SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

August 2022, Vol. 65 182304:1–182304:15
https://doi.org/10.1007/s11432-021-3259-0

Secure coordinated direct and untrusted relay transmissions via interference engineering

Lu LV[1,2], Zan LI[1*], Haiyang DING[3], Yuchen ZHOU[1] & Jian CHEN[1]

[1]*State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an* 710071*, China;*
[2]*National Mobile Communications Research Laboratory, Southeast University, Nanjing* 210096*, China;*
[3]*School of Information and Communications, National University of Defense Technology, Wuhan* 430035*, China*

Received 20 January 2021/Revised 19 March 2021/Accepted 8 May 2021/Published online 25 July 2022

Abstract This paper investigates the physical layer security issue of the coordinated direct and untrusted relay transmissions, considering both uplink and downlink scenarios. To effectively prevent the untrusted relay from eavesdropping on the confidential information it receives, two novel interference-assisted jamming schemes are proposed, where the inter-user interference and the artificial noise are intelligently engineered to degrade the signal reception quality at the untrusted relay, therefore enhancing the physical layer security for the uplink and downlink coordinated transmission, respectively. For each of the two proposed jamming schemes, a lower bound for the ergodic secrecy sum rate (ESSR) is derived in closed form to evaluate the secrecy performance. To obtain more system design insights, we further provide an asymptotic analysis for the ESSR scaling laws over the regimes of the high signal-to-noise ratio and a large number of antennas at the base-station. We carry out computer simulations to confirm the accuracy of the derived theoretical analysis. Our simulation results show that the proposed jamming schemes achieve a similar asymptotic performance limit to the case of using a trusted relay. Moreover, the proposed jamming schemes guarantee perfect security for both uplink and downlink coordinated transmissions, and yield a significant ESSR improvement compared with three other baseline schemes.

Keywords physical layer security, untrusted relay, interference exploitation, coordinated transmission, ergodic secrecy rate

Citation Lv L, Li Z, Ding H Y, et al. Secure coordinated direct and untrusted relay transmissions via interference engineering. Sci China Inf Sci, 2022, 65(8): 182304, https://doi.org/10.1007/s11432-021-3259-0

1 Introduction

As a complement to cryptography-based methods, physical layer security is an effective technique to safeguard wireless communications [1–6]. The key idea of physical layer security is to exploit the dynamic nature of wireless channels, such as fading and interference, to increase the rate of the legitimate channel (from a legitimate transmitter to its legitimate receiver) and/or decrease the rate of the wiretap channel (from the legitimate transmitter to an eavesdropper). Thus, a positive rate difference (i.e., the secrecy rate) is achieved and perfect security can be guaranteed. Recent developments on physical layer security have demonstrated the benefits of utilizing relays to improve the secrecy rate.

Generally, relays can provide cooperative transmission to enhance the legitimate channel. By recruiting the small-cell base-station (BS) as a relay, relay coordinated multi-point transmission schemes were developed to improve the signal reception quality at the legitimate receiver against eavesdropping in [7]. With the aid of multi-antenna techniques, the zero-forcing (ZF) and maximal ratio transmission based secure beamforming strategies were proposed in [8]. To strike a favorable trade-off between the secrecy performance and processing complexity at the relay, various advanced relay selection criteria were devised to lower the secrecy outage probability in [9–11]. In addition to cooperative transmission, relays can also perform cooperative jamming, which exploits interference to impair the wiretap channel. In [12], a dynamic cooperation strategy was developed, where the relay switches between the relaying mode

* Corresponding author (email: zanli@xidian.edu.cn)

(i.e., signal forwarding) and the jamming mode (i.e., artificial noise (AN) injection) to maximize the ergodic secrecy rate. When multiple relays are available, a collaborative jamming scheme that completely nulls out the AN at the legitimate receiver was proposed in [13]. Furthermore, careful integration of cooperation and jamming can take advantage of both for security enhancement, for example in [14], a hybrid cooperative beamforming and jamming strategy using a multi-antenna relay was investigated. In [15, 16], joint beamforming and cooperative jamming were proposed to secure cooperative systems.

The aforementioned studies rely on a common assumption that the relay is a trusted helper to facilitate cooperation. However, this is not always the case. For example, in tactical networks, the relay may have a lower security level to access the confidential message. Such a relay is called an untrusted relay, which plays dual roles as a helper and an eavesdropper [17]. Along this line of research, an exciting result is that perfect security can be still guaranteed by appropriately utilizing the untrusted relay [18–26]. In [18], a destination-based jamming scheme was proposed in an amplify-and-forward (AF) relay network, where the destination shields the source information by transmitting the AN. As a result, only the untrusted relay is misled by the AN, while the destination knows the AN a priori and can cancel it completely. In [19], a source-based jamming scheme was presented, in which the source simultaneously transmits the information-bearing signal and jamming signal, and the jamming signal is used to deliberately confuse the untrusted relay. The joint design of cooperative jamming and relay selection with multiple untrusted relays was investigated in [20]. Robust secure precoding and power allocation for multi-antenna untrusted relay networks were studied in [21]. In [22], a non-orthogonal relaying scheme with antenna selection for improving the secrecy sum rate was analyzed. In [23], the notion of constellation rotation was applied in securing two-way untrusted relay networks. By rotating the signal constellation and emitting the AN, the eavesdropping capability at the untrusted relay is degraded. More recently, secure transmission in untrusted relay networks with non-orthogonal multiple access (NOMA) was studied in [24–26].

Based on the above-reviewed research efforts, we make the following important observations:

• Existing studies focus on secure untrusted relay networks with non-coordinated transmission. However, introducing a well-designed coordinated transmission scheme to untrusted relay networks is beneficial to physical layer security: (1) Coordinated transmission can considerably increase the sum rate of the legitimate channel, which is helpful to improving the secrecy rate; (2) If appropriately engineered, the originally detrimental inter-user interference (IUI) in coordinated transmission can be exploited as a source of useful jamming to confuse the untrusted relay, which has yet been reported in the literature.

• Although our initial work in [26] investigated a security enhanced NOMA coordinated transmission, it has the following disadvantages: (1) The secrecy rate of the relayed user converges to a constant at high the signal-to-noise ratio (SNR), and secrecy may be compromised if the untrusted relay enjoys a much better channel condition; (2) Successive interference cancellation (SIC) is required at all the receivers, resulting in a very high processing complexity; (3) Due to the single antenna setup, the BS fails to decouple the users' signals from the coordinated transmission of the direct user and the untrusted relay into parallel substreams for IUI-free decoding, leading to a secrecy rate floor. Thus far, these drawbacks have not been carefully addressed.

Motivated by the above, in this paper, we investigate secrecy design and performance analysis for coordinated direct transmission for a center user (CU) and relaying transmission for an edge user (EU), where the IUI and AN are intelligently engineered in the uplink and downlink respectively, to combat the untrusted relay without affecting the legitimate signal reception. The main contributions of this paper can be summarized as follows.

• First, we consider coordinated direct and untrusted relay transmission in the uplink, where a novel IUI-aided jamming scheme is proposed to guarantee security. In particular, during the first phase, the IUI from the coordinated transmission of the EU and the CU is exploited to jam the relay, even if the relay has the SIC capability. During the second phase, the BS employs the ZF detection to distinguish the two substreams from the coordinated transmission of the relay and the CU, so as to achieve a higher sum rate. Thanks to the half-duplex constraint, the relay will receive nothing for signal interception.

• Second, we focus on coordinated direct and untrusted relay transmission in the downlink, where a novel AN-aided jamming scheme is devised to improve the transmission secrecy. Particularly, during the first phase, the BS sends the EU's signal and the CU emits the AN. During the second phase, the relay forwards its received signal, and the EU can ideally remove the AN since it already knows the AN in the first phase, such that only the relay is jammed by the AN. The BS sends a superimposed mixture of the CU's signal and the weighted EU's signal, where the weight coefficient is specifically designed to enable the CU to linearly cancel the EU's signal. Thus, the reception quality of the CU will not be degraded,

while the relay overhears nothing in this phase due to its half-duplex feature.

• Third, for each of the proposed schemes, we evaluate the secrecy performance by deriving a lower bound on the ergodic secrecy sum rate (ESSR) and the asymptotic ESSR scaling laws in the high SNR and a large number of antenna regimes. We carry out computer simulations to confirm the accuracy of the derived analytical results. Various useful insights are revealed: (1) The proposed schemes always achieve a positive secrecy sum rate, i.e., perfect security; (2) The proposed schemes outperform three other baseline schemes on the ESSR, and the ESSR gap between them enlarges with an increase in the SNR; (3) The proposed schemes can achieve a similar asymptotic ESSR performance to the case with a trusted relay, making our schemes very attractive for securing coordinated direct and untrusted relay transmissions.

The remainder of this paper is organized as follows. Section 2 introduces the considered system model. In Sections 3 and 4, we investigate the design and analysis for secrecy coordinated direct and untrusted relay transmission in the uplink and downlink, respectively. In Section 5, we provide simulation results to validate the proposed interference assisted jamming schemes. Finally, the paper is briefly concluded in Section 6.

Throughout this paper, the following notations will be used: boldface lowercase and uppercase letters are vectors and matrices, respectively; $\boldsymbol{I}_M$ is an $M \times M$ identity matrix; $[\cdot]^{\mathrm{T}}$ is the transpose operation; $[\cdot]^{\dagger}$ is the Hermitian transpose; $[\cdot]_{n,n}$ is the n-th diagonal element of a square matrix; $\|\cdot\|$ is the Euclidean norm of a vector; $\log(\cdot)$ is the natural logarithm; $\mathrm{E}[\cdot]$ is the expectation operation; "$\simeq$" indicates "be asymptotically equal to"; $\Gamma(\cdot)$ is the Gamma function; and $\mathrm{Ei}[\cdot]$ is the exponential integral function [27, eq. (8.211.1)].

2 System model

Consider a cooperative communication scenario consisting of one BS, one AF relay (R), one CU located very close to the BS, and one EU located at the cell edge. Hereafter, we use subscripts b, r, cu, and eu to denote the BS, R, CU, and EU, respectively. The direct BS-CU link is available for signal transmission. However, the direct BS-EU link is assumed to be severely blocked due to obstacles, and thus, the BS has to ask for the relaying service of R to communicate with the EU. We assume that R is data level untrusted and acts as an eavesdropper to decipher the confidential information of EU and CU. The BS is equipped with M antennas, while the other nodes have a single antenna. All nodes work in a half-duplex mode.

All the channels undergo quasi-static block fading and channel reciprocity is assumed. Specifically, the channel vectors between the BS and CU/R are denoted by $\boldsymbol{h}_{\mathrm{b,cu}}$ and $\boldsymbol{h}_{\mathrm{b,r}}$, whose elements are $h_{m,\mathrm{cu}}$ and $h_{m,\mathrm{r}}$ for $m = 1, \ldots, M$, and the channel coefficients between R and CU/EU are denoted by $h_{\mathrm{r,cu}}$ and $h_{\mathrm{r,eu}}$. With all the antennas at the BS being located much closer to each other compared to their distances to CU and R, it is reasonable to assume that the elements in $\boldsymbol{h}_{\mathrm{b,cu}}$ and $\boldsymbol{h}_{\mathrm{b,r}}$ follow independent and identically distributed complex Gaussian distribution with zero mean and variances of $\lambda_{\mathrm{b,cu}}$ and $\lambda_{\mathrm{b,r}}$. Similarly, the channel coefficients $h_{\mathrm{r,cu}}$ and $h_{\mathrm{r,eu}}$ are modeled as independent complex Gaussian random variables with mean equal to zero and variances equal to $\lambda_{\mathrm{r,cu}}$ and $\lambda_{\mathrm{r,eu}}$. We consider both the channel's large-scale path loss and the small-scale fading, such that $\lambda_{\mathrm{b,cu}} = d_{\mathrm{b,cu}}^{-\eta}$, $\lambda_{\mathrm{b,r}} = d_{\mathrm{b,r}}^{-\eta}$, $\lambda_{\mathrm{r,cu}} = d_{\mathrm{r,cu}}^{-\eta}$, and $\lambda_{\mathrm{r,eu}} = d_{\mathrm{r,eu}}^{-\eta}$, where d denotes the distance and η denotes the path-loss exponent. In addition, the average transmit power of each node is limited to P, the additive white Gaussian noise (AWGN) at each node has zero mean and variance of λ_0, and the transmission bandwidth is normalized to one.

3 Uplink secure coordinated transmission

This section first proposes a novel IUI-aided jamming scheme for secure uplink coordinated transmission. Then, the ESSR analysis is presented to verify the security advantages of the proposed scheme.

3.1 Scheme description

As shown in Figure 1, the proposed scheme can be carried out over two consecutive phases. During the first phase, CU and EU send the signals s_1 and s_2, respectively, where $\mathrm{E}[|s_1|^2] = \mathrm{E}[|s_2|^2] = 1$.

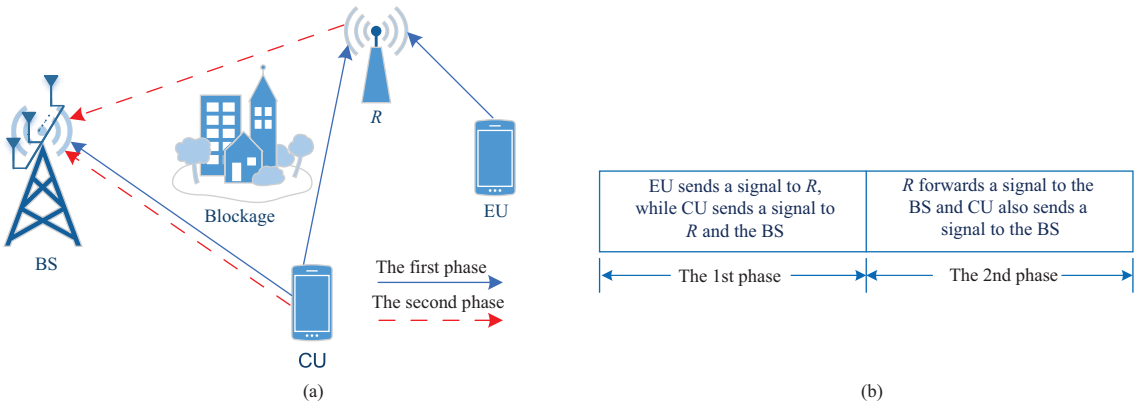

Figure 1 (Color online) The IUI-aided jamming scheme for uplink secure coordinated transmission. (a) An illustration of the IUI-aided jamming; (b) general principle of the IUI-aided jamming.

Accordingly, the received signals at the BS and R can be expressed as

$$\boldsymbol{y}_{\mathrm{b},1} = \sqrt{P}\boldsymbol{h}_{\mathrm{b,cu}}s_1 + \boldsymbol{n}_{\mathrm{b},1}, \tag{1}$$

$$y_{\mathrm{r},1} = \sqrt{P}h_{\mathrm{r,cu}}s_1 + \sqrt{P}h_{\mathrm{r,eu}}s_2 + n_{\mathrm{r}}, \tag{2}$$

where $\boldsymbol{n}_{b,1}$ is the AWGN vector at the BS of the first phase and n_{r} is the AWGN at R.

To maximally enhance the signal reception quality, the BS applies a detection vector $\boldsymbol{p} = \boldsymbol{h}_{\mathrm{b,cu}}^{\dagger}/\|\boldsymbol{h}_{\mathrm{b,cu}}\|$ to its observations. Therefore, the transmission rate at the BS for s_1 is given by

$$R_{\mathrm{b}}^{s_1} = \frac{1}{2}\log\left(1+\rho\|\boldsymbol{h}_{\mathrm{b,cu}}\|^2\right), \tag{3}$$

where $\rho = P/\lambda_0$ denotes the average SNR at each node. On the other hand, R tries to decode s_1 and s_2 for interception. Here, we make a worst-case assumption from the legitimate users' perspective that R has an enhanced eavesdropping capability and can perform SIC [26], which yields a performance lower bound for the investigated system. Without loss of generality, it is assumed that R decodes s_1 and s_2 using the SIC ordering $s_1 \to s_2$, and the reverse SIC ordering can be treated similarly. When R decodes s_1, the simultaneous signal transmission of CU will cause the IUI to its signal decoding, and such IUI can be judiciously exploited to degrade R's signal reception quality. As thus, the achievable eavesdropping rate (also means the channel capacity) at R for s_1 is given by

$$R_{\mathrm{r}}^{s_1} = \frac{1}{2}\log\left(1+\frac{|h_{\mathrm{r,cu}}|^2}{|h_{\mathrm{r,eu}}|^2+1/\rho}\right). \tag{4}$$

After that, R decodes s_2 using SIC. If $R_{\mathrm{r}}^{s_1} < R_{\mathrm{b}}^{s_1}$ (which means that the channel capacity of s_1 falls below its transmission rate), R cannot decode s_1 correctly, and s_1 is exploited as a useful jamming signal to confuse R. Otherwise, R can first decode and remove s_1 perfectly, and then decode s_2 without interference. Accordingly, the achievable eavesdropping rate at R for s_2 is given by

$$R_{\mathrm{r}}^{s_2} = \begin{cases} \dfrac{1}{2}\log\left(1+\dfrac{|h_{\mathrm{r,eu}}|^2}{|h_{\mathrm{r,cu}}|^2+1/\rho}\right), & \text{if } R_{\mathrm{r}}^{s_1} < R_{\mathrm{b}}^{s_1}, \\ \dfrac{1}{2}\log(1+\rho|h_{\mathrm{r,eu}}|^2), & \text{otherwise.} \end{cases} \tag{5}$$

During the second phase, R retransmits its received signal using the AF protocol, and simultaneously, the CU sends a new signal $s_{1'}$ to the BS. The aim of the coordinated transmission of CU and R is to exploit the half-duplex feature of R for improving the secrecy rate. Therefore, the received signal at the BS can be written as

$$\begin{aligned} \boldsymbol{y}_{\mathrm{b},2} &= G_{\mathrm{ul}}\boldsymbol{h}_{\mathrm{b,r}}y_{\mathrm{r},1} + \sqrt{P}\boldsymbol{h}_{\mathrm{b,cu}}s_{1'} + \boldsymbol{n}_{\mathrm{b},2} \\ &\overset{\text{(i)}}{=} \sqrt{P}\boldsymbol{H}_{\mathrm{b}}\begin{bmatrix} G_{\mathrm{ul}}h_{\mathrm{r,eu}}s_2 \\ s_{1'} \end{bmatrix} + \boldsymbol{H}_{\mathrm{b}}\begin{bmatrix} G_{\mathrm{ul}}n_{\mathrm{r}} \\ 0 \end{bmatrix} + \boldsymbol{n}_{\mathrm{b},2}, \end{aligned} \tag{6}$$

where $G_{\rm ul}=\sqrt{1/(\lambda_{\rm r,cu}+\lambda_{\rm r,eu}+1/\rho)}$ denotes the relay amplifying gain in the uplink, $\boldsymbol{n}_{b,2}$ is the AWGN vector at the BS of the second phase, and $\boldsymbol{H}_{\rm b}=[\boldsymbol{h}_{\rm b,r},\boldsymbol{h}_{\rm b,cu}]$ denotes the $M\times 2$ channel matrix from the BS to R and CU. In this paper, we employ a fixed-gain AF relay (i.e., the relay amplifying gain is determined by the statistical channel coefficients) instead of a variable-gain AF relay (i.e., the relay amplifying gain is determined by the instantaneous channel coefficients). The reasons are given as follows. On one hand, the use of a fixed-gain AF relay can yield a tractable secrecy performance analysis and obtain useful design insights. On the other hand, the performance using a fixed-gain untrusted relay is comparable to that using a variable-gain untrusted relay [28]. In (6), step (i) is obtained based on removing the known interference s_1, since the BS already received a copy of s_1 in the first phase.

Based on the received signal given in (6), the ZF equalization can be applied at the BS to decouple the two signal streams from R and CU, as follows:

$$\begin{aligned}\tilde{\boldsymbol{y}}_{\rm b,2}=\boldsymbol{P}\boldsymbol{y}_{\rm b,2}&=\begin{bmatrix}\sqrt{P}G_{\rm ul}h_{\rm r,eu}s_2\\ \sqrt{P}s_{1'}\end{bmatrix}+\begin{bmatrix}G_{\rm ul}n_{\rm r}\\ 0\end{bmatrix}+\boldsymbol{P}\boldsymbol{n}_{\rm b,2}\\&=\begin{bmatrix}\sqrt{P}G_{\rm ul}h_{\rm r,eu}s_2\\ \sqrt{P}s_{1'}\end{bmatrix}+\begin{bmatrix}n_{\rm b}\\ n'_{\rm b}\end{bmatrix},\end{aligned}\tag{7}$$

where $\boldsymbol{P}=(\boldsymbol{H}_{\rm b}^{\dagger}\boldsymbol{H}_{\rm b})^{-1}\boldsymbol{H}_{\rm b}^{\dagger}$ denotes the ZF equalization matrix, and $n_{\rm b}$ and $n'_{\rm b}$ denote the equalized AWGNs corresponding to the signal streams from R and CU, respectively. Particularly, the variances of $n_{\rm b}$ and $n'_{\rm b}$ are $\lambda_{\rm b}=\lambda_0G_{\rm ul}^2+\lambda_0\big[(\boldsymbol{H}_{\rm b}^{\dagger}\boldsymbol{H}_{\rm b})^{-1}\big]_{1,1}$ and $\lambda'_{\rm b}=\lambda_0\big[(\boldsymbol{H}_{\rm b}^{\dagger}\boldsymbol{H}_{\rm b})^{-1}\big]_{2,2}$.

Thus, the transmission rates at the BS for s_2 and $s_{1'}$ can be expressed, respectively, by

$$R_{\rm b}^{s_2}=\frac{1}{2}\log\bigg(1+\frac{\rho|h_{\rm r,eu}|^2t_1}{t_1+1/G_{\rm ul}^2}\bigg),\tag{8}$$

$$R_{\rm b}^{s_{1'}}=\frac{1}{2}\log\big(1+\rho t_2\big),\tag{9}$$

where $t_1=1/[(\boldsymbol{H}_{\rm b}^{\dagger}\boldsymbol{H}_{\rm b})^{-1}]_{1,1}$ and $t_2=1/[(\boldsymbol{H}_{\rm b}^{\dagger}\boldsymbol{H}_{\rm b})^{-1}]_{2,2}$. Due to the half-duplex feature, R cannot overhear the signal transmission of CU, and thus, its achievable eavesdropping rate for $s_{1'}$ is $R_{\rm r}^{s_{1'}}=0$.

The uplink secrecy sum rate achieved by the proposed IUI-aided jamming scheme is given by

$$R_{\rm ssr,ul}=\big\{R_{\rm b}^{s_1}-R_{\rm r}^{s_1}\big\}^+\!+\big\{R_{\rm b}^{s_2}-R_{\rm r}^{s_2}\big\}^+\!+\big\{R_{\rm b}^{s_{1'}}-R_{\rm r}^{s_{1'}}\big\}^+\triangleq R_{\rm sr,ul}^{s_1}+R_{\rm sr,ul}^{s_2}+R_{\rm sr,ul}^{s_{1'}}.\tag{10}$$

Remark 1. From (10), we obtain the following important observations. (1) $R_{\rm b}^{s_1}$ increases with ρ while $R_{\rm r}^{s_1}$ approaches a constant in the high ρ regime, shown in (3) and (4), respectively. Thus, a positive $R_{\rm sr,ul}^{s_1}$ can be obtained. (2) $R_{\rm b}^{s_2}$ increases with ρ, as shown in (8), however, $R_{\rm r}^{s_2}$ in (5) converges to a constant when ρ goes to infinity, since we have $R_{\rm r}^{s_1}<R_{\rm b}^{s_1}$ with a high probability in this case. Thus, a positive $R_{\rm sr,ul}^{s_2}$ is obtained. (3) $R_{\rm sr,ul}^{s_{1'}}$ is always positive. As a result, the proposed IUI-aided jamming scheme can achieve perfect security for the uplink coordinated transmission.

Remark 2. The IUI-aided jamming scheme brings a new view about interference, where the originally harmful IUI can be utilized as a constructive resource to improve physical layer security, i.e., it serves as a useful jamming signal to confound the untrusted relay. Specifically, the beauty of this scheme lies in the fact that the transmission secrecy is guaranteed not by relying on external jammers, but rather by exploiting the IUI that originates from the coordinated transmission of EU and CU. Thus, the IUI-aided jamming scheme can be efficiently implemented in practical wireless communication systems.

3.2 Secrecy rate analysis

To evaluate the uplink secrecy performance achieved by the proposed IUI-aided jamming scheme, we analyze the ESSR lower bound and the ESSR scaling law in the sequel.

A lower bound of the uplink ESSR using Jensen's inequality can be expressed as

$$\bar{R}_{\rm ssr,ul}^{\rm lb}\triangleq\Big\{\mathrm{E}\big[R_{\rm b}^{s_1}\big]-\mathrm{E}\big[R_{\rm r}^{s_1}\big]\Big\}^+\!+\Big\{\mathrm{E}\big[R_{\rm b}^{s_2}\big]-\mathrm{E}\big[R_{\rm r}^{s_2}\big]\Big\}^+\!+\mathrm{E}\big[R_{\rm b}^{s_{1'}}\big].\tag{11}$$

An explicit expression for the ESSR lower bound is provided in Theorem 1.

Theorem 1. An ESSR lower bound of the IUI-aided jamming scheme can be approximated as

$$\bar{R}_{\mathrm{ssr,ul}}^{\mathrm{lb}} \approx \left\{ \sum_{m=0}^{M-1} \frac{\Xi_1(m,\rho)}{2m!(\rho\lambda_{\mathrm{b,cu}})^m} - \frac{\kappa \Xi_2(\kappa,\rho)}{2(\kappa-1)} \right\}^+ + \left\{ \widehat{\sum_{m,n}} \frac{(2\rho\lambda_{\mathrm{r,eu}})^{-1}\Xi_3(m,r_n)}{m!(\tilde{G}^2\lambda_{\mathrm{b,r}})^m} - \big(I_1+I_2\big) \right\}^+ + \sum_{m=0}^{M-2} \frac{\Lambda\big(m,\frac{1}{\rho\lambda_{\mathrm{b,cu}}}\big)}{2(\rho\lambda_{\mathrm{b,cu}})^m m!}, \tag{12}$$

where $\widehat{\sum}_{m,n}$ is the short-hand-notation for $\sum_{m=0}^{M-2}\sum_{n=1}^{N}$, I_1, I_2, $\Xi_i(\cdot,\cdot)$ $(i=1,2,3)$, and $\Lambda(\cdot,\cdot)$ is given in the proof below.

Proof. Since $\|\boldsymbol{h}_{\mathrm{b,cu}}\|^2$ follows the Gamma distribution with parameter $(M,\lambda_{\mathrm{b,cu}})$, the probability density function (PDF) of $\tilde{X}=\rho\|\boldsymbol{h}_{\mathrm{b,cu}}\|^2$ is given by $f_{\tilde{X}}(x)=(\frac{x}{\rho\lambda_{\mathrm{b,cu}}})^{M-1}\Gamma^{-1}(M)\mathrm{e}^{-\frac{x}{\rho\lambda_{\mathrm{b,cu}}}}$. Using this result, we can compute $\mathrm{E}[R_{\mathrm{b}}^{s_1}]$ as follows:

$$\mathrm{E}\big[R_b^{\tilde{x}_c}\big] \overset{(a.1)}{=} \sum_{m=0}^{M-1} \frac{1}{2m!(\rho\lambda_{\mathrm{b,cu}})^m} \int_0^{\infty} \frac{x^m \mathrm{e}^{-\frac{x}{\rho\lambda_{\mathrm{b,cu}}}}}{1+x}\mathrm{d}x \overset{(a.2)}{=} \sum_{m=0}^{M-1} \frac{\Xi_1(m,\rho)}{2m!(\rho\lambda_{\mathrm{b,cu}})^m}, \tag{13}$$

where step (a.1) follows from [27, eq. (8.352.2)], step (a.2) follows from [27, eq. (3.353.5)], and $\Xi_1(m,\rho)$ is shown as

$$\Xi_1(m,\rho) = (-1)^{m-1}\mathrm{e}^{\frac{1}{\rho\lambda_{\mathrm{b,cu}}}}\mathrm{Ei}\Big(-\frac{1}{\rho\lambda_{\mathrm{b,cu}}}\Big) + \sum_{k=1}^{m}(k-1)!(-1)^{m-k}(\rho\lambda_{\mathrm{b,cu}})^k. \tag{14}$$

Then, we define $\tilde{Y}=\frac{|h_{\mathrm{r,cu}}|^2}{|h_{\mathrm{r,eu}}|^2+1/\rho}$, for which the cumulative distribution function (CDF) can be calculated as $F_{\tilde{Y}}(y)=1-\frac{\kappa}{\kappa+y}\mathrm{e}^{-\frac{y}{\rho\lambda_{\mathrm{r,cu}}}}$, where $\kappa=\frac{\lambda_{\mathrm{r,cu}}}{\lambda_{\mathrm{r,eu}}}$. As such, we can derive $\mathrm{E}[R_{\mathrm{r}}^{s_1}]$ as

$$\mathrm{E}[R_r^{\tilde{x}_c}] \overset{(a.3)}{=} \frac{\kappa\Xi_2(\kappa,\rho)}{2(\kappa-1)}, \tag{15}$$

$$\Xi_2(\kappa,\rho) = \mathrm{e}^{\frac{1}{\rho\lambda_{\mathrm{r,cu}}}}\mathrm{Ei}\left(-\frac{1}{\rho\lambda_{\mathrm{r,cu}}}\right) - \mathrm{e}^{\frac{\kappa}{\rho\lambda_{\mathrm{r,cu}}}}\mathrm{Ei}\left(-\frac{\kappa}{\rho\lambda_{\mathrm{r,cu}}}\right), \tag{16}$$

where step (a.3) follows [27, eq. (3.352.4)]. Summarizing results in (13) and (15), the ergodic secrecy rate of s_1 is derived.

Next, we calculate the ergodic secrecy rate of s_2. Since t_1 follows the chi-square distribution with $2(M-1)$ degrees of freedom, its CDF is given by $F_{t_1}(t)=1-\mathrm{e}^{-t/\lambda_{\mathrm{b,r}}}\sum_{m=0}^{M-2}t^m/(\lambda_{\mathrm{b,r}}^m m!)$. Here, we define $\tilde{Z}=\frac{\rho|h_{\mathrm{r,eu}}|^2 t_1}{t_1+1/G_{\mathrm{ul}}^2}$, we can compute $\mathrm{E}[R_{\mathrm{b}}^{s_2}]$ by

$$\begin{aligned}
\mathrm{E}\big[R_{\mathrm{b}}^{s_2}\big] &= \sum_{m=0}^{M-2} \frac{(2\rho\lambda_{\mathrm{r,eu}})^{-1}}{m!(G_{\mathrm{ul}}^2\lambda_{\mathrm{b,r}})^m} \int_0^{\infty} w^{-m}\mathrm{e}^{-\frac{w}{\rho\lambda_{\mathrm{r,eu}}}} \left(\int_0^{\infty}\frac{z^m\mathrm{e}^{-\eta(w)z}}{1+z}\mathrm{d}z\right)\mathrm{d}w \\
&\overset{(a.4)}{=} \sum_{m=0}^{M-2} \frac{(2\rho\lambda_{\mathrm{r,eu}})^{-1}}{m!(G_{\mathrm{ul}}^2\lambda_{\mathrm{b,r}})^m} \int_0^{\infty} w^{-m}\mathrm{e}^{-\frac{w}{\rho\lambda_{\mathrm{r,eu}}}} \underbrace{\left[(-1)^{m-1}\mathrm{e}^{\eta(w)}\mathrm{Ei}\big(-\eta(w)\big) + \sum_{k=1}^{m}\frac{(k-1)!(-1)^{m-k}}{\eta^k(w)}\right]}_{\triangleq\Lambda(m,\eta(w))}\mathrm{d}w \\
&\overset{(a.5)}{=} \sum_{m=0}^{M-2} \frac{(2\rho\lambda_{\mathrm{r,eu}})^{-1}}{m!(G_{\mathrm{ul}}^2\lambda_{\mathrm{b,r}})^m} \sum_{n=1}^{N} \underbrace{\big(1-\theta_n^2\big)^{\frac{1}{2}}\Lambda(m,\eta(\tan r_n))(\tan r_n)^{-m}\mathrm{e}^{-\frac{\tan r_n}{\lambda_{\mathrm{r,eu}}}}\sec^2 r_n}_{\triangleq\Xi_3(m,r_n)},
\end{aligned} \tag{17}$$

where $\eta(w)=\frac{1}{G_{\mathrm{ul}}^2\lambda_{\mathrm{b,r}}w}+\frac{1}{\rho\lambda_{\mathrm{r,eu}}}$, $r_n=\frac{\pi}{4}(\theta_n+1)$, $\theta_n=\cos(\frac{2n-1}{2N}\pi)$, and N is an accuracy vs. complexity parameter. In (17), step (a.4) follows from [27, eq. (3.353.5)] and step (a.5) follows from the Gauss-Chebyshev (G-C) quadrature [29, eq. (25.4.45)]. Here, the Guass-Chebyshev quadrature approximation is applied due to the following reasons: (i) The Guass-Chebyshev quadrature approximation is an effective and tractable approach to approximate the value of a definite integral, as indicated in [26]; (ii) Compared

with other approximation methods such as the Newton-Cotes quadrature approximation, the Guass-Chebyshev quadrature approximation can achieve a higher algebraic accuracy, as indicated in [30].

With the total probability theorem, we can rewrite $\mathrm{E}[R_{\mathrm{r}}^{s_2}]$ as

$$\begin{aligned}\mathrm{E}\big[R_r^{\tilde{x}_e}\big] &= \frac{1}{2}\iint\limits_{\mathcal{D}}\left(\int_{\frac{v}{w+\frac{1}{\rho}}}^{\infty}\log\left(1+\frac{w}{v+\frac{1}{\rho}}\right)\mathrm{d}F_{\tilde{X}}(x)-\int_0^{\frac{v}{w+\frac{1}{\rho}}}\log(1+\rho w)\mathrm{d}F_{\tilde{X}}(x)\right)f_V(v)f_W(w)\mathrm{d}v\mathrm{d}w\\ &= \iint\limits_{\mathcal{D}}\log\left(1+\frac{w}{v+\frac{1}{\rho}}\right)\frac{\mathrm{e}^{-\frac{v}{\lambda_{\mathrm{r,cu}}}-\frac{w}{\lambda_{\mathrm{r,eu}}}}}{2\lambda_{\mathrm{r,cu}}\lambda_{\mathrm{r,eu}}}\mathrm{d}v\mathrm{d}w\\ &\quad+\iint\limits_{\mathcal{D}}\log\left(\frac{1+\rho v}{1+\frac{v}{w+\frac{1}{\rho}}}\right)F_{\tilde{X}}\left(\frac{v}{w+\frac{1}{\rho}}\right)\frac{\mathrm{e}^{-\frac{v}{\lambda_{\mathrm{r,cu}}}-\frac{w}{\lambda_{\mathrm{r,eu}}}}}{2\lambda_{\mathrm{r,cu}}\lambda_{\mathrm{r,eu}}}\mathrm{d}v\mathrm{d}w,\end{aligned}\tag{18}$$

where $\mathcal{D}=\{(v,w)\mid 0\leqslant v<\infty, w\leqslant w<\infty\}$. We denote the first and the second integrals in (18) as I_1 and I_2. Particularly, applying the G-C quadrature again, we approximate I_1 as

$$I_1\approx-\frac{\pi^2\mathrm{e}^{-\frac{1}{\rho\lambda_{\mathrm{r,eu}}}}}{8N\lambda_{\mathrm{r,cu}}}\sum_{n=1}^{N}(1-\theta_n^2)^{\frac{1}{2}}\mathrm{e}^{-\frac{\tan r_n}{\lambda_{\mathrm{r,cu}}}-\frac{\tan r_n}{\lambda_{\mathrm{r,eu}}}}\mathrm{Ei}\left(-\frac{\tan r_n+1/\rho}{\lambda_{\mathrm{r,eu}}}\right)\sec^2 r_n.\tag{19}$$

To simplify I_2, we define $\alpha=\frac{v}{w+\frac{1}{\rho}}$ and $\delta=\rho v$, for which the Jacobian matrix is given by

$$\boldsymbol{J}=\begin{bmatrix}\frac{\mathrm{d}w}{\mathrm{d}\alpha} & \frac{\mathrm{d}w}{\mathrm{d}\delta}\\ \frac{\mathrm{d}v}{\mathrm{d}\alpha} & \frac{\mathrm{d}v}{\mathrm{d}\delta}\end{bmatrix}=\begin{bmatrix}-\frac{\delta}{\rho\alpha^2} & \frac{1}{\rho\alpha}\\ 0 & \rho^{-1}\end{bmatrix}.\tag{20}$$

The determinant of $\boldsymbol{J}$ is equal to $-\frac{\delta}{(\rho\alpha)^2}$. Based on this result, we can derive I_2 as

$$\begin{aligned}I_2 &= \frac{\mathrm{e}^{-\frac{1}{\rho\lambda_{\mathrm{r,eu}}}}}{2\rho^2\lambda_{\mathrm{r,cu}}\lambda_{\mathrm{r,eu}}}\int_0^{\infty}\int_0^{\infty}\log\left(\frac{1+\delta}{1+\alpha}\right)\frac{\delta F_{\tilde{X}}(\alpha)}{\alpha^2}\mathrm{e}^{-\xi(\alpha)\delta}\mathrm{d}\alpha\mathrm{d}\delta\\ &\overset{(a.6)}{=} \frac{\mathrm{e}^{-\frac{1}{\rho\lambda_{\mathrm{r,eu}}}}}{2\rho^2\lambda_{\mathrm{r,cu}}\lambda_{\mathrm{r,eu}}}\int_0^{\infty}\underbrace{\Big((\xi^{-1}(\alpha)-1)\mathrm{e}^{\xi(\alpha)}\mathrm{Ei}(-\xi(\alpha))-\log(1+\alpha)+1\Big)}_{\triangleq\Theta(\alpha)}\frac{F_{\tilde{X}}(\alpha)}{\alpha^2\xi^2(\alpha)}\mathrm{d}\alpha\\ &\overset{(a.7)}{\approx} \frac{\pi^2\mathrm{e}^{-\frac{1}{\rho\lambda_{\mathrm{r,eu}}}}}{8N\rho^2\lambda_{\mathrm{r,cu}}\lambda_{\mathrm{r,eu}}}\sum_{n=1}^{N}(1-\theta_n^2)^{\frac{1}{2}}\Theta(\tan r_n)\frac{F_{\tilde{X}}(\tan r_n)}{\xi^2(\tan r_n)}\csc^2 r_n,\end{aligned}\tag{21}$$

where $\xi(\alpha)=\frac{1}{\rho\lambda_{\mathrm{r,cu}}}+\frac{1}{\rho\lambda_{\mathrm{r,eu}}\alpha}$, step (a.6) follows from [27, eqs. (3.351.3) and (4.337.5)], and step (a.7) follows from the the G-C quadrature. Using results in (17)–(21), the ergodic secrecy rate of s_2 is derived.

Similarly, the CDF of t_2 is given by $F_{t_2}(t)=1-\mathrm{e}^{-t/\lambda_{\mathrm{b,cu}}}\sum_{m=0}^{M-2}t^m/(\lambda_{\mathrm{b,cu}}^m m!)$. Thus, we can compute the ergodic rate of $s_{1'}$ by

$$\mathrm{E}\big[R_{\mathrm{b}}^{s_{1'}}\big]=\sum_{m=0}^{M-2}\frac{\Lambda\big(m,\frac{1}{\rho\lambda_{\mathrm{b,cu}}}\big)}{2(\rho\lambda_{\mathrm{b,cu}})^m m!},\tag{22}$$

where we have applied [27, eq. (3.353.5)]. Hence, we complete the proof.

In general, one can simply use Theorem 1 to evaluate the secrecy performance achieved by the proposed scheme without doing the time-consuming computer simulations. However, the expression is still complicated which contains multiple summations and the exponential integral function, and it is difficult to get useful insights into the fundamental performance limits. This motivates us to study the ESSR scaling law in the regime of $\rho\to\infty$ and $M\to\infty$, respectively, as shown below.

Corollary 1 (Scaling law with ρ)**.** When M is finite and $\rho\to\infty$, we obtain that the ergodic secrecy rates for s_1, s_2, and $s_{1'}$ scale the same as $\frac{1}{2}\log\rho$. Thus, the ESSR scaling law of $\frac{3}{2}\log\rho$ is achieved.

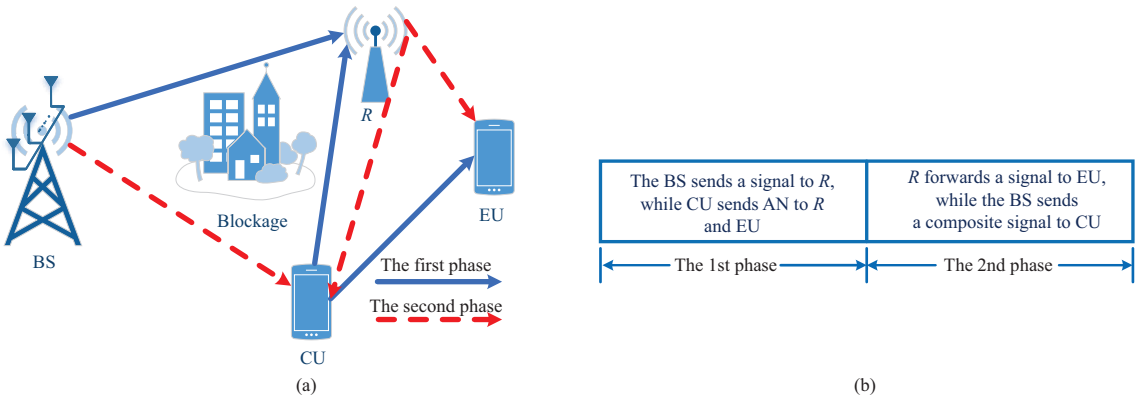

Figure 2 (Color online) The AN-aided jamming scheme for downlink secure coordinated transmission. (a) An illustration of the AN-aided jamming; (b) general principle of the AN-aided jamming.

Corollary 2 (Scaling law with M)**.** When $M \to \infty$ with any finite ρ, it can be verified that the ergodic secrecy rates for s_1 and $s_{1'}$ scale the same as $\frac{1}{2}\log M$, while the ergodic secrecy rate for s_2 approaches a constant. As a result, the ESSR scaling law of $\log M$ is obtained.

Proof. In the high ρ regime, we can readily obtain from (3), (8), and (9) that

$$\left\{\mathrm{E}\left[R_{\mathrm{b}}^{s_1}\right], \mathrm{E}\left[R_{\mathrm{b}}^{s_2}\right], \mathrm{E}\left[R_{\mathrm{b}}^{s_{1'}}\right]\right\} \overset{\rho\to\infty}{\longrightarrow} \frac{1}{2}\log\rho. \tag{23}$$

On the other hand, when $\rho \to \infty$, we can know from (4) and (5) that $\mathrm{E}[R_{\mathrm{r}}^{s_1}]$ and $\mathrm{E}[R_{\mathrm{r}}^{s_2}]$ approach constants. As a result, an ESSR scaling law of $\frac{3}{2}\log\rho$ is obtained.

Based on the extreme value theory, when M is sufficiently large, it is shown that $\|\boldsymbol{h}_{\mathrm{b,cu}}\|^2 \to M\lambda_{\mathrm{b,cu}}$ with a high probability. Then, we can asymptotically express $\mathrm{E}[R_{\mathrm{b}}^{s_1}]$ as $\mathrm{E}[R_{\mathrm{b}}^{s_1}] \overset{M\to\infty}{\longrightarrow} \frac{1}{2}\log M$. Similarly, when $M \to \infty$, we know that $t_1 \to M\lambda_{\mathrm{b,r}}$ and $t_2 \to M\lambda_{\mathrm{b,cu}}$. Using the above result, we can obtain that $\mathrm{E}[R_{\mathrm{b}}^{s_2}]$ approaches a constant while $\mathrm{E}[R_{\mathrm{b}}^{s_{1'}}] \overset{M\to\infty}{\longrightarrow} \frac{1}{2}\log M$. This completes the proof.

Remark 3. Corollaries 1 and 2 provide a simple but effective way to enhance security: a higher ESSR can be obtained by increasing the transmit power P and/or the number of antennas M at the BS.

Remark 4. Consider a scenario where the relay is trusted. We can readily derive that the scaling laws for the ergodic sum rate are $\frac{3}{2}\log\rho$ with SNR and $\log M$ with the number of antennas at the BS, respectively. Therefore, the IUI-aided jamming scheme achieves the same performance limit as that of the trusted relay, thus making it applicable for uplink secure transmission.

4 Downlink secure coordinated transmission

This section first devises a new AN-aided jamming scheme for downlink coordinated transmission. Then, the ESSR analysis is provided to evaluate the proposed scheme.

4.1 Scheme description

As depicted in Figure 2, the proposed scheme consists of two phases as follows. During the first phase, the BS sends the confidential signal s_2 intended for the EU. Simultaneously, CU emits the AN s_z to interfere with the signal reception of R. In particular, both s_2 and s_z satisfy $\mathrm{E}[|s_2|^2] = \mathrm{E}[|s_z|^2] = 1$. Thus, the received signal at R can be expressed as

$$y_{\mathrm{r}} = \sqrt{P}\boldsymbol{h}_{\mathrm{b,r}}\boldsymbol{q}_1 s_2 + \sqrt{P}h_{\mathrm{r,cu}}s_z + n_{\mathrm{r}}, \tag{24}$$

where $\boldsymbol{q}_1 = \boldsymbol{h}_{\mathrm{b,r}}^{\dagger}/\|\boldsymbol{h}_{\mathrm{b,r}}\|$ denotes the precoding vector at the BS of the first phase.

Based on the received signal, R attempts to decode s_2 for the confidential information interception. The achievable eavesdropping rate at R for s_2 is given by

$$R_{\mathrm{r}}^{s_2} = \frac{1}{2}\log\left(1 + \frac{\|\boldsymbol{h}_{\mathrm{b,r}}\|^2}{|h_{\mathrm{r,cu}}|^2 + 1/\rho}\right). \tag{25}$$

The EU receives and caches s_z to facilitate the subsequent AN cancellation, as discussed later.

During the second phase, R retransmits its received signal to the EU following the AF protocol. In the same time, the BS sends a superimposed mixture of s_2 and s_1, where s_1 is intended to CU with $\mathrm{E}[|s_1|^2]=1$. Specifically, the transmission of s_1 is to exploit the half-duplex feature of R for secrecy rate enhancement, while the transmission of s_2 is to enable linear interference cancellation of R's forwarded interference at CU. The received signal at EU and CU can be expressed, respectively, as

$$\begin{aligned} y_{\mathrm{eu}} &= G_{\mathrm{dl}} h_{\mathrm{r,eu}} y_{\mathrm{r}} + n_{\mathrm{eu}} \\ &\overset{\text{(ii)}}{=} \sqrt{P} G_{\mathrm{dl}} \boldsymbol{h}_{\mathrm{b,r}} \boldsymbol{q}_1 h_{\mathrm{r,eu}} s_2 + G_{\mathrm{dl}} h_{\mathrm{r,e}} n_{\mathrm{r}} + n_{\mathrm{eu}}, \qquad (26) \\ y_{\mathrm{cu}} &= G_{\mathrm{dl}} h_{\mathrm{r,cu}} y_{\mathrm{r}} + \boldsymbol{h}_{\mathrm{b,cu}} \boldsymbol{q}_2 (\sqrt{P-P_0} s_1 + \omega_0 s_2) + n_{\mathrm{cu}}, \\ &\overset{\text{(iii)}}{=} \sqrt{P} G_{\mathrm{dl}} \boldsymbol{h}_{\mathrm{b,r}} \boldsymbol{q}_1 h_{\mathrm{r,cu}} s_2 + G_{\mathrm{dl}} h_{\mathrm{r,cu}} n_{\mathrm{r}} + \sqrt{P-P_0} \boldsymbol{h}_{\mathrm{b,cu}} \boldsymbol{q}_2 s_1 + \omega_0 \boldsymbol{h}_{\mathrm{b,cu}} \boldsymbol{q}_2 s_2 + n_{\mathrm{cu}}, \qquad (27) \end{aligned}$$

where n_{eu} and n_{cu} are the AWGNs at EU and CU, and $G_{\mathrm{dl}} = \sqrt{1/(M\lambda_{\mathrm{b,r}} + \lambda_{\mathrm{r,cu}} + 1/\rho)}$ denotes the relay amplifying gain in the downlink. In (27), P_0 denotes the average transmit power of s_2, ω_0 denotes the weight coefficient with $\mathrm{E}[|\omega_0|^2] = P_0$, and $\boldsymbol{q}_2$ denotes the precoding vector at the BS of the second phase with $\mathrm{E}[|\boldsymbol{q}_2^{\dagger}\boldsymbol{q}_2|] \leqslant 1$ (i.e., the average transmit power of the precoding vector at the BS should be less than one). To maximize the signal reception quality at CU, the BS chooses the precoding vector as $\boldsymbol{q}_2 = \boldsymbol{h}_{\mathrm{b,cu}}^{\dagger}/\|\boldsymbol{h}_{\mathrm{b,cu}}\|$. Furthermore, steps (ii) and (iii) are obtained based on s_z cancellation at EU and CU since they already received a copy of s_z in the first phase.

To remove the intentional interference s_2 received at CU, the weight coefficient ω_0 is specifically designed to satisfy the following equality: $\sqrt{P} G_{\mathrm{dl}} \boldsymbol{h}_{\mathrm{b,r}} \boldsymbol{q}_1 h_{\mathrm{r,cu}} s_2 + \omega_0 \boldsymbol{h}_{\mathrm{b,cu}} \boldsymbol{q}_2 s_2 = 0$, for which the solution of ω_0 is given by $\omega_0 = -\frac{\sqrt{P} G_{\mathrm{dl}} \boldsymbol{h}_{\mathrm{b,r}} \boldsymbol{q}_1 h_{\mathrm{r,cu}}}{\boldsymbol{h}_{\mathrm{b,cu}} \boldsymbol{q}_2}$. Due to the average transmit power constraint, namely, $P_0 \leqslant P$, the following inequality should be meet:

$$G_{\mathrm{dl}} M \lambda_{\mathrm{b,r}} \lambda_{\mathrm{r,cu}} \leqslant M \lambda_{\mathrm{b,cu}}. \qquad (28)$$

To prove (28), we first multiply ρ in its left-hand side, thus yielding $\frac{\gamma_{\mathrm{b,r}}\gamma_{\mathrm{r,cu}}}{\gamma_{\mathrm{b,r}}+\gamma_{\mathrm{r,cu}}+1} \approx \min\{\gamma_{\mathrm{b,r}}, \gamma_{\mathrm{r,cu}}\} \leqslant \gamma_{\mathrm{b,r}}$, where $\gamma_{\mathrm{b,r}} = \rho M \lambda_{\mathrm{b,r}}$ and $\gamma_{\mathrm{r,cu}} = \rho \lambda_{\mathrm{r,cu}}$. Recall that CU is located very close to the BS, it is reasonable to have $d_{\mathrm{b,cu}} < d_{\mathrm{b,r}}$. Hence, we obtain that $\gamma_{\mathrm{b,r}} < \gamma_{\mathrm{b,cu}}$, where $\gamma_{\mathrm{b,cu}} = \rho M \lambda_{\mathrm{b,cu}}$, and thus, inequality in (28) strictly holds. This implies that in the proposed scheme, CU can perfectly cancel out the intentional interference s_2 first and then decode its desired signal s_1 in an interference-free fashion.

After the interference cancellation, the EU decodes s_2 with the transmission rate as

$$R_{\mathrm{eu}}^{s_2} = \frac{1}{2} \log \left(1 + \frac{\rho \|\boldsymbol{h}_{\mathrm{b,r}}\|^2 |h_{\mathrm{r,eu}}|^2}{|h_{\mathrm{r,eu}}|^2 + 1/G_{\mathrm{dl}}^2} \right), \qquad (29)$$

and the CU decodes s_1 with the transmission rate as

$$R_{\mathrm{cu}}^{s_1} = \frac{1}{2} \log \left(1 + \frac{\epsilon \rho \|\boldsymbol{h}_{\mathrm{b,cu}}\|^2}{G_{\mathrm{dl}}^2 |h_{\mathrm{r,cu}}|^2 + 1} \right), \qquad (30)$$

where $\epsilon = 1 - \frac{\gamma_{\mathrm{b,r}}\gamma_{\mathrm{r,cu}}}{\gamma_{\mathrm{b,cu}}(\gamma_{\mathrm{b,r}}+\gamma_{\mathrm{r,cu}}+1)}$. On the other hand, with the half-duplex feature, R cannot listen to the BS transmission when it carries out information forwarding. As a result, the achievable eavesdropping rate at R for s_1 is given by $R_{\mathrm{r}}^{s_1} = 0$, implying that s_1 is securely received with the proposed scheme.

The downlink secrecy sum rate achieved by the proposed AN-aided jamming scheme is given by

$$R_{\mathrm{ssr,dl}} = \left\{ R_{\mathrm{eu}}^{s_2} - R_{\mathrm{r}}^{s_2} \right\}^+ + \left\{ R_{\mathrm{cu}}^{s_1} - R_{\mathrm{r}}^{s_1} \right\}^+ \triangleq R_{\mathrm{sr,dl}}^{s_2} + R_{\mathrm{sr,dl}}^{s_1}. \qquad (31)$$

Remark 5. To implement the intentional interference cancellation, the BS has to acquire the instantaneous channel state information (CSI) of $\boldsymbol{h}_{\mathrm{b,r}}$, $\boldsymbol{h}_{\mathrm{b,cu}}$, and $h_{\mathrm{r,cu}}$, as well as the statistical CSI of $\lambda_{\mathrm{b,r}}$, $\lambda_{\mathrm{b,cu}}$, and $\lambda_{\mathrm{r,cu}}$, to set w_0 and P_0. The instantaneous CSI can be obtained as follows.

Before data transmission, R first broadcasts a pilot, based on which the BS can estimate $\boldsymbol{h}_{\mathrm{b,r}}$. Then, CU broadcasts a pilot and the BS can estimate $\boldsymbol{h}_{\mathrm{b,cu}}$. Lastly, R amplifies and forwards its received pilot from CU, and the BS can estimate $h_{\mathrm{r,cu}}$ by canceling out $\boldsymbol{h}_{\mathrm{b,r}}$ (which is already known to the BS). Furthermore, the statistical CSI can be readily obtained by averaging $\boldsymbol{h}_{\mathrm{b,r}}$, $\boldsymbol{h}_{\mathrm{b,cu}}$, and $h_{\mathrm{r,cu}}$. The channel training overhead, which contains only three pilot transmissions, is reasonably negligible in the quasi-static block fading scenario [26].

Remark 6. It is clear that $R_{\rm eu}^{s_2}$ increases with ρ, while $R_{\rm r}^{s_2}$ is upper bounded if ρ is sufficiently large, and a positive $R_{\rm sr,dl}^{s_2}$ can be achieved. Furthermore, $R_{\rm sr,dl}^{s_1}$ is always positive. Thus, the AN-aided jamming scheme can yield a positive secrecy sum rate and guarantee perfect security.

4.2 Secrecy rate analysis

A lower bound of the ESSR in downlink is obtained as

$$\bar{R}_{\rm ssr,dl}^{\rm lb} = \left\{\mathrm{E}\left[R_{\rm e}^{x_e}\right] - \mathrm{E}\left[R_r^{x_e}\right]\right\}^+ + \mathrm{E}\left[R_c^{x_c}\right], \tag{32}$$

where we have used the Jensen's inequality and the fact that $\mathrm{E}[R_r^{x_c}] = 0$. An analytical closed-form expression for the ESSR lower bound is given in the following theorem.

Theorem 2. The ESSR lower bound of the AN-aided jamming scheme can be approximated as

$$\bar{R}_{\rm ssr,dl}^{\rm lb} \approx \left\{\widetilde{\sum_{m,n}}\frac{\pi^2}{8N}\left[\frac{\binom{M-1}{m}\Phi_1(m,r_n)}{\rho^m\lambda_{\rm b,r}^{M-1}\Gamma(M)} - \frac{\Phi_2(m,r_n)}{\lambda_{\rm r,cu}m!}\right]\right\}^+ + \widetilde{\sum_{m,n}}\frac{\pi^2\Phi_3(m,r_n)}{8N\lambda_{\rm r,cu}m!}, \tag{33}$$

where $\widetilde{\sum}_{m,n}$ is the short-hand-notation for $\sum_{m=0}^{M-1}\sum_{n=1}^{N}$, and $\Phi_i(\cdot,\cdot)$ $(i=1,2,3)$ is defined below.

Proof. Since $\|\boldsymbol{h}_{\rm b,r}\|^2$ follows the Gamma distribution with parameter $(M,\lambda_{\rm b,r})$, and its PDF is given by $f_U(u) = (u/\lambda_{\rm b,r})^{M-1}\Gamma^{-1}(M)\mathrm{e}^{-u/\lambda_{\rm b,r}}$. Then, we define $X = \frac{\rho\|\boldsymbol{h}_{\rm b,r}\|^2|h_{\rm r,eu}|^2}{|h_{\rm r,eu}|^2+1/G_{\rm dl}^2}$, for which the CDF can be calculated as

$$\begin{aligned} F_X(x) &= \int_0^{\frac{x}{\rho}} f_U(u)\mathrm{d}u + \int_{\frac{x}{\rho}}^{\infty}\Pr\left(|h_{\rm r,eu}|^2 < \frac{x}{G_{\rm dl}^2(\rho u - x)}\right) f_U(u)\mathrm{d}u \\ &\overset{\text{(b.1)}}{=} 1 - \frac{\rho^{-M}}{\lambda_{\rm b,r}^{M-1}\Gamma(M)}\int_0^{\infty}(x+s)^{M-1}\mathrm{e}^{-\frac{s}{\rho\lambda_{\rm b,r}}-\frac{x}{\rho\lambda_{\rm b,r}}-\frac{x}{\lambda_{\rm r,eu}G_{\rm dl}^2 s}}\mathrm{d}s, \end{aligned} \tag{34}$$

where step (b.1) is based on the linear change of variable $u = \frac{s+x}{\rho}$. Thus, we can compute $\mathrm{E}[R_{\rm eu}^{s_2}]$ by

$$\begin{aligned} \mathrm{E}\left[R_{\rm e}^{x_e}\right] &= \sum_{m=0}^{M-1}\frac{\binom{M-1}{m}\rho^{-M}}{2\lambda_{\rm b,r}^{M-1}\Gamma(M)}\int_0^{\infty} s^{M-m-1}\mathrm{e}^{-\frac{s}{\rho\lambda_{\rm b,r}}}\left(\int_0^{\infty}\frac{x^m\mathrm{e}^{-\mu(s)x}}{1+x}\mathrm{d}x\right)\mathrm{d}s \\ &\overset{\text{(b.2)}}{=} \sum_{m=0}^{M-1}\frac{\binom{M-1}{m}\rho^{-M}}{2\lambda_{\rm b,r}^{M-1}\Gamma(M)}\int_0^{\infty} s^{M-m-1}\mathrm{e}^{-\frac{s}{\rho\lambda_{\rm b,r}}}\Lambda(m,\mu(s))\mathrm{d}s \\ &\overset{\text{(b.3)}}{\approx} \sum_{m=0}^{M-1}\frac{\binom{M-1}{m}\rho^{-M}\pi^2}{8N\lambda_{\rm b,r}^{M-1}\Gamma(M)}\sum_{n=1}^{N}\underbrace{\left(1-\theta_n^2\right)^{\frac{1}{2}}\Lambda(m,\mu(\tan r_n))(\tan r_n)^{M-m-1}\mathrm{e}^{-\frac{\tan r_n}{\rho\lambda_{\rm b,r}}}\sec^2 r_n}_{\triangleq\Phi_1(m,r_n)}, \end{aligned} \tag{35}$$

where $\mu(s) = \frac{1}{\lambda_{\rm r,eu}G_{\rm dl}^2 s} + \frac{1}{\rho\lambda_{\rm b,r}}$. In (35), step (b.2) is based on the use of [27, eq. (3.353.5)], and step (b.3) is obtained by the change of variable $s = \tan r$ and applying the G-C quadrature [29, eq. (25.4.45)].

Then, we define $Y = \frac{\|\boldsymbol{h}_{\rm b,r}\|^2}{|h_{\rm r,cu}|^2+1/\rho}$ and $Z = \frac{\epsilon\rho\|\boldsymbol{h}_{\rm b,cu}\|^2}{G_{\rm dl}^2|h_{\rm r,cu}|^2+1}$. Following derivations similar to those in (35), we can derive $\mathrm{E}[R_{\rm r}^{s_2}]$ and $\mathrm{E}[R_{\rm cu}^{s_1}]$ by

$$\begin{aligned} \mathrm{E}\left[R_{\rm r}^{s_2}\right] &\overset{\text{(b.4)}}{=} \frac{1}{2}\int_0^{\infty}\sum_{m=0}^{M-1}\frac{\beta^m(v)f_V(v)}{m!}\left(\int_0^{\infty}\frac{y^m}{1+y}\mathrm{e}^{-\beta(v)y}\mathrm{d}y\right)\mathrm{d}v \\ &\overset{\text{(b.5)}}{=} \sum_{m=0}^{M-1}\frac{1}{2\lambda_{\rm r,cu}m!}\int_0^{\infty}\beta^m(v)\mathrm{e}^{-\frac{v}{\lambda_{\rm r,cu}}}\Lambda(m,\beta(v))\mathrm{d}v \\ &\overset{\text{(b.6)}}{=} \sum_{m=0}^{M-1}\frac{\pi^2}{8N\lambda_{\rm r,cu}m!}\sum_{n=1}^{N}\underbrace{\left(1-\theta_n^2\right)^{\frac{1}{2}}\Lambda(m,\beta(\tan r_n))\beta^m(\tan r_n)\mathrm{e}^{-\frac{\tan r_n}{\lambda_{\rm r,cu}}}\sec^2 r_n}_{\triangleq\Phi_2(m,r_n)}, \end{aligned} \tag{36}$$

$$\mathrm{E}\left[R_{\rm cu}^{s_1}\right] \overset{\text{(b.7)}}{=} \frac{1}{2}\int_0^{\infty}\sum_{m=0}^{M-1}\frac{\phi^m(v)f_V(v)}{m!}\left(\int_0^{\infty}\frac{z^m}{1+z}\mathrm{e}^{-\phi(v)z}\mathrm{d}z\right)\mathrm{d}v$$

$$\overset{\text{(b.8)}}{=} \sum_{m=0}^{M-1} \frac{1}{2\lambda_{\mathrm{r,cu}} m!} \int_0^{\infty} \phi^m(v) \mathrm{e}^{-\frac{v}{\lambda_{\mathrm{r,cu}}}} \Lambda(m, \phi(v)) \mathrm{d}v$$

$$\overset{\text{(b.9)}}{=} \sum_{m=0}^{M-1} \frac{\pi^2}{8N\lambda_{\mathrm{r,cu}} m!} \sum_{n=1}^{N} \underbrace{\left(1-\theta_n^2\right)^{\frac{1}{2}} \Lambda(m, \phi(\tan r_n)) \phi^m(\tan r_n) \mathrm{e}^{-\frac{\tan r_n}{\lambda_{\mathrm{r,cu}}}} \sec^2 r_n}_{\triangleq \Phi_3(m, r_n)}, \tag{37}$$

where $\beta(v) = \frac{v+1/\rho}{\lambda_{\mathrm{b,r}}}$ and $\phi(v) = \frac{G_{\mathrm{d}}^2 v+1}{\epsilon\rho\lambda_{\mathrm{b,cu}}}$. In (36) and (37), steps (b.4) and (b.7) follow from [27, eq. (8.352.2)], steps (b.5) and (b.8) follow from [27, eq. (3.353.5)], and steps (b.6) and (b.9) are obtained by using the G-C quadrature. Now, by summarizing results in (35)–(37), we prove the theorem.

Next, we investigate the ESSR scaling laws in the regime of $\rho, M \to \infty$ to gain clear insights.

Corollary 3 (Scaling law with ρ)**.** When M is finite and $\rho \to \infty$, we verify that the ergodic secrecy rates of s_1 and s_2 both scale as $\frac{1}{2}\log\rho$. Therefore, the ESSR scaling law of $\log\rho$ can be achieved.

Corollary 4 (Scaling law with M)**.** When $M \to \infty$ with any finite ρ, we have the following observations: (1) The ergodic secrecy rate of s_1 scales as $\frac{1}{2}\log M$; (2) The ergodic secrecy rate of s_2 asymptotically approaches zero. Hence, the ESSR scaling law is $\frac{1}{2}\log M$.

Proof. The proof is similar to that of Corollaries 1 and 2, which are omitted here for brevity.

Remark 7. Similar to the uplink scenario, increasing the transmit power and the number of antennas at the BS can be beneficial for enhancing the ESSR.

Remark 8. Consider a scenario where the relay is trusted. It is easily shown that the ergodic sum rates asymptotically scale as $\log\rho$ over SNR and $\log M$ over the number of antennas at the BS, respectively. Thus, the proposed AN-aided jamming scheme yields very similar asymptotic performance limits as that of the trusted relay, which provides security benefits for downlink transmission.

5 Numerical results

This section provides simulation results to evaluate the secrecy performance of the investigated system. For the purpose of illustration, we assume that the BS, R, CU, and EU are located at coordinates $(0,0)$, $(0.6,0)$, $(0.4,0.3)$, and $(1,0)$ in meter (m) in a two-dimensional plane, respectively. The pathloss exponent is selected as $\eta = 2.7$, and the G-C quadrature parameter is chosen as $N = 10$.

5.1 Secrecy performance in the uplink

In Figure 3(a), the ergodic secrecy rate performance of the IUI-aided jamming scheme is evaluated. At first glance, the derived ESSR lower bound agrees with the simulation result, which shows the validity of the theoretical analysis. Furthermore, it is observed from the figure that the ergodic secrecy rates of s_2, s_1, and $s_{1'}$ increase with ρ and behave like $\frac{1}{2}\log\rho$ when ρ is large. Hence, an ESSR scaling law of $\frac{3}{2}\log\rho$ is achieved. This verifies the result in Corollary 1.

Figure 3(b) depicts the ergodic secrecy rate performance of the IUI-aided jamming scheme as a function of M. Unlike the downlink case, the secrecy of both CU and EU benefits from increasing M since: (1) the ergodic secrecy rates of s_1 and $s_{1'}$ are improved by increasing M and scale as $\frac{1}{2}\log M$ in the large M region; (2) the ergodic secrecy rate of s_2 first increases and then converges to a constant. This is because the ergodic secrecy rate of s_2 is determined by the dual-hop relaying link, and the worse link R-EU dominates the overall performance. As a consequence, the ESSR of the system increases with M and scales as $\log M$, which confirms Corollary 2.

Figure 4 shows the uplink secrecy performance comparison. Here, three baseline schemes are incorporated as follows:

• Uplink-baseline-1 is a coordinated scheme utilizing the AN. Specifically, in the first phase, the EU transmits to R and the BS sends the AN to jam R; in the second phase, R and CU transmit to the BS simultaneously.

• Uplink-baseline-2 is a non-coordinated scheme without CU. Specifically, the first phase is the same as that of uplink-baseline-1; in the second phase, R forwards its signal to the BS.

• Uplink-baseline-3 is the scheme designed for uplink in [26].

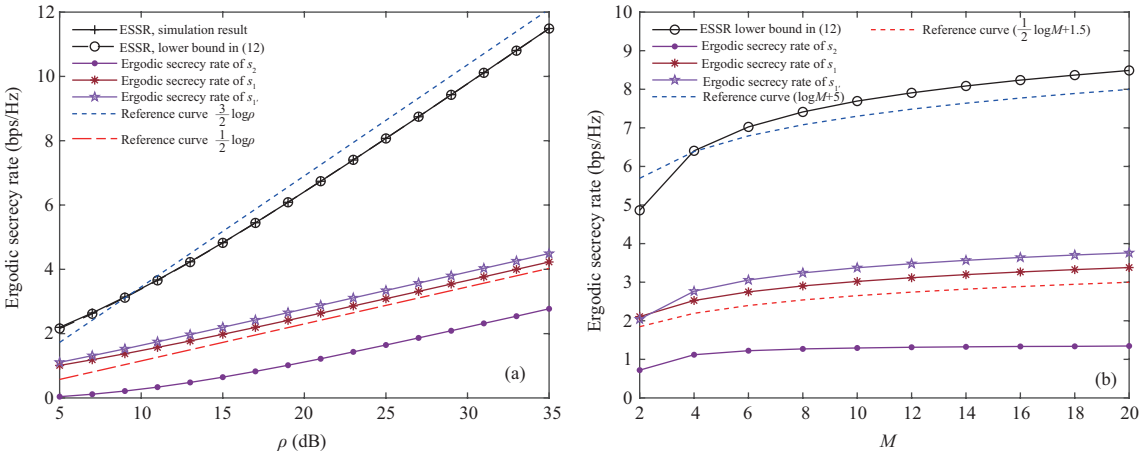

Figure 3 (Color online) Secrecy performance of the IUI-aided jamming scheme versus (a) ρ with $M = 4$ and (b) M with $\rho = 20$ dB.

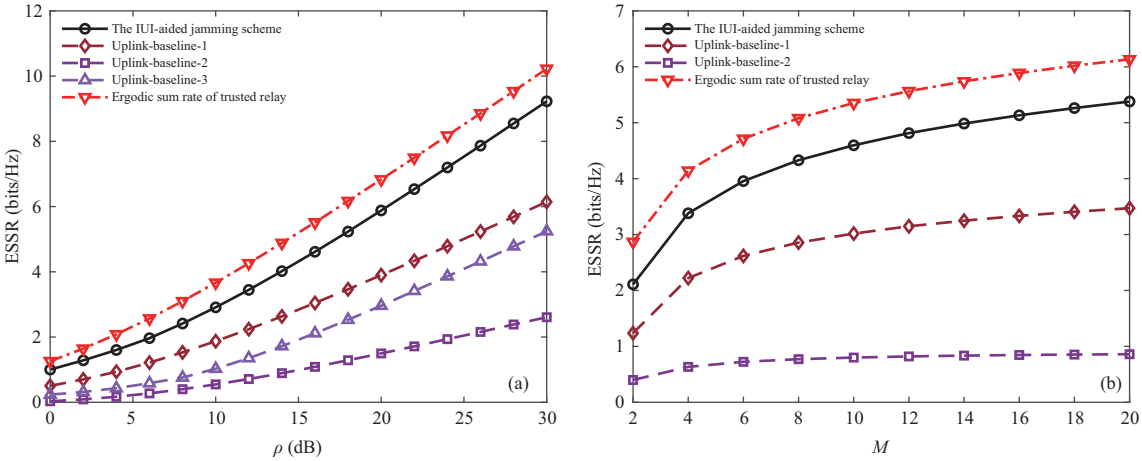

Figure 4 (Color online) Performance comparison of the IUI-aided jamming and the baseline schemes. (a) $M = 3$; (b) $\rho = 10$ dB.

In these two figures, the ergodic sum rate achieved by a trusted relay is also shown to characterize the secrecy performance degradation, for which the transmission procedure is the same as in uplink-baseline-2. As can be observed from the figure, the ESSR achieved by the proposed IUI-aided jamming scheme is significantly higher than that achieved by the baseline schemes, and the ESSR gap between the proposed scheme and the baseline schemes enlarges as ρ and M increase. The reason behind such a phenomenon is that the proposed scheme can achieve a higher ESSR scaling laws according to ρ and M over the baseline schemes, and thus, the ESSR achieved by the proposed scheme increases the fastest in the large ρ and M regions. It is further observed from the figure that the proposed scheme exhibits a similar behavior to that of the trusted relay case. This indicates that the proposed scheme provides a good security guarantee for uplink coordinated direct and untrusted relay transmission.

5.2 Secrecy performance in the downlink

Figure 5(a) plots the ergodic secrecy rate performance achieved by the proposed AN-aided jamming scheme versus ρ. We first observe from this figure that with the proposed scheme, the ergodic secrecy rates of s_2 and s_1 both increase with ρ and scale as $\frac{1}{2}\log\rho$ in the high SNR regime (i.e., $\rho \geqslant 25$ dB), and the ESSR of the system scales as $\log\rho$ in the high SNR regime, which are consistent with our findings in Corollary 1. It is also observed from the figure that the derived ESSR lower bound in Theorem 2 is very close to the simulated one when $\rho \geqslant 18$ dB, verifying the accuracy of the analytical result.

In Figure 5(b), the ergodic secrecy rate performance versus M achieved by the proposed AN-aided jamming scheme is illustrated. From the figure, we observe that the ergodic secrecy rate of s_2 converges to zero when M becomes sufficiently large, due to the simple fact that both the transmission rate and the

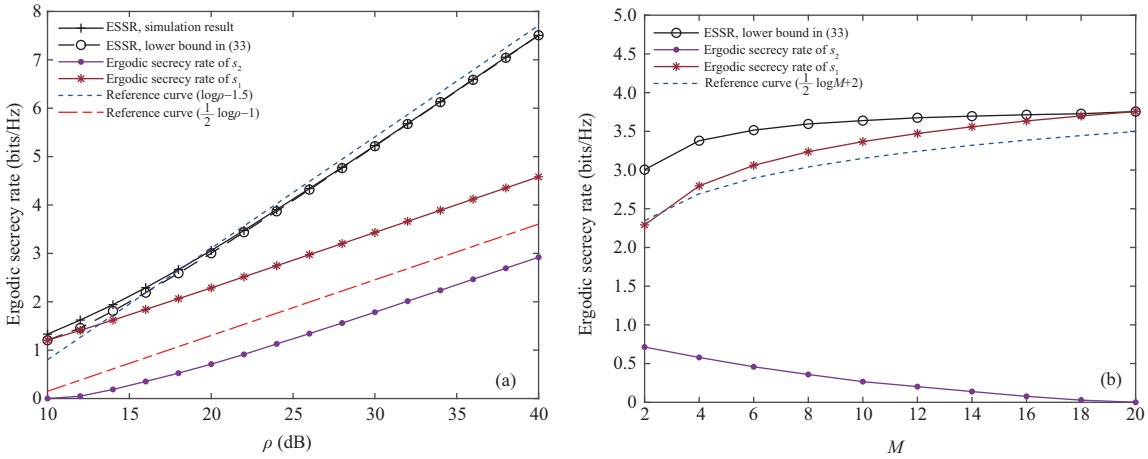

Figure 5 (Color online) Secrecy performance of the AN-aided jamming scheme versus (a) ρ with $M = 2$; (b) M with $\rho = 20$ dB.

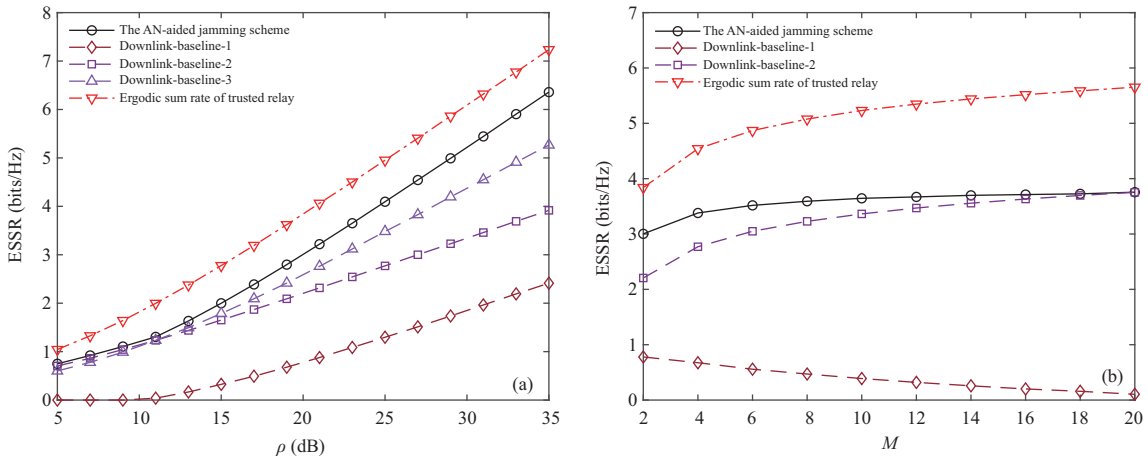

Figure 6 (Color online) Performance comparison of the AN-aided jamming and the baseline schemes. (a) $M = 2$. (b) $\rho = 20$ dB.

eavesdropping rate of s_2 increase with M and the latter is the dominant factor in the large M region. The ergodic secrecy rate of s_1 increases as M increases since the signal reception quality at CU is enhanced. As a result, the ESSR of the system benefits from the increased M. It is also seen from Figure 5(b) that the ESSR lower bound has the same slope as that of the reference curve with large M. This means that the proposed scheme achieves the ESSR scaling law of $\frac{1}{2}\log M$, thus validating Corollary 2.

Figure 6 shows the secrecy benefits of the proposed AN-aided jamming scheme. Here, we consider three baseline schemes as follows:

• Downlink-baseline-1 is a non-coordinated scheme without CU. In the first phase, the BS transmits to R and EU sends the AN to jam R; in the second phase, R forwards its signal to EU.

• Downlink-baseline-2 is a coordinated scheme without jamming. Specifically, in the first phase, the BS transmits to R; while the second phase is similar to that of the proposed scheme.

• Downlink-baseline-3 is the scheme designed for downlink in [26].

Similarly, the ergodic sum rate achieved by a trusted relay is also plotted. From this figure, we have the following observations. (1) A typical trend from Figure 6(a) is that the ESSRs of all the schemes increase with an increase in ρ. Particularly, the proposed scheme outperforms the three baseline schemes, due to the improved ESSR scaling laws according to ρ and M. Moreover, the ESSR achieved by the proposed scheme has the same increasing slope as the trusted relay case, showing its advantage in secure transmission. (2) It is observed from Figure 6(b) that the proposed scheme, the downlink-baseline-2, and the trusted relay case benefit from increasing M. The ESSR of the downlink-baseline-2 converges to that of the proposed scheme because the ergodic secrecy rate of s_2 approaches zero if M is sufficiently large. It is also seen that the ESSR gap between the proposed scheme and the downlink-baseline-1 enlarges as M increases, since the performance of the downlink-baseline-1 degrades with increasing M.

6 Conclusion

In this paper, we investigated security enhanced designs for coordinated direct and untrusted relay transmission in an AF relaying system. The potential of interference engineering for physical layer security was examined. Particularly, two novel interference assisted jamming schemes, namely the IUI-aided jamming and the AN-aided jamming, were proposed to ensure secrecy for the uplink and downlink coordinated transmission, respectively. The analytical closed-form expressions for the ESSR lower bound and the ESSR scaling law were derived to evaluate the system performance. The results demonstrate that the proposed schemes can achieve perfect security with a positive secrecy sum rate and provide a significantly higher ESSR than three other baseline schemes.

Although a two-user scenario is considered in this paper, the proposed interference assisted jamming schemes can be extended to a multiuser scenario, as discussed next. Consider that the BS connects to one or more EUs and one or more CUs. For the uplink, during the first phase, one EU and one CU can be scheduled for simultaneous transmission. During the second phase, another new CU can be scheduled for coordinated transmission. For the downlink, during the first phase, all CUs can perform distributed beamforming to jam R. During the second phase, one CU can be scheduled for signal reception. Optimal user scheduling and distributed beamforming design in the multiuser coordinated direct and untrusted relay transmission scenario deserves further investigation.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61901313, 61941105, 61771366, 61901312, 61971320), National Natural Science Foundation of China for Outstanding Young Scholars (Grant No. 61825104), Natural Science Fundamental Research Plan of Shaanxi Province (Grant No. 2020JQ-306), China Postdoctoral Science Foundation (Grant Nos. BX20190264, 2019M650258), and Open Research Fund of National Mobile Communications Research Laboratory, Southeast University (Grant No. 2020D07).

References

1 Qi Q, Chen X M, Zhong C J, et al. Physical layer security for massive access in cellular Internet of Things. Sci China Inf Sci, 2020, 63: 121301
2 Wu Y P, Khisti A, Xiao C S, et al. A survey of physical layer security techniques for 5G wireless networks and challenges ahead. IEEE J Sel Areas Commun, 2018, 36: 679–695
3 Yue X W, Liu Y W, Yao Y Y, et al. Secure communications in a unified non-orthogonal multiple access framework. IEEE Trans Wirel Commun, 2020, 19: 2163–2178
4 Lv L, Jiang H, Ding Z G, et al. Secure non-orthogonal multiple access: an interference engineering perspective. IEEE Netw, 2021, 35: 278–285
5 Li X W, Zhao M L, Liu Y W, et al. Secrecy analysis of ambient backscatter NOMA systems under I/Q imbalance. IEEE Trans Veh Technol, 2020, 69: 12286–12290
6 Li B, Qi X H, Huang K, et al. Security-reliability tradeoff analysis for cooperative NOMA in cognitive radio networks. IEEE Trans Commun, 2019, 67: 83–96
7 Zheng T X, Wang H M, Yuan J. Physical-layer security in cache-enabled cooperative small cell networks against randomly distributed eavesdroppers. IEEE Trans Wirel Commun, 2018, 17: 5945–5958
8 Huang Y Z, Wang J L, Zhong C, et al. Secure transmission in cooperative relaying networks with multiple antennas. IEEE Trans Wirel Commun, 2016, 15: 6843–6856
9 Lei H J, Yang Z X, Park K H, et al. Secrecy outage analysis for cooperative NOMA systems with relay selection schemes. IEEE Trans Commun, 2019, 67: 6282–6298
10 Pan G F, Lei H J, Deng Y S, et al. On secrecy performance of MISO SWIPT systems with TAS and imperfect CSI. IEEE Trans Commun, 2016, 64: 3831–3843
11 Feng Y H, Yan S H, Liu C X, et al. Two-stage relay selection for enhancing physical layer security in non-orthogonal multiple access. IEEE Trans Inform Forensic Secur, 2019, 14: 1670–1683
12 Deng H, Wang H M, Guo W, et al. Secrecy transmission with a helper: to relay or to Jam. IEEE Trans Inform Forensic Secur, 2015, 10: 293–307
13 Dong L, Han Z, Petropulu A P, et al. Improving wireless physical layer security via cooperating relays. IEEE Trans Signal Process, 2010, 58: 1875–1888
14 Cao Y, Zhao N, Pan G F, et al. Secrecy analysis for cooperative NOMA networks with multi-antenna full-duplex relay. IEEE Trans Commun, 2019, 67: 5574–5587
15 Zhou F H, Chu Z, Sun H J, et al. Artificial noise aided secure cognitive beamforming for cooperative MISO-NOMA using SWIPT. IEEE J Sel Areas Commun, 2018, 36: 918–931
16 Wang Q, Zhou F H, Hu R Q, et al. Energy efficient robust beamforming and cooperative jamming design for IRS-assisted MISO networks. IEEE Trans Wirel Commun, 2021, 20: 2592–2607
17 He X, Yener A. Cooperation with an untrusted relay: a secrecy perspective. IEEE Trans Inform Theor, 2010, 56: 3807–3827
18 Wang L F, Elkashlan M, Huang J, et al. Secure transmission with optimal power allocation in untrusted relay networks. IEEE Wirel Commun Lett, 2014, 3: 289–292
19 Atapattu S, Ross N, Jing Y D, et al. Source-based jamming for physical-layer security on untrusted full-duplex relay. IEEE Commun Lett, 2019, 23: 842–846

20 Sun L, Ren P Y, Du Q H, et al. Security-aware relaying scheme for cooperative networks with untrusted relay nodes. IEEE Commun Lett, 2015, 19: 463–466
21 Li Q Z, Yang L. Artificial noise aided secure precoding for MIMO untrusted two-way relay systems with perfect and imperfect channel state information. IEEE Trans Inform Forensic Secur, 2018, 13: 2628–2638
22 Lv L, Ni Q, Ding Z G, et al. Cooperative non-orthogonal relaying for security enhancement in untrusted relay networks. In: Proceedings of IEEE International Conference on Communications (ICC), Paris, 2017
23 Xu H B, Sun L. Encryption over the air: securing two-way untrusted relaying systems through constellation overlapping. IEEE Trans Wirel Commun, 2018, 17: 8268–8282
24 Xiang Z W, Yang W W, Pan G F, et al. Secure transmission in non-orthogonal multiple access networks with an untrusted relay. IEEE Wirel Commun Lett, 2019, 8: 905–908
25 Arafa A, Shin W, Vaezi M, et al. Secure relaying in non-orthogonal multiple access: trusted and untrusted scenarios. IEEE Trans Inform Forensic Secur, 2020, 15: 210–222
26 Lv L, Jiang H, Ding Z G, et al. Secrecy-enhancing design for cooperative downlink and uplink NOMA with an untrusted relay. IEEE Trans Commun, 2020, 68: 1698–1715
27 Gradshteyn I S, Ryzhik I M. Table of Integrals, Series, Products. San Diego: Academic, 2007
28 Huang J, Mukherjee A, Swindlehurst A L. Secure communication via an untrusted non-regenerative relay in fading channels. IEEE Trans Signal Process, 2013, 61: 2536–2550
29 Abramowitz M, Stegun I. Handbook of Mathematical Functions With Formulas, Graphs, and Mathematical Tables. New York: Dover, 1972
30 Li Y, Li Y Z, Chu X L, et al. Performance analysis of relay selection in cooperative NOMA networks. IEEE Commun Lett, 2019, 23: 760–763