Secure Connectivity Probability of Multi-hop Clustered Randomize-and-Forward Networks

Xiaowei Wang, Zhou Su, and Guangyi Wang

This work investigates secure cluster-aided multi-hop randomize-and-forward networks. We present a hop-by-hop multi-hop transmission scheme with relay selection, which evaluates for each cluster the relays that can securely receive the message. We propose an analytical model to derive the secure connectivity probability (SCP) of the hop-by-hop transmission scheme. For comparison, we also analyze SCPs of traditional end-to-end transmission schemes with two relay-selection policies. We perform simulations, and our analytical results verify that the proposed hop-by-hop scheme is superior to end-to-end schemes, especially with a large number of hops or high eavesdropper channel quality. Numerical results also show that the proposed hop-by-hop scheme achieves near-optimal performance in terms of the SCP.

Keywords: Multi-hop network, Randomize-and-forward, Relay selection, Secure connectivity probability, Physical-layer security.

I. Introduction

With the rapidly growing demand for secrecy in wireless networks, physical-layer security has attracted much attention. By exploring the heterogeneity of legitimate and wiretap channels, physical-layer security aims to achieve a non-zero secrecy rate and protect legitimate users from eavesdropping [1]. On some occasions, the legitimate channel deteriorates considerably or even becomes inferior to the wiretap channel. Then, the secrecy rate becomes very low or zero. To address this situation, cooperative relaying transmission has been proposed to enhance the secrecy rate [2]. Relaying has also led to the development of numerous theories and methods to further promote security, among which relay selection is an effective approach to achieve high performance and simple implementation.

The aim of relay selection is to maximize the secrecy rate or minimize the outage probability. In the case where the optimal selection algorithm is too complex and requires substantial resources, more practical relay-selection algorithms have been carefully designed to reduce costs and achieve satisfactory performance [3], [4]. Relay selection for two-hop secure transmissions was initially studied in [3], where a relay and a friendly jammer were selected to maximize the secrecy rate. Then, research into relay selection was extended to other types of relays, such as full-duplex relays [5], two-way relays [6], buffer-aided relays [7], and cognitive relays [8]. Another efficient method to promote security is to employ multiple antennas. Multiple-antenna relaying enables the use of a variety of techniques to optimize performance, such as secure beamforming, antenna selection, and full-duplex relaying [9]. In [10], Chen and others considered a large-scale multiple-input multiple-output relaying system, and they compared the secure outage probabilities of amplify-and-

Manuscript received Mar. 23, 2017; revised June 1, 2017; accepted June 7, 2017. This work was supported by National Natural Science Foundation of China under grant 61703264 and Shanghai Municipal Science and Technology Commission under grant 12JC1404201.

Xiaowei Wang (corresponding author, wang.xw@outlook.com) and Zhou Su (zhousu@ieee.org) are with Department of Automation, Shanghai University, China. Xiaowei Wang is also with College of Information Engineering, Shanghai Maritime University, China.

Guangyi Wang (wanggyi@hdu.edu.cn) is with the School of Electronics and Information, Hangzhou Dianzi University, China.

forward (AF) and decode-and-forward (DF) protocols. When multiple antennas are not available owing to cost or hardware limitations, virtual MIMO is an alternative method that uses multiple nodes for cooperative relaying.

While many works focus on secure transmission in two-hop relaying networks, the need for secrecy in multi-hop relaying networks has also attracted attention. Lee [11] considered the secrecy rate of a three-hop full-duplex DF relaying network and designed a cooperative transmission scheme. A suboptimal power-allocation algorithm was proposed to maximize the lower bound of secrecy rate. Further, in [12], Lee studied the optimal power allocation in a secure multi-hop network with a single DF relay at each hop and a secure beamforming design of a multi-hop network with multiple cooperative relays at each hop. In [13], Wang and others considered a clustered secure multi-hop network, and proposed a joint relay and jammer selection method to minimize secure outage probability. However, they did not present a mathematical analysis of the secure outage probability, and only provided simulation results. Duy and Kong [14] considered three multi-hop transmission protocols for a clustered multi-hop DF relay network, gave the end-to-end secrecy rate, and analyzed the end-to-end secrecy outage probability for each protocol. From the above studies, one defect of multi-hop relaying is that the secrecy message is exposed to the eavesdropper at each hop. If the eavesdropper can hear all hops and combine the signals, the system secrecy rate could be considerably reduced.

In [15], Koyluoglu and others proposed an RF multi-hop relaying strategy that adds independent randomness to each hop by randomly choosing a codeword for each transmitter. By employing the proposed strategy, they show that eavesdroppers cannot combine the signals from multiple hops, and securing each hop is sufficient to secure the entire path. Then, research into the security performance of RF relaying was presented in [16], which reported that the message is secure if two hops are both secure, and which proved that the dual-hop RF strategy is superior to the DF strategy in terms of the secure outage probability. Cai and others [17] discussed the secure connectivity probability (SCP) for RF two-hop relaying networks. However, existing works are confined to dual-hop RF relaying, and the performance of an RF strategy in multi-hop networks has not been fully investigated.

Another important issue pertaining to existing works is that only the end-to-end performance is considered. When eavesdroppers are present and the information leakage of each hop is critical, a hop-by-hop analysis becomes significant. In this study, we consider a multi-hop secure transmission in a linear RF network, where the transmission is assisted by multiple relay clusters. We investigate the SCP of RF multi-hop relaying, which is an important metric used to evaluate the performance of multi-hop networks and to describe the secure connectivity between the source and the destination. Then, we propose a hop-by-hop transmission scheme with relay selection at each cluster. Instead of assuming that all relays can decode securely as in [13], we consider the different decoding abilities of the relays. Relay selection is performed between the nodes that decode securely in each cluster. Consequently, the derivation of SCP depends on the secure decoding of relays of each hop. In addition, for comparison purposes, we analyze end-to-end RF multi-hop schemes with relay selection.

II. System Model

As shown in Fig. 1, the considered network consists of a source (S), N RF relay clusters, a destination (D), and an eavesdropper (E). Cluster n has K_n nodes and $K_n \geq 1$. We assume that the direct link between S and D is blocked by obstacles. The transmission from S to D is assisted by the N relay clusters via $N + 1$ hops during $N + 1$ time slots, while the eavesdropper wiretaps each hop. All of the nodes are equipped with a single antenna, work in half-duplex mode, and can only receive from their previous adjacent node. All of the wireless links are assumed to experience independent slow Rayleigh fading.

In the first time slot, S transmits the securely encoded message to cluster 1. One of the nodes in cluster 1 is selected as the relay and forwards the message to cluster 2. Then, the message is delivered via each of the selected relays, denoted by r_n, $n = 1, \ldots, N$, and is finally received by D. The eavesdropper listens to all $N + 1$ hops, but cannot combine the signals owing to the independent randomness of each hop.

Let $h_{n,k,j}$ and $h_{n,k,\mathrm{E}}$ respectively denote the fading coefficient from node k to legitimate receiving node j and

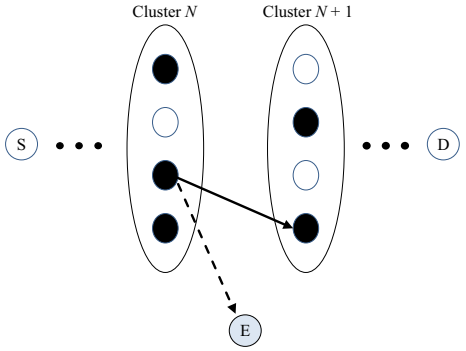


Fig. 1. System model.

https://doi.org/10.4218/etrij.17.0117.0199

E of hop n. Define $\alpha_{n,k,j} = |h_{n,k,j}|^2/\sigma^2$ and $\beta_{n,k,j} = |h_{n,k,\mathrm{E}}|^2/\sigma^2$ as the channel-to-noise-ratio (CNR) of node j and E, respectively. Here, σ^2 is the variance of complex additive white Gaussian noise (AWGN). All CNRs follow an exponential distribution with parameters λ_{M}, λ_{E} for the legitimate and eavesdropper channels, respectively. The exponential distribution with parameter λ is denoted by Exp(λ). Let $r_0 = \mathrm{S}$, $r_{N+1} = \mathrm{D}$, and the secrecy rate of hop n is thus given by

$$R_s(n) = \left[(1 + P_n\alpha_{n,r_{n-1},r_n}) - \log(1 + P_n\beta_{n,r_{n-1},\mathrm{E}})\right]^+, \quad n = 1, \ldots, N+1. \tag{1}$$

Here, $[x]^+ = \max(x, 0)$ and P_n is the transmit power of hop n. The secure probability of hop n is defined as

$$\begin{aligned} P_{\mathrm{sec}}(n) &= \Pr(R_s(n) > 0) \\ &= \Pr(\alpha_{n,r_{n-1},r_n} > \beta_{n,r_{n-1},\mathrm{E}}). \end{aligned} \tag{2}$$

III. Optimal and End-to-End Multi-hop Schemes

First, we analyzed as benchmarks the optimal multi-hop transmission scheme with relay selection and traditional end-to-end scheme with two relay-selection policies.

1. Optimal Scheme

The optimal transmission scheme is to find the combination of N selected relays that maximize the system SCP. Then, the message from S is delivered following the selected relay path. In RF relaying networks, the entire transmission is secure if all hops are secure. The SCP given a combination of selected relays is

$$P_{\mathrm{sc}} = \prod_{n=1}^{N+1} P_{\mathrm{sec}}(n) = \prod_{n=1}^{N+1} \Pr(\alpha_{n,r_{n-1},r_n} > \beta_{n,r_{n-1},\mathrm{E}}). \tag{3}$$

The optimal selection criterion is given by

$$(r_1^*, r_2^*, \ldots, r_N^*) = \arg \max_{(r_1,\ldots,r_N)} P_{\mathrm{sc}}, \tag{4}$$

and the SCP of the optimal scheme is

$$P_{\mathrm{sc}}^{\mathrm{opt}} = \max_{(r_1,\ldots,r_N)} P_{\mathrm{sc}}. \tag{5}$$

To calculate the best combination of selected relays, a central controller collects legitimate and eavesdropper channel information of all hops, evaluates the system SCP of each combination, and searches for the combination that maximizes SCP. Note that the number of relay combinations is $\prod K_n$, so the computational complexity is somewhat high when N and K_ns are large. Moreover, the signaling overhead can also be high. To overcome these issues, we allow each cluster to choose its own relay for the proposed hop-by-hop scheme and end-to-end scheme.

2. End-to-End Scheme

In traditional end-to-end multi-hop transmission schemes, clusters do not consider the decodability of receiving nodes, and they implement relay selection from all nodes within them. Moreover, the RF strategy randomizes each hop, so the relay selection is designed to enhance either the current hop or the next hop. Thus, we consider two relay selection policies for the end-to-end scheme, namely E2EMinE and E2EMaxL.

A. Relay Selection

The first selection policy (E2EMinE) chooses the node, whose CNR to the eavesdropper of the next hop is the minimum of all K_n nodes. E2EMinE is expressed as

$$r_n = \arg \min_{k=1,\ldots,K_n} \beta_{n+1,k,\mathrm{E}}, n = 1, \ldots, N. \tag{6}$$

When the selected relay works as the transmitter of hop $n + 1$, the eavesdropper CNR is the minimum from among K_n exponential random variables and $\beta_{n+1,r_n,E} \sim$ Exp($K_n\lambda_{\mathrm{E}}$). By doing this, E2EMinE degrades the eavesdropper channel and enhances the secure probability of hop $n + 1$.

The second selection policy (E2EMaxL) aims to promote the legitimate CNR of hop n and chooses the node whose CNR from the transmitter of the previous stop is the maximum, which is expressed as

$$r_n = \arg \max_{k=1,\ldots,K_n} \alpha_{n,r_{n-1},k}, n = 1, \ldots, N. \tag{7}$$

Thus, α_{n,r_{n-1},r_n} is the maximum from among K_n independent exponential random variables, and its cumulative distribution function (CDF) is given by

$$F_n(x) = (1 - e^{-\lambda_{\mathrm{M}}x})^{K_n}. \tag{8}$$

B. Secure Connectivity Probability

Similar to (3), the SCP of the end-to-end multi-hop transmission scheme is given by

$$P_{\mathrm{sc}}^{\mathrm{E2EMinE}} = \prod_{n=1}^{N+1} P_{\mathrm{sec}}(n). \tag{9}$$

The first hop of the E2EMinE policy is a traditional three-node model, so the secure probability of hop 1 is computed as

$$P_{\text{sec}}(1) = \Pr(\alpha_{1,\text{S},r_1} > \beta_{1,\text{S,E}}) = \frac{\eta}{\eta+1}. \quad (10)$$

where $\eta = \lambda_{\text{E}}/\lambda_{\text{M}}$. From hop 2 to hop N, the eavesdropper CNR of hop n follows an exponential distribution with parameter $K_{n-1}\lambda_{\text{E}}$, and the legitimate CNR follows an exponential distribution with parameter λ_{M}. The secure probabilities of hop 2 to hop N can be calculated as

$$\begin{aligned} P_{\text{sec}}(n) &= \Pr(\alpha_{n,r_{n-1},r_n} > \beta_{n,r_{n-1},\text{E}}) \\ &= \frac{\eta K_{n-1}}{\eta K_{n-1}+1}. \end{aligned} \quad (11)$$

Similarly, the secure probability of the last hop is given by

$$\begin{aligned} P_{\text{sec}}(N+1) &= \Pr(\alpha_{N+1,r_N,\text{D}} > \beta_{N+1,r_N,\text{E}}) \\ &= \frac{\eta K_N}{\eta K_N+1}. \end{aligned} \quad (12)$$

Substituting the secure probabilities of all hops into (9), the SCP of the E2EMinE scheme is obtained as

$$P_{\text{sc}}^{\text{E2EMinE}} = \frac{\eta}{\eta+1}\prod_{n=1}^{N}\frac{\eta K_n}{\eta K_n+1}. \quad (13)$$

For the E2EMaxL scheme, the node with the maximum receiving legitimate CNR from the previous cluster or S is selected as the transmitter of the next hop. Hence, the legitimate CNR of each hop is the maximum value of all the receiving nodes. According to the distribution of $\beta_{n,r_{n-1},\text{E}}$ and (8), the secure probabilities of hop 1 to hop N can be formulated as

$$\begin{aligned} P_{\text{sec}}(n) &= \Pr\left(\alpha_{n,r_{n-1},r_n} > \beta_{n,r_{n-1},\text{E}}\right) \\ &= \int\int f_n(x)\lambda_{\text{E}}e^{-\lambda_{\text{E}}y}\text{d}x\text{d}y \\ &= \int_0^{\infty}\lambda_{\text{E}}e^{-\lambda_{\text{E}}y}\left(1-\left(1-e^{-\lambda_{\text{M}}y}\right)_n^K\right)\text{d}y. \\ &= 1-\sum_{j=0}^{K_n}\binom{K_n}{j}\frac{(-1)^j\eta}{\eta+j}. \end{aligned} \quad (14)$$

The transmission of the last hop is a traditional three-node model, so its secure probability is given by

$$P_{\text{sec}}(N+1) = \frac{\eta}{\eta+1}. \quad (15)$$

Similar to (9), the production of all hops' secure probabilities yields the SCP of the E2EMaxL scheme. Now, consider the special case where $\eta = 1$. Then,

$$\begin{aligned} P_{\text{sec}}(n) &= 1-\Pr\left(\alpha_{n,r_{n-1},r_n} < \beta_{n,r_{n-1},\text{E}}\right) \\ &= \frac{K_n}{K_n+1} \end{aligned} \quad (16)$$

and we obtain

$$P_{\text{sc}}^{\text{E2EMaxL}} = P_{\text{sc}}^{\text{E2EMinE}} = \frac{1}{2}\prod_{n=1}^{N}\frac{K_n}{K_n+1}. \quad (17)$$

IV. Hop-by-Hop Multi-hop Scheme

In this section, we describe the hop-by-hop transmission scheme and its relay-selection policy. Then, we derive the expressions of SCP for the hop-by-hop scheme.

1. Hop-by-Hop Transmission Scheme

We propose a hop-by-hop multi-hop transmission scheme, which is denoted by HbHMinE, considering the decodability of the nodes. For each cluster, the relay is selected only among the nodes that can achieve a non-zero secrecy rate. The candidate nodes are referred to as secure relays. To calculate the secure relay set, we first give the secrecy rate of the receiving node k in cluster n as

$$R_s(n,k) = \left[\log\left(1+P_n\alpha_{n,r_{n-1},k}\right) - \log\left(1+P_n\beta_{n,r_{n-1},\text{E}}\right)\right]^+. \quad (18)$$

Here, r_{n-1} is replaced by S if $n = 1$. Thus, the condition for node k to become a secure relay is $R_s(n, k) > 0$. Then, the secure relay set of cluster n is expressed as

$$R_{\text{sec}}(n) = \{k|\alpha_{n,r_{n-1},k} > \beta_{n,r_{n-1},\text{E}}, k = 1,\ldots,K_n\}. \quad (19)$$

The number of secure relays in cluster n is denoted by i_n. If $i_n > 0$, hop n is regarded as secure, and one of the i_n secure relays is selected to transmit the message in the next hop. If $i_n = 0$, cluster n has not received the secrecy message successfully, which means that the entire multi-hop transmission is insecure and the remaining hops are not necessary.

Cluster n requires a dominant node or local controller to collect instantaneous channel information from the secure relays of cluster n to the eavesdropper. The best relay is selected according to the policy expressed as

$$r_n = \arg\min_{k\in R_{\text{sec}}(n)}\beta_{n+1,k,\text{E}}, \quad n = 1,\ldots,N. \quad (20)$$

Channel information from the selected relay to each node in cluster $n + 1$ is also needed for data transmission. Unlike the end-to-end multi-hop transmission scheme, the

performance of the relay-selection policy of the HbHMinE scheme relies on the number of secure relays. The proposed policy (20) minimizes the eavesdropper CNR of the next hop and increases the possibility that the next cluster enjoys more secure relays.

Here, the eavesdropper's CNR of hop $n+1$ is the minimum of i_n independent exponential random values with parameter λ_E, so it conforms to an exponential distribution with parameter $i_n\lambda_E$. Owing to the independence of wireless links, $\alpha_{n+1,r_n,k}$ is still an exponential distributed with parameter λ_M.

2. Hop-by-Hop Secure Connectivity Probability

In order to derive the SCP of the hop-by-hop multi-hop transmission scheme, we first define the following probabilities.

- $P_{\text{sec}}(n)$: secure probability of hop n. If the signal can be securely received by at least one relay in cluster n, hop n is secure. When $n = N+1$, $P_{\text{sec}}(N+1)$ is the SCP of the multi-hop transmission.
- $P_{\text{sec}}(n|i_{n-1})$: conditional secure probability of hop n given that there are i_{n-1} secure relays in cluster $n-1$.
- $\Pr(i_n)$: probability that there are i_n, $1 \le i_n \le K_n$ secure relays in cluster n.
- $\Pr(i_n|i_{n-1})$: the conditional probability of i_n secure relays in cluster n given that there are i_{n-1} secure relays in cluster $n-1$.

In the hop-by-hop multi-hop scheme, if the message is finally received by D, it means that no information leakage occurred in any of the previous hops, and the multi-hop transmission is secure. Hence, the SCP can be calculated by the probability that the message is securely received by D.

We now derive the above probabilities. In the first time slot, if hop 1 is secure, it means that at least one relay's CNR is larger than $\beta_{1,\text{S,E}}$. The secure probability of hop 1 is given by

$$P_{\text{sec}}(1) = 1 - \Pr(\beta_{1,\text{S,E}} > \max_k \alpha_{1,\text{S},k}). \tag{21}$$

From hop 2 to hop $N+1$, the wiretap channel is determined by i_{n-1} because of the relay-selection policy. $P_{\text{sec}}(n)$ can be decomposed by the law of total probability with respect to all possible i_{n-1}. Hence, the SCP of the multi-hop network $P_{\text{sc}}^{\text{HbHMinE}}$ is described as

$$\begin{aligned} P_{\text{sc}}^{\text{HbHMinE}} &= P_{\text{sec}}(N+1) \\ &= \sum_{i_N=1}^{K_N} \Pr(i_N) P_{\text{sec}}(N+1|i_N). \end{aligned} \tag{22}$$

Because the final hop is a traditional three-node model and $\beta_{N+1,r_N,E} \sim \text{Exp}(i_N\lambda_E)$, $P_{\text{sec}}(N+1|i_n)$ is calculated as

$$P_{\text{sec}}(N+1|i_N) = \Pr\left(\beta_{N+1,r_N,\text{E}} < \alpha_{N+1,r_N,\text{D}}\right) = \frac{\eta i_N}{\eta i_N + 1}. \tag{23}$$

Furthermore, $\Pr(i_n)$ can also be decomposed by the law of total probability, and is written as

$$\Pr(i_n) = \sum_{i_{n-1}=1}^{K_{n-1}} \Pr(i_{n-1})\Pr(i_n|i_{n-1}), n = 2, \ldots, N. \tag{24}$$

Note that $\Pr(i_n)$ is a recursive function, and its initial function $\Pr(i_1)$ is calculated as follows. For $i_1 = K_1$,

$$\Pr(i_1) = \Pr(\beta_{1,\text{S,E}} < \min_k \alpha_{1,\text{S},k}) = \frac{\eta}{\eta + K_1}. \tag{25}$$

For $i_1 < K_1$, the event that i_1 relays' CNRs are greater than $\beta_{1,S,E}$ is equivalent to the event that the value of $\beta_{1,S,E}$ is between the $(K_1 - i_1)$-th and $(K_1 - i_1 + 1)$-th smallest relay CNRs. We obtain

$$\Pr(i_1) = \Pr\left(\alpha_{(K_1-i_1)} < \beta_{1,\text{S,E}} < \alpha_{(K_1-i_1+1)}\right). \tag{26}$$

Here, $\alpha_{(k)}$ denotes the k-th smallest relay CNR of the current hop. Using results from order statistics, the joint PDF of $\alpha_{(k)}$ and $\alpha_{(k+1)}$ is given by

$$\begin{aligned} &f_{k,k+1}(x,y) \\ &= \frac{(K_n)!F(x)^{k-1}(1-F(y))^{K_n-k-1}f(x)f(y)}{(k-1)!(K_n-k-1)!} \\ &= \frac{(K_n)!\lambda_M^2\left(1-e^{-\lambda_M x}\right)^{k-1}e^{-\lambda_M x}e^{-(K_n-k)\lambda_M y}}{(k-1)!(K_n-k-1)!}. \end{aligned} \tag{27}$$

Using the triple integral, $\Pr(i_1)$ with $i_1 < K_1$ is given by

$$\begin{aligned} \Pr(i_1) &= \int\int\int \lambda_{\text{E}} e^{-\lambda_{\text{E}} z} f_{k,k+1}(x,y)\text{d}x\text{d}y\text{d}z \\ &= \binom{K_1}{i_1+1} i_1(i_1+1)\lambda_{\text{M}}^2\lambda_{\text{E}} \\ &\quad \int_0^\infty (1-e^{-\lambda_{\text{M}}x})^{K_1-i_1-1}e^{-\lambda_{\text{M}}x}\left(\int_x^\infty e^{-\lambda_{\text{E}}z}\text{d}z\int_z^\infty e^{-i_1\lambda_{\text{M}}y}\text{d}y\right)\text{d}x \\ &= \binom{K_1}{i_1+1}\frac{\eta(i_1+1)}{\eta+i_1}\int_0^\infty (1-e^{-\lambda_{\text{M}}x})^{K_1-i_1-1}e^{-(\lambda_{\text{E}}+i_1\lambda_{\text{M}}+\lambda_{\text{M}})x}\text{d}x \\ &= \binom{K_1}{i_1+1}\frac{\eta(i_1+1)}{\eta+i_1}\sum_{j=0}^{K_1-i_1-1}\binom{K_1-i_1-1}{j}\frac{(-1)^j}{\eta+i_1+j+1}, \end{aligned} \tag{28}$$

where $k = K_1 - i_1$.

Now, we derive the conditional probability $\Pr(i_n|i_{n-1})$ in (24). Similar to the analysis of $\Pr(i_1)$, when $n > 1$ and $i_n = K_n$,

$$\Pr(i_n|i_{n-1}) = \Pr\left(\beta_{n,r_{n-1},\mathrm{E}} < \min_k \alpha_{n,r_{n-1},k}\right) = \frac{\eta i_{n-1}}{\eta i_{n-1} + K_n}. \tag{29}$$

When $i_n < K_n$,

$$\begin{aligned}
&\Pr(i_n|i_{n-1}) = \Pr\left(\alpha_{(K_n-i_n)} < \beta_{n,r_{n-1},\mathrm{E}} < \alpha_{(K_n-i_n+1)}\right) \\
&= \int\int\int i_{n-1}\lambda_\mathrm{E} e^{-i_{n-1}\lambda_\mathrm{E} z} f_{k,k+1}(x,y)\mathrm{d}x\mathrm{d}y\mathrm{d}z \\
&= \binom{K_n}{i_n+1} i_{n-1} i_n (i_n+1)\lambda_\mathrm{M}^2 \lambda_\mathrm{E} \\
&\quad \int_0^\infty \left(1-e^{-\lambda_\mathrm{M} x}\right)^{K_n-i_n-1} e^{-\lambda_\mathrm{M} x} \\
&\quad \left(\int_x^\infty e^{-i_{n-1}\lambda_\mathrm{E} z}\mathrm{d}z \int_z^\infty e^{-i_n\lambda_\mathrm{M} y}\mathrm{d}y\right)\mathrm{d}x \\
&= \binom{K_n}{i_n+1}(i_n+1)\lambda_\mathrm{M} \\
&\quad \int_0^\infty \left(1-e^{-\lambda_\mathrm{M} x}\right)^{K_n-i_n-1} e^{-(i_{n-1}\lambda_\mathrm{E}+i_n\lambda_\mathrm{M}+\lambda_\mathrm{M})x}\mathrm{d}x \\
&= \binom{K_n}{i_n+1}(i_n+1)\sum_{j=0}^{K_n-i_n-1}\binom{K_n-i_n-1}{j} \\
&\quad \frac{(-1)^j}{i_{n-1}\eta + i_n + j + 1}.
\end{aligned} \tag{30}$$

Substituting all of the above results into (22), we can obtain the SCP for the HbHMinE scheme.

3. Comparison Schemes

From the analysis of the proposed HbHMinE scheme, we conclude that the transmission can be relayed only if the secure relay set of the current hop is not null. Moreover, relay selection only influences the next hop when the selected node works as the transmitter, and the selection policy is designed with respect to the channels of the next hop. While the proposed selection policy for HbHMinE in (20) minimizes the eavesdropper CNR, we also discuss the policies that maximize the legitimate CNR.

If a certain secure relay of cluster n is to transmit in hop $n+1$, the legitimate channel is a $1 \times K_{n+1}$ vector. The selection policies that maximize the legitimate relay rate are HbHMaxMinL and HbHMaxMaxL, which are respectively described as

$$r_n = \arg \max_{k \in R_{\mathrm{sec}}(n)} \min_j \alpha_{n+1,k,j}, \quad n = 1, \ldots, N. \tag{31}$$

and

$$r_n = \arg \max_{k \in R_{\mathrm{sec}}(n)} \max_j \alpha_{n+1,k,j}, \quad n = 1, \ldots, N. \tag{32}$$

It is complicated to derive the order statistical functions given the two relay-selection policies. Therefore, in this paper, we only provide simulation results of the SCP for the above two relay-selection policies.

For comparison, we also discuss conventional multi-hop transmission with a single RF relay at each intermediate hop. In this case, each hop is a basic three-node wiretap channel model and achieves a secure probability of $\eta/\eta + 1$. Hence, the SCP of the system is given by

$$P_{\mathrm{sc}}^{\mathrm{single}} = \left(\frac{n}{n+1}\right)^{N+1}. \tag{33}$$

V. Simulation Results

In this section, we provide experiment results for the SCP performance of the proposed HbHMinE scheme, as well as for the HbHMaxMaxL, HbHMaxMinL, E2EMinE, and E2EMaxL schemes. The SCPs for the optimal scheme and single-relay scheme are also presented as benchmarks. To clarify the illustration, we assume that each cluster has K relays.

In Fig. 2, we demonstrate the SCPs with respect to K for all cluster-aided multi-hop schemes and the optimal scheme, where K ranges from 2 to 8. N is set to be 5 and η is set to be 1. As proven in Section III-2(B), where SCPs for the two end-to-end schemes are identical when $\eta = 1$, we do not distinguish the two schemes in Fig. 2. The first observation is that analytical and simulation results of the proposed HbHMinE, as well as the end-to-end schemes, are in agreement, so our theoretical analysis is validated. As expected, the SCPs for all schemes increase as K increases, which shows the advantage of the proposed relay-selection technique. The SCP of HbHMinE is close to that of the optimal scheme, and it is higher than that of all of the other schemes. The HbHMaxMaxL scheme outperforms the HbHMaxMinL scheme, and both of them outperform the end-to-end schemes. The SCP of the end-to-end schemes is lower than that of all of the hop-by-hop schemes, which shows the advantage of hop-aware multi-hop relaying.

The SCPs with respect to the number of clusters are plotted in Fig. 3. N ranges from 1 to 6, and K is set to be 5, while η is set to be 1. Because the analytical results have been verified in Fig. 2, in the remainder of this section, the curves are depicted from the analytical results. First, we observe that the SCP of the HbHMinE scheme is close to that of the optimal scheme, and it remains almost constant as N increases. This suggests that the proposed RF hop-by-hop scheme adapts well to the multi-hop scenario. The SCPs of HbHMaxMaxL, HbHMaxMinL, and the end-to-end schemes decrease as N increases. The end-to-end scheme is inferior to all hop-by-hop schemes,

https://doi.org/10.4218/etrij.17.0117.0199

and HbHMaxMaxL slightly outperforms HbHMaxMinL. The SCP of the single-relay scheme is much lower than that of all the other cluster-aided schemes, and decreases rapidly as N increases.

Figure 4 shows the SCPs with respect to η, which ranges from 0.5 to 3. Recall that $\eta = \lambda_E/\lambda_M$. A large value of η means that a legitimate channel is statistically better than an eavesdropper channel, and vice versa. K and N are both set to be 5. As expected, the SCPs of all schemes increase with η, and the single-relay scheme is the lowest of them all. The SCP gap between HbHMinE and the optimal scheme becomes smaller as η increases. As opposed to the above two figures where the HbHMaxMaxL scheme is always superior to HbHMaxMinL, when η is higher than 2.5, HbHMaxMinL performs better than HbHMaxMaxL. Moreover, the curves of E2EMinE and E2EMaxL are no longer in agreement. When $\eta > 1$, E2EMinE is inferior to E2EMaxL, and when $\eta < 1$, E2EMinE is superior to E2EMaxL and even to the HbHMaxMaxL and HbHMaxMinL schemes when $\eta = 0.5$. The reason for this is that when the eavesdropper link is strong, it is more effective to choose the node that minimizes the eavesdropper link rather than maximizes the legitimate link.

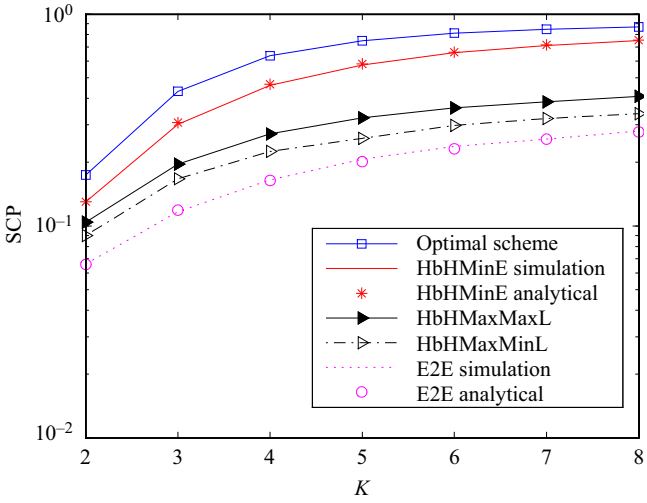


Fig. 2. SCP vs. number of nodes per cluster.

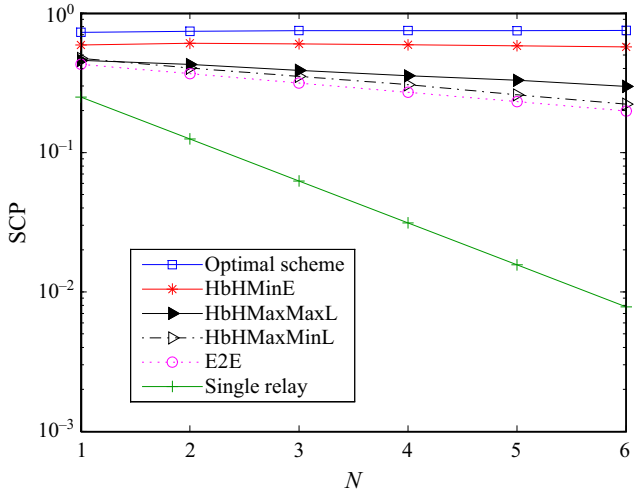


Fig. 3. SCP vs. number of clusters.

VI. Discussion and Conclusions

In this study, we investigated secure multi-hop transmission assisted by multiple RF relay clusters. We proposed a hop-by-hop transmission scheme with relay selection, and we derived analytical expressions of the SCP for the hop-by-hop transmission scheme. In addition, we studied end-to-end transmission schemes using two relay-selection policies. The experiment results validate our theoretical analysis and show that the SCP of the hop-by-hop transmission scheme is close to that of the optimal scheme. They also show that the proposed hop-by-hop scheme is superior to other comparison schemes, especially with a large number of hops or high eavesdropper channel quality.

In the system model, we assumed that there is a single eavesdropper. For the multiple-eavesdropper case, if each hop is wiretapped by multiple non-colluding eavesdroppers, the equivalent eavesdropper CNR is the maximum. If the eavesdroppers collude, the equivalent eavesdropper CNR is the summation of all of the CNR values. In the above cases, the framework of the computing SCP still applies, but the equivalent eavesdropper CNR is promoted and the SCP would be reduced. Other techniques, such as the use of multiple antennas and precoding are required. To promote the secrecy performance of clustered multi-hop transmission, another effective method is to explore the diversity of relay clusters. All of the above issues can be addressed in future works.

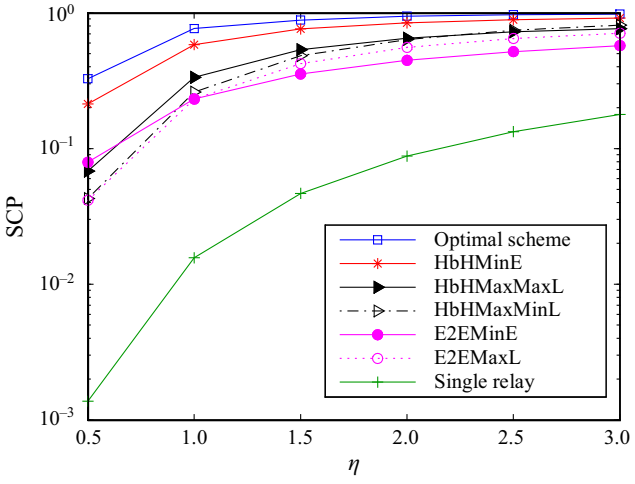


Fig. 4. SCP vs. parameter ratio of eavesdropper and legitimate channels.

References

[1] J. Barros and M.R.D. Rodrigues, "Secrecy Capacity of Wireless Channels," *IEEE Int. Symp. Inform. Theory*, Seattle, USA, Jul. 2006, pp. 356–360.

[2] L. Lai and H.E. Gamal, "The Relay-Eavesdropper Channel: Cooperation for Secrecy," *IEEE Trans. Inform. Theory*, vol. 54, no. 9, Sept. 2008, pp. 4005–4019.

[3] I. Krikidis, J.S. Thompson, and S. Mclaughlin, "Relay Selection for Secure Cooperative Networks with Jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, Oct. 2009, pp. 5003–5011.

[4] 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, Oct. 2013, pp. 2099–2111.

[5] I. Krikidis et al., "Full-Duplex Relay Selection for Amplify-and-Forward Cooperative Networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 12, Dec. 2012, pp. 4381–4393.

[6] X. Ding et al., "Security-Reliability Tradeoff Analysis of Artificial Noise Aided Two-Way Opportunistic Relay Selection," *IEEE Trans. Veh. Technol.*, vol. 66, no. 5, May 2017, pp. 3930–3941.

[7] G. Chen et al., "Max-Ratio Relay Selection in Secure Buffer-Aided Cooperative Wireless Networks," *IEEE Trans. Inform. Forensics Security*, vol. 9, no. 4, Apr. 2014, pp. 719–729.

[8] Y. Liu et al., "Relay Selection for Security Enhancement in Cognitive Relay Networks," *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, Feb. 2015, pp. 46–49.

[9] X. Chen et al., "Multi-Antenna Relay Aided Wireless Physical Layer Security," *IEEE Commun. Mag.*, vol. 53, no. 12, Dec. 2015, pp. 40–46.

[10] X. Chen et al., "Large-Scale MIMO Relaying Techniques for Physical Layer Security: AF or DF?" *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, Sept. 2015, pp. 5135–5146.

[11] J. Lee, "Full-Duplex Relay for Enhancing Physical Layer Security in Multi-hop Relaying Systems," *IEEE Commun. Lett.*, vol. 19, no. 4, Apr. 2015, pp. 525–528.

[12] J. Lee, "Optimal Power Allocation for Physical Layer Security in Multihop DF Relay Networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, Jan. 2016, pp. 28–38.

[13] L. Wang et al., "Cluster-Based Cooperative Jamming in Wireless Multi-hop Networks," *IEEE PIMRC*, London, UK, Sept. 8–11, 2013, pp. 169–174.

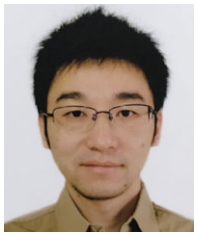
[14] T.T. Duy and H.Y. Kong, "Secrecy Performance Analysis of Multihop Transmission Protocols in Cluster Networks," *Wireless Personal Commun.*, vol. 82, no. 4, June 2015, pp. 2505–2518.

[15] O.O. Koyluoglu, C.E. Koksal and H.E. Gamal, "On Secrecy Capacity Scaling in Wireless Networks," *IEEE Trans. Infrom. Theory*, vol. 58, no. 5, May 2012, pp. 3000–3015.

[16] J. Mo, M. Tao and Y. Liu, "Relay Placement for Physical Layer Security: A Secure Connection Perspective," *IEEE Commun. Lett.*, vol. 16, no. 6, June 2012, pp. 878–881.

[17] C. Cai et al., "Secure Connectivity Using Randomize-and-Forward Strategy in Cooperative Wireless Networks," *IEEE Commun. Lett.*, vol. 17, no. 7, July 2013, pp. 1340–1343.

Xiaowei Wang received her BS degree in communication engineering from Jiangsu University, Zhenjiang, China, MS degree in control theory and engineering from Shanghai University, China, and PhD degree in communication and information systems from Shanghai Jiao Tong University, China. From June 2014 to June 2017, she worked as a postdoctoral fellow at the Department of Automation, Shanghai University. Currently, she is working with the College of Information Engineering, Shanghai Maritime University, Shanghai, PR China. Her research interests are in the fields of communication theory, wireless networks, and physical layer security.



Zhou Su received his BE and ME degrees from Xi'an Jiaotong University, China, and his PhD degree from Waseda University, Tokyo, Japan, all in electronics and information engineering. His research interests include multimedia communication, web performance, and network traffic. He received the best paper award at the International Conference CHINACOM2008, and the Funai Information Technology Award for Young Researchers 2009. He is an associate editor of IET Communications. He is a chair of an interest group of the IEEE Comsoc Society, Multimedia Communications Technical Committee, MENIG. He also served as a symposium co-chair at several international conferences, including IEEE VTC Spring 2016 and IEEE CCNC2011.

Guangyi Wang received his PhD degree in electronic science and technology from the South China University and Technology, Guangzhou, China, in 2004. He is currently a professor in the School of Electronics and Information, Hangzhou Dianzi University, China. His research interests include chaotic communications, chaotic information encryption, nonlinear circuits and systems, and memristor circuits.

https://doi.org/10.4218/etrij.17.0117.0199