Secure Routing in Multihop Wireless Ad-hoc Networks with Decode-and-Forward Relaying

Jianping Yao, Suili Feng, *Member, IEEE*, Xiangyun Zhou, *Member, IEEE*, and Yuan Liu, *Member, IEEE*

***Abstract*—In this paper, we study the problem of secure routing in a multihop wireless ad-hoc network in the presence of randomly distributed eavesdroppers. Specifically, the locations of the eavesdroppers are modeled as a homogeneous Poisson point process (PPP) and the source-destination pair is assisted by intermediate relays using the decode-and-forward (DF) strategy. We analytically characterize the physical layer security performance of any chosen multihop path using the end-to-end secure connection probability (SCP) for both colluding and non-colluding eavesdroppers. To facilitate finding an efficient solution to secure routing, we derive accurate approximations of the SCP. Based on the SCP approximations, we study the secure routing problem which is defined as finding the multihop path having the highest SCP. A revised Bellman-Ford algorithm is adopted to find the optimal path in a distributed manner. Simulation results demonstrate that the proposed secure routing scheme achieves nearly the same performance as exhaustive search.**

***Index Terms*—Secure connection, physical layer security, multihop routing, homogeneous Poisson point process (PPP), decode-and-forward (DF).**

I. Introduction

NETWORK security is a fundamental issue of communication systems. For wireless networks, secure communication is more challenging due to the broadcast nature of wireless channels. The traditional approach for secure communication is to employ the cryptographic algorithms. Recently, physical layer security has emerged as a complementary technology to the cryptography-based method, which can achieve perfect secrecy by properly designing the encoder-decoder of transceivers according to the channel conditions [1], [2].

Following the recent advances in cooperative communications, physical layer security in relay networks has captured considerable attention [3]–[14]. Relay nodes can achieve cooperative diversity by forwarding information or act as cooperative jammers to degrade eavesdroppers' channel conditions, and thus improve the security of legitimate transmission. As an example, the authors in [3] addressed the secure problem of one source-destination pair with the help of multiple cooperating relays in the presence of one or more eavesdroppers, where three cooperative schemes are considered: decode-and-forward (DF), amplify-and-forward (AF), and cooperative jamming (CJ). The authors in [4] investigated the distributed beamforming of AF relay network with an external eavesdropper. The authors in [5] studied the secure beamforming design in a multiple-antenna relay system for maximizing the secrecy sum rate, where the relay is also an internal eavesdropper. The authors in [6] studied the secure connection probability (SCP) for DF and randomize-and-forward (RaF) relaying strategies where a connection is called secure if the secrecy rate of this connection is positive, as defined in [15]. RaF relaying deviates from the widely-used DF relaying in the way that the relays add independent randomization in each hop when re-encode the received signal [16]. The authors in [7] performed a comprehensive study on the secure transmission in both DF and RaF two-hop relay networks with only channel distribution information of the wiretap channels, where both the fixed-rate and adaptive-rate transmission at the source and relay nodes were considered. The authors in [8] derived the intercept probability expressions of optimal relay selection, and the diversity orders of AF and DF were analyzed. The authors in [9] analyzed the relationship between the secrecy performance and the tolerated number of eavesdroppers. The authors in [10] proposed a tree-formation game to choose secure paths in uplink multihop cellular networks. The authors in [11] considered minimum energy routing in the presence of multiple malicious jammers such that an acceptable end-to-end probability of outage is guaranteed.

A commonly-used assumption in the physical layer security literature is that the channel state information (CSI) or (at least) locations of eavesdroppers are available at legitimate users. To relax such an assumption and take into account the uncertainty of the eavesdroppers' locations, the distribution of the eavesdroppers' locations can be modeled as homogeneous Poisson point processes (PPPs) [17]–[22]. The authors in [17] defined the secrecy transmission capacity to study the

Manuscript received May 26, 2015; revised September 30, 2015, and December 11, 2015; accepted December 22, 2015. This work is supported in part by the National Natural Science Foundation of China under Grants 61340035 and 61401159, in part by the Science & Technology Program of Guangzhou under Grant 2014J4100246, in part by the State Key Laboratory of Integrated Services Networks, Xidian University, under Grant ISN16-02, in part by the Open Research Fund through the National Mobile Communications Research Laboratory, Southeast University, Nanjing, China, under Grant 2016D06, and in part by the Fundamental Research Funds for the Central Universities. This work of X. Zhou was supported by the Australian Research Council under Discovery Projects Grant DP150103905. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. J. Yuan.

J. Yao is with the School of Electrical and Information Engineering, South China University of Technology, Guangzhou 510641, China, and also with the State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China (e-mail: yaojp_scut@qq.com).

S. Feng is with the School of Electrical and Information Engineering, South China University of Technology, Guangzhou 510641, China (e-mail: fengsl@scut.edu.cn).

X. Zhou is with the Research School of Engineering, The Australian National University, Canberra, ACT 0200, Australia (e-mail: xiangyun.zhou@anu.edu.au).

Y. Liu is with the School of Electronic and Information Engineering, South China University of Technology, Guangzhou 510641, China, and also with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (e-mail: eeyliu@scut.edu.cn).

impact of security requirements on throughput in large-scale decentralized networks consisting of PPP distributed legitimate nodes and eavesdroppers. The authors in [18] analyzed the secrecy rates by using regularized channel inversion precoding. The authors in [19] studied the outage performance based on imperfect CSI. The authors in [20] proposed a relay selection strategy to improve the SCP, where the locations of both the relays and eavesdroppers follow homogeneous PPPs.

From the above discussions, we find that the problem of secure routing in wireless multihop networks is still largely an open problem. Existing work on secure routing, such as [10], assumed that the CSI or locations of the eavesdroppers are known to the legitimate users, which is often impractical, especially in ad hoc networks enabled by multihop communications. In practice, the eavesdroppers usually work in a passive way, i.e. they just try to overhear as much information as possible conveyed from the legitimate nodes and they do not attempt to actively thwart (i.e. via jamming, signal insertion) the legitimate nodes. In order to statistically characterize the secrecy performance of such scenarios, a PPP is used to statistically model the locations of the eavesdroppers. In this work, we study secure routing in a large-scale multihop wireless network in the presence of randomly-distributed eavesdroppers whose CSI and locations are unknown to the legitimate users. Both colluding and non-colluding eavesdropper scenarios are analyzed. We assume that the intermediate relay nodes use the DF protocol which is the default relaying strategy in wireless ad hoc networks. We assume that the relays use the same codeword as the source, which is a worse-case scenario from security point of view, and hence, is a commonly-used benchmarking scenario in the literature [23]–[25]. With DF relaying, the eavesdroppers can intercept information from multiple hops by maximal-ratio combining. This directly affects the secure routing solutions, e.g., more hops may lead to worse secrecy performance. In passive eavesdropping scenarios, perfect secrecy cannot be guaranteed since the CSI and location of the eavesdroppers are not available at the transmitters. Hence, we adopt the SCP as useful secrecy metrics to characterize the secrecy performance.

The main contributions of this paper are summarized as follows:

- For a given path from the source to its destination, we derive exact expressions of SCP for both colluding and non-colluding eavesdroppers, which are used to measure the secrecy performance of that path. Having the exact SCP expressions enables us to analyze and compare the performance of different secure routing solutions.
- In order to facilitate finding the secure routing algorithm, we first obtain approximations of the SCP. Based on the SCP approximations, the classical Bellman-Ford routing algorithm is adopted to find the highest SCP path between any given source-to-destination pair in a distributed way.
- We conduct simulations to verify the analytical results on SCP and show the effectiveness of the proposed secure routing algorithm. The numerical results show that the proposed secure routing algorithm performs closely to the exhaustive search.

The remainder of this paper is organized as follows. In Section II, the system model and performance metric are described. In Section III, the exact expressions of SCP for both colluding and non-colluding eavesdroppers are analyzed. In Section IV, we obtain the approximations of SCP, then the secure routing algorithms are derived. In Section V, we present numerical results. Finally, the conclusion is provided in Section VI.

II. System Model and Metric

We consider a large-scale multihop wireless network with arbitrarily distributed relay nodes and eavesdroppers. We assume that all nodes are equipped with a single omni-directional antenna. An N-hop route in the network is a sequence of legitimate nodes $(\{A_i\}, i = 1, \ldots, N+1)$. We assume that every link of the route is exposed to a set of eavesdroppers $(\{E_j\}, j = 1, 2, \ldots)$ denoted by Φ_E. The eavesdroppers are randomly distributed in the network according to a homogeneous PPP with density λ_E. We assume that the eavesdroppers are passive and thus their CSI as well as locations are unknown to the legitimate nodes. We assume that the legitimate nodes (including source, relay and destination nodes) know the distances between each other. The transmitter of every hop uses a separate slot to transmit the message. We assume that all the channels are modeled by large-scale fading with path loss exponent α along with small-scale Rayleigh fading. Each node A_{i+1} only receives information from its former node A_i. The instantaneous received signal-to-noise (SNR) at the legitimate node A_{i+1} and eavesdropper E_j can be respectively given as

$$\mathtt{SNR}_{A_iA_{i+1}} = \frac{p_{A_i}|h_{A_iA_{i+1}}|^2}{d^{\alpha}_{A_iA_{i+1}}}, \tag{1}$$

$$\mathtt{SNR}_{A_iE_j} = \frac{p_{A_i}|h_{A_iE_j}|^2}{d^{\alpha}_{A_iE_j}}, \tag{2}$$

where p_{A_i} denotes the transmit power of the legitimate node A_i; $d_{A_iA_{i+1}}$ and $h_{A_iA_{i+1}}$ represent the distance and channel coefficient between nodes A_i and A_{i+1}, respectively; $d_{A_iE_j}$ and $h_{A_iE_j}$ represent the distance and channel coefficient between nodes A_i and E_j, respectively. We assume that $|h_{A_iA_{i+1}}|^2$ and $|h_{A_iE_j}|^2$ follow exponential distributions with mean equal to one. Then according to [15], the achievable secrecy rate of a single-hop link A_iA_{i+1} is

$$\left[\log_2\left(1+\mathtt{SNR}_{A_iA_{i+1}}\right) - \log_2\left(1+\mathtt{SNR}_{A_iE}\right)\right]^+, \tag{3}$$

where $[x]^+ = \max(x, 0)$; $\mathtt{SNR}_{A_iE}$ represents the received SNR at eavesdroppers from the legitimate node A_i. For the case of non-colluding eavesdroppers, $\mathtt{SNR}_{A_iE}$ is equivalent to $\max\limits_{E_j\in\Phi_E}\left\{\mathtt{SNR}_{A_iE_j}\right\}$, where the maximization operation means the selection of the eavesdropper which has the strongest received signal. For the case of colluding eavesdroppers, $\mathtt{SNR}_{A_iE}$ is equivalent to $\sum\limits_{E_j\in\Phi_E}\mathtt{SNR}_{A_kE_j}$.

Due to the multihop DF relaying, we consider that the eavesdroppers can combine the information from multiple hops. Then according to the definition of secure connection

$$\frac{1}{N}\left(\log_2\left(1+\min_{i=1,\ldots,N}\left\{\mathtt{SNR}_{A_iA_{i+1}}\right\}\right)-\log_2\left(1+I_E\right)\right)>0. \tag{4}$$

$$\mathcal{P}_{DF}=\mathcal{P}\left(\frac{1}{N}\left(\log_2\left(1+\min_{i=1,\ldots,N}\left\{\mathtt{SNR}_{A_iA_{i+1}}\right\}\right)-\log_2\left(1+I_E\right)\right)>0\right). \tag{5}$$

in [15], we say that a given path is secure if the achievable secrecy rate on this path is positive, i.e. (4) shown at the top of the page is satisfied, where I_E is the combined received SNR at eavesdroppers from the legitimate transmitter. Thus the SCP of a given path can be expressed as (5), given at the top of the page.

For a given path, N is fixed and does not impact the SCP, thus we drop $\frac{1}{N}$ in the analysis on a given path. Then, (5) can be written as

$$\mathcal{P}_{DF}=\mathcal{P}\left(\log_2\left\{\frac{1+\min_{i=1,\ldots,N}\left\{\mathtt{SNR}_{A_iA_{i+1}}\right\}}{1+I_E}\right\}>0\right). \tag{6}$$

Note that in (6), the eavesdropping SNR I_E depends on whether the eavesdroppers are colluding or non-colluding. For the case of the non-colluding eavesdroppers, I_E is the maximum SNR after MRC among all eavesdroppers (where eavesdropper applies MRC to combine signals received from all hops). For the case of the colluding eavesdroppers, I_E is the sum of all SNRs after MRC at all the eavesdroppers. The exact expressions of I_E for the both cases will be given in the next section.

III. Secure Connection Probability of a Given Path

In this section, we derive the exact SCP of a given path for both colluding and non-colluding eavesdroppers.

A. SCP for Colluding Eavesdroppers

For the colluding case, the eavesdroppers can share their eavesdropped information. In this case, all the information obtained by the eavesdroppers can be combined, which is the worst scenario from the security point of view. The combined received SNR at eavesdroppers from all hops is given as

$$\begin{aligned} I_{E\_C} &= \sum_{E_j\in\Phi_E}\sum_{k=1}^{N}\mathtt{SNR}_{A_kE_j} \\ &= \sum_{E_j\in\Phi_E}\sum_{k=1}^{N}\frac{p_{A_k}\left|h_{A_kE_j}\right|^2}{d^{\alpha}_{A_kE_j}}. \end{aligned} \tag{7}$$

Then the SCP in (6) can be rewritten as

$$\mathcal{P}_C=\mathcal{P}\left(\log_2\left(\frac{1+\min_{i=1,\ldots,N}\left\{\frac{p_{A_i}\left|h_{A_iA_{i+1}}\right|^2}{d^{\alpha}_{A_iA_{i+1}}}\right\}}{1+\sum_{E_j\in\Phi_E}\sum_{k=1}^{N}\frac{p_{A_k}\left|h_{A_kE_j}\right|^2}{d^{\alpha}_{A_kE_j}}}\right)>0\right), \tag{8}$$

which is equivalent to (9), shown at the top of the next page.

Since each $|h_{A_iA_{i+1}}|^2$ is independent exponentially distributed random variable with unit mean and independent of Φ_E, and $\min_{i=1,\ldots,N}\left\{\frac{p_{A_i}\left|h_{A_iA_{i+1}}\right|^2}{d^{\alpha}_{A_iA_{i+1}}}\right\}$ is also exponentially distributed with the mean of $\sum_{i=1}^{N}\frac{d^{\alpha}_{A_iA_{i+1}}}{p_{A_i}}$. Then (9) can be derived as (10), written at the top of the next page, where the last step η stands as $\left|h_{A_kE_j}\right|^2$ is independent and identically distributed, thus the expectation over the sum of $\left|h_{A_kE_j}\right|^2$ is equal to the product of the expectation over $\left|h_{A_kE_j}\right|^2$. For a homogeneous PPP, the probability generating functional (PGFL) is given by [26]

$$\mathbb{E}_{\Phi_E}\left[\prod_{E_j\in\Phi_E}f\left(x_{E_j}\right)\right]=\exp\left[-\lambda_E\int_{\mathbb{R}^2}1-f\left(x_{E_j}\right)dx_{E_j}\right], \tag{11}$$

where x_{E_j} is the location of E_j.

Then (10) can be turned to

$$\mathcal{P}_C=\exp\left[-\lambda_E\int_{\mathbb{R}^2}1-\prod_{k=1}^{N}\frac{1}{1+\frac{p_{A_k}}{d^{\alpha}_{A_kE_j}}\sum_{i=1}^{N}\frac{d^{\alpha}_{A_iA_{i+1}}}{p_{A_i}}}dx_{E_j}\right]. \tag{12}$$

B. SCP for Non-Colluding Eavesdroppers

In this subsection, we analyze the SCP for non-colluding eavesdroppers. In this case, the eavesdroppers are non-cooperative, so the performance is limited by the eavesdropper which has the strongest received signal. The combined received SNR at eavesdroppers from all hops can be written as

$$\begin{aligned} I_{E\_N} &= \max_{E_j\in\Phi_E}\left\{\sum_{k=1}^{N}\mathtt{SNR}_{A_kE_j}\right\} \\ &= \max_{E_j\in\Phi_E}\left\{\sum_{k=1}^{N}\frac{p_{A_k}\left|h_{A_kE_j}\right|^2}{d^{\alpha}_{A_kE_j}}\right\}. \end{aligned} \tag{13}$$

As the case of colluding eavesdroppers, we also obtain an exact expression of the SCP under the case of non-colluding eavesdroppers. Similar to (8), we can define the SCP for the case of non-colluding eavesdroppers as (14) at the next page.

Since Φ_E is a homogeneous PPP, (14) can be turned to (15), shown at the next page. Then using (11) and (15), we can get (16), presented at the next page.

According to [27], for a set of independent exponential random variables $X=\{X_1,\ldots,X_n\}$ with the parameters

$$\mathcal{P}_C = \mathcal{P}\left(\min_{i=1,\ldots,N}\left\{\frac{p_{A_i}\left|h_{A_iA_{i+1}}\right|^2}{d^{\alpha}_{A_iA_{i+1}}}\right\} > \sum_{E_j\in\Phi_E}\sum_{k=1}^{N}\frac{p_{A_k}\left|h_{A_kE_j}\right|^2}{d^{\alpha}_{A_kE_j}}\right). \tag{9}$$

$$\begin{aligned}\mathcal{P}_C &= \mathbb{E}_{\substack{h_{A_kE_j}\\k=1,\ldots,N},\Phi_E}\left\{\exp\left[-\left(\sum_{i=1}^{N}\frac{d^{\alpha}_{A_iA_{i+1}}}{p_{A_i}}\right)\left(\sum_{E_j\in\Phi_E}\sum_{k=1}^{N}\frac{p_{A_k}\left|h_{A_kE_j}\right|^2}{d^{\alpha}_{A_kE_j}}\right)\right]\right\}\\ &\overset{\eta}{=} \mathbb{E}_{\Phi_E}\left\{\prod_{E_j\in\Phi_E}\prod_{k=1}^{N}\frac{1}{1+\frac{p_{A_k}}{d^{\alpha}_{A_kE_j}}\sum_{i=1}^{N}\frac{d^{\alpha}_{A_iA_{i+1}}}{p_{A_i}}}\right\}.\end{aligned} \tag{10}$$

$$\begin{aligned}\mathcal{P}_N &= \mathcal{P}\left(\log_2\left(\frac{1+\min_{i=1,\ldots,N}\left\{\frac{p_{A_i}\left|h_{A_iA_{i+1}}\right|^2}{d^{\alpha}_{A_iA_{i+1}}}\right\}}{1+\max_{E_j\in\Phi_E}\left\{\sum_{k=1}^{N}\frac{p_{A_k}\left|h_{A_kE_j}\right|^2}{d^{\alpha}_{A_kE_j}}\right\}}\right)>0\right)\\ &= \mathcal{P}\left(\min_{i=1,\ldots,N}\left\{\frac{p_{A_i}\left|h_{A_iA_{i+1}}\right|^2}{d^{\alpha}_{A_iA_{i+1}}}\right\} > \max_{E_j\in\Phi_E}\left\{\sum_{k=1}^{N}\frac{p_{A_k}\left|h_{A_kE_j}\right|^2}{d^{\alpha}_{A_kE_j}}\right\}\right).\end{aligned} \tag{14}$$

$$\mathcal{P}_N = \mathbb{E}_{\substack{h_{A_iA_{i+1}}\\i=1,\ldots,N},\Phi_E}\left\{\prod_{E_j\in\Phi_E}\mathcal{P}\left(\min_{i=1,\ldots,N}\left\{\frac{p_{A_i}\left|h_{A_iA_{i+1}}\right|^2}{d^{\alpha}_{A_iA_{i+1}}}\right\} > \sum_{k=1}^{N}\frac{p_{A_k}\left|h_{A_kE_j}\right|^2}{d^{\alpha}_{A_kE_j}}\middle| h_{A_iA_{i+1}}, \Phi_E\right)\right\}. \tag{15}$$

$$\mathcal{P}_N = \mathbb{E}_{\substack{h_{A_iA_{i+1}}\\i=1,\ldots,N}}\left\{\exp\left[-\lambda_E\int_{\mathbb{R}^2}\mathcal{P}\left(\min_{i=1,\ldots,N}\left\{\frac{p_{A_i}\left|h_{A_iA_{i+1}}\right|^2}{d^{\alpha}_{A_iA_{i+1}}}\right\} < \sum_{k=1}^{N}\frac{p_{A_k}\left|h_{A_kE_j}\right|^2}{d^{\alpha}_{A_kE_j}}\middle| h_{A_iA_{i+1}}\right)dx_{E_j}\right]\right\}. \tag{16}$$

of $\lambda_{X_i}, i = 1,\ldots,n$, the cumulative distribution function (CDF) of the sum of independent not identical exponentially distributed random variables $Y = \sum_{i=1}^{n} X_i$ is given by

$$\mathcal{P}\{Y < y\} = \sum_{i=1}^{n}\delta_i\left(1-\exp\left[-\lambda_{X_i}y\right]\right), \tag{17}$$

where

$$\delta_i = \prod_{j=1,j\neq i}^{n}\frac{\lambda_{X_j}}{\lambda_{X_j}-\lambda_{X_i}}. \tag{18}$$

Basing on (16) and (17), we obtain the SCP in (19) shown at the top of the next page.

IV. Routing Algorithm

In Section III, we derived the exact expressions of the SCP under the cases of colluding and non-colluding eavesdroppers for any given path. In this section, we obtain approximations of the SCP to facilitate finding the secure routing algorithm. The approximations are shown to be close to the exact SCP in Section V. The simple analytical form of the SCP approximations allows us to derive efficient secure routing algorithms.

A. Approximation of SCP for Colluding Eavesdroppers

Lemma 1: Let $a_k\,(k=1,2,\ldots,n)$ be arbitrary constants and $B_k\,(k=1,2,\ldots,n)$ be arbitrary non-negative constants. Let a be anyone of $\{a_k\}$. For an arbitrary positive integer n,

$$\begin{aligned}&\int_{-\infty}^{\infty}\left(1-\prod_{k=1}^{n}\frac{1}{1+B_k(x+a_k)^{-2}}\right)dx\\ &\geq\int_{-\infty}^{\infty}\left(1-\prod_{k=1}^{n}\frac{1}{1+B_k(x+a)^{-2}}\right)dx.\end{aligned} \tag{20}$$

Proof: See Appendix A. ∎

Applying Lemma 1, we can obtain an upper bound of (12) given in (21) where A can be anyone of $\{A_k\}$, shown at the next page. Then we use the upper bound (21) as an approximation of (12).

B. Approximation of SCP for Non-Colluding Eavesdroppers

In Eq. (19), we derived the exact expression of SCP for the case of non-colluding eavesdroppers, which is applicable for all conditions of legitimate nodes' and eavesdroppers' densities. However, the exact expression has a complex form

$$\mathcal{P}_N = \mathbb{E}_{\substack{h_{A_iA_{i+1}} \\ i=1,\ldots,N}} \left\{ \exp\left[-\lambda_E \int_{\mathbb{R}^2} \sum_{k=1}^{N} \prod_{m=1, m\neq k}^{N} \frac{p_{A_m}^{-1} d_{A_m E_j}^{\alpha}}{p_{A_m}^{-1} d_{A_m E_j}^{\alpha} - p_{A_k}^{-1} d_{A_k E_j}^{\alpha}} \exp\left[-\frac{d_{A_k E_j}^{\alpha}}{p_{A_k}} \min_{i=1,\ldots,N} \left\{ \frac{p_{A_i} \left| h_{A_i A_{i+1}} \right|^2}{d_{A_i A_{i+1}}^{\alpha}} \right\} \right] dx_{E_j} \right] \right\}. \tag{19}$$

$$\mathcal{P}_{C\_approx} = \exp\left[-\lambda_E \int_{\mathbb{R}^2} \left(1 - \prod_{k=1}^{N} \frac{1}{1 + \frac{p_{A_k}}{d_{AE_j}^{\alpha}} \left(\sum_{i=1}^{N} \frac{d_{A_i A_{i+1}}^{\alpha}}{p_{A_i}} \right)} \right) dx_{E_j} \right]. \tag{21}$$

$$\begin{aligned} \mathcal{P}_{N\_approx1} &= \mathbb{E}_{\substack{h_{A_iA_{i+1}} \\ i=1,\ldots,N}} \left\{ \exp\left[-\lambda_E \int_{\mathbb{R}^2} \mathcal{P}\left(\min_{i=1,\ldots,N} \left\{ \frac{p_{A_i} \left| h_{A_i A_{i+1}} \right|^2}{d_{A_i A_{i+1}}^{\alpha}} \right\} < \sum_{k=1}^{N} p_{A_k} \frac{\left| h_{AE_j} \right|^2}{d_{AE_j}^{\alpha}} \middle| h_{\substack{A_iA_{i+1} \\ i=1,\ldots,N}} \right) dx_{E_j} \right] \right\} \\ &= \mathbb{E}_{\substack{h_{A_iA_{i+1}} \\ i=1,\ldots,N}} \left\{ \exp\left[-\lambda_E \int_{\mathbb{R}^2} \exp\left[-\frac{d_{AE_j}^{\alpha}}{\sum_{k=1}^{N} p_{A_k}} \min_{i=1,\ldots,N} \left\{ \frac{p_{A_i} \left| h_{A_i A_{i+1}} \right|^2}{d_{A_i A_{i+1}}^{\alpha}} \right\} \right] dx_{E_j} \right] \right\}. \end{aligned} \tag{22}$$

and involves a mathematical expectation. To facilitate finding an efficient solution to the secure routing problem, we resort to an approximation of the SCP. We derive the approximation by considering that the set of legitimate nodes are assumed to share identical distance from an arbitrary eavesdropper. Based on the assumption, we can obtain an approximation of (16) as (22), given at the top of the page.

Using Jensens inequality, (22) can be turned to (23), given at the next page.

Since $\min\limits_{i=1,\ldots,N} \left\{ \frac{p_{A_i} \left| h_{A_i A_{i+1}} \right|^2}{d_{A_i A_{i+1}}^{\alpha}} \right\}$ is exponentially distributed with the mean of $\sum\limits_{i=1}^{N} \frac{d_{A_i A_{i+1}}^{\alpha}}{p_{A_i}}$, then (23) can be derived as (24), written at the top of the next page.

Then (24) can be turned to

$$\mathcal{P}_{N\_approx2} = \exp\left[-K_1 \left(\sum_{k=1}^{N} p_{A_k} \sum_{i=1}^{N} \frac{d_{A_i A_{i+1}}^{\alpha}}{p_{A_i}} \right)^{\frac{2}{\alpha}} \right], \tag{25}$$

where $K_1 = \pi \lambda_E \Gamma(1 + \frac{2}{\alpha}) \Gamma(1 - \frac{2}{\alpha})$ and $\Gamma(\cdot)$ is the gamma function.

C. Routing Algorithm Based on the SCP Approximations

In the former subsections, we derive the approximations of the SCP for both colluding and non-colluding eavesdroppers for any given path. In this subsection, we find the path with highest SCP between an arbitrary source and destination.

1) Colluding Eavesdroppers Case: The routing problem depending on (21) is still formidable to be solved. We assume that the transmit powers of all nodes are the same. Then (21) can be simplified as

$$\mathcal{P}_{C\_approx} = \exp\left[-K_2(N) \left(\sum_{i=1}^{N} d_{A_i A_{i+1}}^{\alpha} \right)^{\frac{2}{\alpha}} \right], \tag{26}$$

where $K_2(N) = \lambda_E \frac{\pi \Gamma(1 - \frac{2}{\alpha}) \Gamma(\frac{2}{\alpha} + N)}{\Gamma(N)}$.

Based on (26), the secure routing problem for finding the highest SCP path can be expressed as

$$\max_{L \in L_{A_S A_D}} \exp\left[-K_2(|L|) \left(\sum_{i \in L} d_{A_i A_{i+1}}^{\alpha} \right)^{\frac{2}{\alpha}} \right], \tag{27}$$

where $L_{A_S A_D}$ is the set of all paths L connecting the pair of source node A_S and destination node A_D. Then (27) is equivalent to

$$\min_{L \in L_{A_S A_D}} K_2(|L|) \left(\sum_{i \in L} d_{A_i A_{i+1}}^{\alpha} \right)^{\frac{2}{\alpha}}. \tag{28}$$

It can be easily shown that (28) can be solved by exhaustive search, but computationally expensive. The routing metric of problem (28) is not isotonic and the problem cannot be solved easily. However, we can prove that the problem (28) can be solved exactly optimally in polynomial time. In the following we detail the process.

Since $|L|$ can only take the value $1, 2, \ldots, N_L - 1$, where the N_L is the number of the legitimate nodes. According to the divide-and-conquer principle [28], then problem (28) can be rewritten as [29]

$$M_t(L^*) = \min_{1 \le v \le N_L - 1} M_t(L_v), \tag{29}$$

where

$$\begin{aligned} M_t(L_v) &= \min_{L \in L_{A_S A_D} : |L| = v} K_2(|L|) \left(\sum_{i \in L} d_{A_i A_{i+1}}^{\alpha} \right)^{\frac{2}{\alpha}} \\ &= \min_{L \in L_{A_S A_D} : |L| = v} K_2(v) \left(\sum_{i \in L} d_{A_i A_{i+1}}^{\alpha} \right)^{\frac{2}{\alpha}} \end{aligned} \tag{30}$$

$$\mathcal{P}_{N\_approx2} = \exp\left[\mathbb{E}_{\substack{h_{A_iA_{i+1}} \\ i=1,\ldots,N}}\left\{-\lambda_E \int_{\mathbb{R}^2} \exp\left[-\frac{d^{\alpha}_{AE_j}}{\sum_{k=1}^{N} p_{A_k}} \min_{i=1,\ldots,N}\left\{\frac{p_{A_i}\left|h_{A_iA_{i+1}}\right|^2}{d^{\alpha}_{A_iA_{i+1}}}\right\}\right] dx_{E_j}\right\}\right]. \tag{23}$$

$$\mathcal{P}_{N\_approx2} = \exp\left[-\lambda_E \int_{\mathbb{R}^2} \frac{\sum_{i=1}^{N} p_{A_i}^{-1} d^{\alpha}_{A_iA_{i+1}}}{\frac{d^{\alpha}_{AE_j}}{\sum_{k=1}^{N} p_{A_k}} + \sum_{i=1}^{N} {p_{A_i}}^{-1} d^{\alpha}_{A_iA_{i+1}}} dx_{E_j}\right]. \tag{24}$$

Here L^* and L_v are the optimal solution to problem (28) and subproblem (30), respectively; $M_t(L^*)$ and $M_t(L_v)$ are the corresponding optimal values of the objective function.

We can solve each subproblem (30) to get the optimal solution to problem (28). But the subproblem (30) is still arduous to be solved, we relax it to

$$M_t(\tilde{L}_v) = \min_{L\in L_{A_SA_D}:|L|\le v} K_2(v)\left(\sum_{i\in L} d^{\alpha}_{A_iA_{i+1}}\right)^{\frac{2}{\alpha}}, \tag{31}$$

where $\tilde{L}_v$ and $M_t(\tilde{L}_v)$ denote the optimal solution and the corresponding optimal value of the objective function to the relaxed problem (31), respectively. In the following, we discuss the relationship between problem (28) and (31).

According to (29) and (30), we can obtain

$$M_t(L^*) = \min_{1\le v\le N_L-1} K_2(v)\left(\sum_{i\in L_v} d^{\alpha}_{A_iA_{i+1}}\right)^{\frac{2}{\alpha}}. \tag{32}$$

Since (31) is the relaxed problem of (30) and L_v is also a feasible solution to (31), then

$$\begin{aligned} M_t(L^*) &\ge \min_{1\le v\le N_L-1} M_t(\tilde{L}_v) \\ &= \min_{1\le v\le N_L-1} K_2(v)\left(\sum_{i\in \tilde{L}_v} d^{\alpha}_{A_iA_{i+1}}\right)^{\frac{2}{\alpha}}. \end{aligned} \tag{33}$$

It can be easily known that $\left|\tilde{L}_v\right| \le v$ since $\tilde{L}_v$ is the optimal solution to the relaxed problem (31) and $K_2\left(\left|\tilde{L}_v\right|\right) \le K_2(v)$, then

$$M_t(L^*) \ge \min_{1\le v\le N_L-1} K_2\left(\left|\tilde{L}_v\right|\right)\left(\sum_{i\in \tilde{L}_v} d^{\alpha}_{A_iA_{i+1}}\right)^{\frac{2}{\alpha}}. \tag{34}$$

Since $\tilde{L}_v$ is also a feasible solution to problem (30), then

$$M_t(L^*) \le \min_{1\le v\le N_L-1} K_2\left(\left|\tilde{L}_v\right|\right)\left(\sum_{i\in \tilde{L}_v} d^{\alpha}_{A_iA_{i+1}}\right)^{\frac{2}{\alpha}}. \tag{35}$$

From (34) and (35), we can easily obtain

$$M_t(L^*) = \min_{1\le v\le N_L-1} \tilde{M}_t(\tilde{L}_v), \tag{36}$$

and

$$\tilde{M}_t(\tilde{L}_v) = K_2\left(\left|\tilde{L}_v\right|\right)\left(\sum_{i\in \tilde{L}_v} d^{\alpha}_{A_iA_{i+1}}\right)^{\frac{2}{\alpha}}. \tag{37}$$

(36) and (37) imply that problem (28) can be solved optimally by solving a sequence of relaxed subproblems (31). Based on the fact that the path loss exponent $\alpha > 2$, it is easy to know that the solution to the relaxed subproblem (31) for a given hop-count v is equivalent to $\min_{L\in L_{A_SA_D}:|L|\le v} \sum_{i\in L} d^{\alpha}_{A_iA_{i+1}}$, which means that each link uses $d^{\alpha}_{A_iA_{i+1}}$ as the link weights to find the path connecting source node A_S and destination node A_D which has the minimum total link weights and is no more than v hops. The problem can be directly solved by the classical Bellman-Ford shortest path algorithm which computes shortest paths from a single source vertex to all of the other vertices in a weighted digraph. A distributed variant of the algorithm is used in distance-vector routing protocols, for example the Routing Information Protocol (RIP) [30]. However, the number of hops $|L|$ in the objective function in (28) changes with the selected path L. Having the weighting factor of $|L|$ in the objective function, the optimization problem cannot be solved directly by using the classical Bellman-Ford algorithm, because it does not take the weighting factor into account. Hence, we develop a revised Bellman-Ford algorithm as shown in Algorithm 1 below. The classical Bellman-Ford algorithm has an implicit property that at its hth iteration, it identifies the optimal path from the source to the destination among all paths of at most h hops. This property is used in Step 1 of the algorithm. On the other hand, Steps 2 and 3 reflect our revision in the Bellman-Ford algorithm in order to solve the problem in (28). The whole procedure is shown in Algorithm 1.

Before using the algorithm, each legitimate node calculates the distances between itself and all other nodes in the network and stores the topology information which contains the neighbor list and transmission distance $d_{A_iA_{i+1}}$ between them. Then it sends its topology information to all neighboring nodes. Note that the value of λ_E does not influence the routing algorithm, since SCP decreases as the value of λ_E increases as shown in the exact expression (12). The optimal secure path will always have the highest SCP which is independent with

Algorithm 1 The routing algorithm for the colluding eavesdroppers case.

Input: The transmission distance $d_{A_iA_{i+1}}$ between the legitimate nodes;

Output:

1: Each legitimate nodes use $d^{\alpha}_{A_iA_{i+1}}$ as link weights , obtain the shortest path $\tilde{L}_v$ in each iteration $v\,(1,\ldots,N_L-1)$ by the classical Bellman-Ford shortest path algorithm;
2: Calculate the function values for each path $\tilde{L}_v$ using (37);
3: Get the optimal path L^* with the minimum function value using (36);
4: **return** L^*;

the value of λ_E. The proposed routing algorithm provides a theoretical basis for finding a link weight $d^{\alpha}_{A_iA_{i+1}}$, which is the key point of a routing algorithm, considering the security. Without the proposed algorithm, the classical Bellman-Ford algorithm does not have a reasonable way to choose a link weight which takes the security into consideration. The complexity of the classical Bellman-Ford algorithm is $O({N_L}^3)$ [30]. From Algorithm 1, it is clear that the computational complexity is dominated by Step 1. Hence, our proposed algorithm has the same level of computational complexity as the classical Bellman-Ford algorithm, which is $O({N_L}^3)$. It is polynomial and much lower than that of the exhaustive search whose complexity is $O((N_L-2)!)$.

2) Non-colluding Eavesdroppers Case: Depending on the SCP approximation (25), the highest SCP path can be presented as the following problem:

$$\max_{L\in L_{A_SA_D}} \exp\left[-K_1\left(\sum_{k\in L} p_{A_k}\sum_{i\in L}\frac{d^{\alpha}_{A_iA_{i+1}}}{p_{A_i}}\right)^{\frac{2}{\alpha}}\right], \quad (38)$$

where $L_{A_SA_D}$ is the set of all paths L connecting the pair of nodes (A_S, A_D). When the network parameters λ_E and α are determined, K_1 is a constant and positive. Then (38) is equivalent to

$$\min_{L\in L_{A_SA_D}}\left(\sum_{k\in L} p_{A_k}\sum_{i\in L}\frac{d^{\alpha}_{A_iA_{i+1}}}{p_{A_i}}\right)^{\frac{2}{\alpha}}. \quad (39)$$

We assume that the transmit powers of all nodes are the same. Then (39) can be simplified as

$$\min_{L\in L_{A_SA_D}}\left(|L|\sum_{i\in L} d^{\alpha}_{A_iA_{i+1}}\right)^{\frac{2}{\alpha}}. \quad (40)$$

Similar to the case of colluding eavesdroppers, we also can prove that problem (40) can be solved optimality by solving a sequence of subproblems

$$M_u(\widehat{L}_u) = \min_{L\in L_{A_SA_D}:|L|\le u}\left(u\sum_{i\in L} d^{\alpha}_{A_iA_{i+1}}\right)^{\frac{2}{\alpha}}, \quad (41)$$

$$M_u(\widehat{L}_u^*) = \min_{1\le u\le N_L-1}\tilde{M}_u(\widehat{L}_u), \quad (42)$$

and

$$\tilde{M}_u(\widehat{L}_u) = \left(\left|\widehat{L}_u\right|\sum_{i\in\widehat{L}_u} d^{\alpha}_{A_iA_{i+1}}\right)^{\frac{2}{\alpha}}, \quad (43)$$

where $\widehat{L}_u^*$ and $\widehat{L}_u$ are the optimal solution to problem (40) and subproblem (41), respectively; $M_u(\widehat{L}_u^*)$ and $M_u(\widehat{L}_u)$ are the corresponding optimal values of the objective function; $\tilde{M}_u(\widehat{L}_u)$ is the function value of (43). The whole procedure is shown in Algorithm 2.

Algorithm 2 The routing algorithm for the non-colluding eavesdroppers case.

Input: The transmission distance $d_{A_iA_{i+1}}$ between the legitimate nodes;

Output:

1: Each legitimate nodes use $d^{\alpha}_{A_iA_{i+1}}$ as link weights , obtain the shortest path $\widehat{L}_u$ in each iteration $u\,(1,\ldots,N_L-1)$ by the classical Bellman-Ford shortest path algorithm;
2: Calculate the function values for each path $\widehat{L}_u$ using (43);
3: Get the optimal path $\widehat{L}_u^*$ with the minimum function value using (42);
4: **return** $\widehat{L}_u^*$;

The computational complexity of Algorithm 2 for the non-colluding eavesdroppers case is the same as Algorithm 1 for the colluding eavesdroppers case which is also $O({N_L}^3)$.

V. Numerical Results and Discussion

In this section, we present numerical results and evaluate the performance of the derived expressions of SCP, then we compare the performance of different routing algorithms on security. We take path loss exponent $\alpha = 4$, and we assume that all the transmit powers are the same.

A. Performance of Derived SCP

We simulate a multihop wireless network, in which the nodes are deployed in a 2000×2000 square area. The eavesdroppers are located at random positions which follow a homogeneous PPP. In this subsection, we consider an example of 6 legitimate nodes $A_1 \sim A_6$, and they locate at $(-10,0)$, $(5\cos(0.75\pi), 5\sin(0.75\pi))$, $(0,0)$, $(5\cos(-0.25\pi), 5\sin(-0.25\pi))$, $(10,0)$ and $(15\cos(0.25\pi), 15\sin(0.25\pi))$. It takes 10000 simulation runs to obtain Monte Carlo simulation results.

Fig. 1 depicts the Monte Carlo simulation results of SCP for different λ_E. It can be seen that our analysis results match with the Monte Carlo simulation results, which validates our analysis.

Fig. 2 illustrates the SCP for the case of colluding eavesdroppers as a function of λ_E. As the value of λ_E and the number of hops grow, the SCP decreases. The gap between the approximation and the exact value of the SCP is small, and we

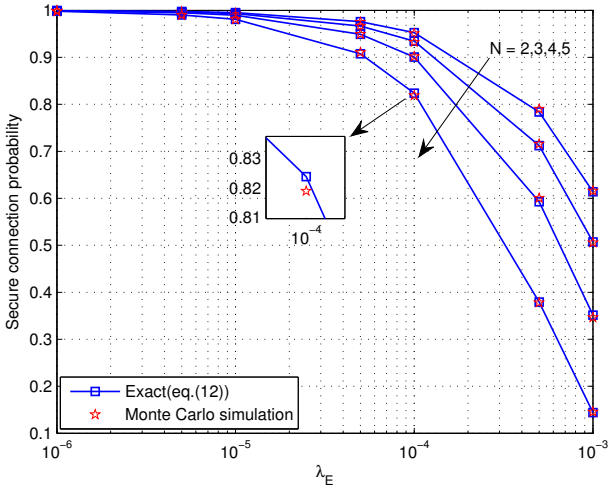


Fig. 1. Monte Carlo simulation results of SCP for colluding eavesdroppers case. The squares represent (12). The stars show the Monte Carlo simulation of (8).

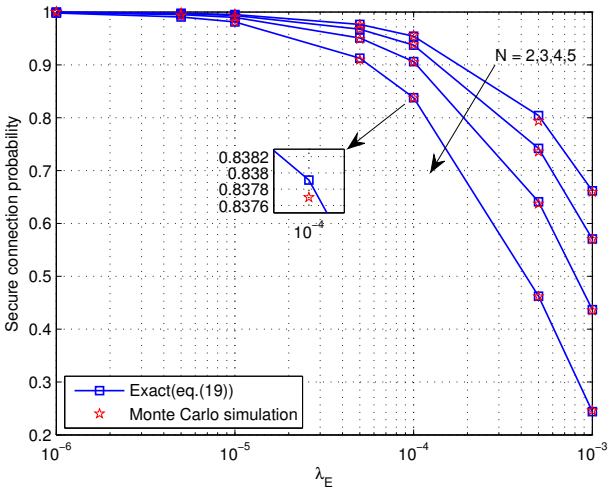


Fig. 3. Monte Carlo simulation results of SCP for non-colluding eavesdroppers case. The squares represent (19). The stars show the Monte Carlo simulation of (14).

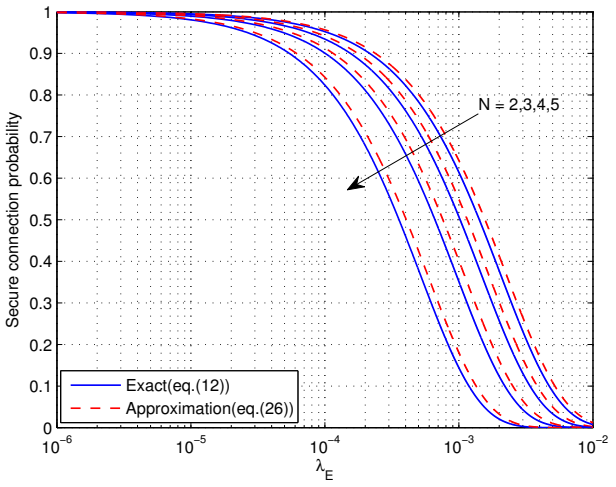


Fig. 2. SCP for colluding eavesdroppers case. The solid lines represent (12) and the dashed lines denote the SCP approximation (26).

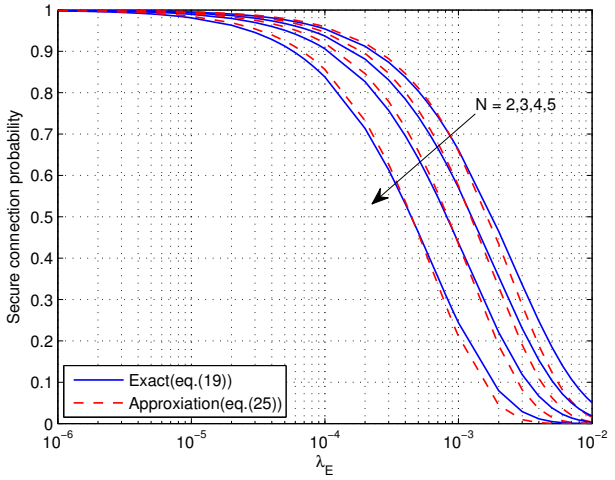


Fig. 4. SCP for non-colluding eavesdroppers case. The solid lines represent (19) and the dashed lines denote SCP approximation (25).

can see that our SCP approximation is a precise approximation of the exact value for all λ_E.

Fig. 3 depicts the Monte Carlo simulation results of SCP for the case of non-colluding eavesdroppers as a function of λ_E. Again, we see that the analytical results match well with the simulation.

Fig. 4 illustrates the SCP for the case of non-colluding eavesdroppers as a function of λ_E. We can see that the SCP approximation (25) is accurate compared to the exact value obtained in (19) for a wide range of λ_E. This implies that the accuracy of the approximation is good for a wide range of eavesdropper density. Hence, the derived routing algorithm based on the approximation will give the optimal result in most cases.

B. Performance of Routing Algorithm

We consider a multihop wireless network in which $N_L = 32$ legitimate nodes are placed uniformly at random on a 50×50 square area in the center of the network. The source node is placed at the lower left corner of the network and the destination is located at the upper right corner. Note that the eavesdroppers are still randomly distributed in the entire network of size 2000×2000. Our goal is to find the route that gives the highest SCP between the source and destination. For comparison, we consider the optimal route from exhaustive search as the benchmark routing algorithm.

In Fig. 5, we present a snapshot of the network for the case of colluding eavesdroppers. The proposed route based on the SCP approximation (26) and the benchmark route by exhaustive search between the source and destination are plotted in the picture. The link weight is $d^{\alpha}_{A_i A_{i+1}}$. The actual source-destination SCP of the proposed route and benchmark route computed by (12) for different λ_E are shown in Table I. It can be seen that our proposed route is exceedingly close to the benchmark route on security.

In Fig. 6, we present a snapshot of the route based on the SCP approximation (25) with the same system nodes as in Fig. 5 under the case of the non-colluding eavesdroppers.

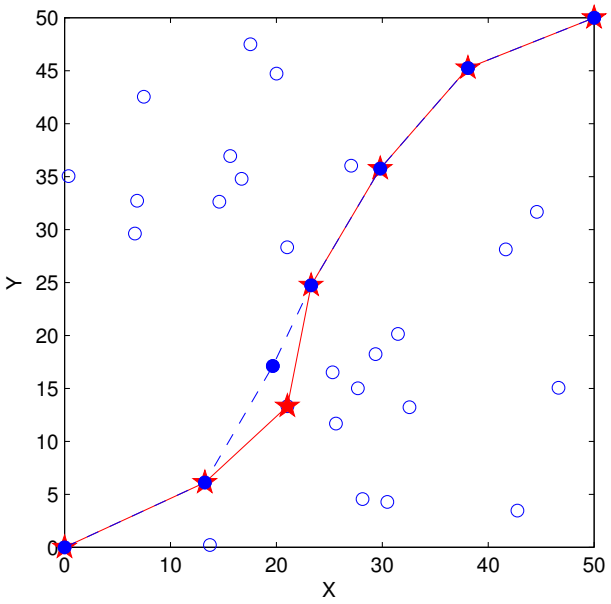


Fig. 5. Routing algorithm based on the SCP approximation (26) under the case of colluding eavesdroppers. A snapshot of the network is shown when $N_L = 32$ legitimate nodes (shown by circles) are placed uniformly at random. The proposed route is plotted by the red solid line and the benchmark route is shown by the blue dashed line.

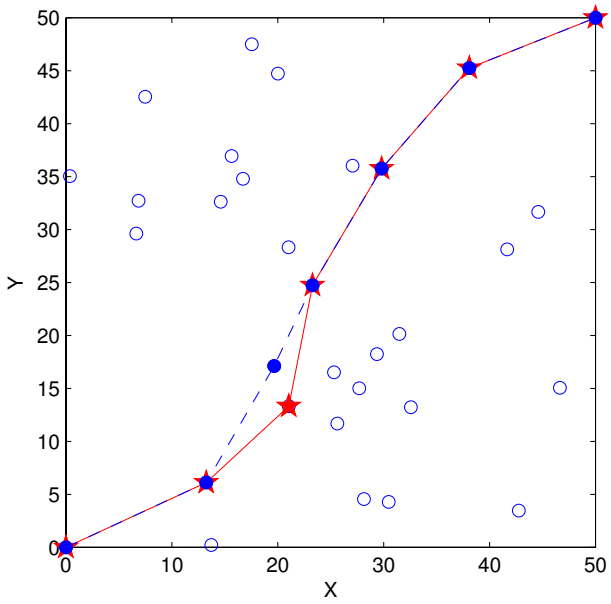


Fig. 6. Routing algorithm based on the SCP approximation (25) under the case of non-colluding eavesdroppers. A snapshot of the network with the same system nodes as in Fig. 5 is shown. The proposed route is plotted by the red solid line and the benchmark route is shown by the blue dashed line.

TABLE I
SCP OF THE ROUTING ALGORITHM UNDER THE CASE OF COLLUDING EAVESDROPPERS FOR DIFFERENT λ_E.

λ_E	10^{-6}	10^{-5}	10^{-4}
proposed route	0.9933	0.9349	0.5103
benchmark route	0.9933	0.9351	0.5112

As shown in the figure, we can derive the same results as the case of colluding eavesdroppers. Specially, the optimal route for the non-colluding case is the same as that for the colluding eavesdroppers. This is because that the eavesdropper with the strongest signal reception contributes the most in the eavesdropping capability of a set of colluding eavesdroppers, unless the density of eavesdroppers becomes comparable to that of the legitimate nodes. This implies that in most scenarios the best secure route against the strongest eavesdropper, which is in fact the non-colluding case, is also likely to be the best route against all eavesdroppers when they collude. The actual source-destination SCP of the proposed route and benchmark route computed by (19) for different λ_E are shown in Table II.

TABLE II
SCP OF THE ROUTING ALGORITHM UNDER THE CASE OF NON-COLLUDING EAVESDROPPERS FOR DIFFERENT λ_E.

λ_E	10^{-6}	10^{-5}	10^{-4}
proposed route	0.9933	0.9373	0.5651
benchmark route	0.9934	0.9375	0.5662

We assume $\lambda_E = 10^{-5}$. For comparison, we consider the optimal route from exhaustive search as the benchmark routing algorithm. For different number of legitimate nodes, we simulate the routing algorithms 1000 times based on the SCP approximation (26) and exhaustive search. However, the computational complexity of the exhaustive search for the case of non-colluding eavesdroppers is too high to simulate, we only show the case of colluding eavesdroppers in the following. Note that enumerating all the routes of the benchmark routing algorithm from the source to the destination becomes prohibitive in a large number of legitimate nodes, so we only simulate the number of the legitimate nodes up to 12. The results are shown in Table III.

In Table III, N_L denotes the number of the legitimate nodes. $\mathcal{P}_{SC\_approx}$ and $\mathcal{P}_{SC\_best}$ represent the exact SCP of the route for the approximation and exhaustive search, respectively. $\mathcal{P}_{EQ\_approx}$ represents the probability of the routes based on the SCP approximation which coincide with the benchmark routes. As shown in the table, the SCP increases with the number of legitimate nodes growing. It is because that more legitimate nodes will give more chance to get a safer route for a given source-destination pair of nodes. The gap between the proposed route and benchmark route is minuscule. The probability of the route based on the SCP approximation choosing the same route as benchmark route is $80.8\% \sim 91.4\%$. Such a small but notable difference in the routes results in very insignificant performance degradation. As we can see, the route based on the SCP approximation is intensely close to the benchmark route on security.

VI. CONCLUSION

This paper studied the secure routing problem in multihop wireless networks. Given a path of a source-destination pair of nodes, we obtained the exact expressions of the secure connection probability (SCP) for both colluding and non-colluding eavesdroppers. Then the SCP approximations were derived to facilitate finding the routing algorithm. Based on the SCP approximations, we solved the routing problem between

TABLE III
COMPARISON OF DIFFERENT ROUTING ALGORITHMS VARYING WITH THE NUMBER OF LEGITIMATE NODES

N_L	4	5	6	7	8	9	10	11	12
$\mathcal{P}_{SC\_best}$	0.8364	0.8522	0.8635	0.8731	0.8794	0.8847	0.8910	0.8949	0.8986
$\mathcal{P}_{SC\_approx}$	0.8360	0.8518	0.8632	0.8728	0.8790	0.8844	0.8908	0.8946	0.8983
$\mathcal{P}_{EQ\_approx}$	91.4%	90.9%	88.1%	87.3%	85.6%	84.3%	85.0%	83.3%	80.8%

an arbitrary pair of nodes to find the highest SCP path connecting them. Our proposed secure routing protocol finds the optimal path in a distributed way by using a revised Bellman-Ford algorithm.

Our work focused on a benchmarking scenario where the most commonly-used DF relaying protocol is assumed. To further improve the secrecy performance, the RaF relaying protocol can be implemented which uses independent codewords at the relays and is specifically designed from the viewpoint of physical layer security. In our future work, we will extend our analysis to this scenario and compare with the benchmarking case to see to what extent the secure routing protocols differ from each other.

APPENDIX A
PROOF OF LEMMA 1

Let

$$f_n(x) = \int_{-\infty}^{\infty} \left(1 - \prod_{k=1}^{n} \frac{1}{1 + B_k (x + a_k)^{-2}}\right) dx, \tag{44}$$

$$g_n(x) = \int_{-\infty}^{\infty} \left(1 - \prod_{k=1}^{n} \frac{1}{1 + B_k (x + a)^{-2}}\right) dx. \tag{45}$$

Let $x = x + a$, then

$$g_n(x) = \int_{-\infty}^{\infty} \left(1 - \prod_{k=1}^{n} \frac{1}{1 + B_k x^{-2}}\right) dx. \tag{46}$$

When $n = 1$,

$$f_1(x) = g_1(x) = \sqrt{B_1}\pi. \tag{47}$$

When $n = 2$,

$$f_2(x) = \frac{\left(\sqrt{B}_1 + \sqrt{B}_2\right)\left(B_1 + \sqrt{B_1 B_2} + B_2 + \widehat{a}^2\right)}{B_1 + 2\sqrt{B_1 B_2} + B_2 + \widehat{a}^2}, \tag{48}$$

$$g_2(x) = \frac{B_1 + \sqrt{B_1 B_2} + B_2}{\sqrt{B}_1 + \sqrt{B}_2}, \tag{49}$$

where $\widehat{a} = a_2 - a_1$, then

$$f_2(x) - g_2(x) = \frac{\widehat{a}^2 \left(B_1 + \sqrt{B_1 B_2} + B_2\right)}{\left(\sqrt{B}_1 + \sqrt{B}_2\right)\left(\widehat{a}^2 + \left(\sqrt{B}_1 + \sqrt{B}_2\right)^2\right)} > 0. \tag{50}$$

When $n = 3$,

$$f_3(x) = \int_{-\infty}^{\infty} \left(1 - \prod_{k=1}^{3} \frac{1}{1 + B_k (x + a_k)^{-2}}\right) dx. \tag{51}$$

Let $x = x + a_3$, then (51) can be turned to

$$f_3(x) = \int_{-\infty}^{\infty} \left(1 - \frac{1}{1 + B_3 x^{-2}} \prod_{k=1}^{2} \frac{1}{1 + B_k (x + b_k)^{-2}}\right) dx, \tag{52}$$

where $b_k = a_k - a_3 (k < 3)$.

$$f_3(x) - g_3(x) = \int_{-\infty}^{\infty} \frac{1}{1 + B_3 x^{-2}} \times \left(\prod_{k=1}^{2} \frac{1}{1 + B_k x^{-2}} - \prod_{k=1}^{2} \frac{1}{1 + B_k (x + b_k)^{-2}}\right) dx. \tag{53}$$

According to first mean value theorem [31], there exists a constant $-\infty \le \varepsilon_1 \le \infty$ holding the equation

$$f_3(x) - g_3(x) = \frac{1}{1 + B_3 \varepsilon_1^{-2}} \times \int_{-\infty}^{\infty} \left(\prod_{k=1}^{2} \frac{1}{1 + B_k x^{-2}} - \prod_{k=1}^{2} \frac{1}{1 + B_k (x + b_k)^{-2}}\right) dx. \tag{54}$$

Then (54) can be rewritten as

$$f_3(x) - g_3(x) = \frac{1}{1 + B_3 \varepsilon_1^{-2}} \left(f_2(x) - g_2(x)\right) > 0. \tag{55}$$

We assume that when $n = j$ and

$$f_j(x) - g_j(x) > 0. \tag{56}$$

Then when $n = j + 1$, we have

$$f_{j+1}(x) = \int_{-\infty}^{\infty} \left(1 - \prod_{k=1}^{j+1} \frac{1}{1 + B_k (x + a_k)^{-2}}\right) dx. \tag{57}$$

Let $x = x + a_{j+1}$, then (57) can be turned to

$$f_{j+1}(x) = \int_{-\infty}^{\infty} \left(1 - \frac{1}{1 + B_{j+1} x^{-2}} \prod_{k=1}^{j} \frac{1}{1 + B_k (x + c_k)^{-2}}\right) dx, \tag{58}$$

where $c_k = a_k - a_{j+1} (k < j + 1)$.

$$f_{j+1}(x) - g_{j+1}(x) = \int_{-\infty}^{\infty} \frac{1}{1 + B_{j+1} x^{-2}} \times \left(\prod_{k=1}^{j} \frac{1}{1 + B_k x^{-2}} - \prod_{k=1}^{j} \frac{1}{1 + B_k (x + c_k)^{-2}}\right) dx. \tag{59}$$

Similar to $n = 3$, (59) can be rewritten to

$$f_{j+1}(x) - g_{j+1}(x) = \frac{1}{1 + B_{j+1}\varepsilon_2^{-2}} \left(f_j(x) - g_j(x)\right) > 0. \tag{60}$$

So we can conclude that $f_n(x)$ is greater than $g_n(x)$ for an arbitrary positive integrate random variable $n > 1$.

ACKNOWLEDGMENT

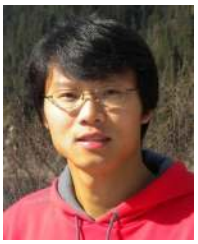
The authors would like to thank the support of National Engineering Technology Research Center of Mobile Ultrasonic Detection.

REFERENCES

[1] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
[3] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
[4] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3532–3545, July 2012.
[5] J. Mo, M. Tao, Y. Liu, and R. Wang, "Secure beamforming for mimo two-way communications with an untrusted relay," *IEEE Trans. Signal Process.*, vol. 62, no. 9, pp. 2185–2199, May 2014.
[6] J. Mo, M. Tao, and Y. Liu, "Relay placement for physical layer security: A secure connection perspective," *IEEE Commun. Lett.*, vol. 16, no. 6, pp. 878–881, June 2012.
[7] T.-X. Zheng, H.-M. Wang, F. Liu, and M. H. Lee, "Outage constrained secrecy throughput maximization for df relay networks," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1741–1755, May 2015.
[8] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 10, pp. 2099–2111, Oct. 2013.
[9] 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, no. 10, pp. 2067–2076, Dec. 2011.
[10] W. Saad, X. Zhou, B. Maham, T. Basar, and H. Poor, "Tree formation with physical layer security considerations in wireless multi-hop networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 11, pp. 3980–3991, Nov. 2012.
[11] A. Sheikholeslami, M. Ghaderi, H. Pishro-Nik, and D. Goeckel, "Jamming-aware minimum energy routing in wireless networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, June 2014, pp. 2313–2318.
[12] Z. Ding, K. Leung, D. Goeckel, and D. Towsley, "On the application of cooperative transmission to secrecy communications," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 2, pp. 359–368, Feb. 2012.
[13] M. Dehghan, D. Goeckel, M. Ghaderi, and Z. Ding, "Energy efficiency of cooperative jamming strategies in secure wireless networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 9, pp. 3025–3029, Sep. 2012.
[14] S. Gerbracht, C. Scheunert, and E. Jorswieck, "Secrecy outage in miso systems with partial channel information," *IEEE Trans. Inf. Foren. Sec.*, vol. 7, no. 2, pp. 704–716, Apr. 2012.
[15] X. Zhou, R. Ganti, and J. Andrews, "Secure wireless network connectivity with multi-antenna transmission," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 425–430, Feb. 2011.
[16] O. Koyluoglu, C. Koksal, and H. Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 3000–3015, May 2012.
[17] X. Zhou, R. Ganti, J. Andrews, and A. Hjorungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.
[18] G. Geraci, H. Dhillon, J. Andrews, J. Yuan, and I. Collings, "Physical layer security in downlink multi-antenna cellular networks," *IEEE Trans. Commun.*, vol. 62, no. 6, pp. 2006–2021, June 2014.
[19] A. Tukmanov, S. Boussakta, Z. Ding, and A. Jamalipour, "Outage performance analysis of imperfect-CSI-based selection cooperation in random networks," *IEEE Trans. Commun.*, vol. 62, no. 8, pp. 2747–2757, May 2014.
[20] C. Cai, Y. Cai, X. Zhou, W. Yang, and W. Yang, "When does relay transmission give a more secure connection in wireless ad hoc networks?" *IEEE Trans. Inf. Foren. Sec.*, vol. 9, no. 4, pp. 624–632, Apr. 2014.
[21] H. Wang, X. Zhou, and M. Reed, "Physical layer security in cellular networks: A stochastic geometry approach," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2776–2787, May 2013.
[22] C. Ma, J. Liu, X. Tian, H. Yu, Y. Cui, and X. Wang, "Interference exploitation in d2d-enabled cellular networks: A secrecy perspective," *IEEE Trans. Commun.*, vol. 63, no. 1, pp. 229–242, Jan. 2015.
[23] J. Li, A. Petropulu, and S. Weber, "On cooperative relaying schemes for wireless physical layer security," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4985–4997, Oct. 2011.
[24] C. Jeong and I.-M. Kim, "Optimal power allocation for secure multi-carrier relay systems," *IEEE Trans. Signal Process.*, vol. 59, no. 11, pp. 5428–5442, Nov. 2011.
[25] C. Wang, H.-M. Wang, and X.-G. Xia, "Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 589–605, Feb 2015.
[26] S. N. Chiu, D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic geometry and its applications*. John Wiley & Sons, 2013.
[27] S. Amari and R. Misra, "Closed-form expressions for distribution of sum of exponential random variables," *IEEE Trans. Rel.*, vol. 46, no. 4, pp. 519–522, Dec. 1997.
[28] L. A. Wolsey, *Integer programming*. Wiley New York, 1998, vol. 42.
[29] M. Saad, "Joint optimal routing and power allocation for spectral efficiency in multihop wireless networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 5, pp. 2530–2539, May 2014.
[30] D. P. Bertsekas, R. G. Gallager, and P. Humblet, *Data networks*. Prentice-Hall International New Jersey, 1992, vol. 2.
[31] A. Jeffrey and D. Zwillinger, *Table of integrals, series, and products*. Academic Press, 2007.

Jianping Yao received the B.E. degree in communication of engineering from Guangdong University of Technology, Guangzhou, China, in 2010 and the M.E. degree in electronics and communication of engineering from South China University of Technology, Guangzhou, China, in 2013, respectively. He is currently pursuing the Ph.D. degree at the School of Electronic and Information Engineering, South China University of Technology, Guangzhou, China. His research interests include physical layer security, full-duplex and stochastic geometry in wireless networks.

Suili Feng (M'05) received the B.S. degree in electrical engineering from South China Institute of Technology, Guangzhou, China, in 1982 and the M.S. and Ph.D. degrees in electronic and communication system from South China University of Technology, Guangzhou, China, in 1989 and 1998, respectively. He was a research assistant in Hong Kong Polytechnic University during 1991-1992 and a visiting scholar in University of South Florida during 1998-1999. He has been with South China University of Technology, Guangzhou, China, since 1989, where he currently works as a Professor in the School of Electronic and Information Engineering. His research interests include wireless networks, computer networks and communication signal processing, etc.



Xiangyun Zhou (M'11) received the B.E. (hons.) degree in electronics and telecommunications engineering and the Ph.D. degree in telecommunications engineering from the Australian National University in 2007 and 2010, respectively. From 2010 to 2011, he worked as a postdoctoral fellow at UNIK - University Graduate Center, University of Oslo, Norway. He joined the Australian National University in 2011 and currently works as a Senior Lecturer. His research interests are in the fields of communication theory and wireless networks.

Dr. Zhou currently serves on the editorial board of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and IEEE COMMUNICATIONS LETTERS. He also served as a guest editor for IEEE COMMUNICATIONS MAGAZINE's feature topic on wireless physical layer security in 2015 and EURASIP Journal on Wireless Communications and Networking's special issue on energy harvesting wireless communications in 2014. He was a co-chair of the ICC workshop on wireless physical layer security at ICC'14 and ICC'15. He was the chair of the ACT Chapter of the IEEE Communications Society and Signal Processing Society from 2013 to 2014. He is a recipient of the Best Paper Award at ICC'11.

Yuan Liu (S'11-M'13) received the B.S. degree from Hunan University of Science and Technology, Xiangtan, China, in 2006; the M.S. degree from Guangdong University of Technology, Guangzhou, China, in 2009; and the Ph.D. degree from Shanghai Jiao Tong University, China, in 2013, all in electronic engineering.

Since Fall 2013, he has been an Assistant Professor with South China University of Technology, Guangzhou. His current research interests include heterogeneous networks, cooperative relay communication, and physical-layer security.

Dr. Liu is the recipient of the Guangdong Province Excellent Master Theses Award in 2010. He has been honored as an Exemplary Reviewer of the IEEE COMMUNICATIONS LETTERS. He is also awarded the IEEE Student Travel Grant for IEEE ICC 2012.