Security-Aware Relaying Scheme for Cooperative Networks With Untrusted Relay Nodes

Li Sun, Pinyi Ren, Qinghe Du, Yichen Wang, and Zhenzhen Gao

***Abstract*—This paper studies the problem of secure transmission in dual-hop cooperative networks with untrusted relays, where each relay acts as both a potential helper and an eavesdropper. A security-aware relaying scheme is proposed, which employs the alternate jamming and secrecy-enhanced relay selection to prevent the confidential message from being eavesdropped by the untrusted relays. To evaluate the performance of the proposed strategies, we derive the lower bound of the achievable ergodic secrecy rate (ESR), and conduct the asymptotic analysis to examine how the ESR scales as the number of relays increases.**

***Index Terms*—Cooperative communications, untrusted relays, relay selection, secrecy rate.**

I. Introduction

RECENTLY, the applications of Physical-Layer Security (PLS) techniques in cooperative networks have attracted considerable attention. Among the candidate PLS solutions, cooperative jamming (CJ), which exploits the cooperating users to transmit the artificial noise, is a promising tool to combat eavesdropping [1], [2]. To harvest the diversity gain while guaranteeing the security requirement, great efforts have also been devoted to combine CJ and relay selection [3]–[5].

Common to [1]–[5] is that all of them assume the relays are trusted, and the eavesdroppers are external entities in addition to legitimate parties. However, in some applications, the relays themselves are *untrusted*, from which the transmitted messages must be kept secret. For example, in heterogeneous networks, the relays may have a lower security clearance (and thus a lower level of information access) than the source-destination pair. The research on untrusted relay systems was pioneered by He and Yener in [6], where the non-zero secrecy rate is proven to be achievable by enlisting the help of the destination who performs jamming. In [7], the joint beamforming design at the source and the relay was proposed for MIMO untrusted relay systems. In [8], the secrecy outage probabilities of several relaying schemes were analyzed. In [9], the power allocation policy was developed for amplify-and-forward (AF) untrusted relay systems.

Although diverse results on untrusted relay systems have been reported, the majority of existing works deal with the simple model with only one relay node. For multi-relay networks, [10] analyzed the relationship between the system secrecy capacity and the number of untrusted relays. Reference [11] proposed to use relay assignment and link adaptation to realize both secure and spectral-efficient communications. However, [10] and [11] only considered the information leakage problem during the first phase of any two-hop transmission. This simplifies the protocol design, but may not hold in practice.

Unlike [10] and [11], we in this paper try to secure the transmissions of both the first and the second phases, and our contributions are threefold: First, an alternate jamming method is introduced to prevent information leakage. Second, both optimal and sub-optimal secrecy-enhanced relay selection policies are proposed. Third, the lower bound of the achievable ergodic secrecy rate (ESR) is derived, and the asymptotic analysis of the ESR is given as well.

II. System Model

We consider a dual-hop AF network consisting of a source (S), a destination (D) and K untrusted relays ($R_k, k = 1, \ldots, K$). The direct link between S and D does not exist. Each node is employed with a single antenna and operates in a half-duplex mode. S transmits its signals frame by frame, and the transmission of each frame is composed of two phases, namely the broadcast phase (1st phase) and the relaying phase (2nd phase). The channel between any node pair (i, j), denoted by h_{ij}, is modeled by a complex Gaussian variable with mean zero and variance μ_{ij}. All channel coefficients remain constant within one frame and vary independently from frame to frame. The channels are assumed to be reciprocal, i.e., $h_{ij} = h_{ji}$. The total transmit power of each phase is constrained by P, and the additive noise at each receiver is characterized by a zero-mean, complex Gaussian variable with variance N_0. We denote the average signal-to-noise-ratio (SNR) per phase by $\rho = P/N_0$. For the considered channel model, $\gamma_{ij} \triangleq \rho|h_{ij}|^2$ follows an exponential distribution with the rate parameter $\lambda_{ij} = (\rho\mu_{ij})^{-1}$. Throughout this paper, $\log(\cdot)$ denotes the base-2 logarithm, $\mathrm{E}[\cdot]$ represents the expectation operator, and $[x]^+ = \max\{0, x\}$.

To prevent the source message from being eavesdropped at the untrusted relays, we propose to use an alternate jamming method, whose details are given as follows.

During the 1st phase, S transmits x_S with power αP and D sends the artificial noise n_D with power $(1-\alpha)P$, where $\alpha \in (0, 1)$ represents the power allocation factor. Thus, the received signal at any relay R_l during this phase is given by

$$y_l^{(1)} = h_{sl}\sqrt{\alpha P}x_S + h_{dl}\sqrt{(1-\alpha)P}n_D + w_l^{(1)}. \quad (1)$$

Manuscript received July 27, 2014; accepted December 10, 2014. Date of publication December 22, 2014; date of current version March 6, 2015. This work was partially supported by the National Natural Science Foundation of China (NSFC) under Grant No. 61102078, the open research fund of National Mobile Communications Research Laboratory, Southeast University under Grant No. 2012D04, and the Fundamental Research Funds for the Central Universities of China. The associate editor coordinating the review of this paper and approving it for publication was K. Tourki.

L. Sun is with the Department of Information and Communications Engineering, Xi'an Jiaotong University, Xi'an 710049, China, and also with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (e-mail: lisun@mail.xjtu.edu.cn).

P. Ren, Q. Du, and Z. Gao are with the Department of Information and Communications Engineering, Xi'an Jiaotong University, Xi'an 710049, China (e-mail: pyren@mail.xjtu.edu.cn; duqinghe@mail.xjtu.edu.cn; zhenzhen.gao@mail.xjtu.edu.cn).

Y. Wang is with the Department of Information and Communications Engineering, Xi'an Jiaotong University, Xi'an 710049, China, and also with the University of Maryland, College Park, MD 20742 USA (e-mail: wangyichen0819@mail.xjtu.edu.cn).

Digital Object Identifier 10.1109/LCOMM.2014.2385095

Throughout this paper, $w_m^{(n)}$ is the additive noise at node $m (m \in \{R_l, D\})$ within the n^{th} phase $(n \in \{1,2\})$.

During the 2nd phase, a single selected relay R_k normalizes its received signal $y_k^{(1)}$ and forwards it with power $\beta P (0 < \beta < 1)$. Note that all the non-selected relays can hear from R_k and act only as eavesdroppers. Therefore, we let S transmit the artificial noise n_S, with power $(1-\beta)P$, to jam these relays. Thus, at the end of the 2nd phase, the received signals at D and $R_l (l = 1,\ldots,K, l \neq k)$ can be expressed respectively as

$$y_d = h_{kd}\eta_k y_k^{(1)} + w_d^{(2)} \tag{2}$$

and

$$y_l^{(2)} = h_{kl}\eta_k y_k^{(1)} + h_{sl}\sqrt{(1-\beta)P}n_S + w_l^{(2)} \tag{3}$$

where $\eta_k = \sqrt{\frac{\beta P}{\alpha P|h_{sk}|^2 + (1-\alpha)P|h_{dk}|^2 + N_0}}$.

Since n_D is the transmitted signal from the destination during the previous phase, D can subtract the term $\sqrt{(1-\alpha)P}\eta_k h_{kd} h_{dk} n_D$ from y_d and then decode the source information based on the remainder. Consequently, the achievable rate at the destination can be calculated by

$$\mathcal{R}_D = \frac{1}{2}\log(1+\gamma_D) = \frac{1}{2}\log\left(1 + \frac{\alpha\beta\gamma_{sk}\gamma_{kd}}{1+\alpha\gamma_{sk}+(1+\beta-\alpha)\gamma_{kd}}\right). \tag{4}$$

Due to the half-duplex constraint, the selected relay R_k receives the source signal in the broadcast phase only, and thus its achievable rate is given by

$$\mathcal{R}_k = \frac{1}{2}\log\left(1+\gamma_k^{(1)}\right) = \frac{1}{2}\log\left(1 + \frac{\alpha\gamma_{sk}}{1+(1-\alpha)\gamma_{kd}}\right). \tag{5}$$

The non-selected relays R_l's $(l \neq k)$, on the other hand, can receive signals during both the 1st and 2nd phases, and combine $y_l^{(1)}$ and $y_l^{(2)}$ to extract the source information. For simplicity, we assume selection combining (SC) is adopted at these relay nodes. After some derivations, we can express the achievable rate at any non-selected relay R_l by

$$\mathcal{R}_l = \frac{1}{2}\log\left(1 + \max\left\{\gamma_l^{(1)}, \gamma_l^{(2)}\right\}\right) \tag{6}$$

where $\gamma_l^{(1)} = \frac{\alpha\gamma_{sl}}{1+(1-\alpha)\gamma_{ld}}$ and $\gamma_l^{(2)} = \frac{\alpha\beta\gamma_{sk}\gamma_{kl}}{\alpha\gamma_{sk}+(1-\beta)\gamma_{sl}(1+\alpha\gamma_{sk}+(1-\alpha)\gamma_{kd})+(1+(1-\alpha)\gamma_{kd})(1+\beta\gamma_{kl})}$.

For untrusted relay systems, any relay node acts as an eavesdropper, no matter whether it is the selected helper or not. According to [1, eq. (11)], the secrecy rate of the system, with R_k being the selected relay, can be calculated as

$$\begin{aligned}\mathcal{R}_s^{(k)} &= \left[\mathcal{R}_D - \max\left\{\mathcal{R}_k, \max_{1\le l\le K, l\neq k}\mathcal{R}_l\right\}\right]^+ \\ &= \left[\frac{1}{2}\log(1+\gamma_D) - \frac{1}{2}\log(1+\gamma_E)\right]^+,\end{aligned} \tag{7}$$

where $\gamma_E = \max\left\{\gamma_k^{(1)}, \max_{1\le l\le K, l\neq k}\{\max\{\gamma_l^{(1)}, \gamma_l^{(2)}\}\}\right\}$.

III. Secrecy-Enhanced Relay Selection

A. Optimal Selection Scheme

The secrecy-enhanced relay selection aims at maximizing the secrecy rate given by (7). To achieve this goal, the selected relay needs to satisfy

$$k^* = \arg\max_{1\le k\le K} \mathcal{R}_s^{(k)}. \tag{8}$$

It can be seen from (4)–(7) that, to select the optimal relay, the instantaneous channel state information (CSI) of all relaying links as well as that of all inter-relay links have to be acquired. Therefore, it is rather difficult to realize the optimal relay selection in practical systems, especially when the number of relays is large. This motivates us to design the sub-optimal relay selection strategy with a lower complexity.

B. Suboptimal Selection Scheme

The suboptimal relay selection scheme can be developed by examining the lower bound of the secrecy rate expression. To fulfil this, we first derive the lower bound of γ_D as follows:

$$\begin{aligned}\gamma_D &= \frac{\beta}{1+\beta-\alpha}\frac{\alpha\gamma_{sk}(1+\beta-\alpha)\gamma_{kd}}{1+\alpha\gamma_{sk}+(1+\beta-\alpha)\gamma_{kd}} \\ &\overset{(a)}{\ge} \frac{\beta}{1+\beta-\alpha}\left(\frac{\alpha\gamma_{sk}(1+\beta-\alpha)\gamma_{kd}}{\alpha\gamma_{sk}+(1+\beta-\alpha)\gamma_{kd}} - \frac{1}{4}\right) \\ &\ge \frac{\beta\min\left(\alpha\gamma_{sk}, (1+\beta-\alpha)\gamma_{kd}\right)}{2(1+\beta-\alpha)} - \frac{\beta}{4(1+\beta-\alpha)},\end{aligned} \tag{9}$$

where (a) is obtained by using [12, eq. (21)].

On the other hand, γ_E can be re-written as

$$\begin{aligned}\gamma_E &= \max\left\{\gamma_k^{(1)}, \max_{1\le l\le K, l\neq k}\left\{\max\left\{\gamma_l^{(1)}, \gamma_l^{(2)}\right\}\right\}\right\} \\ &= \max\left\{\max_{1\le l\le K}\left\{\gamma_l^{(1)}\right\}, \max_{1\le l\le K, l\neq k}\left\{\gamma_l^{(2)}\right\}\right\}.\end{aligned} \tag{10}$$

Since $\gamma_l^{(2)} (l \neq k)$ can be upper bounded by

$$\begin{aligned}\gamma_l^{(2)} &< \frac{\alpha\beta\gamma_{sk}\gamma_{kl}}{((1-\beta)\gamma_{sl}+1+\beta\gamma_{kl})(1+(1-\alpha)\gamma_{kd})} \\ &< \frac{\alpha\beta\gamma_{sk}\gamma_{kl}}{\beta\gamma_{kl}(1+(1-\alpha)\gamma_{kd})} = \frac{\alpha\gamma_{sk}}{1+(1-\alpha)\gamma_{kd}} = \gamma_k^{(1)},\end{aligned} \tag{11}$$

γ_E can be further simplified as

$$\gamma_E = \max_{1\le l\le K}\left\{\gamma_l^{(1)}\right\} = \max_{1\le l\le K}\left\{\frac{\alpha\gamma_{sl}}{1+(1-\alpha)\gamma_{ld}}\right\}. \tag{12}$$

By substituting (9) and (12) into (7), we can obtain the lower bound of the instantaneous secrecy rate under the assumption that R_k is the selected relay. Now, instead of maximizing the secrecy rate in (7), we try to maximize this lower bound, and develop the sub-optimal relay selection strategy as

$$k^* = \arg\max_{1\le k\le K}\min\left(\alpha\gamma_{sk}, (1+\beta-\alpha)\gamma_{kd}\right). \tag{13}$$

The proposed scheme in (13) only requires the instantaneous CSIs of the source-relay and relay-destination links, and does not depend on the availability of the inter-relay channel coefficients. Thus, it can be realized in a distributed manner [3], which enjoys a low complexity.

IV. Ergodic Secrecy Rate Analysis

In this section, the lower bound of the ESR achieved by the proposed sub-optimal strategy is derived. For mathematical convenience, we assume all λ_{sk}'s are identical and denote them by λ_{sr}. The same assumption holds as well for all λ_{kd}'s, i.e., $\lambda_{kd} = \lambda_{rd}$ for all k's. By plugging (9) and (12) into (7) and letting $k = k^*$, we can lower bound the ESR by (14), which is shown at the bottom of the next page.

For the considered channel model, $\alpha\gamma_{sk}$ and $(1+\beta-\alpha)\gamma_{kd}$ are exponentially distributed with rate parameters $\frac{\lambda_{sr}}{\alpha}$ and $\frac{\lambda_{rd}}{(1+\beta-\alpha)}$, respectively. Let $Z=\min(\alpha\gamma_{sk^*},(1+\beta-\alpha)\gamma_{k^*d})$. According to the probability density function (PDF) of exponential variables and order statistics, the PDF of Z can be expressed as $f_Z(z)=K\lambda e^{-\lambda z}(1-e^{-\lambda z})^{K-1}$, where $\lambda=\frac{\lambda_{sr}}{\alpha}+\frac{\lambda_{rd}}{(1+\beta-\alpha)}$. Therefore, after some mathematical manipulations, we have

$$\begin{aligned}&\mathrm{E}\left[\frac{1}{2}\log\left(1+\frac{\beta\left[2\min\left(\alpha\gamma_{sk^*},(1+\beta-\alpha)\gamma_{k^*d}\right)-1\right]}{4(1+\beta-\alpha)}\right)\right]\\&=\frac{K}{2\ln 2}\sum_{k=0}^{K-1}\binom{K-1}{k}\frac{(-1)^k}{k+1}\left[\ln\left(1-\frac{\beta}{4(1+\beta-\alpha)}\right)\right.\\&\left.-e^{\frac{(k+1)\lambda(4+3\beta-4\alpha)}{2\beta}}E_i\left(-\frac{(k+1)\lambda(4+3\beta-4\alpha)}{2\beta}\right)\right],\end{aligned}\tag{15}$$

where we have utilized [13, eq. (4.337.1)], and $E_i(x)$ is the exponential integral function defined in [13, eq. (8.21)].

Now attention is shifted to the calculation of $\mathrm{E}[\frac{1}{2}\log(1+\max_{1\le l\le K}\frac{\alpha\gamma_{sl}}{1+(1-\alpha)\gamma_{ld}})]=\mathrm{E}[\frac{1}{2}\log(1+\gamma_E)]$. By resorting to the order statistics, we can obtain the cumulative distribution function (CDF) of γ_E as

$$F_{\gamma_E}(x)=\left[1-\frac{\lambda_{rd}}{\lambda_{rd}+\frac{\lambda_{sr}(1-\alpha)}{\alpha}x}e^{-\frac{\lambda_{sr}}{\alpha}x}\right]^K.\tag{16}$$

Using the above CDF expression and doing some tedious derivations, we have

$$\begin{aligned}&\mathrm{E}\left[\frac{1}{2}\log\left(1+\max_{1\le l\le K}\frac{\alpha\gamma_{sl}}{1+(1-\alpha)\gamma_{ld}}\right)\right]\\&=\frac{-1}{2\ln 2}\sum_{k=1}^{K}\binom{K}{k}\left(\frac{-\alpha\lambda_{rd}}{\lambda_{sr}(1-\alpha)}\right)^k\underbrace{\int_0^\infty G(x)e^{-\frac{\lambda_{sr}kx}{\alpha}}dx}_{I_1},\end{aligned}\tag{17}$$

where $G(x)=(1+x)^{-1}(x+\frac{\lambda_{rd}\alpha}{\lambda_{sr}(1-\alpha)})^{-k}$. Exploiting [13, eq. (3.352.4)], [13, eq. (3.353.2)], and the partial fraction expansion technique, we can simplify I_1 as

$$\begin{aligned}I_1=&-A_{11}e^{\frac{\lambda_{sr}k}{\alpha}}E_i\left(-\frac{\lambda_{sr}k}{\alpha}\right)-A_{21}e^{\frac{\lambda_{rd}k}{1-\alpha}}E_i\left(-\frac{\lambda_{rd}k}{1-\alpha}\right)\\&+\sum_{p=2}^{k}A_{2p}\left[\sum_{t=1}^{p-1}\frac{(t-1)!}{(p-1)!}\left(-\frac{\lambda_{sr}k}{\alpha}\right)^{p-t-1}\left(\frac{\alpha\lambda_{rd}}{\lambda_{sr}(1-\alpha)}\right)^{-t}\right.\\&\left.-\frac{\left(-\frac{\lambda_{sr}k}{\alpha}\right)^{p-1}}{(p-1)!}e^{\frac{\lambda_{rd}k}{1-\alpha}}E_i\left(-\frac{\lambda_{rd}k}{1-\alpha}\right)\right],\end{aligned}\tag{18}$$

where A_{ip} ($i=1,2$ and $1\le p\le k$) is given by $A_{ip}=\frac{1}{(\sigma_i-p)!}\left[\frac{d^{\sigma_i-p}}{dx^{\sigma_i-p}}[(x-\rho_i)^{\sigma_i}G(x)]\right]\Big|_{x=\rho_i}$ with $\sigma_1=1$, $\sigma_2=k$, $\rho_1=-1$, and $\rho_2=-\frac{\lambda_{rd}\alpha}{\lambda_{sr}(1-\alpha)}$.

Substituting (15), (17), and (18) into (14), we can obtain the closed-form expression for the ESR lower bound. However, we omit its explicit expression due to page limit. The tightness of this bound will be verified via simulations in Section VI.

V. Asymptotic Analysis of Ergodic Secrecy Rate

Now we focus on the large-K case and study how the ESR scales as the number of relays increases. Here, the extreme-value theory (EVT) will be used to facilitate the analysis. The main results of EVT can be found in [14, Sec. III].

The lower bound of ESR is shown in (14). To perform the asymptotic analysis, we define $\gamma_D^{(k)}=\frac{\beta[2\min(\alpha\gamma_{sk},(1+\beta-\alpha)\gamma_{kd})-1]}{4(1+\beta-\alpha)}$. It can be easily verified that $\gamma_D^{(k)}$ belongs to Type I domain of attraction (See [14] for its definition.). Consequently, $\max_{1\le k\le K}\gamma_D^{(k)}$ converges in distribution to $a_K^D\mu+b_K^D$ as $K\to\infty$, where μ is a Gumbel-distributed random variable [14], and a_K^D and b_K^D are respectively given by

$$a_K^D=\frac{\beta}{2\lambda(1+\beta-\alpha)}\tag{19}$$

and

$$b_K^D=a_K^D\ln\left(Ke^{-\frac{1}{2}\lambda}\right)=\frac{\beta\ln\left(Ke^{-\frac{\lambda}{2}}\right)}{2\lambda(1+\beta-\alpha)}.\tag{20}$$

Based on *Lemma* in [14], there exist sequences of constants $c_K^D=\frac{\log(e)a_K^D}{1+b_K^D}$ and $d_K^D=\log(1+b_K^D)$ such that $\log(1+\max_{1\le k\le K}\gamma_D^{(k)})$ can be well approximated by $c_K^D\delta^D+d_K^D$ for large K, where δ^D obeys the Gumbel distribution.

Following similar steps we can derive that, as K tends to infinity, $\log(1+\max_{1\le l\le K}\frac{\alpha\gamma_{sl}}{1+(1-\alpha)\gamma_{ld}})$ converges in distribution to $c_K^R\delta^R+d_K^R$, where δ^R is a random variable following the Gumbel distribution, and c_K^R and d_K^R are given as $c_K^R=\frac{\log(e)a_K^R}{1+b_K^R}$ and $d_K^R=\log(1+b_K^R)$, with a_K^R and b_K^R being calculated by

$$a_K^R=\frac{\alpha}{\lambda_{sr}}\left(1+\frac{1-\alpha}{\lambda_{rd}+\frac{(1-\alpha)\lambda_{sr}b_K^R}{\alpha}}\right)^{-1}\tag{21}$$

and

$$b_K^R=\frac{\alpha}{\lambda_{sr}}\left(W\left(\frac{K\lambda_{rd}}{1-\alpha}e^{\frac{\lambda_{rd}}{1-\alpha}}\right)-\frac{\lambda_{rd}}{1-\alpha}\right)\tag{22}$$

respectively. In (22), $W(x)$ is the Lambert-W function.

By combining the above results with (14) and performing the statistical average, we have (for large K)

$$\mathcal{R}_s^{(LB)}\approx\left[\frac{1}{2}\left(\kappa\left(c_K^D-c_K^R\right)+\left(d_K^D-d_K^R\right)\right)\right]^+\tag{23}$$

where $\kappa\approx 0.577$ is the Euler constant.

$$\begin{aligned}\mathcal{R}_s\ge&\mathrm{E}\left\{\left[\frac{1}{2}\log\frac{1+\frac{\beta[2\min(\alpha\gamma_{sk^*},(1+\beta-\alpha)\gamma_{k^*d})-1]}{4(1+\beta-\alpha)}}{1+\max_{1\le l\le K}\frac{\alpha\gamma_{sl}}{1+(1-\alpha)\gamma_{ld}}}\right]^+\right\}\ge\left\{\mathrm{E}\left(\frac{1}{2}\log\frac{1+\frac{\beta[2\min(\alpha\gamma_{sk^*},(1+\beta-\alpha)\gamma_{k^*d})-1]}{4(1+\beta-\alpha)}}{1+\max_{1\le l\le K}\frac{\alpha\gamma_{sl}}{1+(1-\alpha)\gamma_{ld}}}\right)\right\}^+\\=&\left\{\mathrm{E}\left[\frac{1}{2}\log\left(1+\frac{\beta\left[2\min\left(\alpha\gamma_{sk^*},(1+\beta-\alpha)\gamma_{k^*d}\right)-1\right]}{4(1+\beta-\alpha)}\right)\right]-\mathrm{E}\left[\frac{1}{2}\log\left(1+\max_{1\le l\le K}\frac{\alpha\gamma_{sl}}{1+(1-\alpha)\gamma_{ld}}\right)\right]\right\}^+\triangleq\mathcal{R}_s^{(LB)}.\end{aligned}\tag{14}$$

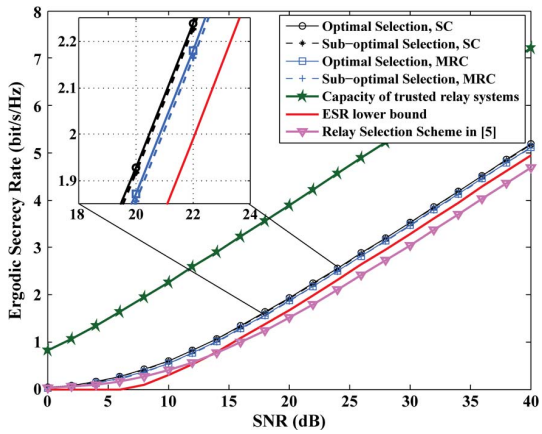

Fig. 1. Ergodic secrecy rate versus the average SNR per phase, where $K = 4$, $\mu_{sr} = 3$, $\mu_{rd} = 5$, and $\mu_{rr} = \mathrm{E}[|h_{R_iR_j}|^2] = 10$ for all i's and j's.

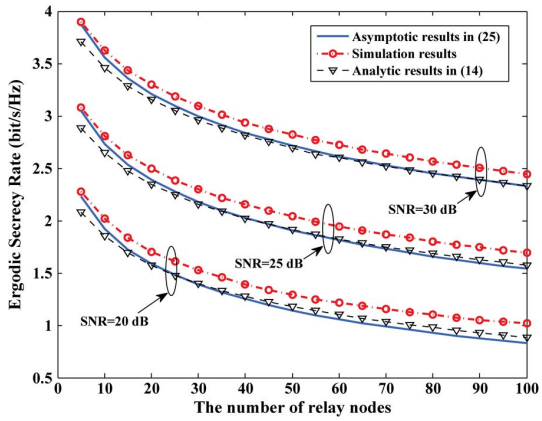

Fig. 2. Ergodic secrecy rate versus the number of relay nodes (K), where $\mu_{sr} = \mu_{rd} = \mu_{rr} = 10$.

It is not hard to verify that, as $K \to \infty$, $c_K^D \ll d_K^D$ and $c_K^R \ll d_K^R$. Therefore, the asymptotic expression for the lower bound of the ESR can be further approximated as

$$\mathcal{R}_s^{(LB)} \approx \left[\frac{1}{2}\left(d_K^D - d_K^R\right)\right]^+ = \left[\frac{1}{2}\log\frac{1+b_K^D}{1+b_K^R}\right]^+. \quad (24)$$

By plugging (20) and (22) into (24) and exploiting the fact $W(x) \approx \ln x - \ln\ln x$ for large x, we can re-write (24) as

$$\mathcal{R}_s^{(LB)} \approx \left[\frac{1}{2}\log\frac{1+a_K^D\ln K - \frac{1}{2}\lambda a_K^D}{1+\frac{\alpha}{\lambda_{sr}}\left(\ln\frac{K\lambda_{rd}}{1-\alpha} - \ln\ln\left(\frac{K\lambda_{rd}}{1-\alpha}e^{\frac{\lambda_{rd}}{1-\alpha}}\right)\right)}\right]^+. \quad (25)$$

It can be proven that the right-hand side of (25) is a decreasing function of K. This implies that, although the untrusted relays can assist the $S \to D$ transmission, the achievable ESR will degrade when deploying more relays.

VI. Simulation Results and Discussions

In this section, simulations are carried out to validate the proposed schemes. For simplicity, we set $\alpha = \beta = 0.5$. In the following figures, the notation "SNR" represents the ratio of P to N_0, i.e., ρ in Section II.

Fig. 1 exhibits the ESR performances for the proposed optimal and suboptimal relay selection schemes, where two combining methods (i.e., MRC and SC) are assumed to be adopted at the relay nodes. The ESR of the AF system with trusted relays, which is the Shannon capacity of the system, is provided to show the performance loss incurred by the untrustworthy behaviors of the relays. In addition, we compare the ESR achieved by our design with that of the selection policy in [5, eq. (10)]. It is observed from Fig. 1 that, the proposed sub-optimal relay selection scheme can achieve near-optimal performance, and the ESR differences between the sub-optimal and the optimal schemes are negligible. When MRC is adopted, the proposed policy in (13) works as well, and its achieved ESR performance is also very satisfactory. Further, the derived lower bound is tight for medium to high SNRs, verifying our theoretical analysis. A final observation is that, our scheme can yield a significant performance gain compared to the existing counterpart in [5].

The achievable ESR versus the number of relays (K) for the suboptimal relay selection scheme is depicted in Fig. 2, where the results in (14) and (25) are also plotted. Fig. 2 shows that, the ESR decreases as K increases, which is in accordance with the analysis in Section V. An intuitive explanation to this phenomenon is that, although the existence of more relays provides a higher probability to select a better helper, it also increases the amount of information leakage, where the latter is the dominant factor.

References

[1] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
[2] X. Zhou, M. Tao, and R. A. Kennedy, "Cooperative jamming for secrecy in decentralized wireless networks," in *Proc. IEEE ICC*, Ottawa, ON, Canada, Jun. 2012, pp. 2339–2344.
[3] A. Bletsas, A. Khisti, D. P. Reed, and A. Lippman, "A simple cooperative diversity method based on network path selection," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 3, pp. 659–672, Mar. 2006.
[4] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay selection for secure cooperative networks with jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003–5011, Oct. 2009.
[5] V. N. Q. Bao and N. L.-T. M. Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 12, pp. 6076–6085, Dec. 2013.
[6] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, Aug. 2010.
[7] C. Jeong, I.-M. Kim, and D. I. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system," *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 310–325, Jan. 2012.
[8] J. Huang, A. Mukherjee, and A. L. Swindlehurst, "Secure communication via an untrusted non-regenrative relay in fading channels," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2536–2550, May 2013.
[9] L. Wang, M. Elkashlan, J. Huang, N. H. Tran, and T. Q. Duong, "Secure transmission with optimal power allocation in untrusted relay networks," *IEEE Wireless Commun. Lett.*, vol. 3, no. 3, pp. 289–292, Jun. 2014.
[10] L. Sun, T. Zhang, Y. Li, and H. Niu, "Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3801–3807, Oct. 2012.
[11] H. Khodakarami and F. Lahouti, "Link adaptation with untrusted relay assignment: Design and performance analysis," *IEEE Trans. Commun.*, vol. 61, no. 12, pp. 4874–4883, Dec. 2013.
[12] A. Behnad, R. Parseh, and H. Khodakarami, "Upper bound for the performance metrics of amplify-and-forward cooperative networks based on harmonic mean approximation," in *Proc. 18th ICT*, Ayia Napa, Cyprus, May 2011, pp. 157–161.
[13] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. New York, NY, USA: Academic, 2007.
[14] Ö. Oyman, "Opportunism in multiuser relay channels: Scheduling, routing and spectrum reuse," in *Proc. IEEE ISIT*, Nice, France, Jun. 2007, pp. 286–290.