need to derive the probability $\mathbb{P}\Big(\bigcap_{i=1}^m\Big\{\frac{|h_{S,E_i}|^2}{\sum_{j\in\mathcal{R}_1}|h_{R_j,E_i}|^2}<\gamma_e\Big\}\Big)$.

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

$$\mathbb{P}\Big(\bigcap_{i=1}^m\Big\{\frac{|h_{S,E_i}|^2}{\sum_{j\in\mathcal{R}_1}|h_{R_j,E_i}|^2}<\gamma_e\Big\}\Big) \quad (7)$$
$$=\sum_{l=0}^{n-1}\mathbb{P}\Big(\bigcap_{i=1}^m\Big\{\frac{|h_{S,E_i}|^2}{\sum_{j\in\mathcal{R}_1}|h_{R_j,E_i}|^2}<\gamma_e\Big\}\Big|B_l\Big)\mathbb{P}(B_l)$$
$$\overset{(d)}{=}\sum_{l=0}^{n-1}\prod_{i=1}^m\mathbb{P}\Big(\frac{|h_{S,E_i}|^2}{\sum_{j\in\mathcal{R}_1}|h_{R_j,E_i}|^2}<\gamma_e\Big|B_l\Big)\mathbb{P}(B_l)$$
$$\overset{(e)}{=}\sum_{l=0}^{n-1}\prod_{i=1}^m\mathbb{E}\left[1-e^{-\gamma_e\sum_{j\in\mathcal{R}_1}|h_{R_j,E_i}|^2}\right]\mathbb{P}(B_l)$$
$$\overset{(f)}{=}\sum_{l=0}^{n-1}\prod_{i=1}^m\left(1-\prod_{j\in\mathcal{R}_1}\mathbb{E}\left[e^{-\gamma_e|h_{R_j,E_i}|^2}\right]\right)\mathbb{P}(B_l)$$
$$=\sum_{l=0}^{n-1}\left[1-\left(\frac{1}{1+\gamma_e}\right)^l\right]^m\binom{n-1}{l}(1-e^{-\tau})^l(e^{-\tau})^{n-1-l}$$
$$=\sum_{l=0}^{n-1}\sum_{k=1}^m\binom{m}{k}(-1)^k\binom{n-1}{l}c^{lk}(1-e^{-\tau})^l(e^{-\tau})^{n-1-l}$$
$$\overset{(g)}{=}\sum_{k=1}^m\binom{m}{k}(-1)^k\Big[(1-e^{-\tau})c^k+e^{-\tau}\Big]^{n-1}$$

where (d) 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.1 with random relay selection scheme. The TOP P_{ran}^{to} and SOP P_{ran}^{so} can be given by

$$P_{ran}^{to} = 1 - \left(e^{-\tau} + \frac{1 - e^{-(1+\gamma)\tau}}{1+\gamma}\right)^{2n-2} \tag{8}$$

and

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

where $c = \frac{1}{1+\gamma_e}$.

Remark 2: The distributions of I_1 and I_2 are not used in determining the P_{ran}^{to} 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_{ran}^{so} in (9) is identical to P_{bst}^{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 ε_s and reliability requirement ε_t. 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 τ is a critical parameter in determining the eavesdropper-tolerance capability. Too large τ will do harm to the end-to-end transmission, while too small τ is not enough to interfere the eavesdroppers. Therefore, finding a optimal τ is the key to solving our considered problem. Before solving the problem, we establish the following lemma based on the Stochastic Ordering in [37].

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

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

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

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

Lemma 5: The TOP P_{bst}^{to} for opportunistic relaying scheme increases as τ increases.

Proof: For any $0 < \tau_1 < \tau_2$, we use random vector $\mathbf{I}_1 = (I_1^1, I_2^1)$ to represent the interferences in two phases when the noise-generating threshold is τ_1 and $\mathbf{I}_2 = (I_1^2, I_2^2)$ to represent those interferences for τ_2. For any upper set $U = \big\{(I_1, I_2) \big| I_1 \ge x \ge 0, I_2 \ge y \ge 0\big\}$, we always have

$$\mathbb{P}(\mathbf{I}_1 \in U) = \mathbb{P}(I_1^1 \ge x)\mathbb{P}(I_2^1 \ge y)$$

and

$$\mathbb{P}(\mathbf{I}_2 \in U) = \mathbb{P}(I_1^2 \ge x)\mathbb{P}(I_2^2 \ge y).$$

It is easy to see that $\mathbb{P}(I_1^1 \ge x) < \mathbb{P}(I_1^2 \ge x)$ and $\mathbb{P}(I_2^1 \ge y) < \mathbb{P}(I_2^2 \ge y)$, since more interference can be generated as τ increases. Therefore, we have $\mathbb{P}(\mathbf{I}_1 \in U) < \mathbb{P}(\mathbf{I}_2 \in U)$ and then $\mathbf{I}_1 \le_{st} \mathbf{I}_2$ according to Lemma 4. Define the term $\mathbb{P}\left(|h_{S,R_b}|^2 \ge \gamma I_1, |h_{R_b,D}|^2 \ge \gamma I_2\right)$ in (6) by $\Gamma(\mathbf{I})$ which decreases as $\mathbf{I}$ increases, where $\mathbf{I} = (I_1, I_2)$. 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 $P_{bst}^{to}(\tau_1) < P_{bst}^{to}(\tau_2)$, which indicates the TOP P_{bst}^{to} increases with τ. ■

Lemma 6: The SOP P_{bst}^{so} for opportunistic relaying scheme decreases as τ 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 $0 \le \tau_1 < \tau_2$, we use two random variables $|\mathcal{R}_1^1|$ and $|\mathcal{R}_1^2|$ to represent the number of noise-generating relays in the first phase, where

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

and

$$|\mathcal{R}_1^2| \sim B(n-1, 1-e^{-\tau_2}).$$

It is shown in [38] that $|\mathcal{R}_1^1| \le_{st} |\mathcal{R}_1^2|$. Applying Lemma 4 again, we can see that

$$\mathbb{E}\left[1 - \left(\frac{1}{1+\gamma_e}\right)^{|\mathcal{R}_1^1|}\right] < \mathbb{E}\left[1 - \left(\frac{1}{1+\gamma_e}\right)^{|\mathcal{R}_1^2|}\right]$$

Therefore, the SOP P_{bst}^{so} decreases as τ increases.

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

$$1 - (\frac{1}{1+\gamma_e})^l \in [0, 1).$$

Thus, the term $\left[1 - \left(\frac{1}{1+\gamma_e}\right)^l\right]^m$ decreases with m. Therefore, the SOP P_{bst}^{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 ε_s and reliability constraint ε_t is

$$m^*_{bst} = max\{m : G(m,n,\tau^b_{bst}) \geq \sqrt{1-\varepsilon_s}\}, \quad (10)$$

where

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

$c = \frac{1}{1+\gamma_e}$ and τ^b_{bst} is the solution of $P^{to}_{bst} = \varepsilon_t$.

Proof: As shown in (3), we need to find the optimal τ 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^{to}_{bst} increases with τ according to Lemma 5, in order to guarantee the reliability (i.e., $P^{to}_{bst} \leq \varepsilon_t$), τ must take values in the region $[0,\tau_m]$, where τ_m is the solution of $P^{to}_{bst} = \varepsilon_t$.

Next, we need to prove that τ_m is the optimal τ (i.e.,$\tau^b_{bst} = \tau_m$). 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 $M_{bst}(\tau') \geq M_{bst}(\tau_m)+1$. 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 τ, 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

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

We can see that the above two inequalities are contradictory. Thus, for any $\tau \in [0,\tau_m)$ we always have $M_{bst}(\tau) \leq M_{bst}(\tau_m)$ (i.e., $\tau^b_{bst} = \tau_m$) and thus the eavesdropper-tolerance capability is $m^*_{bst} = M_{bst}(\tau^b_{bst})$. ∎

B. Eavesdropper-Tolerance Capability for Random Relay Selection

Applying the same approach, we can establish the following lemma regarding the eavesdropper-tolerance capability for random relay selection.

Lemma 7: Consider the network scenario in Fig.1 with random relay selection scheme. The eavesdropper-tolerance capability under the security constraint ε_s and reliability constraint ε_t is

$$m^*_{ran} = max\{m : G(m,n,\tau^b_{ran}) \geq \sqrt{1-\varepsilon_s}\}, \quad (11)$$

where

$$G(m,n,\tau^b_{ran}) = \sum_{k=1}^{m}\binom{m}{k}(-1)^k\left[(1-e^{-\tau^b_{ran}})c^k + e^{-\tau^b_{ran}}\right]^{n-1},$$

$c = \frac{1}{1+\gamma_e}$ and τ^b_{ran} is the solution of

$$e^{-\tau} + \frac{1-e^{-(1+\gamma)\tau}}{1+\gamma} = (1-\varepsilon_t)^{\frac{1}{2n-2}}.$$

Remark 3: Although the exact expressions for m^*_{bst} and m^*_{ran} are not available, it is easy to calculate them numerically due to the monotonicity of $G(m,n,\tau)$ with respect to m, after calculating the corresponding optimal noise-generating threshold τ for these two relay selection schemes.

V. Numerical Results and Discussion

In this section, we first verify our theoretical model for TOP and SOP through extensive simulations. We then explore how the number of relays n, the *SIR* thresholds γ, γ_e, the security constraint ε_s and the reliability constraint ε_t affect the eavesdropper-tolerance capability for opportunistic relaying scheme. Besides, we illustrate the inherent tradeoffs between the eavesdropper-tolerance capability and security/reliability constraint. Finally, we compare the opportunistic relaying scheme with the random relay selection scheme with respect to the eavesdropper-tolerance capability.

A. Model Validation

A simulator was developed in C++ to simulate the message transmission from the source S to the destination D based on the transmission scheme in section II-A, which is now available at [39]. The *SIR* threshold for legitimate receivers is fixed as $\gamma = 10$ and that for eavesdroppers is fixed as $\gamma_e = 0.5$. The total number of end-to-end transmissions is fixed as 100000. The channel varies randomly and independently from one transmission to another. The simulated TOP (SOP) is calculated as the ratio of the number of transmissions suffering from transmission outage (secrecy outage) to the total number 100000. Notice that the simulations with other settings can be easily performed by our simulator as well.

Extensive simulations have been conducted to verify our TOP and SOP models. For the TOP, we considered three different network scenarios of $\tau = 0.05$, 0.075 and 0.1, which correspond to low interference, moderate interference and high interference compared to the considered network size. For the SOP, we also considered three different network scenarios of $(m = 100, \tau = 0.05)$, $(m = 100, \tau = 0.1)$ and $(m = 500, \tau = 0.05)$, which correspond to sparse eavesdroppers with low interference, sparse eavesdroppers with high interference, and dense eavesdroppers with low interference. The corresponding simulated results and theoretical results are summarized in Fig. 2 and Fig.3.

Fig.2 and Fig.3 indicate clearly that the simulated results match nicely with the theoretical ones for both TOP and SOP, so our theoretical model can be used to efficiently explore the eavesdropper-tolerance capability. A further careful observation of Fig.2 shows that there is still a very small gap between the simulated results and the theoretical results when the number of relays n is very small. For example, for the case that $\tau = 0.075$, the simulated value for P^{to}_{bst} is 0.10314 while the theoretical value is 0.07329 for $n = 30$, compared to the simulated value of 0.46626 and theoretical value of

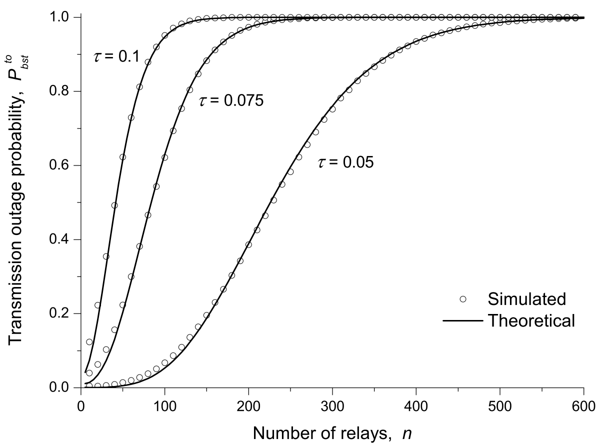

Fig. 2. TOP for opportunistic relaying P_{bst}^{to} vs. number of relays n with different settings of τ, when $\gamma = 10$.

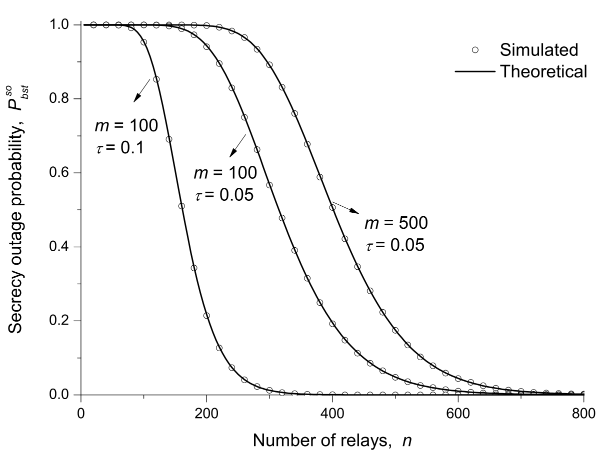

Fig. 3. SOP for opportunistic relaying P_{bst}^{so} vs. number of relays n with different settings of m and τ, when $\gamma_e = 0.5$.

0.46645 for $n = 80$. This is because that the Central Limit Theorem used in deriving our theoretical result fails to model the pdf of the total interference I_1 and I_2 very well for small values of n. We can see from Fig.2 that P_{bst}^{to} increases with n. This suggests that although the best relay selection scheme can benefit the transmission as n increases, the interferences from the noise-generating relays dominate the tendency of the received SIR at legitimate receivers. By comparing these three curves in Fig.2, it can also be observed that P_{bst}^{to} increases as τ increases, which agrees with Lemma 5. This is due to the reason that more interferences will be generated at the intended receiver for lager τ, and thus it is more difficult for the receivers to successfully recover the messages.

We can see from Fig.3 that P_{bst}^{so} decreases as n increases. This is because more interferences can be generated at the eavesdroppers by distributing more relays for a specific τ. By comparing these three curves in Fig.3, it can also be observed that P_{bst}^{so} increases as m increases while decreases

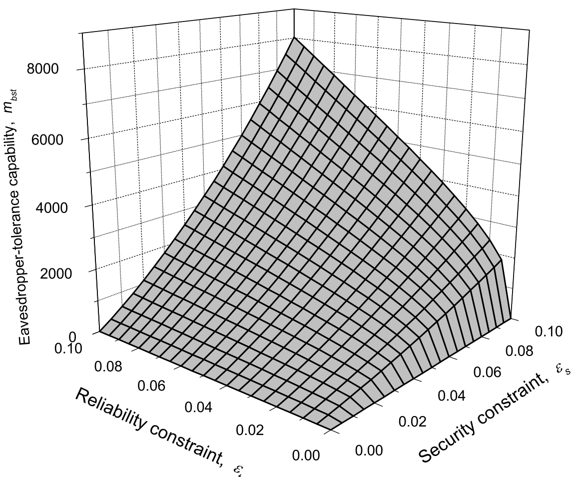

Fig. 4. Eavesdropper-tolerance capability m_{bst}^{*} for opportunistic relaying vs. reliability constraint ε_t and security constraint ε_s with $n = 2000$, $\gamma = 10$ and $\gamma_e = 0.5$.

as τ 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 τ would generate more interferences at the eavesdroppers, so it is more difficult for them to successfully decode the messages.

B. Eavesdropper-tolerance Performances

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}^{*} vs. ε_t and ε_s for the network scenario of $n = 2000, \gamma = 10, \gamma_e = 0.5$, which implies that the eavesdroppers have a much better decoding ability than the legitimate receivers. We can observe from Fig.4 that m_{bst}^{*} increases as ε_t and ε_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 ε_t increases as ε_s decreases in order to guarantee a certain level of eavesdropper-tolerance capability. For example, ε_t has to increase from 0.04 to 0.085 as ε_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 m_{bst}^{*} vs. n in Fig.5 with $\varepsilon_t = 0.01$ and $\varepsilon_s = 0.01$ for different settings of γ and γ_e. It can be observed from Fig.5 that m_{bst}^{*} increases as n increases. This is because that although the optimal threshold τ_{bst}^{b} decreases as n increase for a specific reliability

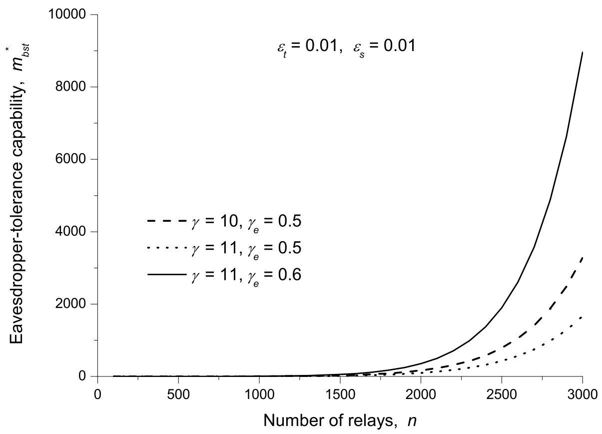

Fig. 5. Eavesdropper-tolerance capability m^*_{bst} for opportunistic relaying vs. number of relays n with $\varepsilon_t = 0.01$, and $\varepsilon_s = 0.01$.

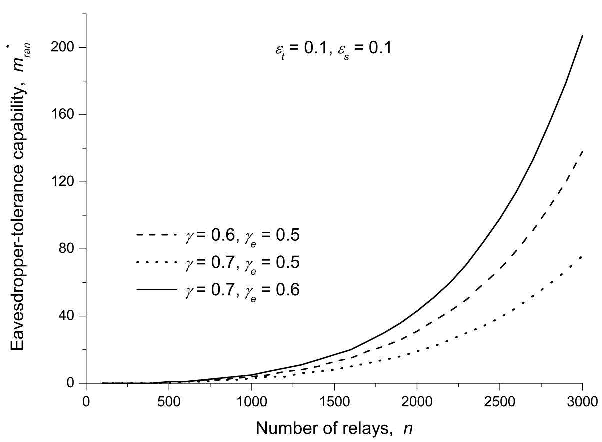

Fig. 6. Eavesdropper-tolerance capability m^*_{ran} for random relay selection vs. number of relays n with $\varepsilon_t = 0.1$, and $\varepsilon_s = 0.1$.

constraint ε_t, the corresponding expected number of noise-generating nodes increases, so more interferences can be generated to suppress the eavesdroppers while the desired reliability can still be ensured. By comparing the three curves, we can also observe that m^*_{bst} increases as γ_e increases, while decreases as γ increases. This is intuitive since decreasing the decoding ability (i.e.,increasing γ_e) of the eavesdroppers would decrease the SOP, while decreasing the decoding ability (i.e.,increasing γ) of legitimate receivers would increase the TOP. It is interesting to notice that m^*_{bst} increases dramatically when n is above some threshold in Fig.5. For example, for the case that $\gamma = 11$ and $\gamma_e = 0.6$ this threshold is about 2500. Thus, distributing more relays would be an efficient approach to enhance the eavesdropper-tolerance capability in the construction of a network.

In order to explore the efficiency of the opportunistic relaying scheme, we also illustrate the eavesdropper-tolerance capability m^*_{ran} of random relay selection scheme vs. the number of relays n in Fig.6 with $\varepsilon_t = 0.1$ and $\varepsilon_s = 0.1$ for different setting of γ and γ_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^*_{ran} also increases as γ_e increases, while decreases as γ 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.6 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 γ, it will decreases to 0 if we increases γ 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 τ 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. Fist, we define a function

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

where

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

is an indicator function and then I_1 can be formulated as

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

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

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

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

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

and

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

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

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

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 $0 \le k \le n-2$. 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

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

where

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

and

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

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 $min\{|h_{S,R_j}|^2, |h_{R_j,D}|^2\}$ for each relay R_j. It is notable that $S_j, j = 1, \cdots, n$ is an exponential random variable with mean $\frac{1}{2}$. Then, we have

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

Now, applying the law of total probability, we have

$$\begin{aligned}
&\mathbb{P}\Big(|h_{S,R_b}|^2 \ge x, |h_{R_b,D}|^2 \ge y\Big) \qquad (12)\\
&= \sum_{k=1}^{n} \mathbb{P}\left(|h_{S,R_k}|^2 \ge x, |h_{R_k,D}|^2 \ge y, A_k\right)\\
&= \sum_{k=1}^{n} \mathbb{P}\left(|h_{S,R_k}|^2 \ge x, |h_{R_k,D}|^2 \ge y, \bigcap_{j=1,j\neq k}^{n} (S_j \le S_k)\right)\\
&\overset{(h)}{=} \sum_{k=1}^{n} \int_0^\infty \mathbb{P}\Bigg(|h_{S,R_k}|^2 \ge x, |h_{R_k,D}|^2 \ge y,\\
&\quad S_k = s, \bigcap_{j=1,j\neq k}^{n} (S_j \le s)\Bigg) ds\\
&= \sum_{k=1}^{n} \int_0^\infty \mathbb{P}\Big(|h_{S,R_k}|^2 \ge x, |h_{R_k,D}|^2 \ge y, S_k = s\Big)\\
&\quad \times \mathbb{P}\left(\bigcap_{j=1,j\neq k}^{n} (S_j \le s)\right) ds\\
&= \sum_{k=1}^{n} \int_0^\infty \mathbb{P}\Big(|h_{S,R_k}|^2 \ge x, |h_{R_k,D}|^2 \ge y, S_k = s\Big)\\
&\quad \times (1 - e^{-2s})^{n-1} ds,
\end{aligned}$$

where (h) integrates over all the values S_k can take.

When $x \ge y \ge 0$, (12) can be reduced to

$$\begin{aligned}
&\mathbb{P}\Big(|h_{S,R_b}|^2 \ge x, |h_{R_b,D}|^2 \ge y\Big) \qquad (13)\\
&= \sum_{k=1}^{n} \Bigg\{ \int_x^\infty \mathbb{P}\Big(|h_{S,R_k}|^2 = s, |h_{R_k,D}|^2 \ge s\Big)(1 - e^{-2s})^{n-1} ds\\
&\quad + \int_y^x \mathbb{P}\Big(|h_{S,R_k}|^2 > x, |h_{R_k,D}|^2 = s\Big)(1 - e^{-2s})^{n-1} ds\\
&\quad + \int_x^\infty \mathbb{P}\Big(|h_{S,R_k}|^2 > s, |h_{R_k,D}|^2 = s\Big)(1 - e^{-2s})^{n-1} ds \Bigg\}\\
&= 2n \int_x^\infty \frac{(1 - e^{-2s})^{n-1}}{e^{2s}} ds + n e^{-x} \int_y^x \frac{(1 - e^{-2s})^{n-1}}{e^{s}} ds\\
&= 1 - (1 - e^{-2x})^{n-1} + n e^{-x} \int_{e^{-x}}^{e^{-y}} (1 - t^2)^{n-1} dt\\
&= 1 - (1 - e^{-2x})^{n-1} + n e^{-x} \Big[\varphi(n, y) - \varphi(n, x)\Big],
\end{aligned}$$

where

$$\varphi(n, x) = e^{-x} {}_2F_1\left(\frac{1}{2}, 1-n; \frac{3}{2}; e^{-2x}\right)$$

and ${}_2F_1$ is the Gaussian hypergeometric function.

Similarly, when $0 \le x < y$, (12) can be reduced to

$$\begin{aligned}
&P\Big(|h_{S,R_b}|^2 \ge x, |h_{R_b,D}|^2 \ge y\Big) \qquad (14)\\
&= 1 - (1 - e^{-2y})^{n-1} + n e^{-y} \Big[\varphi(n, x) - \varphi(n, y)\Big]
\end{aligned}$$

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

References

[1] S. Narayanan and P. University, *Two-hop Forwarding in Wireless Networks*. Polytechnic University, 2006.

[2] W. Stallings, *Creptography and network security: principles and practice*, 5th ed. Prentice Hall, January 2010.

[3] Y. Xie, S. Tang, Y. Xiang, and J. Hu, "Resisting web proxy-based http attacks by temporal and spatial locality behavior," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 24, no. 7, pp. 1401–1410, 2013.

[4] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[5] P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*, 1994, pp. 124–134.

[6] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2515–2534, 2008.

[7] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *CoRR*, vol. abs/1011.3754, 2010. [Online]. Available: http://arxiv.org/abs/1011.3754

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

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

[10] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[11] U. Maurer, "Secret key agreement by public discussion from common information," *Information Theory, IEEE Transactions on*, vol. 39, no. 3, pp. 733–742, 1993.

[12] A. Hero, "Secure space-time communication," *Information Theory, IEEE Transactions on*, vol. 49, no. 12, pp. 3235–3249, 2003.

[13] R. Negi and S. Goel, "Secret communication using artificial noise," in *IEEE Vehicular Technology Conference*, 2005, pp. 1906–1910.

[14] S. Goel and R. Negi, "Secret communication in presence of colluding eavesdroppers," in *IEEE Military Communications Conference*, 2005, pp. 1501–1506.

[15] J. Barros and M. R. Rodrigues, "Secrecy capacity of wireless channels," in *IEEE International Symposium on Information Theory*, 2006, pp. 356–360.

[16] E. Tekin and A. Yener, "The general gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2735–2751, 2008.

[17] X. Zhou, R. Ganti, J. Andrews, and A. Hjørungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun*, vol. 10, no. 8, pp. 2764–2775, 2011.

[18] C. Capar, D. Goeckel, B. Liu, and D. Towsley, "Secret communication in large wireless networks without eavesdropper location information," in *INFOCOM, 2012 Proceedings IEEE*, 2012, pp. 1152–1160.

[19] L. Dong, Z. Han, A. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process*, vol. 58, pp. 1875–1888, 2010.

[20] J. Li, A. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *Signal Processing, IEEE Transactions on*, vol. 59, no. 10, pp. 4985–4997, 2011.

[21] B. Han and J. Li, "Secrecy capacity maximization for secure cooperative ad-hoc networks," in *INFOCOM, 2013 Proceedings IEEE*, 2013, pp. 2796–2804.

[22] J. Vilela, M. Bloch, J. Barros, and S. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 2, pp. 256–266, 2011.

[23] J. Vilela, P. Pinto, and J. Barros, "Position-based jamming for enhanced wireless secrecy," *Information Forensics and Security, IEEE Transactions on*, vol. 6, no. 3, pp. 616–627, 2011.

[24] J. Huang and A. Swindlehurst, "Cooperative jamming for secure communications in mimo relay networks," *IEEE Transactions on Signal Processing*, vol. 59, no. 10, pp. 4871–4884, 2011.

[25] I. Krikidis, J. Thompson, and S. Mclaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun*, vol. 8, no. 10, pp. 5003–5011, 2009.

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

[27] R. Bassily and S. Ulukus, "Deaf cooperation and relay selection strategies for secure communication in multiple relay networks," *Signal Processing, IEEE Transactions on*, vol. 61, no. 6, pp. 1544–1554, 2013.

[28] S. Vasudevan, D. Goeckel, and D. Towsley, "Security-capacity trade-off in large wireless networks using keyless secrecy," in *ACM international symposium on Mobile ad hoc networking and computing*, 2010, pp. 21–30.

[29] M. Haenggi, "The secrecy graph and some of its properties," in *IEEE International Symposium on Information Theory*, 2008, pp. 539–543.

[30] Y. Liang, H. Poor, and L. Ying, "Secrecy throughput of manets under passive and active attacks," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6692–6702, 2011.

[31] D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 29, pp. 2067–2076, 2011.

[32] A. Bletsas, S. Khisti, D. Reed, and A. Lippman, "A simple cooperative diversity method based on network path selection," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 3, pp. 659–672, Mar. 2006.

[33] A. Sheikholeslami, D. Goeckel, H. Pishro-Nik, and D. Towsley, "Physical layer security from inter-session interference in large wireless networks," in *Proceeding of IEEE INFOCOM 2012*, 2012, pp. 1179–1187.

[34] Y. Shen, X. Jiang, and J. Ma, "Flexible relay selection for secure communication in two-hop wireless networks," in *Modeling Optimization in Mobile, Ad Hoc Wireless Networks (WiOpt), 2013 11th International Symposium on*, 2013, pp. 648–651.

[35] Y. Zhang, Y. Shen, and X. Jiang, "Eavesdropper tolerance capability study in two-hop cooperative wireless networks," in *2013 2nd IEEE/CIC International Conference on Communications in China (ICCC): QRS: QoS, Reliability and Security*, 2013, pp. 219–223.

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

[37] M. Shaked and J. Shanthikumar, *Stochastic orders*, 1st ed., ser. Springer Series in Statistics. Springer, Nov. 2010.

[38] A. Klenke and L. Mattner, "Stochastic ordering of classical discrete distributions," *Advances in Applied Probability*, vol. 42(2), pp. 393–410, 2010.

[39] C++ simulator for two-hop transmission with cooperative jamming and opportunistic relaying. [Online]. Available: http://mdlval.blogspot.jp/