Secure Transmission for Multiuser Relay Networks

Sung-Il Kim, Il-Min Kim, *Senior Member, IEEE*, and Jun Heo, *Member, IEEE*

***Abstract*—We investigate secure transmission for multiuser relay networks, where the undesired users who are not selected for data reception may overhear the source message as eavesdroppers. In this system, the secrecy performance may deteriorate as the number of users increases, since the number of eavesdroppers also increases. In order to address this issue, we consider a multiuser relay scheme with cooperative jamming (MUCJ). In this scheme, the desired user sends a jamming signal to the relay while the source sends its message to the relay, and then the relay amplifies and forwards the received signal to the desired user. Since the jamming can be subtracted only at the desired user, it acts as interference to prevent the eavesdroppers from intercepting the source message. We propose an optimal user selection scheme for the MUCJ, which is optimal in the sense of maximizing the secrecy rate. For the existing multiuser relay scheme (MURS) without cooperative jamming and the MUCJ, we derive the ergodic secrecy rates and analyze the asymptotic secrecy rate gains. We reveal that the ergodic secrecy rate can be increased as the number of users grows and much higher secrecy rate can be achieved by the MUCJ.**

***Index Terms*—Cooperative jamming, multiuser relay networks, physical layer security, secrecy capacity, secure communications, untrustworthy users.**

I. Introduction

RECENTLY, physical (PHY) layer security has attracted a lot of interest in wireless communications. Due to the broadcast nature of wireless medium, in wireless communications, adversaries may make unauthorized access to the data which is intended for legitimate receiver(s). This eavesdropping issue has been typically addressed by cryptography at a higher layer. However, such approach involves complex and (often) difficult key distribution and management. On the other hand, in the PHY layer security, eavesdropping can be prevented by using secure channel codes and/or various signal processing techniques without requiring secret keys. In [1], for a basic channel model (namely, degraded wiretap channel), the concept of secrecy rate was studied, which can be defined as a maximum achievable transmission rate at which the legitimate receiver can reliably decode the signals whereas an eavesdropper cannot obtain any information. This work was extended to Gaussian broadcasting channels [2]. Subsequently, a lot of publications have recently devoted to the PHY layer security. For wireless fading channels [3]–[5] and for wireless relay communications [6]–[15], secure communications were studied. Also, as an effective approach to prevent eavesdropping, various jamming techniques were investigated in [6]–[11], and beamforming and power allocation methods were proposed in [12]–[15].

Multiuser diversity is a technique that has been widely studied to exploit the characteristic that different users undergo independent fading channels in wireless communications [16], [17]. This concept was applied to the relay networks where a relay assists the transmission of the source data to the destination, which extends the cell coverage and/or improves the system throughput [18]–[21]. To exploit the multiuser diversity in the relay networks, a particular user who has the best end-to-end (e2e) channel quality, among all users, is opportunistically selected as the destination. This opportunistic scheduling improves the performance and the diversity [18]–[21].

Although the multiuser diversity improves the performance of wireless networks with *no* security requirement [18]–[21], it can be actually detrimental when a security requirement is imposed to the system. Since the transmitted signal is broadcasted to the undesired users who are not selected for data reception (as well as to the desired user), the undesired users might eavesdrop the signal. In [22], the multiuser diversity in secure communications was investigated, and the authors revealed that the secrecy performance got worse as the number of users grows. This result is opposite to what the conventional multiuser diversity achieves with no security requirement. To address this issue and to effectively exploit the multiuser diversity for secure relay networks, in this paper, we will utilize the concept of cooperative jamming where jamming signals are used to degrade the eavesdropper(s).

In [23]–[25], jamming techniques were studied for relay networks assuming that the relay is *untrustworthy*. In the jamming schemes, the destination sends a jamming signal to the relay, and thus, the relay is not able to decode the signal. On the other hand, the destination is not affected by the jamming signal, because the jamming signal is known at the destination and it can be subtracted by self-interference cancellation at the destination. Very recently, the jamming technique was investigated for relay networks, assuming that the relay is trustworthy and there is an external eavesdropper [26]. However, all these works were limited to the case of single destination terminal, and thus, multiuser diversity has not been considered. In our work, considering the scenario of multiple users, we will utilize the jamming technique to address the issue of multiuser diversity. To the best of our

Manuscript received August 20, 2014; revised December 01, 2014; accepted February 22, 2015. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. Lifeng Lai. This work was supported in part by the Seoul R&BD Program [WR080951, Establishment of Bell Labs in Seoul/Research of Services & Application for Broadband Convergent Networks and their Enabling Sciences], and in part by the Natural Sciences and Engineering Research Council (NSERC).

S.-I. Kim and J. Heo are with the School of Electrical Engineering, Korea University, Seoul 136-701, Korea (e-mail: dudux@korea.ac.kr; junheo@korea.ac.kr).

I.-M. Kim is with the Department of Electrical and Computer Engineering, Queen's University, Kingston, ON, K7L 3N6, Canada (e-mail: ilmin.kim@queensu.ca).

Digital Object Identifier

knowledge, the secure communication for multiuser relay networks exploiting multiuser diversity has not been investigated yet.

Specifically, we consider a multiuser relay scheme with cooperative jamming (MUCJ), assuming that the relay is trustworthy and there are multiple users or eavesdroppers. The MUCJ is working as follows. In the first time slot, the desired user sends a jamming signal to the relay while the source sends the message to the relay. In the second time slot, the relay amplifies and forwards the received signal to the desired user. The undesired users who act as multiple eavesdroppers also receive the signal from the relay. However, the undesired users cannot decode the signal due to the presence of the jamming signal in the received signal. On the other hand, the desired user can decode the signal by self-interference cancellation.

The main contributions of this paper are as follows:

i) We propose an optimal user selection scheme for the MUCJ, which is optimal in the sense of maximizing the secrecy rate.
ii) We exploit *multiuser diversity* in secure relay networks. We demonstrate that, by the MUCJ, the ergodic secrecy rate can be increased as the number of users grows. That is, the aforementioned issue of multiuser diversity with security requirement is resolved.
iii) We derive the exact ergodic secrecy rate for the existing multiuser relay scheme (MURS), which has not been investigated yet in the literature.
iv) We derive the ergodic secrecy rate for the MUCJ by obtaining tight upper and lower bounds. Then we investigate the tightness of both bounds, and verify that both bounds asymptotically converge to the exact secrecy rate.
v) We analyze the asymptotic secrecy rate gains of the MUCJ over the MURS to obtain insights.
vi) We propose optimal power allocation schemes which maximize the secrecy rate of the MUCJ.

The remainder of this paper is organized as follows. In Section II, the system model and the conventional scheme are described. Section III describes the MUCJ, and Section IV presents the ergodic secrecy rates of both schemes. The asymptotic secrecy rate gains are analyzed in analyzed in Section V. Section VI presents the optimal power allocation schemes for the MUCJ. In Section VII, the numerical results are given, and then, we conclude this paper in Section VIII.

Notation: We use $A := B$ to denote that A, by definition, equals B, and use $A =: B$ to denote that B, by definition, equals A. For a random variable X, $f_X(\cdot)$ and $F_X(\cdot)$ denote its probability density function (PDF) and cumulative density function (CDF), respectively. Also, $x \sim \mathcal{CN}(m, \Omega)$ indicates that x is a circularly symmetric complex-valued Gaussian random variable with mean m and variance Ω. The expectation and probability operators are denoted by $\mathbb{E}(\cdot)$ and $\mathbb{P}(\cdot)$, respectively. We also use $[x]^+$ to denote $\max(0, x)$ for a real number x. Also, the operator $\setminus$ denotes the set substraction. Finally, $\log(\cdot)$ and $\ln(\cdot)$ denote the base-2 and natural logarithms, respectively.

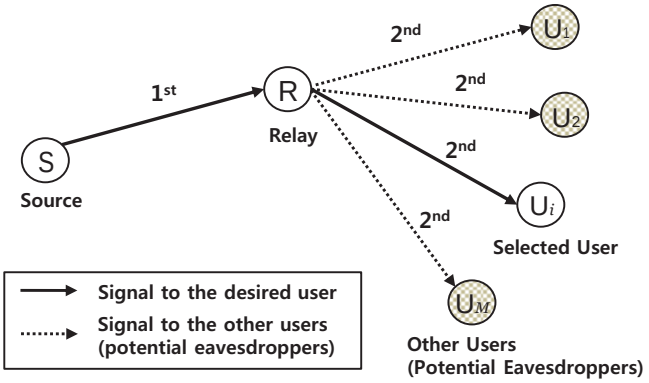

Fig. 1. System model for the MURS.

II. System Model and Conventional Scheme

A. System Model

We consider a downlink relay network with a source (S), a relay (R), and multiple receivers, which will be referred to as the users (U_j, $j = 1, \ldots, M$). The transmitted signals from the source are relayed by amplify-and-forward (AF) strategy at the relay. All the nodes are assumed to be equipped with a single antenna and they are working in the half-duplex mode. Every wireless link is assumed to be reciprocal and quasi-static with independent Rayleigh fading. The channel coefficient of each wireless link is constant within each frame but varies from one frame to another. The direct links from the source to the multiple users are not considered, assuming long distance or high attenuation of the signals. The noise associated with every channel is modelled as a mutually independent additive white Gaussian noise (AWGN) which has zero mean and unit variance. The AWGN at node i is denoted by η_i, $i \in \{S, R, U_1, \ldots, U_M\}$. The channel coefficient between node i and node j is denoted by $h_{ij} \sim \mathcal{CN}(0, \Omega_{ij})$ for $i, j \in \{S, R, U_1, \ldots, U_M\}$. The instantaneous and average channel power gains between node i and node j are denoted by $\gamma_{ij} := |h_{ij}|^2$ and $\overline{\gamma}_{ij} := \Omega_{ij}$, respectively. The channels from the relay to the users, i.e., h_{RU_j}, are assumed to be independent and identically distributed (i.i.d.), for which the average channel power gain is denoted by $\overline{\gamma}_{RU}$.

For channel estimation in the system, the source sends a pilot symbol to the relay and the relay sends another pilot symbol to the users. The channel h_{SR} can be estimated by the relay and h_{RU_j} can be estimated by each receiver as in [27]. Then the estimated channel state information (CSI) can be fed back to the source through the relay; specifically, the channel power gains γ_{SR} and γ_{RU_j} are fed back for the user selection. Thus, in this paper, it is assumed that the source can obtain the CSI of the channels h_{SR} and h_{RU_j}. During the channel estimation, however, the channels between the users, i.e., $h_{U_iU_j}$ for $i \neq j$, cannot be estimated by each user U_i because the users do not send any pilots.

B. Conventional Multiuser Relay Scheme

In the multiuser relay systems, it is possible to select the best user who has the highest e2e SNR among all users [18]–

[21]. In the first time slot, the source transmits the signal (intended *only* for the selected user) to the relay, and in the second time slot, the relay broadcasts the signal. In this paper, this conventional multiuser relay scheme is referred to as the MURS, which is shown in Fig. 1. Note that the transmitted signal is received not only by the selected user, but also by any other users. In this sense, the other users can be considered as (potential) eavesdroppers. In the following, we mathematically describe this scheme and analyze the secrecy rate.

The received signal at U_i is given by

$$y_{U_i} = \sqrt{E_R^c}\beta_c h_{SR} h_{RU_i} x_S + \beta_c h_{RU_i}\eta_R + \eta_{U_i} \quad (1)$$

where x_S is the transmitted signal and the amplifying coefficient β_c is given by $\beta_c := \sqrt{\frac{E_R^c}{E_S^c|h_{SR}|^2+1}}$. In the above equation, E_S^c and E_R^c, respectively, denote the source and relay powers for the MURS. Then the e2e SNR for U_i is given by [28]

$$\mathrm{SNR}^c(U_i) := \frac{E_S^c E_R^c \gamma_{SR}\gamma_{RU_i}}{E_S^c\gamma_{SR} + E_R^c\gamma_{RU_i} + 1}. \quad (2)$$

Among all M users, the particular user whose e2e SNR is the highest is selected and referred to as Bob, denoted by $\mathcal{B}_c$:

$$\mathcal{B}_c := \arg\max_{U_i\in\mathcal{U}} \{\mathrm{SNR}^c(U_i)\} \quad (3)$$

where $\mathcal{U} = \{U_1, \ldots, U_M\}$ denotes the set of all M users. Once $\mathcal{B}_c$ is selected, among all the remaining $(M-1)$ users, the user whose e2e SNR is the highest is determined and referred to as Eve, denoted by $\mathcal{E}_c$:

$$\mathcal{E}_c := \arg\max_{U_j\in\mathcal{U}\setminus\{\mathcal{B}_c\}} \{\mathrm{SNR}^c(U_j)\}. \quad (4)$$

Note that $\mathcal{E}_c$ is the worst eavesdropper from the perspective of Bob.

Given all channels, the instantaneous secrecy rate of the MURS is defined as

$$C_c := \left[\frac{1}{2}\log(\rho_c)\right]^+ \quad (5)$$

where ρ_c is defined as

$$\rho_c := \frac{1+\mathrm{SNR}^c(\mathcal{B}_c)}{1+\mathrm{SNR}^c(\mathcal{E}_c)}. \quad (6)$$

In the MURS, unfortunately, the secrecy rate C_c does not reasonably improve when the source power E_S^c and the relay power E_R^c are increased. This is because the capacity $\frac{1}{2}\log(1+\mathrm{SNR}^c(\mathcal{E}_c))$ of Eve increases whenever the capacity $\frac{1}{2}\log(1+\mathrm{SNR}^c(\mathcal{B}_c))$ of Bob increases. Even worse is that, in the MURS, the secrecy rate decreases as the number M of users increases. Clearly, this is opposite to the conventional *insecure* multiuser relay scheme with *no* security requirement. For the insecure system, the capacity is given by $\frac{1}{2}\log(1+\mathrm{SNR}^c(\mathcal{B}_c))$, which grows as the number M of users increases, which is known as the multiuser diversity. However, when a security requirement is imposed, the secrecy rate is determined by the difference between the capacities for Bob and Eve, and the difference between the capacities becomes smaller as the number of the users grows. Thus, the secrecy rate decreases as M increases in the MURS.[1] In Fig. 2, for the MURS, we present the ergodic capacity $\mathbf{E}[\frac{1}{2}\log(1+\mathrm{SNR}^c(\mathcal{B}_c))]$ with no security requirement and the ergodic secrecy rate $\mathbf{E}[\frac{1}{2}\log(\rho_c)]$ with security requirement. The source power and the relay power are set to be the same: $E^c = E_S^c = E_R^c$. Recall that the noise variance is assumed to be one in this paper; thus, we have $\frac{E^c}{\sigma^2} = E^c$ (dB). As expected before, with security requirement, the secrecy rate of the MURS degrades as the number M of the users increases.

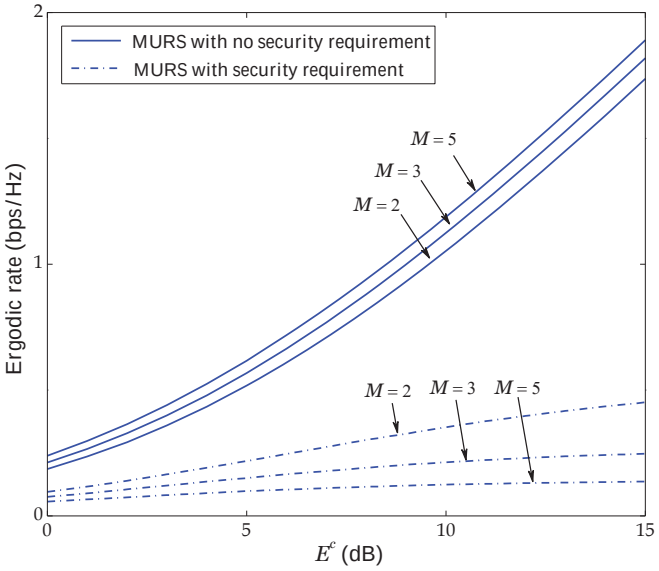

Fig. 2. Ergodic capacity comparison of the MURS with and without security requirement; $E_S^c = E_R^c = E^c$, $\overline{\gamma}_{SR} = \overline{\gamma}_{RU} = 1$.

In the next section, we consider the MUCJ in order to address the issue above.

III. Multiuser Relay Scheme with Cooperative Jamming

In this section, we describe the MUCJ, which ensures that the performance improves as the number of the users increases. Let $\mathcal{B}_p$ and $\mathcal{E}_p$ denote the selected user (Bob) and the worst eavesdropper (Eve), respectively. Then the MUCJ, as depicted in Fig. 3, operates as follows:

i) In the first time slot, the source sends a desired signal x_S (intended *only* for Bob) to the relay. At the same time, Bob sends a random jamming signal x_J to the relay.
ii) In the second time slot, the relay amplifies and forwards the received signal, which is composed of x_S and x_J, to Bob.

Once the transmission is completed, Bob subtracts the jamming signal from the signal he received, since he knows the jamming signal. On the other hand, any other users $U_k(\neq \mathcal{B}_p)$ including Eve cannot subtract the jamming signal from the received signal, since they know neither the jamming signal x_J nor the channel $h_{\mathcal{B}_p U_k}$ between Bob and U_k. Note that, in the first time slot, other users $U_k(\neq \mathcal{B}_p)$ also receive the jamming

[1]For one-hop communications (with no relay), a similar observation was made in [22].

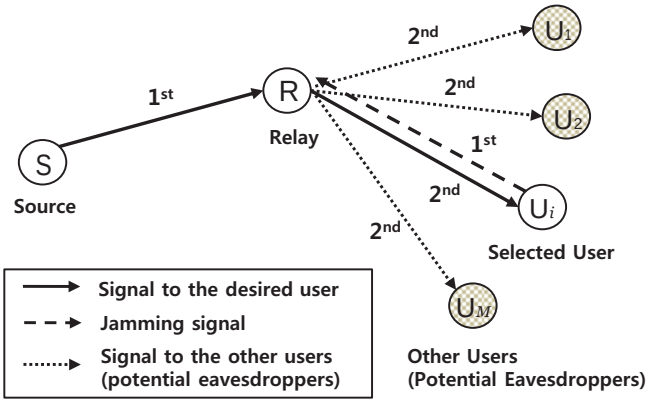

Fig. 3. System model for the MUCJ.

signal transmitted from Bob, which is given by $h_{\mathcal{B}_p U_k} x_J$. However, they cannot estimate x_J because they do not know $h_{\mathcal{B}_p U_k}$.[2] Therefore, once the transmission is completed, other users $U_k (\neq \mathcal{B}_p)$ cannot subtract the jamming signal from the signals they received. In the following, we mathematically describe this scheme and analyze the instantaneous secrecy rate.

Let $U_i \in \mathcal{U}$ represent the potential candidate users for Bob. Then the received signal at U_i is given by

$$y_{U_i} = \sqrt{E_S^p}\beta_p h_{SR} h_{RU_i} x_S + \sqrt{E_J^p}\beta_p h_{RU_i}^2 x_J + \beta_p h_{RU_i}\eta_R + \eta_{U_i} \quad (7)$$

where the amplifying coefficient β_p is given by $\beta_p := \sqrt{\frac{E_R^p}{E_S^p|h_{SR}|^2 + E_J^p|h_{RU_i}|^2 + 1}}$. In the above equation, E_S^p, E_R^p, and E_J^p, respectively, denote the source, relay, and jamming powers for the MUCJ. After subtracting the jamming signal term $\sqrt{E_J^p}\beta_p h_{RU_i}^2 x_J$ from (7), the received signal at U_i is given by

$$\tilde{y}_{U_i} = \sqrt{E_S^p}\beta_p h_{SR} h_{RU_i} x_S + \beta_p h_{RU_i}\eta_R + \eta_{U_i}. \quad (8)$$

The e2e SNR at U_i is then represented as

$$\mathrm{SNR}_{\mathcal{B}}^p(U_i) := \frac{E_S^p E_R^p \gamma_{SR}\gamma_{RU_i}}{E_S^p\gamma_{SR} + (E_R^p + E_J^p)\gamma_{RU_i} + 1}. \quad (9)$$

Let $U_j \in \mathcal{U} \setminus \{U_i\}$ represent the potential candidate users for Eve. The received signal at U_j is given by

$$y_{U_j} = \sqrt{E_S^p}\beta_p h_{SR} h_{RU_j} x_S + \sqrt{E_J^p}\beta_p h_{RU_i} h_{RU_j} x_J + \beta_p h_{RU_j}\eta_R + \eta_{U_j}. \quad (10)$$

[2]It is assumed that the undesired users $U_k (\neq \mathcal{B}_p)$ cannot estimate the jamming signal since they do not know the CSI. Specifically, the undesired users do not know the CSI of the channel $h_{\mathcal{B}_p U_k}$ between Bob and them and the phase of the channel $h_{R\mathcal{B}_p}$ between the relay and Bob. A similar assumption was made in [26] and [29].

The e2e SNR at U_j is then represented as

$$\mathrm{SNR}_{\mathcal{E}}^p(U_j) := \frac{E_S^p E_R^p \gamma_{SR}\gamma_{RU_j}}{E_R^p E_J^p \gamma_{RU_i}\gamma_{RU_j} + E_R^p\gamma_{RU_j} + E_S^p\gamma_{SR} + E_J^p\gamma_{RU_i} + 1}. \quad (11)$$

We now propose a user selection scheme, in which the user having largest SNR is selected as follows:

$$\mathcal{B}_p := \arg\max_{U_i \in \mathcal{U}} \{\gamma_{RU_i}\}. \quad (12)$$

This simple user selection scheme turns out to be optimal in the sense of secrecy rate. To show the optimality, we first formulate the secrecy rate for U_i as follows. Given U_i, the secrecy rate $C_s(U_i)$ for U_i is given by the difference between the capacity of U_i and the capacity of the particular user excluding U_i who has the highest capacity. Mathematically, $C_s(U_i)$ is given by

$$C_s(U_i) := \left[C^{\mathcal{B}}(U_i) - \max_{U_j \in \mathcal{U}\setminus\{U_i\}} \{C^{\mathcal{E}}(U_j)\}\right]^+ \quad (13)$$

where $C^{\mathcal{B}}(U_i) := \frac{1}{2}\log(1 + \mathrm{SNR}_{\mathcal{B}}^p(U_i))$ is the capacity for U_i. For $U_j \in \mathcal{U} \setminus \{U_i\}$, the capacity $C^{\mathcal{E}}(U_j)$ is defined as $C^{\mathcal{E}}(U_j) := \frac{1}{2}\log(1 + \mathrm{SNR}_{\mathcal{E}}^p(U_j))$. Note that, when U_i is selected as the destination, $C_s(U_i)$ is the secrecy rate of the transmission. Now let $\hat{\mathcal{B}}_p$ denote the user who gives the highest secrecy rate:

$$\hat{\mathcal{B}}_p := \arg\max_{U_i \in \mathcal{U}} \{C_s(U_i)\}. \quad (14)$$

In the following lemma, we show the optimality of the proposed user selection scheme.

Lemma 1: The user selection scheme of (12) is equivalent to (14), i.e., $\mathcal{B}_p = \hat{\mathcal{B}}_p$.

Proof: See Appendix A. ■

From this lemma, it can be seen that our proposed user selection scheme maximizes $C_s(U_i)$.

For the proposed user selection scheme of (12) or (14), the instantaneous secrecy rate is given by

$$\begin{aligned} C_p &:= \max_{U_i \in \mathcal{U}} \{C_s(U_i)\} \\ &= \left[C^{\mathcal{B}}(\mathcal{B}_p) - \max_{U_j \in \mathcal{U}\setminus\{\mathcal{B}_p\}} \{C^{\mathcal{E}}(U_j)\}\right]^+ \\ &= \left[C^{\mathcal{B}}(\mathcal{B}_p) - C^{\mathcal{E}}(\mathcal{E}_p)\right]^+ \\ &= \left[\frac{1}{2}\log(\rho_p)\right]^+ \end{aligned} \quad (15)$$

where ρ_p is given by

$$\rho_p := \frac{1 + \mathrm{SNR}_{\mathcal{B}}^p(\mathcal{B}_p)}{1 + \mathrm{SNR}_{\mathcal{E}}^p(\mathcal{E}_p)}. \quad (16)$$

In the above equations, $\mathcal{E}_p$ is referred to as Eve and defined as follows:

$$\begin{aligned} \mathcal{E}_p &:= \arg\max_{U_j \in \mathcal{U}\setminus\{\mathcal{B}_p\}} \left\{C^{\mathcal{E}}(U_j)\right\} \\ &\overset{(a)}{=} \arg\max_{U_j \in \mathcal{U}\setminus\{\mathcal{B}_p\}} \{\gamma_{RU_j}\} \end{aligned} \quad (17)$$

where the equality (a) holds since $C^{\mathcal{E}}(U_m) \geq C^{\mathcal{E}}(U_n)$ is equivalent to $\gamma_{RU_m} \geq \gamma_{RU_n}$.

Rather interestingly, the selected Bob and Eve are actually the same for the MURS and the MUCJ, although the user selection criteria and the obtained secrecy rate expressions are different for the two schemes. This is shown in the following lemma.

Lemma 2: The Bob and Eve selected by the MURS and the MUCJ are the same: $\mathcal{B}_c = \mathcal{B}_p$ and $\mathcal{E}_c = \mathcal{E}_p$.

Proof: Since the inequality $\text{SNR}^c(U_m) \geq \text{SNR}^c(U_n)$ is equivalent to $\gamma_{RU_m} \geq \gamma_{RU_n}$, $\mathcal{B}_c$ in (3) and $\mathcal{E}_c$ in (4) can be rewritten as $\mathcal{B}_c = \arg\max_{U_i \in \mathcal{U}}\{\gamma_{RU_i}\}$ and $\mathcal{E}_c = \arg\max_{U_j \in \mathcal{U}\setminus\{\mathcal{B}_c\}}\{\gamma_{RU_j}\}$, respectively. Therefore, the criteria for selecting Bob in both schemes are the same, i.e., $\mathcal{B}_c = \mathcal{B}_p$. Furthermore, the criteria for selecting Eve in both schemes are also the same, i.e., $\mathcal{E}_c = \mathcal{E}_p$. ■

From Lemma 2, we can simplify the notations for Bob and Eve as $\mathcal{B} := \mathcal{B}_c = \mathcal{B}_p$ and $\mathcal{E} := \mathcal{E}_c = \mathcal{E}_p$, respectively. Therefore, we use $\mathcal{B}$ and $\mathcal{E}$ throughout this paper.

In the following two sections, for the MURS and the MUCJ, we will derive the ergodic secrecy rates and analytically compare the two schemes. In the analysis and the comparison, it is important to ensure that the two schemes use the same amount of total power, because the MUCJ additionally consumes jamming power compared to the MURS. For fair comparison, therefore, we define the total power of the MURS as $E^c_{tot} = E^c_S + E^c_R$ and that of the MUCJ as $E^p_{tot} = E^p_S + E^p_R + E^p_J$. Then, throughout this paper, we will ensure $E^c_{tot} = E^p_{tot}$.

IV. Ergodic Secrecy Rate Analysis

In this section, we first derive the ergodic secrecy rate of the MURS. Then we investigate the ergodic secrecy rate of the MUCJ by deriving upper and lower bounds of the secrecy rate. Finally, we show that both bounds asymptotically approach the exact secrecy rate.

A. Exact Analysis for the MURS

In this subsection, we derive the exact ergodic secrecy rate of the MURS. We first rewrite the SNR ρ_c in (6) as follows:

$$\rho_c = \frac{(E^c_R\gamma_{R\mathcal{B}}+1)(E^c_S\gamma_{SR}+E^c_R\gamma_{R\mathcal{E}}+1)}{(E^c_R\gamma_{R\mathcal{E}}+1)(E^c_S\gamma_{SR}+E^c_R\gamma_{R\mathcal{B}}+1)}. \quad (18)$$

Then the ergodic secrecy rate is given by

$$\begin{aligned}\overline{C}_c &:= \mathbb{E}\Big\{\Big[\frac{1}{2}\log(\rho_c)\Big]^+\Big\} \\ &\overset{(b)}{=} \mathbb{E}\Big\{\frac{1}{2}\log(\rho_c)\Big\} \\ &= \frac{1}{2\ln 2}(A_1 - A_2 - A_3 + A_4) \end{aligned} \quad (19)$$

where $A_1 := \mathbb{E}\big[\ln(E^c_R\gamma_{R\mathcal{B}}+1)\big]$, $A_2 := \mathbb{E}\big[\ln(E^c_S\gamma_{SR} + E^c_R\gamma_{R\mathcal{B}}+1)\big]$, $A_3 := \mathbb{E}\big[\ln(E^c_R\gamma_{R\mathcal{E}}+1)\big]$, and $A_4 := \mathbb{E}\big[\ln(E^c_S\gamma_{SR}+E^c_R\gamma_{R\mathcal{E}}+1)\big]$. Note that the inequality $\rho_c \geq 1$ always holds since $\text{SNR}^c(\mathcal{B}_c) \geq \text{SNR}^c(\mathcal{E}_c)$ from (3) and (4); thus, we drop $[\cdot]^+$ and the equality (b) holds.

Using [32, eq. (4.337.2)], we can show that $A_1 = \Psi_1(E^c_R)$, where $\Psi_1(a)$ is defined as

$$\begin{aligned}\Psi_1(a) &:= \int_0^\infty \ln(ax+1) f_{\gamma_{R\mathcal{B}}}(x)dx \\ &= \sum_{i=0}^{M-1}\binom{M-1}{i}\frac{(-1)^i M}{i+1} e^{\frac{i+1}{a\overline{\gamma}_{RU}}}\mathbf{E}_1\Big(\frac{i+1}{a\overline{\gamma}_{RU}}\Big). \end{aligned} \quad (20)$$

In (20), $\mathbf{E}_1(s) := \int_s^\infty e^{-u}\frac{1}{u}du$ denotes the exponential integral function, and the PDF of $\gamma_{R\mathcal{B}}$ is given as follows [31, eq. (3)]: $f_{\gamma_{R\mathcal{B}}}(x) = \sum_{i=0}^{M-1}\binom{M-1}{i}\frac{(-1)^i M}{\overline{\gamma}_{RU}} e^{-\frac{(i+1)x}{\overline{\gamma}_{RU}}}$. Also, using the result of [31, eq. (12)], we can show that $A_2 = \Psi_2(E^c_S, E^c_R)$, where $\Psi_2(a,b)$ is defined as

$$\begin{aligned}\Psi_2(a,b) &:= \sum_{i=0}^{M-1}\binom{M-1}{i}(-1)^i M\Big\{\frac{q_{im}}{a\overline{\gamma}_{SR}} \\ &\times\Big[a\overline{\gamma}_{SR}e^{\frac{1}{a\overline{\gamma}_{SR}}}\mathbf{E}_1\Big(\frac{1}{a\overline{\gamma}_{SR}}\Big) - \xi_1 e^{\frac{1}{\xi_1}}\mathbf{E}_1\Big(\frac{1}{\xi_1}\Big)\Big] \\ &+\frac{1-q_{im}(i-m)}{b\overline{\gamma}_{RU}} \\ &\times\Big[a\overline{\gamma}_{SR} + (a\overline{\gamma}_{SR}-1)e^{\frac{1}{a\overline{\gamma}_{SR}}}\mathbf{E}_1\Big(\frac{1}{a\overline{\gamma}_{SR}}\Big)\Big]\Big\}. \end{aligned} \quad (21)$$

In (21), $m := \frac{b\overline{\gamma}_{RU}}{a\overline{\gamma}_{SR}} - 1$, $\xi_1 := \frac{b\overline{\gamma}_{RU}}{i+1}$, and

$$q_{im} := \begin{cases}\frac{1}{i-m}, & \text{for } i \neq m, \\ 0, & \text{for } i = m.\end{cases} \quad (22)$$

Similar to the derivation of A_1, we can show that $A_3 = \Psi_3(E^c_R)$, where $\Psi_3(a)$ is defined as

$$\begin{aligned}\Psi_3(a) &:= \int_0^\infty \ln(ax+1) f_{\gamma_{R\mathcal{E}}}(x)dx \\ &= \sum_{k=0}^{M-2}\binom{M-2}{k}\frac{(-1)^k M(M-1)}{k+2} \\ &\times e^{\frac{k+2}{a\overline{\gamma}_{RU}}}\mathbf{E}_1\Big(\frac{k+2}{a\overline{\gamma}_{RU}}\Big). \end{aligned} \quad (23)$$

In (23), the PDF of $\gamma_{R\mathcal{E}}$ is given as follows [30, eq. (12)]: $f_{\gamma_{R\mathcal{E}}}(x) = M(M-1)\sum_{k=0}^{M-2}\frac{\binom{M-2}{k}(-1)^k}{\overline{\gamma}_{RU}} e^{-\frac{(k+2)x}{\overline{\gamma}_{RU}}}$. Using the PDF of $\gamma_{R\mathcal{E}}$, we can show that $A_4 = \Psi_4(E^c_S, E^c_R)$, where $\Psi_4(a,b)$ is defined as

$$\begin{aligned}\Psi_4(a,b) &:= \sum_{k=0}^{M-2}\binom{M-2}{k}(-1)^k M(M-1)\Big\{\frac{q_{km}}{a\overline{\gamma}_{SR}} \\ &\times\Big[a\overline{\gamma}_{SR}e^{\frac{1}{a\overline{\gamma}_{SR}}}\mathbf{E}_1\Big(\frac{1}{a\overline{\gamma}_{SR}}\Big) - \xi_2 e^{\frac{1}{\xi_2}}\mathbf{E}_1\Big(\frac{1}{\xi_2}\Big)\Big] \\ &+\frac{1-q_{km}(k-m)}{b\overline{\gamma}_{RU}} \\ &\times\Big[a\overline{\gamma}_{SR} + (a\overline{\gamma}_{SR}-1)e^{\frac{1}{a\overline{\gamma}_{SR}}}\mathbf{E}_1\Big(\frac{1}{a\overline{\gamma}_{SR}}\Big)\Big]\Big\}. \end{aligned} \quad (24)$$

In (24), ξ_2 is defined as $\xi_2 := \frac{b\overline{\gamma}_{RU}}{k+2}$. Finally, substituting the results for A_i, $i = 1, \cdots, 4$ into (19), the exact ergodic secrecy rate is obtained for the MURS.

$$\rho_p = \frac{\big((E_S^p E_R^p \gamma_{SR} + E_R^p + E_J^p)(\gamma_{R\mathcal{B}} + \frac{1}{E_R^p}) - \alpha\big)\big(E_J^p \gamma_{R\mathcal{B}} + 1 + \frac{E_S^p \gamma_{SR}}{E_R^p \gamma_{R\mathcal{E}} + 1}\big)}{(E_S^p \gamma_{SR} + (E_R^p + E_J^p)\gamma_{R\mathcal{B}} + 1)(E_S^p \gamma_{SR} + E_J^p \gamma_{R\mathcal{B}} + 1)} \tag{25}$$

$$\begin{aligned}\rho_p &\overset{(c)}{\leq} \frac{(E_S^p E_R^p \gamma_{SR} + E_R^p + E_J^p)(\gamma_{R\mathcal{B}} + \frac{1}{E_R^p})\big(E_J^p \gamma_{R\mathcal{B}} + 1 + \frac{E_S^p \gamma_{SR}}{E_R^p \gamma_{R\mathcal{E}} + 1}\big)}{(E_S^p \gamma_{SR} + (E_R^p + E_J^p)\gamma_{R\mathcal{B}} + 1)(E_S^p \gamma_{SR} + E_J^p \gamma_{R\mathcal{B}} + 1)} \\ &=: \rho_{p_U}\end{aligned} \tag{26}$$

B. Upper-Bound Analysis for the MUCJ

Unlike the MURS, it is difficult to derive the exact ergodic secrecy rate of the MUCJ. This is because the expression of ρ_p in (16) is given in a much more complicated form due to the complex SNR expressions in (9) and (11). Instead of tackling the exact ergodic secrecy rate, therefore, we derive bounds: an upper-bound in this subsection and a lower-bound in the next subsection.

We first define the ratio α between the jamming power and the relay power as follows: $\alpha := \frac{E_J^p}{E_R^p} \geq 0$. Using α, we then rewrite ρ_p in (16) as (25), shown at the top of the page. Dropping α in (25), we obtain an SNR upper-bound ρ_{p_U} in (26), shown at the top of the page, where the equality (c) holds only when $E_J^p = 0$. The exact ergodic secrecy rate is given by

$$\begin{aligned}\overline{C}_p &:= \mathbb{E}\Big\{\Big[\frac{1}{2}\log(\rho_p)\Big]^+\Big\} \\ &\overset{(d)}{=} \mathbb{E}\Big\{\frac{1}{2}\log(\rho_p)\Big\}.\end{aligned} \tag{27}$$

Note that the inequality $\rho_p \geq 1$ always holds since $\text{SNR}_{\mathcal{B}}^p(\mathcal{B}_p) \geq \text{SNR}_{\mathcal{E}}^p(\mathcal{E}_p)$ from (12) and (17); thus, we drop $[\cdot]^+$ and the equality (d) holds. Using the SNR upper-bound in (26), an upper-bound $\overline{C}_p^U$ of the ergodic secrecy rate is given as follows:

$$\begin{aligned}\overline{C}_p &\leq \mathbb{E}\Big[\frac{1}{2}\log(\rho_{p_U})\Big] \\ &= \frac{1}{2\ln 2}(I_1 - I_2 - I_3 + I_4) \\ &=: \overline{C}_p^U\end{aligned} \tag{28}$$

where $I_1 := \mathbb{E}\big[\ln\big((E_S^p E_R^p \gamma_{SR} + E_R^p + E_J^p)(\gamma_{R\mathcal{B}} + \frac{1}{E_R^p})\big)\big]$, $I_2 := \mathbb{E}\big[\ln(E_S^p \gamma_{SR} + (E_R^p + E_J^p)\gamma_{R\mathcal{B}} + 1)\big]$, $I_3 := \mathbb{E}\big[\ln(E_S^p \gamma_{SR} + E_J^p \gamma_{R\mathcal{B}} + 1)\big]$, and $I_4 := \mathbb{E}\big[\ln\big(E_J^p \gamma_{R\mathcal{B}} + 1 + \frac{E_S^p \gamma_{SR}}{E_R^p \gamma_{R\mathcal{E}} + 1}\big)\big]$.

We can show that I_1 is given by

$$\begin{aligned}I_1 &= \ln\Big(\frac{1}{E_R^p}\Big) + \int_0^\infty \ln(E_S^p E_R^p x + E_R^p + E_J^p) f_{\gamma_{SR}}(x)dx \\ &\quad + \int_0^\infty \ln(E_R^p x + 1) f_{\gamma_{R\mathcal{B}}}(x)dx \\ &= \ln\Big(1 + \frac{E_J^p}{E_R^p}\Big) + e^{\frac{E_R^p + E_J^p}{E_S^p E_R^p \overline{\gamma}_{SR}}} \mathbf{E}_1\Big(\frac{E_R^p + E_J^p}{E_S^p E_R^p \overline{\gamma}_{SR}}\Big) + \Psi_1(E_R^p)\end{aligned} \tag{29}$$

where $f_{\gamma_{SR}}(x) = \frac{1}{\overline{\gamma}_{SR}} e^{-\frac{x}{\overline{\gamma}_{SR}}}$. Also, we can show that the terms I_2 and I_3 are given by $I_2 = \Psi_2(E_S^p, E_R^p + E_J^p)$ and $I_3 = \Psi_2(E_S^p, E_J^p)$, respectively. Finally, I_4 is derived as follows: $I_4 = \int_0^\infty \ln(1+w) f_{W_1}(w)dw$ where W_1 is defined as $W_1 := E_J^p \gamma_{R\mathcal{B}} + \frac{E_S^p \gamma_{SR}}{E_R^p \gamma_{R\mathcal{E}} + 1}$. It is possible to derive the PDF of W_1 in a one integral form with finite upper and lower limits as (30), shown at the top of the next page, where $\kappa := w - E_J^p z$ (see Appendix B). It does not appear that the integral in (30) can be solved in closed-form with any integration formulas or techniques in the literature. However, one can easily evaluate the integration for I_4 utilizing standard software such as Matlab or Mathematica. Overall, using the expressions for I_i, $i = 1, \cdots, 4$, the upper-bound of the ergodic secrecy rate in (28) is obtained for the MUCJ.

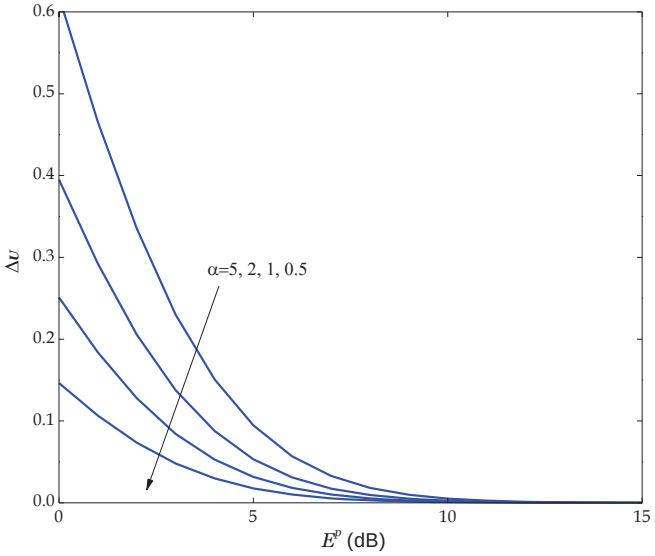

Fig. 4. Δ_U versus E^p; $E_S^p = E_R^p = E_J^p/\alpha = E^p$, $\overline{\gamma}_{SR} = \overline{\gamma}_{RU} = 1$, $M = 3$.

In order to investigate how tight the derived upper-bound is, we define the difference between the upper-bound and the exact ergodic secrecy rate as follows: $\Delta_U := \overline{C}_p^U - \overline{C}_p$. In the following lemma, we show that the upper-bound is asymptotically exact.

Lemma 3: Let $E^p = E_S^p = E_R^p = \frac{E_J^p}{\alpha}$. When $E^p \to \infty$, the difference Δ_U approaches zero:

$$\lim_{E^p \to \infty} \Delta_U = 0. \tag{31}$$

Proof: The difference Δ_U can be written as $\Delta_U = -\frac{1}{2}\mathbb{E}\left[\log\left(1 - \frac{\alpha}{(E^p \gamma_{SR} + \alpha + 1)(E^p \gamma_{R\mathcal{B}} + 1)}\right)\right]$. Then (31) follows

$$f_{W_1}(w) = \sum_{i=0}^{M-2} \binom{M-2}{i} \frac{(-1)^i M(M-1)}{\overline{\gamma}_{RU}} \int_0^{\frac{w}{E_J^p}} \frac{e^{-\frac{(i+2)z}{\overline{\gamma}_{RU}} - \frac{\kappa(1+E_R^p z)}{E_S^p \overline{\gamma}_{SR}}}}{((i+1)E_S^p \overline{\gamma}_{SR} + E_R^p \overline{\gamma}_{RU}\kappa)^2} \Big[e^{\frac{(i+1)z}{\overline{\gamma}_{RU}} + \frac{E_R \kappa z}{E_S \overline{\gamma}_{SR}}} \big((i+1)E_S^p \overline{\gamma}_{SR} + (\kappa + E_S^p \overline{\gamma}_{SR})E_R^p \overline{\gamma}_{RU}\big) - E_R^p \overline{\gamma}_{RU}\kappa(1+E_R^p z) - E_S^p \overline{\gamma}_{SR}\big((i+1)(E_R^p z+1) + E_R^p \overline{\gamma}_{RU}\big) \Big] dz \quad (30)$$

from Δ_U with $E^p \to \infty$. ■

This result shows that the upper-bound asymptotically matches with the exact one as E^p increases. Furthermore, the upper-bound is asymptotically exact as α decreases. That is, one can see that the difference Δ_U converges to zero when $\alpha \to 0$: $\lim_{\alpha\to 0} \Delta_U = 0$, because we have $\lim_{\alpha\to 0} \overline{C}_p = \lim_{\alpha\to 0} \overline{C}_p^U$ from $\lim_{\alpha\to 0} \rho_p = \lim_{\alpha\to 0} \rho_{p_U}$. In order to numerically evaluate the tightness of the upper-bound, the numerical results for the difference Δ_U are presented in Fig. 4. The results demonstrate that the upper-bound becomes tighter as $E^p \to \infty$ and $\alpha \to 0$.

C. Lower-Bound Analysis for the MUCJ

In this subsection, we investigate the ergodic secrecy rate of the MUCJ by deriving a lower-bound. To this end, we first rewrite ρ_p as (32), shown at the top of the next page. Then, we obtain an SNR lower-bound ρ_{p_L} in (33), shown at the top of the next page, where the equalities in (e) and (f) hold only when $E_S^p = 0$ and $E_J^p = 0$, respectively. Based on this SNR lower-bound, a lower-bound $\overline{C}_p^L$ of the ergodic secrecy rate can be given by

$$\begin{aligned} \overline{C}_p &\geq \mathbb{E}\Big[\frac{1}{2}\log(\rho_{p_L})\Big] \\ &= \frac{1}{2\ln 2}(L_1 - L_2 - L_3 + L_4) \\ &=: \overline{C}_p^L \end{aligned} \quad (34)$$

where $L_1 := \mathbb{E}\big[\ln((E_S^p\gamma_{SR}+1)(E_R^p\gamma_{R\mathcal{B}}+1))\big]$, $L_2 := \mathbb{E}\big[\ln(E_S^p\gamma_{SR} + (E_R^p + E_J^p)\gamma_{R\mathcal{B}} + 1)\big]$, $L_3 := \mathbb{E}\big[\ln(E_S^p\gamma_{SR} + E_J^p\gamma_{R\mathcal{B}} + 1)\big]$, and $L_4 := \mathbb{E}\big[\ln(E_J^p\gamma_{R\mathcal{B}} + 1)\big]$.

Following the derivation procedure for I_1 in (29), we obtain the result for L_1 as follows: $L_1 = e^{\frac{1}{E_S^p\overline{\gamma}_{SR}}}\mathbf{E}_1\big(\frac{1}{E_S^p\overline{\gamma}_{SR}}\big) + \Psi_1(E_R^p)$. Also, the terms L_2, L_3, and L_4 are given by $L_2 = \Psi_2(E_S^p, E_R^p + E_J^p)$, $L_3 = \Psi_2(E_S^p, E_J^p)$, and $L_4 = \Psi_1(E_J^p)$, respectively. Using the expressions for L_i, $i = 1, \cdots, 4$, we obtain the lower-bound of the ergodic secrecy rate in (34).

In order to investigate how tight the derived lower-bound is, we define the difference between the lower-bound and the exact ergodic secrecy rate as follows: $\Delta_L := \overline{C}_p - \overline{C}_p^L$. In the following lemma, we show that the lower-bound is asymptotically exact.

Lemma 4: Let $E^p = E_S^p = E_R^p = \frac{E_J^p}{\alpha}$. When $E^p \to \infty$, the difference Δ_L converges to zero:

$$\lim_{E^p\to\infty} \Delta_L = 0. \quad (35)$$

Proof: The difference Δ_L can be written as $\Delta_L = \frac{1}{2}\mathbb{E}\Big[\log\Big(1 + \frac{\alpha E^p\gamma_{R\mathcal{B}}}{(E^p\gamma_{SR}+1)(E^p\gamma_{R\mathcal{B}}+1)}\Big) + \log\Big(1 + \frac{E^p\gamma_{SR}}{(E^p\gamma_{R\mathcal{E}}+1)(\alpha E^p\gamma_{R\mathcal{B}}+1)}\Big)\Big]$. Then (35) follows from Δ_L with $E_p \to \infty$. ■

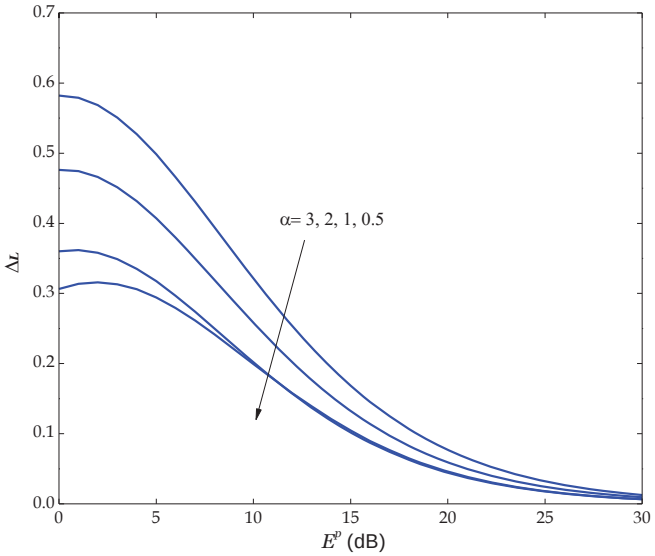

Fig. 5. Δ_L versus E^p; $E_S^p = E_R^p = E_J^p/\alpha = E^p$, $\overline{\gamma}_{SR} = \overline{\gamma}_{RU} = 1$, $M = 3$.

This result shows that the lower-bound asymptotically matches with the exact one as power E^p increases. To numerically evaluate the tightness of the lower-bound, the numerical results for the difference Δ_L are presented in Fig. 5. The results demonstrate that the lower-bound becomes tighter as $E^p \to \infty$. Although the lower-bound seems less tighter than the upper-bound for the same E^p, it provides a simpler analytical expression than the upper-bound. Finally, from Lemmas 3 and 4, we have the following corollary showing that the upper-bound and the lower-bound asymptotically meet each other, implying that they asymptotically approach the exact one.

Corollary 1: Let $E^p = E_S^p = E_R^p = \frac{E_J^p}{\alpha}$. When $E^p \to \infty$, the upper and lower bounds converge to the exact ergodic secrecy rate as follows: $\lim_{E^p\to\infty} \overline{C}_p^U = \lim_{E^p\to\infty} \overline{C}_p^L = \lim_{E^p\to\infty} \overline{C}_p$. ■

V. Asymptotic Secrecy Rate Gain

In this section, using the ergodic secrecy rate expressions derived in the previous section, we analyze asymptotic secrecy rate gains of the MUCJ over the MURS. Specifically, we will present instantaneous and average rate gains for several asymptotic cases. This analysis gives us useful insights into

$$\rho_p = \frac{((E_S^p\gamma_{SR}+1)(E_R^p\gamma_{R\mathcal{B}}+1)+E_J^p\gamma_{R\mathcal{B}})\big(E_J^p\gamma_{R\mathcal{B}}+1+\frac{E_S^p\gamma_{SR}}{E_R^p\gamma_{R\mathcal{E}}+1}\big)}{(E_S^p\gamma_{SR}+(E_R^p+E_J^p)\gamma_{R\mathcal{B}}+1)(E_S^p\gamma_{SR}+E_J^p\gamma_{R\mathcal{B}}+1)} \tag{32}$$

$$\begin{aligned}\rho_p &\overset{(e)}{\geq} \frac{((E_S^p\gamma_{SR}+1)(E_R^p\gamma_{R\mathcal{B}}+1)+E_J^p\gamma_{R\mathcal{B}})(E_J^p\gamma_{R\mathcal{B}}+1)}{(E_S^p\gamma_{SR}+(E_R^p+E_J^p)\gamma_{R\mathcal{B}}+1)(E_S^p\gamma_{SR}+E_J^p\gamma_{R\mathcal{B}}+1)}\\ &\overset{(f)}{\geq} \frac{(E_S^p\gamma_{SR}+1)(E_R^p\gamma_{R\mathcal{B}}+1)(E_J^p\gamma_{R\mathcal{B}}+1)}{(E_S^p\gamma_{SR}+(E_R^p+E_J^p)\gamma_{R\mathcal{B}}+1)(E_S^p\gamma_{SR}+E_J^p\gamma_{R\mathcal{B}}+1)}\\ &=: \rho_{p_L}\end{aligned} \tag{33}$$

the two schemes. To this end, let us define the instantaneous and average secrecy rate gains as

$$G := C_p - C_c, \tag{36}$$
$$\overline{G} := \mathbb{E}\big[C_p\big] - \mathbb{E}\big[C_c\big]. \tag{37}$$

In the following, we analyze the gains for three asymptotic cases: i) the source power goes to infinity, ii) the relay power goes to infinity, and iii) the power of every node goes to infinity, all subject to the same total network power constraint for both schemes. In the following lemma, we consider the first scenario.

Lemma 5: Let $E_S = E_S^p = E_S^c$. Suppose the source power goes to infinity, $E_S \to \infty$, with $\frac{E_{tot}^c}{E_{tot}^p} = 1$. The instantaneous and average secrecy rate gains are given by

$$\lim_{E_S\to\infty} G = \frac{1}{2\ln 2}\left[\ln\left(\frac{(E_R^p\gamma_{R\mathcal{B}}+1)(E_R^c\gamma_{R\mathcal{E}}+1)}{(E_R^c\gamma_{R\mathcal{B}}+1)(E_R^p\gamma_{R\mathcal{E}}+1)}\right)\right], \tag{38}$$

$$\begin{aligned}\lim_{E_S\to\infty} \overline{G} = \frac{1}{2\ln 2}\big[&\Psi_1(E_R^p) - \Psi_1(E_R^c) + \Psi_3(E_R^c)\\ &-\Psi_3(E_R^p)\big].\end{aligned} \tag{39}$$

Proof: When $E_S \to \infty$, the SNRs ρ_c and ρ_p in (6) and (16), respectively, are given by $\lim_{E_S\to\infty}\rho_c = \frac{E_R^c\gamma_{R\mathcal{B}}+1}{E_R^c\gamma_{R\mathcal{E}}+1}$, $\lim_{E_S\to\infty}\rho_p = \frac{E_R^p\gamma_{R\mathcal{B}}+1}{E_R^p\gamma_{R\mathcal{E}}+1}$. Using these results, we can easily obtain (38). Also, using the results in (20) and (23), we can obtain (39). ■

Using the result of Lemma 5, we can prove the following theorem.

Theorem 1: Let $E_S = E_S^p = E_S^c$. Suppose the source power goes to infinity, $E_S \to \infty$, with $\frac{E_{tot}^c}{E_{tot}^p} = 1$. The MURS is better than or equal to the MUCJ: $\lim_{E_S\to\infty} G \leq 0$, where the equality holds only when $E_J^p = 0$.

Proof: The inequality $\lim_{E_S\to\infty} G \leq 0$ can be rewritten as follows: $(E_R^p\gamma_{R\mathcal{B}}+1)(E_R^c\gamma_{R\mathcal{E}}+1) \leq (E_R^p\gamma_{R\mathcal{E}}+1)(E_R^c\gamma_{R\mathcal{B}}+1)$. Then this inequality is reduced to $(E_R^p - E_R^c)(\gamma_{R\mathcal{B}} - \gamma_{R\mathcal{E}}) \leq 0$. First, we always have $\gamma_{R\mathcal{B}} \geq \gamma_{R\mathcal{E}}$ because Bob and Eve are selected as in (12) and (17), respectively. Second, we also have $E_R^p \leq E_R^c$, because we assume that $E_S^p = E_S^c$ and $E_{tot}^p = E_{tot}^c$ (Recall that $E_{tot}^p = E_S^p + E_R^p + E_J^p$ and $E_{tot}^c = E_S^c + E_R^c$). In this case, $E_R^c = E_R^p + E_J^p$, so that we have $E_R^p \leq E_R^c$. Overall, the inequality $(E_R^p - E_R^c)(\gamma_{R\mathcal{B}} - \gamma_{R\mathcal{E}}) \leq 0$ always holds. ■

The results of Lemma 5 and Theorem 1 can be intuitively explained as follows. When the source power is very high, the jamming signal from Bob to the relay in the first time slot becomes much weaker compared to the signal from the source. Therefore, the effect of the jamming, which acts as interference at Eve, also becomes very weaker when being amplified and forwarded at the relay. This means that the jamming is ineffective in this case, so that we can find that the gains in (38) and (39) do not depend on the jamming power E_J^p. Therefore, in this case, it is not efficient to use any power for such jamming. In the MURS, since no power is *wasted* for jamming, more power can be used at the relay, so that this additional relay power improves the secrecy rate of the MURS compared to the MUCJ. However, the performance loss of the MUCJ compared to the MURS is generally very small for the following reason. Since *both* SNRs of Bob ($E_R^c\gamma_{R\mathcal{B}}$) and Eve ($E_R^c\gamma_{R\mathcal{E}}$) increase as the relay power E_R^c increases, the additional relay power used by the MURS improves only very slightly the secrecy rate of the MURS. Therefore, the secrecy rate gain G is close to zero, meaning that the performance of both schemes is almost the same. We will numerically confirm this in Section VII.

In the following lemma, we consider the second asymptotic scenario where the relay power is very large.

Lemma 6: Let $E_R = E_R^p = E_R^c$. Suppose the relay power goes to infinity, $E_R \to \infty$, with $\frac{E_{tot}^c}{E_{tot}^p} = 1$. The instantaneous and average secrecy rate gains are given by

$$\lim_{E_R\to\infty} G = \frac{1}{2\ln 2}\left[\ln\Big(\frac{E_S^p\gamma_{SR}+1}{1+\frac{E_S^p\gamma_{SR}}{E_J^p\gamma_{R\mathcal{B}}+1}}\Big)\right], \tag{40}$$

$$\begin{aligned}\lim_{E_R\to\infty} \overline{G} = \frac{1}{2\ln 2}\Big[&e^{\frac{1}{E_S^p\overline{\gamma}_{SR}}}\mathbf{E}_1\Big(\frac{1}{E_S^p\overline{\gamma}_{SR}}\Big) + \Psi_1(E_J^p)\\ &-\Psi_2(E_S^p, E_J^p)\Big].\end{aligned} \tag{41}$$

Proof: See Appendix C. ■

Using the result of Lemma 6, we can prove the following theorem.

Theorem 2: Let $E_R = E_R^p = E_R^c$. Suppose the relay power goes to infinity, $E_R \to \infty$, with $\frac{E_{tot}^c}{E_{tot}^p} = 1$. The MUCJ is better than or equal to the MURS: $\lim_{E_R\to\infty} G \geq 0$, where the equality holds only when $E_S^p = 0$ and/or $E_J^p = 0$.

Proof: Since $E_J^p\gamma_{R\mathcal{B}} \geq 0$ in (40), we can easily obtain the result $\lim_{E_R\to\infty} G \geq 0$. ■

The results of Lemma 6 and Theorem 2 can be intuitively explained as follows. When the relay power is very high,

$$\Lambda = \ln\left(\frac{(\beta E_{tot}^p\gamma_{SR}+1)(E_R^p\gamma_{R\mathcal{B}}+1)(E_J^p\gamma_{R\mathcal{B}}+1)}{(\beta E_{tot}^p\gamma_{SR}+(E_R^p+E_J^p)\gamma_{R\mathcal{B}}+1)(\beta E_{tot}^p\gamma_{SR}+E_J^p\gamma_{R\mathcal{B}}+1)}\right)+\lambda(E_R^p+E_J^p-(1-\beta)E_p^{tot}) \quad (49)$$

the secrecy rate of the MURS becomes close to zero since $\lim_{E_R^c\to\infty}\rho_c = 1$. This is because all the potential eavesdroppers may reliably decode the source message whenever Bob decodes the source message, since the high relay power makes the transmission between the relay and the users reliable and all the users share the same channel h_{SR} and source power E_S^c. With the MURS, therefore, one cannot securely transmit the source message. On the other hand, in the MUCJ, the jamming prevents the potential eavesdroppers from intercepting the source message by acting as interference. Thus, the secrecy rate of the MUCJ is larger in this case. In Section VII, we will demonstrate that the secrecy rate gains can be (very) significant.

In the following lemma, we consider the third asymptotic scenario where the power of every terminal is very large.

Lemma 7: Let $E^p = E_S^p = E_R^p = \frac{E_J^p}{\alpha}$ and $E^c = E_S^c = E_R^c$. Suppose the power of every node goes to infinity, $E^p \to \infty$ and $E^c \to \infty$, with $\frac{E^c}{E^p} = 1+\frac{\alpha}{2}$ and $\frac{E_{tot}^c}{E_{tot}^p} = 1$. The instantaneous and average secrecy rate gains are given by

$$\lim_{E^p\to\infty, E^c\to\infty} G \to \infty, \quad (42)$$

$$\lim_{E^p\to\infty, E^c\to\infty} \overline{G} \to \infty. \quad (43)$$

Proof: We rewrite ρ_c and ρ_{p_L}, respectively, as follows: $\rho_c = \frac{(E^c\gamma_{R\mathcal{B}}+1)(E^c\gamma_{SR}+E^c\gamma_{R\mathcal{E}}+1)}{(E^c\gamma_{R\mathcal{E}}+1)(E^c\gamma_{SR}+E^c\gamma_{R\mathcal{B}}+1)}$, $\rho_{p_L} = \frac{(E^p\gamma_{SR}+1)(E^p\gamma_{R\mathcal{B}}+1)(\alpha E^p\gamma_{R\mathcal{B}}+1)}{(E^p\gamma_{SR}+(1+\alpha)E^p\gamma_{R\mathcal{B}}+1)(E^p\gamma_{SR}+\alpha E^p\gamma_{R\mathcal{B}}+1)}$. When $E^p\to\infty$, ρ_{p_L} is given by $\lim_{E^p\to\infty}\rho_{p_L}\to\infty$. Since $\rho_p \geq \rho_{p_L}$, we have $\lim_{E^p\to\infty}\rho_p \to \infty$. Furthermore, when $E^c\to\infty$, we have $\lim_{E^c\to\infty}\rho_c = \frac{\gamma_{R\mathcal{B}}(\gamma_{SR}+\gamma_{R\mathcal{E}})}{\gamma_{R\mathcal{E}}(\gamma_{SR}+\gamma_{R\mathcal{B}})}$. From these results, we obtain the secrecy rate gains in (42) and (43). ■

From the result of Lemma 7, we immediately obtain the following theorem.

Theorem 3: Let $E^p = E_S^p = E_R^p = \frac{E_J^p}{\alpha}$ and $E^c = E_S^c = E_R^c$. Suppose the power of every node goes to infinity, $E^p \to \infty$ and $E^c\to\infty$, with $\frac{E^c}{E^p} = 1+\frac{\alpha}{2}$ and $\frac{E_{tot}^c}{E_{tot}^p} = 1$. The MUCJ is better than the MURS: $\lim_{E^p\to\infty, E^c\to\infty} G > 0$.

Proof: The result can be easily obtained from (42). ■

The results of Lemma 7 and Theorem 3 can be intuitively explained as follows. In the MURS, the capacity of Eve increases whenever the capacity of Bob increases. Therefore, the secrecy rate of the MURS becomes saturated to a constant in this case. In the MUCJ, however, the capacity of Eve does not necessarily increase whenever the capacity of Bob increases, since the SNR of Eve is degraded by the jamming signal. Therefore, the asymptotic rate of the MUCJ goes to infinity, and thus, the secrecy rate gains also go to infinity. This means that the MUCJ is particularly very efficient when the transmit power of every node is very large.

Additionally, when the number M of users goes to infinity, we obtain the asymptotic ergodic secrecy rate of the MUCJ in the following lemma.

Lemma 8: When the number M of users goes to infinity, $M\to\infty$, the ergodic secrecy rate of the MUCJ is given by

$$\lim_{M\to\infty}\overline{C}_p = \frac{1}{2\ln 2}e^{\frac{E_R^p+E_J^p}{E_S^pE_R^p\overline{\gamma}_{SR}}}\mathbf{E}_1\left(\frac{E_R^p+E_J^p}{E_S^pE_R^p\overline{\gamma}_{SR}}\right). \quad (44)$$

Proof: See Appendix D. ■

This result shows that the asymptotic ergodic secrecy rate does *not* grow with M, but converges to a constant. This is because the first hop (S-R link) becomes a bottle neck for the overall ergodic secrecy rate since the SNR γ_{SR} of the first hop does not improve as M increases.

VI. Optimal Power Allocation for the MUCJ

In this section, we propose optimal power allocation schemes which maximize the secrecy rate of the MUCJ. The optimization problem for the MUCJ is given by

Optimal Power Allocation:

$$(E_{S,\text{opt}}^p, E_{R,\text{opt}}^p, E_{J,\text{opt}}^p) = \arg\max_{E_S^p,E_R^p,E_J^p}\ln(\rho_p),$$
$$\text{subject to } E_S^p+E_R^p+E_J^p = E_{tot}^p. \quad (45)$$

Unfortunately, due to the complex SNR expression of ρ_p in (16), it is very difficult to analytically derive the optimal powers $E_{S,\text{opt}}^p, E_{R,\text{opt}}^p$, and $E_{J,\text{opt}}^p$. Thus, we numerically obtain the optimal power allocation of (45) although the complexity is fairly high.

For analytical tractability, we will carry out the power optimization using an SNR bound in the following. Specifically, we perform power optimization based on the SNR lower-bound ρ_{p_L} in (33). Note that the SNR lower-bound ρ_{p_L} is asymptotically tight with the exact SNR ρ_p in the sense that $\lim_{E^p\to\infty}\ln(\rho_{p_L}) = \lim_{E^p\to\infty}\ln(\rho_p)$, where $E^p = E_S^p = E_R^p = E_J^p/\alpha$. Using ρ_{p_L}, the asymptotically optimal power allocation problem is given by

Asymptotically Optimal Power Allocation:

$$(E_{S,\text{aopt}}^p, E_{R,\text{aopt}}^p, E_{J,\text{aopt}}^p) = \arg\max_{E_S^p,E_R^p,E_J^p}\ln(\rho_{p_L}),$$
$$\text{subject to } E_S^p+E_R^p+E_J^p = E_{tot}^p. \quad (46)$$

In order to solve (46), we rewrite the problem as in the following form:

$$(\beta_{\text{aopt}}, E_{R,\text{aopt}}^p, E_{J,\text{aopt}}^p) = \arg\max_{\beta}\max_{E_R^p,E_J^p}\ln(\rho_{p_L}),$$
$$\text{subject to } E_R^p+E_J^p = (1-\beta)E_{tot}^p \text{ and } 0\leq\beta\leq 1 \quad (47)$$

where β is defined as $\beta := \frac{E_S^p}{E_{tot}^p}$. We first focus on the inner-optimization as follows:

$$(E_{R,\text{aopt}}^p, E_{J,\text{aopt}}^p) = \arg\max_{E_R^p,E_J^p}\ln(\rho_{p_L}),$$
$$\text{subject to } E_R^p+E_J^p = (1-\beta)E_{tot}^p. \quad (48)$$

For analytical derivation of the solution to (48), the Lagrangian cost function is written as (49), shown at the top of the page,

$$\Upsilon(\beta) := \ln\left(\frac{(\beta E_{tot}^p\gamma_{SR}+1)((1-\beta)E_{tot}^p\gamma_{R\mathcal{B}}+\beta E_{tot}^p\gamma_{SR}+2-\varphi(\beta))(\varphi(\beta)-\beta E_{tot}^p\gamma_{SR})}{\varphi(\beta)(\beta E_{tot}^p\gamma_{SR}+(1-\beta)E_{tot}^p\gamma_{R\mathcal{B}}+1)}\right) \quad (53)$$

where λ is the Lagrangian multiplier. Setting the derivatives of the Lagrangian cost function Λ with respect to E_R^p, E_J^p, and λ, respectively, equal to zero ($\frac{\partial\Lambda}{\partial E_R^p}=0$, $\frac{\partial\Lambda}{\partial E_J^p}=0$, and $\frac{\partial\Lambda}{\partial\lambda}=0$) and solving the three equations, we obtain the solution to (48) as follows:

$$E_{J,\text{aopt}}^p(\beta) = \frac{\varphi(\beta)-\beta E_{tot}^p\gamma_{SR}-1}{\gamma_{R\mathcal{B}}}, \quad (50)$$

$$E_{R,\text{aopt}}^p(\beta) = (1-\beta)E_{tot}^p - E_J^p \quad (51)$$

where $\varphi(\beta)$ is defined as follows: $\varphi(\beta) := \sqrt{(1+\beta E_{tot}^p\gamma_{SR})^2+(\beta(1-\beta)\gamma_{SR}\gamma_{R\mathcal{B}}(E_{tot}^p)^2-1)}$. Substituting (50) and (51) into (47), we obtain the optimization problem for β as follows:

$$\beta_{\text{aopt}} = \arg\max_{\beta}\Upsilon(\beta),$$
$$\text{subject to } 0\le\beta\le 1 \quad (52)$$

where the function $\Upsilon(\beta)$ is defined as (53), shown at the top of the page. It is very challenging to mathematically derive a closed-form solution of β_{aopt} because the function $\Upsilon(\beta)$ is given in a very complicated form. However, it is fairly easy to numerically obtain β_{aopt} because the searching is done over finite and narrow one-dimensional range ($0\le\beta\le 1$). Note that the computational complexity required to numerically solve (52) is absolutely much lower than that of (45). Overall, the asymptotically optimal power allocation is obtained as follows: $E_{J,\text{aopt}}^p(\beta_{\text{aopt}})$ by (50), $E_{R,\text{aopt}}^p(\beta_{\text{aopt}})$ by (51), and $E_{S,\text{aopt}}^p(\beta_{\text{aopt}})=\beta_{\text{aopt}}E_{tot}^p$, where β_{aopt} is determined from (52).

VII. Numerical Results

In this section, we present numerical results for the ergodic secrecy rates and the asymptotic secrecy rate gains for the two schemes. We assume the average squared channel gains as $\overline{\gamma}_{SR}=\overline{\gamma}_{RU}=1$. The node powers are assumed as $E_S^p=E_R^p=\frac{E_J^p}{\alpha}=E^p$ and $E_S^c=E_R^c=E^c$. For fair comparison, the powers E^c and E^p are assumed to be $E=E^p=\frac{E^c}{1+\frac{\alpha}{2}}$; then the total powers of the two schemes are the same as $E_{tot}^p=E_{tot}^c=(2+\alpha)E$.

Fig. 6 presents the ergodic secrecy rates of the two schemes when $\alpha=0.3$ and $M=2,3,5$. One can see that the analysis for the MURS perfectly matches with the simulation. Also, the upper and lower bounds for the MUCJ asymptotically match with the simulation as shown in Corollary 1. In particular, the upper-bound is generally very tight and it becomes slightly less tight in the low power E regime. One can also see that the MUCJ significantly outperforms the MURS, especially in the high power E regime, since the secrecy rate of the MUCJ increases as E grows, while that of the MURS converges to a constant. This is because the jamming degrades the SNRs of the undesired users in the MUCJ, whereas there is no degradation to the undesired users in the MURS. As a result,

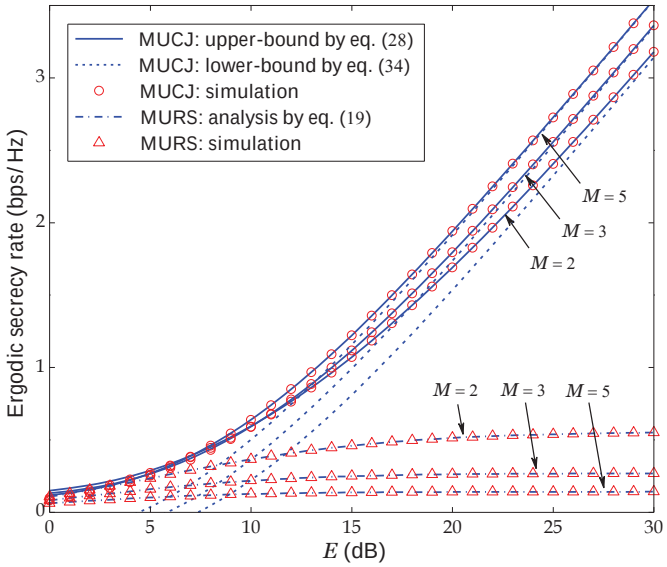

Fig. 6. Ergodic secrecy rates of the MURS and the MUCJ; $E^p=E$, $E^c=(1+\alpha/2)E$, and $\alpha=0.3$.

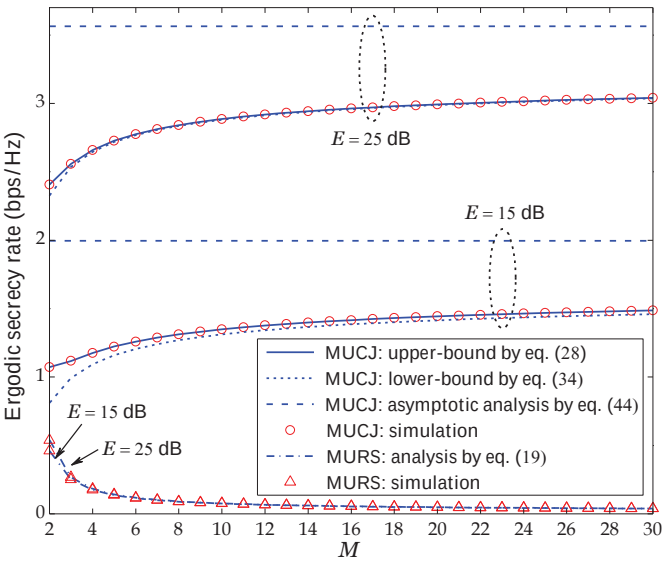

Fig. 7. Ergodic secrecy rates versus M; $E^p=E$, $E^c=(1+\alpha/2)E$, and $\alpha=0.3$.

there is significant ergodic secrecy rate gap between the two schemes in the high power E regime, and this shows the effect of the jamming in the MUCJ. As explained earlier, we can find that the ergodic secrecy rate of the MURS decreases as the number M of users grows, while that of the MUCJ increases with M.

In Fig. 7, we present the ergodic secrecy rates of the two schemes versus M when $\alpha=0.3$ and $E=15,25$ dB. As demonstrated in Fig. 6, one can see that the ergodic secrecy

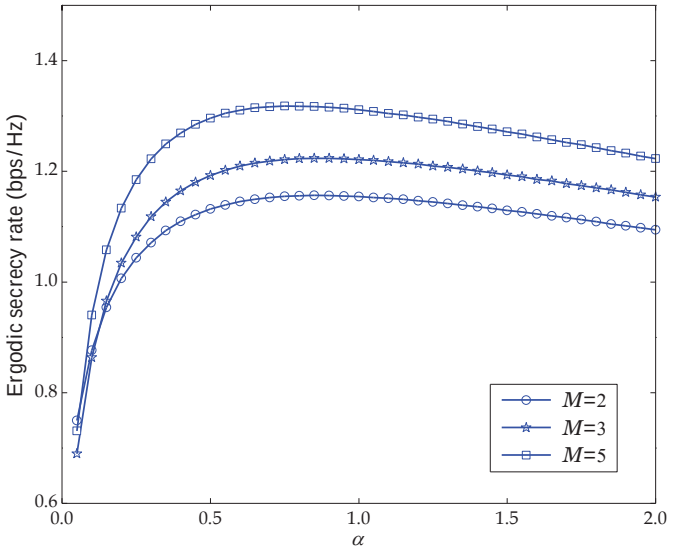

Fig. 8. Ergodic secrecy rate of the MUCJ versus α; $E^p = 15$ dB.

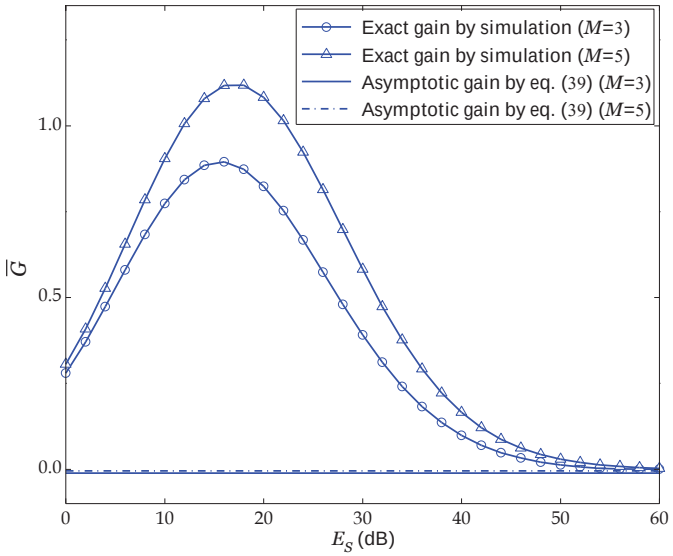

Fig. 9. Average secrecy rate gain $\overline{G}$ when $E_S \to \infty$; $E_S = E_S^p = E_S^c$, $E_R^p = E_J^p/\alpha = 15$ dB, $E_R^c = E_S^p + E_J^p$, and $\alpha = 0.3$.

rate of the MURS decreases as M grows, while that of the MUCJ increases. One can also see that the ergodic secrecy rate of the MUCJ continuously approaches the asymptotic result as M grows. In the MURS, the growing number of users is detrimental since the increase of the obtained information at Eve is more significant than that at Bob, so that this incurs the decrease of the ergodic secrecy rate. This can be verified as follows. Since $\gamma_{RB} \geq \gamma_{RE}$ because Bob and Eve are selected as in (12) and (17), respectively, an upper-bound of the SNR ρ_c in (6) is given by $\rho_c \leq \frac{E_R^c \gamma_{RB}+1}{E_R^c \gamma_{RE}+1} =: \rho_c^U$. The SNR ρ_c^U is the same as that for one-hop multiuser communications (with no relay) in [22]. From the result in [22, eq. (19)], we can verify that the ergodic secrecy rate goes to zero as follows: $\lim_{M\to\infty} \mathbb{E}[\frac{1}{2}\log(\rho_c^U)] = 0$. Therefore, we can easily obtain that the ergodic secrecy rate of the MURS decreases and finally reaches zero as the number of users grows as follows: $\lim_{M\to\infty} \mathbb{E}[\frac{1}{2}\log(\rho_c)] = 0$. However, in the MUCJ, the ergodic secrecy rate grows with M, and then finally converges to the asymptotic result.

Fig. 8 depicts the ergodic secrecy rate of the MUCJ versus α when $E^p = 15$ dB and $M = 2, 3, 5$. Note that the increase of α is equivalent to the increase of the jamming power E_J^p. In the low α range, the ergodic secrecy rate of the MUCJ quickly increases as α grows. However, one can see that the performance slowly decreases as α grows, even though Bob consumes more jamming power. Moreover, very strong jamming makes the ergodic secrecy rate approach zero as $\lim_{E_J^p\to\infty} \overline{C}_p = 0$ since $\lim_{E_J^p\to\infty} \rho_p = 1$. This result shows the effect of the jamming in the MUCJ as the jamming power E_J^p grows.

In the following, we present numerical results of the average secrecy rate gain $\overline{G}$ of the MUCJ over the MURS.

In Fig. 9, by setting the powers as $E_S = E_S^p = E_S^c$, $E_R^p = \frac{E_J^p}{\alpha} = 15$ dB, $E_R^c = E_S^p + E_J^p$, and $\alpha = 0.3$, we present the average secrecy rate gain $\overline{G}$ when the source power is very high. One can see that the asymptotic gain in (39) is close to

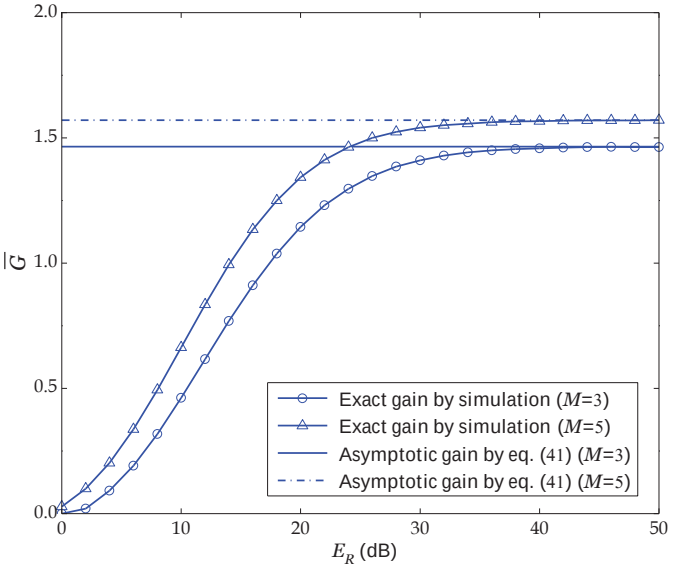

Fig. 10. Average secrecy rate gain $\overline{G}$ when $E_R \to \infty$; $E_R = E_R^p = E_R^c$, $E_S^p = E_J^p/\alpha = 15$ dB, $E_S^c = E_S^p + E_J^p$, and $\alpha = 0.3$.

zero and asymptotically matches with the exact secrecy rate gain by simulation. Interestingly, the exact secrecy rate gain in Fig. 9 has a peak point around 10–20 dB source power range, then it decreases and finally goes close to zero as the source power increases. As explained in Lemma 5, this phenomenon is related with the diminishing effect of the jamming due to its relatively low power compared to the source signal as the source power increases. For this reason, the effect of the jamming finally disappears with very high source power. As a result, the average secrecy rate gain $\overline{G}$ is close to zero. It means that the jamming may not be helpful when the source only has a very large transmit power.

In Fig. 10, by setting the powers as $E_R = E_R^p = E_R^c$, $E_S^p =$

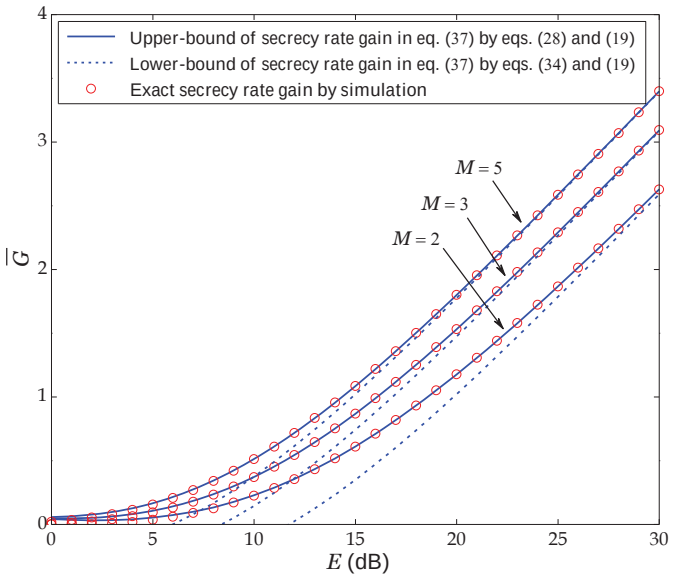

Fig. 11. Average secrecy rate gain $\overline{G}$ when $E \to \infty$; $E^p = E$, $E^c = (1+\alpha/2)E$, and $\alpha = 0.3$.

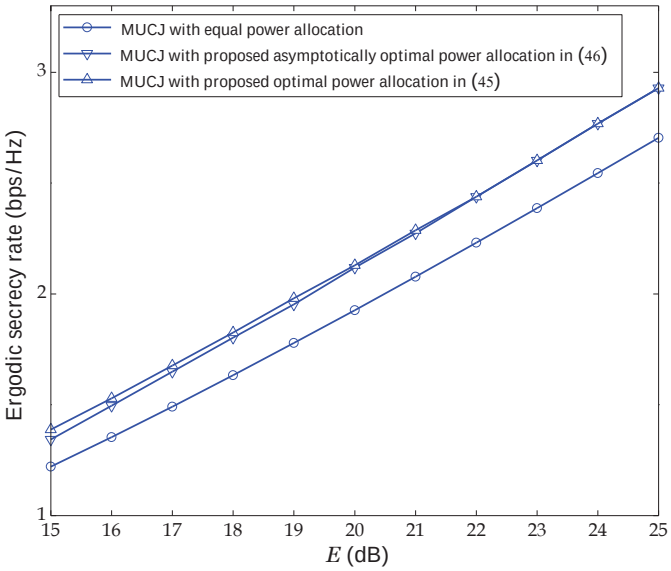

Fig. 12. Ergodic secrecy rates of the MUCJ with equal and proposed power allocations; $M = 3$.

$\frac{E_J^p}{\alpha} = 15$ dB, $E_S^c = E_S^p + E_J^p$, and $\alpha = 0.3$, we present the average secrecy rate gain $\overline{G}$ when the relay power is very high. As opposed to the result in Fig. 9, the average secrecy rate gain increases as the relay power grows, and then it approaches a constant which is derived in (41). This shows that we can achieve positive secrecy rate gain when the relay power is high compared to the other powers. The asymptotic secrecy rate of the MURS becomes essentially zero when the relay power is very high, so that the asymptotic average secrecy rate gain becomes the same as the ergodic secrecy rate of the MUCJ in this case.

Fig. 11 represents the average secrecy rate gain $\overline{G}$ when the power E grows. The accuracy of both bounds is similar to the results in Fig. 6. As expected in Lemma 7, the average secrecy rate gain increases as the power E grows. From this result, we can confirm that the MUCJ is particularly very effective compared to the MURS in the high power E regime.

In Fig. 12, we present the ergodic secrecy rates of the MUCJ with equal and proposed power allocations when $M = 3$. For the MUCJ with equal power allocation, the power E is set to be $E = E_S^p = E_R^p = E_J^p = \frac{E_{tot}^p}{3}$. For the MUCJ with the proposed power allocations, the total power E_{tot}^p is set to be $E_{tot}^p = 3E$ for fair comparison. One can see that significant performance gains can be achieved by the proposed optimal and asymptotically optimal power allocation schemes. Moreover, the secrecy rate of the asymptotically optimal power allocation scheme is close to that of the optimal power allocation scheme in the whole E regime. Recall that the asymptotically optimal power allocation scheme in (46) is much easier to be numerically solved than the optimal power allocation scheme in (45). As E grows, the secrecy rate of the asymptotically optimal scheme approaches that of the optimal scheme. This is because the SNR lower-bound ρ_{p_L} in (46) is asymptotically matched with the exact SNR ρ_p in (45).

Fig. 13 presents the secrecy outage probabilities of the two

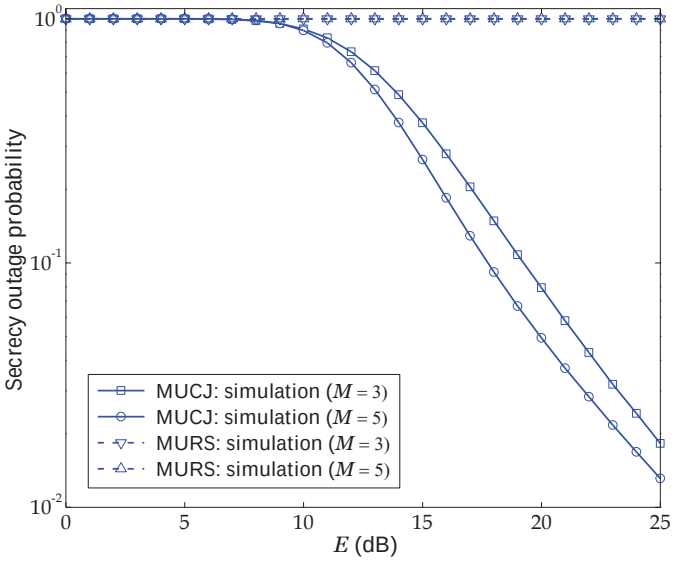

Fig. 13. Secrecy outage probabilities of the MUCJ and the MUCJ; $E^p = E$, $E^c = (1+\alpha/2)E$, $\alpha = 0.3$, and $R_s = 1$.

schemes when $\alpha = 0.3$, $M = 3, 5$, and $R_s = 1$ where R_s is the target secrecy rate. Specifically, the secrecy outage probability is given by $P_{out}(R_s) := \mathbb{P}\{C < R_s\} = \mathbb{P}\{\rho < 2^{2R_s}\}$ where C is the instantaneous secrecy rate, and ρ is the e2e SNR of the system. For the MUCJ, the instantaneous secrecy rate C_p is given by (15) and the e2e SNR ρ_p is given by (25). For the MURS, the instantaneous secrecy rate C_c is given by (5) and the e2e SNR ρ_c is given by (18). Similar with the results of the ergodic secrecy rate, one can see that the MUCJ significantly outperforms the MURS when the secrecy outage probability is considered as a performance metric. Also, the secrecy outage probability of the MUCJ decreases as M grows, while the MURS has very poor secrecy outage performance.

VIII. Conclusion

In this paper, we investigated the secure transmission for multiuser relay networks, where the undesired users who are not selected for data reception may overhear the source message as eavesdroppers. In the secure multiuser systems, the secrecy capacity of the conventional scheme deteriorates as the number of users increases. In order to address this issue, we proposed a new multiuser relay scheme by employing cooperative jamming. We derived the ergodic secrecy capacity of both schemes. We also analyzed the asymptotic secrecy capacity gains. We revealed that the proposed scheme could be very effective, since the jamming in the proposed scheme prevented the eavesdroppers from intercepting the source message.

Appendix A
Proof of Lemma 1

Let us define $\hat{U}$ as $\hat{U} := \arg\max_{U_i \in \mathcal{U}} \{C^{\mathcal{B}}(U_i)\}$. First, from (14), we have

$$\Big[C^{\mathcal{B}}(\hat{\mathcal{B}}_p) - \max_{U_j \in \mathcal{U}\setminus\{\hat{\mathcal{B}}_p\}} \{C^{\mathcal{E}}(U_j)\}\Big]^+ \geq \Big[C^{\mathcal{B}}(\hat{U}) - \max_{U_j \in \mathcal{U}\setminus\{\hat{U}\}} \{C^{\mathcal{E}}(U_j)\}\Big]^+. \quad \text{(A.1)}$$

Second, we can show that the following holds:

$$\Big[C^{\mathcal{B}}(\hat{U}) - \max_{U_j \in \mathcal{U}\setminus\{\hat{U}\}} \{C^{\mathcal{E}}(U_j)\}\Big]^+ \overset{(g)}{\geq} \Big[C^{\mathcal{B}}(\hat{\mathcal{B}}_p) - \max_{U_j \in \mathcal{U}\setminus\{\hat{U}\}} \{C^{\mathcal{E}}(U_j)\}\Big]^+ \quad \text{(A.2)}$$

$$\overset{(h)}{\geq} \Big[C^{\mathcal{B}}(\hat{\mathcal{B}}_p) - \max_{U_j \in \mathcal{U}\setminus\{\hat{\mathcal{B}}_p\}} \{C^{\mathcal{E}}(U_j)\}\Big]^+. \quad \text{(A.3)}$$

The inequality (g) holds since $C^{\mathcal{B}}(\hat{U}) \geq C^{\mathcal{B}}(\hat{\mathcal{B}}_p)$ from the definition of $\hat{U}$. Furthermore, the inequality (h) holds, since $\max_{U_j \in \mathcal{U}\setminus\{\hat{\mathcal{B}}_p\}}\{C^{\mathcal{E}}(U_j)\} \geq \max_{U_j \in \mathcal{U}\setminus\{\hat{U}\}}\{C^{\mathcal{E}}(U_j)\}$. Since the inequality $\text{SNR}^p_{\mathcal{B}}(U_m) \geq \text{SNR}^p_{\mathcal{B}}(U_n)$ is equivalent to $\gamma_{RU_m} \geq \gamma_{RU_n}$, the inequality $C^{\mathcal{B}}(U_m) \geq C^{\mathcal{B}}(U_n)$ is equivalent to $\gamma_{RU_m} \geq \gamma_{RU_n}$. Furthermore, since the inequality $\text{SNR}^p_{\mathcal{E}}(U_m) \geq \text{SNR}^p_{\mathcal{E}}(U_n)$ is equivalent to $\gamma_{RU_m} \geq \gamma_{RU_n}$, the inequality $C^{\mathcal{E}}(U_m) \geq C^{\mathcal{E}}(U_n)$ is also equivalent to $\gamma_{RU_m} \geq \gamma_{RU_n}$. Overall, the inequality $C^{\mathcal{B}}(U_m) \geq C^{\mathcal{B}}(U_n)$ is equivalent to $C^{\mathcal{E}}(U_m) \geq C^{\mathcal{E}}(U_n)$. Therefore, from the inequality $\max_{U_j \in \mathcal{U}\setminus\{\hat{\mathcal{B}}_p\}}\{C^{\mathcal{B}}(U_j)\} \geq \max_{U_j \in \mathcal{U}\setminus\{\hat{U}\}}\{C^{\mathcal{B}}(U_j)\}$, which always holds from the definition of $\hat{U}$, we have $\max_{U_j \in \mathcal{U}\setminus\{\hat{\mathcal{B}}_p\}}\{C^{\mathcal{E}}(U_j)\} \geq \max_{U_j \in \mathcal{U}\setminus\{\hat{U}\}}\{C^{\mathcal{E}}(U_j)\}$.

From (A.1) and (A.3), we conclude that $\hat{\mathcal{B}}_p = \hat{U}$, because otherwise it is not possible to satisfy both (A.1) and (A.3). Finally, since $C^{\mathcal{B}}(U_m) \geq C^{\mathcal{B}}(U_n)$ is equivalent to $\gamma_{RU_m} \geq \gamma_{RU_n}$, we have $\hat{U} = \arg\max_{U_i \in \mathcal{U}}\{C^{\mathcal{B}}(U_i)\} = \arg\max_{U_i \in \mathcal{U}}\{\gamma_{RU_i}\} = \mathcal{B}_p$. Overall, we have $\mathcal{B}_p = \hat{\mathcal{B}}_p$.

Appendix B
Derivation of $f_{W_1}(w)$ for I_4

We define the SNR expressions as $X := \gamma_{SR}, Y := \gamma_{R\mathcal{E}}$, and $Z := \gamma_{R\mathcal{B}}$. Then W_1 is expressed as $W_1 = E^p_J Z + \frac{E^p_S X}{E^p_R Y + 1}$, and we have the CDF of W_1 as

$$\begin{aligned} &F_{W_1}(w) \\ &= \mathbb{P}(W_1 \leq w) \\ &= \mathbb{P}\bigg(X \leq \frac{(E^p_R Y + 1)(w - E^p_J Z)}{E^p_S}, Y \leq Z, Z \leq \frac{w}{E^p_J}\bigg) \\ &= \int_0^{\frac{w}{E^p_J}} \int_0^z \int_0^{\frac{(E^p_R y + 1)(w - E^p_J z)}{E^p_S}} f_X(x) f_{Y,Z}(y,z) dx dy dz \end{aligned} \quad \text{(B.1)}$$

where the joint PDF of Y and Z is given as follows [22, eq. (6)]: $f_{Y,Z}(y,z) = \sum_{i=0}^{M-2} \binom{M-2}{i} \frac{(-1)^i M(M-1)}{\overline{\gamma}^2_{RU}} e^{-\frac{(i+1)y+z}{\overline{\gamma}_{RU}}}$. Differentiating the CDF in (B.1), we have the PDF of W_1 as

$$\begin{aligned} &f_{W_1}(w) \\ &= \int_0^{\frac{w}{E^p_J}} \int_0^z \Big(\frac{E^p_R y + 1}{E^p_S}\Big) \\ &\quad \times f_X\Big(\frac{(E^p_R y + 1)(w - E^p_J z)}{E^p_S}\Big) f_{Y,Z}(y,z) dy dz \\ &= \sum_{i=0}^{M-2} \binom{M-2}{i} \frac{(-1)^i M(M-1)}{E^p_S \overline{\gamma}_{SR} \overline{\gamma}^2_{RU}} \\ &\quad \times \int_0^{\frac{w}{E^p_J}} \int_0^z (E^p_R y + 1) e^{-\frac{(i+1)y+z}{\overline{\gamma}_{RU}}} e^{-\frac{(E^p_R y + 1)(w - E^p_J z)}{E^p_S \overline{\gamma}_{SR}}} dy dz. \end{aligned} \quad \text{(B.2)}$$

Solving the integration in (B.2) with respect to y, we have the result in (30).

Appendix C
Proof of Lemma 6

When the relay power is very high, the SNRs ρ_c and ρ_p, respectively, are expressed as follows: $\lim_{E_R \to \infty} \rho_p = \frac{E^p_S \gamma_{SR} + 1}{1 + \frac{E^p_S \gamma_{SR}}{E^p_J \gamma_{R\mathcal{B}} + 1}}$ and $\lim_{E_R \to \infty} \rho_c = 1$. From these results, we can easily obtain the secrecy rate gain G in (40). Averaging the instantaneous secrecy rate gain G in (40), we have

$$\begin{aligned} \lim_{E_R \to \infty} \overline{G} = \frac{1}{2 \ln 2} \Big\{ &\mathbb{E}\big[\ln(E^p_S \gamma_{SR} + 1)\big] \\ &+ \mathbb{E}\big[\ln(E^p_J \gamma_{R\mathcal{B}} + 1)\big] \\ &- \mathbb{E}\big[\ln(E^p_S \gamma_{SR} + E^p_J \gamma_{R\mathcal{B}} + 1)\big] \Big\}. \end{aligned} \quad \text{(C.1)}$$

Using the result for L_1, we obtain the first term as follows: $\mathbb{E}\big[\ln(E^p_S \gamma_{SR} + 1)\big] = e^{\frac{1}{E^p_S \overline{\gamma}_{SR}}} \mathbf{E}_1\big(\frac{1}{E^p_S \overline{\gamma}_{SR}}\big)$. The other terms are given by $\mathbb{E}\big[\ln(E^p_J \gamma_{R\mathcal{B}} + 1)\big] = \Psi_1(E^p_J)$ and $\mathbb{E}\big[\ln(E^p_S \gamma_{SR} + E^p_J \gamma_{R\mathcal{B}} + 1)\big] = \Psi_2(E^p_S, E^p_J)$. Substituting the results into (C.1), we have the result in (41).

Appendix D
Proof of Lemma 8

When $M \to \infty$, for Bob, the SNR $\text{SNR}^p_{\mathcal{B}}(\mathcal{B})$ in (16) is given by $\lim_{M \to \infty} \text{SNR}^p_{\mathcal{B}}(\mathcal{B}) = \frac{E^p_S E^p_R \gamma_{SR}}{E^p_R + E^p_J}$ where this can be easily obtained from $\lim_{M \to \infty} \gamma_{R\mathcal{B}} \to \infty$, whereas γ_{SR} is independent of M.

When $M \to \infty$, for Eve, the SNR $\text{SNR}_{\mathcal{E}}^{p}(\mathcal{E})$ in (16) is also given by $\lim_{M\to\infty} \text{SNR}_{\mathcal{E}}^{p}(\mathcal{E}) = 0$ where this can be easily obtained from $\lim_{M\to\infty} \gamma_{R\mathcal{B}} \to \infty$ and $\lim_{M\to\infty} \gamma_{R\mathcal{E}} \to \infty$, whereas γ_{SR} is independent of M.

From these results, we obtain the asymptotic ρ_p as follows: $\lim_{M\to\infty} \rho_p = \lim_{M\to\infty} \frac{1+\text{SNR}_{\mathcal{B}}^{p}(\mathcal{B})}{1+\text{SNR}_{\mathcal{E}}^{p}(\mathcal{E})} = 1 + \frac{E_S^p E_R^p \gamma_{SR}}{E_R^p + E_J^p}$. We finally obtain the asymptotic ergodic secrecy rate of the MUCJ as follows: $\lim_{M\to\infty} \overline{C}_p = \lim_{M\to\infty} \mathbb{E}\left[\frac{1}{2}\log_2(\rho_p)\right] = \frac{1}{2\ln 2}\mathbb{E}\left[\ln\left(1 + \frac{E_S^p E_R^p \gamma_{SR}}{E_R^p + E_J^p}\right)\right]$. Using the result in (29), we can easily obtain (44).

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

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

[3] M. Bloch, J. Barros, M. R. D. Rodriques, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[4] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 6, no. 54, pp. 2470–2492, June 2008.

[5] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–5403, Oct. 2008.

[6] 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.

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

[8] J. Huang and A. L. Swindlehurst, "Cooperative jamming for secure communications in MIMO relay networks," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4871–4884, Oct. 2011.

[9] Y. Liu, J. Li, and A. P. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Inf. Forensics and Security*, vol. 61, no. 8, pp. 3801–3807, Oct. 2012.

[10] J. Yang, I.-M. Kim, and D. I. Kim, "Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2840–2852, June 2013.

[11] J. Yang, I.-M. Kim, and D. I. Kim, "Power-constrained optimal cooperative jamming for multiuser broadcast channel," *IEEE Wireless Comm. Lett.*, vol. 2, no. 4, pp. 411–414, Aug. 2013.

[12] 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.

[13] 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.

[14] J. Kim, A. Ikhlef, and R. Schober, "Combined relay selection and cooperative beamforming for physical layer security," *Jounal of Communications and Networks*, vol. 14, no. 4, pp. 364–373, Aug. 2012.

[15] C. Jeong and I.-M. Kim, "Optimal power allocation for secure multicarrier relay systems," *IEEE Trans. Signal Process.*, vol. 59, no. 11, pp. 5428–5442, Nov. 2011.

[16] R. Knopp and P. Humblet, "Information capacity and power control in single-cell multiuser communication," in *Proc. IEEE ICC*, June 1995, pp. 331–335.

[17] P. Viswanath, D. N. C. Tse, and R. Laroia, "Opportunistic beamforming using dumb antennas," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1277–1294, June 2002.

[18] J. Kim, D. S. Michalopoulos, and R. Schober, "Diversity analysis of multi-user multi-relay networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 7, pp. 2380–2389, July 2011.

[19] S. Chen, W. Wang, and X. Zhang, "Performance analysis of multiuser diversity in cooperative multi-relay networks under Rayleigh-fading channels," *IEEE Trans. Wireless Commun.*, vol. 8, no. 7, pp. 3415–3419, July 2009.

[20] N. Yang, M. Elkashlan, and J. Yuan, "Impact of opportunistic scheduling on cooperative dual-hop relay networks," *IEEE Trans. Commun.*, vol. 59, no. 3, pp. 689–694, Mar. 2011.

[21] X. Zhang, W. Wang, and X. Ji, "Multiuser diversity in multiuser two-hop cooperative relay wireless networks: System model and performance analysis," *IEEE Trans. Veh. Technol.*, vol. 58, no. 2, pp. 1031–1036, Feb. 2009.

[22] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, "On multiuser secrecy rate in flat fading channel," in *Proc. IEEE MILCOM*, Oct. 2009, pp. 1–7.

[23] X. He and A. Yener, "Two-hop secure communication using an untrusted relay," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, pp. 1–13, Nov. 2009.

[24] 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.

[25] J. Huang, A. Mukherjee, and A. L. Swindlehurst, "Secure communication via an untrusted non-regenerative relay in fading channels," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2536–2550, May 2013.

[26] K.-H. Park, T. Wang, and M.-S. Alouini, "On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1741–1750, Sep. 2013.

[27] N. Yang, P. L. Yeoh, M. Elkashlan, J. Yuan, and I. B. Collings, "Cascaded TAS/MRC in MIMO multiuser relay networks," *IEEE Trans. Wireless Commun.*, vol. 11, no. 10, pp. 3829–3839, Oct. 2012.

[28] J. N. Laneman, D. N. C. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[29] T.-H. Chang, W.-C. Chiang, Y.-W. Peter Hong, and C.-Y. Chi, "Training sequence design for discriminatory channel estimation in wireless MIMO systems," *IEEE Trans. Signal Process.*, vol. 58, no. 12, pp. 6223–6237, Dec. 2010.

[30] S. S. Ikki and M. H. Ahmed, "On the performance of amplify-and-forward cooperative diversity with the N^{th} best-relay selection scheme," in *Proc. IEEE ICC*, June 2009, pp. 1–6.

[31] L. Fan, X. Lei, and W. Li, "Exact closed-form expression for ergodic capacity of amplify-and-forward relaying in channel-noise-assisted cooperative networks with relay selection," *IEEE Comm. Lett.*, vol. 15, no. 3, pp. 332–333, Mar. 2011.

[32] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. San Diego, CA:Academic, 2007.