This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2018.2848648, IEEE Transactions on Vehicular Technology

Secure Two-Way Transmission via Wireless-Powered Untrusted Relay and External Jammer

Milad Tatar Mamaghani, Ali Kuhestani, *Student Member, IEEE*, and Kai-Kit Wong, *Fellow, IEEE*

***Abstract*—In this paper, we propose a two-way secure communication scheme where two transceivers exchange confidential messages via a wireless-powered untrusted amplify-and-forward (AF) relay in the presence of an external jammer. We take into account both friendly jamming (FJ) and Gaussian noise jamming (GNJ) scenarios. Based on the time switching (TS) architecture at the relay, the data transmission is done in three phases. In the first phase, both the energy-starved nodes, the untrustworthy relay and the jammer, are charged by non-information radio frequency (RF) signals from the sources. In the second phase, the two sources send their information signals and concurrently, the jammer transmits artificial noise to confuse the curious relay. Finally, the third phase is dedicated to forward a scaled version of the received signal from the relay to the sources. For the proposed secure transmission schemes, we derive new closed-form lower-bound expressions for the ergodic secrecy sum rate (ESSR) in the high signal-to-noise ratio (SNR) regime. We further analyze the asymptotic ESSR to determine the key parameters; the high SNR slope and the high SNR power offset of the jamming based scenarios. To highlight the performance advantage of the proposed FJ, we also examine the scenario of without jamming (WoJ). Finally, numerical examples and discussions are provided to acquire some engineering insights, and to demonstrate the impacts of different system parameters on the secrecy performance of the considered communication scenarios. The numerical results illustrate that the proposed FJ significantly outperforms the traditional one-way communication and the constellation rotation (CR) approach, as well as our proposed benchmarks, the two-way WoJ and GNJ scenarios.**

***Index Terms*—Wireless power transfer, Physical layer security, Two-way communication, Untrusted relaying, Jammer**

I. Introduction

A. Background and Motivation

COOPERATIVE relaying improves energy efficiency, extends coverage, and increases the throughput of wireless communication networks. Accordingly, in recent years, the benefits of relaying have been viewed from the standpoint of wireless physical-layer security (PLS) [1] which has been recognized as an emerging design paradigm to enhance the security of next generation wireless networks [2]. In the context of relaying-based transmission networks, a key area of interest is the untrusted relaying where the source-destination communication is assisted by a relay which may also be a potential eavesdropper [2], [3]. In practice, untrusted relaying scenario may occur in large-scale wireless systems such as heterogeneous networks, device-to-device (D2D) communications and Internet-of-things (IoT) applications, where the data of sources are often retransmitted by several intermediate nodes with low security clearance.

Secure transmission employing an untrusted relay was first studied in [4], where an achievable non-zero secrecy rate is obtained through jamming signal transmission. To be specific, two general types of jamming signals have been proposed in the literature to improve the PLS of wireless networks: 1) friendly jamming (FJ) and 2) Gaussian noise jamming (GNJ). In the former, the jamming signal is a priori known at the legal receiver [1]–[6], while in the latter, the legitimate receiver has no information about the jamming signal and hence, the receiver considers the jamming signal as an interfering signal [7], [8]. We mention that FJ offers better secrecy performance compared to GNJ, due to the fact that the legitimate receiver cancels the pre-defined jamming signal. Of course, this performance advantage is obtained at the cost of higher implementational complexity to the network. In the area of untrusted relaying, for the first time, the authors in [9] proposed destination-based cooperative jamming (CJ) technique to achieve a positive secrecy rate for a one-way untrusted relay, in which the jammer is co-located with the destination receiver. Motivated by the pioneering work [9], a great deal of research has been dedicated in the field of one-way untrusted relaying [10]–[13].

Recently, several works have considered the more interesting scenario of two-way untrusted relaying [14]–[17], where physical-layer network coding can enhance the security of communication by receiving a superimposed signal from the two sources instead of each individual signal. The authors in [14] proposed a game-theoretic power control scheme between the two sources and multiple jammers, where single user decoding (SUD) is assumed for the untrusted relay to extract the information signal. We note that, in the SUD operation, the relay attempts to decode one message while the other signal is considered as an interference. However, the untrusted relay in two-way relaying can potentially eavesdrop the legitimate transmissions according to another advanced strategy namely multi-user decoding (MUD), in which the relay attempts to decode two information signals transmitted by the two sources. It is worth noting that the MUD can be considered as the worst case scenario in untrusted relaying networks [15], [16]. In [15], the authors proposed iterative algorithms to

This work is supported in part by EPSRC under grant EP/K015893/1.

M. T. Mamaghani and A. Kuhestani are with the Department of Electrical Engineering, Amirkabir University of Technology, Tehran, Iran. (e-mail: {m.tatarmamaghani, a.kuhestani}@aut.ac.ir).

K.-K. Wong is with the Department of Electronic and Electrical Engineering, University College London, London WC1E 6BT, U.K. (e-mail: kai-kit.wong@ucl.ac.uk).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2018.2848648, IEEE Transactions on Vehicular Technology

jointly optimize the pre-coding vector at the multiple antenna sources and the precoding vector at the multiple antenna MUD relaying network such that the instantaneous secrecy sum rate without friendly jammer is maximized. Then, a joint optimization of transmit covariance matrices and relay selection was proposed in [16] for a two-way MUD relaying network and in the absence of a friendly jammer. The proposed optimal algorithm in [16] is solved through the semi-definite programming combined with a line search method and thus suffers from high computational complexity. Xu *et al.* in [17] proposed a new secure transmission protocol based on constellation rotation approach in the presence of a SUD untrusted relay and without employing any jammer. Finally, optimal power allocation and secrecy sum rate analysis in the two-way untrusted relaying conducting MUD has been studied in [18]. The authors in [18] highlighted that FJ scenario improves the secrecy performance significantly compared to without employing an external jammer.

A paramount issue in many wireless communication applications is this fact that some of communication nodes may not have access to permanent power sources due to mobility. Furthermore, frequent recharging and replacement of batteries would be inconvenient in certain circumstances; e.g., in wireless body area network applications, where medical devices are required to be implanted inside patients' body. For such network, energy harvesting (EH) from ambient resources, e.g., solar and wind has been introduced as a promising approach to prolong the lifetime of energy-constrained wireless nodes [19]. However, conventional EH methods are usually uncontrollable, and thus may not satisfy the quality of service (QoS) requirement of wireless networks. To overcome this issue, a new type of EH solution called wireless information and power transfer (WIPT) was introduced in [20]. The key idea behind WIPT is to capture radio frequency (RF) signal propagated by a source node and then converting the RF signal to direct current to charge its battery, and also for signal processing or information transmission. In the area of cooperative networks, two main relaying protocols, i.e., time switching (TS) and power splitting (PS) policies have been proposed to implement the WIPT technology. In recent research, great efforts have been dedicated to the study of WIPT for non-security based [21], [22] and security based systems [23], [24]. To be specific, the authors in [23] proposed employing a wireless-powered jammer to provide secure communication between a source and a destination. Then, the authors in [23] derived a closed-form expression for the throughput, and characterized the long-term behavior of the proposed protocol. In untrusted relaying networks, Kalamkar *et al.* in [24] studied secure one-way communication in the presence of an untrusted relay based on WIPT technology, where either TS or PS is adopted at the relay.

B. Our Contributions and Key Results

In contrast to the aforementioned works, in this paper we take into account the PLS of a two-way amplify-and-forward (AF) relaying, where two sources exchange confidential messages using an untrustworthy MUD relay with the help of an external jammer to enhance the PLS. A self-reliant cooperative wireless network is proposed in which the relay and jammer as energy-starved helping devices are powered with wireless energy of RF signals. We assume that the TS receiver architecture is adopted at both the relay and jammer. The role of the relay is to harvest the energy in order to forward the received information signal to the sources, while the mission of the jammer is to utilize the harvested energy to degrade the wiretap channel of the untrusted relay. For this proposed secure transmission scheme, we derive new tight lower-bound expressions for the ergodic secrecy sum rate (ESSR) of the following three scenarios in the high signal-to-noise ratio (SNR) regime: 1) Without jamming (WoJ), where the jammer is not activated, 2) FJ, where the jamming signal is known a priori at the two sources, and 3) GNJ, where the jamming signal is unknown at the sources. We further characterize the high SNR slope and the high SNR power offset for the ESSR of the WoJ, FJ, and GNJ scenarios, to explicitly determine the impact of network parameters on the ESSR [25]. Based on our analytical results, we further highlight the impact of several system design parameters including the EH time ratio, power allocation factor, transmit SNR, nodes distance, and path loss exponent on the ESSR performance. Numerical examples show that the proposed two-way FJ provides significantly better ESSR compared with its traditional counterparts namely the one-way communication [24] and the two-way constellation rotation (CR) based communication [17], as well as our proposed WoJ and GNJ schemes. We also observe that unlike the ESSR performance of WoJ, FJ, one-way communication, and CR, the ESSR of GNJ scenario is limited to a secrecy rate ceiling in the high SNR regime. This interesting observation indicates the importance of sharing a pre-defined jamming signal between the two sources.

Our work is different from the following most related papers: While the authors in [21], considered a point-to-point communication based on the WIPT strategies via a relay, they investigated the throughput analysis. Unlike [21], we adopt the WIPT technology to develop an EH based communication network under the constraint of secure transmission. Therefore, the use of EH in [21] is fundamentally different from our work. Different from [14], [18], in this work, we consider using wireless-powered relay and jammer to help the secure communication. Different from [14], we assume that the MUD is adopted at the untrusted relay to consider the worst-case scenario in our network. It is worth noting that this is the first paper studying the GNJ scenario in untrusted relaying network. In [24], the authors studied the one-way secure transmission based on wireless EH at the untrusted relay. Different from [24], we consider the two-way untrusted MUD relaying in which two sources are able to exchange their information. Furthermore, we propose to employ an external jammer to boost the secrecy sum rate of the network. This paper is also fundamentally different from [23] where a wireless-powered jammer is utilized to facilitate the secure communication between a pair of source-destination nodes. Different from [23], in our work, extending the coverage area of transmission by using a relay is undeniable in terms of practicality inasmuch as we assume lack of direct link between

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2018.2848648, IEEE Transactions on Vehicular Technology

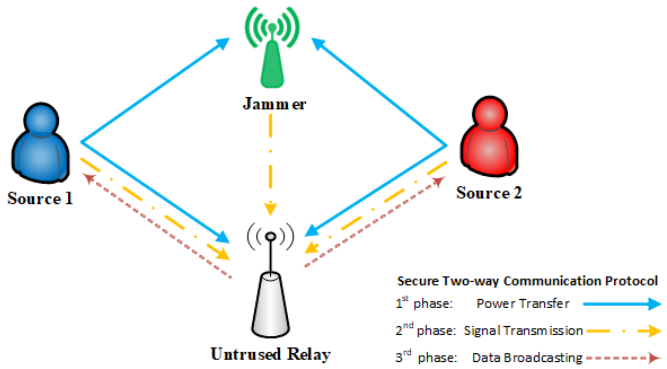


Fig. 1. System model of a wireless-powered secure two-way network using an untrusted relay and an external jammer.

the two communication nodes. In other words, in our proposed scheme a relay must be exploited to provide communication. This scenario is applicable for communication networks when two sources are located far apart or within heavily shadowed areas. Therefore, the network design and the performance analysis of our work is different from [23].

The remainder of this paper is organized as follows. System model and the proposed relaying protocols are presented in Section II, followed by signals and powers representation in Section III. Section IV and V investigate the secrecy performance of the proposed protocol and derive new closed-form expressions for the ESSR, as well as analyze the asymptotic ESSR including the high SNR slope and the high SNR power offset. Simulation results and discussions are detailed in Section VI. Finally, conclusions are given in Section VII.

II. System Model

We consider a two-way communication scenario illustrated in Fig. 1, where the two transceivers called ($\mathcal{S}_1$) and ($\mathcal{S}_2$) communicate with each other via an untrusted AF relay ($\mathcal{R}$). In the proposed system, we assume that all the nodes are equipped with a single antenna and operate in half-duplex mode, i.e., sending and receiving data concurrently is not possible. The direct link between $\mathcal{S}_1$ and $\mathcal{S}_2$ is assumed to be unavailable. As such, using the relay service is mandatory [21]. Unlike $\mathcal{S}_1$ and $\mathcal{S}_2$ that need to decode one signal, we assume that $\mathcal{R}$ adopts MUD to extract both of the sources' signals. Additionally, the channels between the nodes are assumed to be reciprocal, following a quasi-static block-fading Rayleigh model, where the channel properties remain constant over the block time of one message exchange. We denote h_{ij} as the channel coefficient between the nodes i and j, with channel reciprocity where $h_{ij} = h_{ji}$. The channel power gain $|h_{ij}|^2$ follows an exponential distribution with mean μ_{ij}. We also denote $f_{|h_{ij}|^2}(x)$ as the probability density function (PDF) of random variable (RV) $|h_{ij}|^2$. Furthermore, we assume that the sources have perfect knowledge of the channel state information (CSI) of the links $\mathcal{S}_1$–$\mathcal{R}$, $\mathcal{S}_2$–$\mathcal{R}$, and $\mathcal{J}$–$\mathcal{R}$ [14].

Three secure transmission scenarios taken into account in this paper are detailed as follows:

• *WoJ scenario*: To see how employing a jammer can impact on the secrecy performance of the proposed communication network, the WoJ scenario is studied, in which the data transmission policy is as follows. At the beginning, $\mathcal{R}$ is charged by the two sources in the first phase to facilitate the relaying. Next, $\mathcal{S}_1$ and $\mathcal{S}_2$ start to send their superimposed signals to $\mathcal{R}$ in the second phase, followed by forwarding the received data to the sources after amplification by $\mathcal{R}$ during the last phase. Finally, each source decodes the signal of the opposite node. It is worth mentioning that the WoJ brings high simplicity with very low cost compared with the FJ and GNJ scenarios.

• *FJ scenario*: In this scenario, one external jammer ($\mathcal{J}$) is employed to enhance the security of the network by degrading the relay channel capacity through sending its jamming signal. In the FJ scenario, the data exchange between two sources is implemented in three phases. In the first phase, as shown with solid lines in Fig. 1, $\mathcal{S}_1$ and $\mathcal{S}_2$ transmit non-information signals toward $\mathcal{J}$ and $\mathcal{R}$, to charge them via the RF signals. Note that both $\mathcal{R}$ and $\mathcal{J}$ are assumed to be energy-starved nodes, yet equipped with rechargeable batteries with infinite capacity. It is also assumed that most of the nodes' energy are consumed for data transmission, and energy consumption for signal processing is ignored for simplicity [21]. During the second phase, the source nodes send their information signals to $\mathcal{R}$. Simultaneously, $\mathcal{J}$ deteriorates the channel capacity of $\mathcal{R}$ by transmitting the jamming signal powered by the sources in the first stage, as demonstrated with dashed lines. Finally, $\mathcal{R}$ broadcasts the scaled version of the received signal to $\mathcal{S}_1$ and $\mathcal{S}_2$, and then each source extracts its corresponding information signal after self-interference and jamming signal cancellation, as demonstrated with dotted lines in Fig. 1. In this scenario we assume the sources have perfect knowledge of the jamming signal transmitted by $\mathcal{J}$ for they have paid for the jamming service. In other words, we assume that the jamming signal can be fully canceled at the sources but cannot be removed at the relay. This is a common assumption in the FJ literature, e.g., [14], [23], [26], and [27], where the pre-defined jamming signal can be generated by using some pseudo-random codes or some cryptographic signals that are known to both the friendly jammer and the sources but not available to the curious relay. We also note that the FJ scenario has been widely exploited in the literature for both performance analysis and network optimization design [5], [6], [14], [18], [28].

For the sake of availability of the jamming signal at the sources, we can use either 1) Cryptography-based or 2) PLS-based approaches, where the former can be practically realized similar to the methods used in the literature, e.g., [29], [30], where a large set of random sequences (jamming signals) with Gaussian distribution can be pre-stored at the friendly jammer and their indices are the keys. The friendly jammer indiscriminately selects a sequence and sends its key to the sources before the data transmission period, which can ensure the two legitimate users obtain the jamming signal before exchanging their confidential messages. Note that the key can be sent in a secret manner as the corresponding random sequence is only available at the sources (and also stored at the friendly jammer) such that any potential eavesdropper cannot

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2018.2848648, IEEE Transactions on Vehicular Technology

access the random sequence[1].

Apart from the above-mentioned cryptography-based approach, another method based on the PLS can be used[2], which adopts the CJ technique. In this scheme, the transmission of the jamming signal from $\mathcal{J}$ to $\mathcal{S}_1$ and $\mathcal{S}_2$ can be accomplished before data transmission, leading to the acquisition of the jamming signal solely by the legitimate receivers. In light of this method, $\mathcal{J}$ sends the specific jamming signal to $\mathcal{S}_1$, while simultaneously, $\mathcal{S}_2$ transmits an artificial noise to confuse the curious $\mathcal{R}$. Owning to the fact that we assume no direct link between the two sources, the wiretap channel can be adequately deteriorated by the artificial noise sent by the other source node. Accordingly, $\mathcal{R}$ fails to decode the transmitted jamming signal while $\mathcal{S}_1$ can confidentially achieve the predefined jamming signal. The same procedure can be implemented by exchanging the role of $\mathcal{S}_1$ and $\mathcal{S}_2$ to obtain the jamming signal by $\mathcal{S}_2$ as well. In addition, another method based on the destination-based CJ could also be implemented wherein before data transmission $\mathcal{J}$ sends the specific jamming signal to $\mathcal{R}$, while simultaneously, $\mathcal{S}_1$ transmits an artificial noise to confuse $\mathcal{R}$. In the next step, the relay broadcasts the amplified version of the received signal and consequently, $\mathcal{S}_1$ can extract the jamming signal. The same procedure can also be implemented by $\mathcal{S}_2$ to obtain the jamming signal. In this method, there is no need to utilize the other source for generating artificial noise and each of the sources pays their own jamming service.

Remark 1: A problem may arise here is that the friendly jammer might fail to harvest enough energy to send the jamming signal to the sources or jam the untrusted relay which could decrease the efficiency of the proposed scenario to a great extent. To consider this fact in our work, we take into account the power outage phenomenon at the energy harvesting-based nodes, i.e., the energy-limited nodes might not be activated to participate in the transmission when they are not sufficiently charged. As we shall see later, for adequately high transmit SNRs by the communication nodes during the EH phase, $\mathcal{J}$ and $\mathcal{R}$ are most likely to harvest enough energy to participate in the next phases for data transmission. However, in the low SNR regime the energy harvesting nodes go to sleep and the secure transmission is compromised. Therefore, the amount of transmit power by the sources during the EH phase plays a paramount role in the proposed FJ scenario, and hence, intelligently setting this parameter enables us to benefit from the efficiency of the FJ in the long-running transmission. Needless to say that there are also various advanced methods which can be employed to ensure that the energy harvesting and then the power transfer are most likely enabled successfully. For example, extending the number of antennas at the jammer side and/or at the sources and using the maximum ratio combining (MRC) and the maximum ratio transmission (MRT) techniques, to name but a few. Investigating such scenarios with optimal parameters is left for our future work.

[1]It should be noted that the key-assisted approach is normally exclusively used for cryptography to secure the transmission, while physical-layer methods are traditionally adopted when the shared keys are not available or too hard to implement. However, some recent works, e.g., [31], [32], have considered applying physical-layer security to enhance cryptographic secrecy, showing the potentials to have the best of both worlds of secrecy approaches.

[2]As known, the information theoretic based PLS has emerged as an alternative security paradigm to traditional cryptographic methods. While the increased complexity of cryptography effectively boosts the security level of wireless transmissions, it suffers from: 1) more processing resources for encryption and decryption and hence, increasing the imposed latency, 2) additional redundancy which leads to an increased overhead and, 3) easy to be decrypted by an eavesdropper using an exhaustive key search (also known as brute-force attack). Based on these reasons, the PLS solution relying on exploiting the physical characteristics of wireless channels is more attractive specially when the low-complexity users are energy-harvesting based nodes [2], [3].

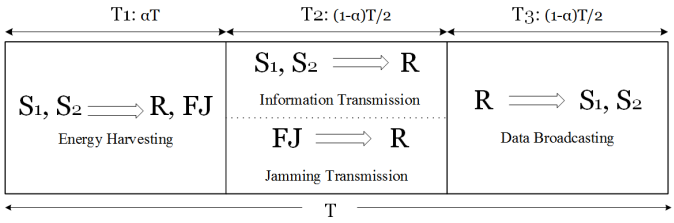


Fig. 2. Time switching relaying protocol for two-way secure communication via a wireless-powered untrusted relay and a jammer.

• *GNJ scenario*: In this scenario, the data transmission protocol is the same as the FJ. Different from the FJ, the two sources have no knowledge about the jamming signal and therefore, the jamming signal is considered as an interfering signal at $\mathcal{S}_1$ and $\mathcal{S}_2$. Based on this fact, the proposed GNJ network experiences performance loss compared with the FJ scenario. In contrast to FJ that the secrecy performance advantage is obtained at the cost of higher implementational complexity, the GNJ scenario enjoys having little workload of online computation.

A. Time Switching Relaying Protocol

Fig. 2 describes the proposed wireless EH two-way relaying transmission protocol. Using the TS policy, the relay switches from EH to information encoding, and completes a round of data exchange in three phases over a period of T. To be specific, in the first phase with the duration of $T_1 = \alpha T$ $(0 < \alpha < 1)$, both $\mathcal{R}$ and $\mathcal{J}$ harvest the energy of the RF signals transmitted by $\mathcal{S}_1$ and $\mathcal{S}_2$. In the second time slot which lasts $T_2 = (1-\alpha)\frac{T}{2}$, $\mathcal{S}_1$ and $\mathcal{S}_2$ send their information signals to $\mathcal{R}$, and simultaneously $\mathcal{J}$ transmits its jamming signal. Finally, in the third phase, $\mathcal{R}$ broadcasts the scaled version of the received signal. It is worth noting that the parameter α which indicates the ratio of EH time to the total transmission time of one period has significant impact on the system performance, i.e., related to the value of α, the secrecy rate of the proposed network is changed as will be shown numerically in Section VI.

III. Signals and Powers Representation

In the following, the signals and powers corresponding to the WoJ, FJ, and GNJ scenarios are presented. We first denote $x_{\mathcal{S}_i}$, $i \in \{1, 2\}$, and x_J as the information signals and the jamming signal with the powers of $P_{\mathcal{S}_i}$ and P_{TJ}, respectively.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2018.2848648, IEEE Transactions on Vehicular Technology

A. Energy Harvesting at the Relay and Jammer

1) Without Jamming: In the first phase, the two source nodes send non-information signals, to charge the relay. The received power at $\mathcal{R}$ is given by

$$P_{\mathcal{R}} = P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{R}}|^2 + P_{\mathcal{S}_2}|h_{\mathcal{S}_2\mathcal{R}}|^2. \quad (1)$$

Based on the proposed TS protocol, the harvested energy E_{HR} in the duration of αT at $\mathcal{R}$ is given by

$$E_{HR} = \eta\alpha T(P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{R}}|^2 + P_{\mathcal{S}_2}|h_{\mathcal{S}_2\mathcal{R}}|^2), \quad (2)$$

where η represents the energy conversion efficiency factor, and $0 < \eta < 1$. The relay uses the harvested energy obtained in the first phase (2) to retransmit the received signal in the third phase with the power P_{TR} which can be written as

$$P_{TR} = \frac{E_{HR}}{(1-\alpha)\frac{T}{2}} = \beta^{-1}(P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{R}}|^2 + P_{\mathcal{S}_2}|h_{\mathcal{S}_2\mathcal{R}}|^2), \quad (3)$$

where β is defined as $\beta \triangleq \frac{1-\alpha}{2\eta\alpha}$.

2) Friendly Jamming/Gaussian noise jamming: In the FJ and GNJ scenarios, EH at $\mathcal{R}$ is the same as the WoJ scheme. Similarly, for the received power at $\mathcal{J}$ in the first phase, can be written as

$$P_{\mathcal{J}} = P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{J}}|^2 + P_{\mathcal{S}_2}|h_{\mathcal{S}_2\mathcal{J}}|^2, \quad (4)$$

and the amount of harvested energy at $\mathcal{J}$ during one frame of communication can be represented as

$$E_{HJ} = \eta\alpha T(P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{J}}|^2 + P_{\mathcal{S}_2}|h_{\mathcal{S}_2\mathcal{J}}|^2). \quad (5)$$

Furthermore, during the second phase, $\mathcal{J}$ uses the harvested energy in (5) to transmit its jamming signal with the power of P_{TJ}, which can be expressed as

$$P_{TJ} = \frac{E_{HJ}}{(1-\alpha)\frac{T}{2}} = \beta^{-1}(P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{J}}|^2 + P_{\mathcal{S}_2}|h_{\mathcal{S}_2\mathcal{J}}|^2). \quad (6)$$

Note that in the aforementioned scenarios, $P_{\mathcal{R}}$ and $P_{\mathcal{J}}$ should be more than the minimum predefined threshold power (Θ) to activate the harvesting circuitry, unless the helper nodes will remain inactive.

B. Signals Representation

1) Without Jamming: For the WoJ scenario, the received signal at $\mathcal{R}$ in the second phase, can be expressed as

$$y_{\mathcal{R}} = \sqrt{P_{\mathcal{S}_1}}x_{\mathcal{S}_1}h_{\mathcal{S}_1\mathcal{R}} + \sqrt{P_{\mathcal{S}_2}}x_{\mathcal{S}_2}h_{\mathcal{S}_2\mathcal{R}} + n_{\mathcal{R}}, \quad (7)$$

where $n_{\mathcal{R}}$ is considered as a zero-mean additive white Gaussian noise (AWGN) at $\mathcal{R}$. Based on the received signal $y_{\mathcal{R}}$ in (7) and considering the MUD at $\mathcal{R}$, the SNR at $\mathcal{R}$ can be obtained as

$$\gamma_{\mathcal{R}} = \frac{P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{R}}|^2 + P_{\mathcal{S}_2}|h_{\mathcal{S}_2\mathcal{R}}|^2}{N_0}, \quad (8)$$

where N_0 denotes the power of AWGN at $\mathcal{R}$, and for simplicity the processing noise is ignored [24].

Finally, in the third phase, $\mathcal{R}$ broadcasts the amplified version of the received signal which is given by

$$x_{\mathcal{R}} = Gy_{\mathcal{R}}, \quad (9)$$

where G is the scaling factor of $\mathcal{R}$ as

$$G = \sqrt{\frac{P_{TR}}{P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{R}}|^2 + P_{\mathcal{S}_2}|h_{\mathcal{S}_2\mathcal{R}}|^2 + N_0}}. \quad (10)$$

Next, we focus on the received signal at $\mathcal{S}_2$, from which similar expressions can be derived for the received signal at $\mathcal{S}_1$. By using (7) and (9), the received signal at $\mathcal{S}_2$ after self-interference cancellation can be expressed as

$$y_{\mathcal{S}_2} = \sqrt{P_{\mathcal{S}_1}}Gh_{\mathcal{S}_1\mathcal{R}}h_{\mathcal{R}\mathcal{S}_2}x_{\mathcal{S}_1} + Gh_{\mathcal{R}\mathcal{S}_2}n_{\mathcal{R}} + n_{\mathcal{S}_2}. \quad (11)$$

Substituting (10) into (11), the received instantaneous end-to-end SNR at $\mathcal{S}_2$ after some algebraic manipulations can be obtained as

$$\gamma_{\mathcal{S}_2} = \frac{P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{R}}|^2|h_{\mathcal{R}\mathcal{S}_2}|^2}{N_0|h_{\mathcal{R}\mathcal{S}_2}|^2 + N_0\beta + \epsilon}, \quad (12)$$

where $\epsilon = \frac{N_0^2\beta}{P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{R}}|^2 + P_{\mathcal{S}_2}|h_{\mathcal{S}_2\mathcal{R}}|^2}$. Following the same procedure for calculation of $\gamma_{\mathcal{S}_2}$, the resultant instantaneous end-to-end SNR at $\mathcal{S}_1$ is also given by

$$\gamma_{\mathcal{S}_1} = \frac{P_{\mathcal{S}_2}|h_{\mathcal{S}_2\mathcal{R}}|^2|h_{\mathcal{R}\mathcal{S}_1}|^2}{N_0|h_{\mathcal{R}\mathcal{S}_1}|^2 + N_0\beta + \epsilon}. \quad (13)$$

2) Friendly Jamming: For the FJ scenario, the received signal at $\mathcal{R}$ in the second phase, can be expressed as

$$y_{\mathcal{R}} = \sqrt{P_{\mathcal{S}_1}}x_{\mathcal{S}_1}h_{\mathcal{S}_1\mathcal{R}} + \sqrt{P_{\mathcal{S}_2}}x_{\mathcal{S}_2}h_{\mathcal{S}_2\mathcal{R}} + \sqrt{P_{TJ}}x_{\mathcal{J}}h_{\mathcal{J}\mathcal{R}} + n_{\mathcal{R}}. \quad (14)$$

Substituting P_{TJ} given by (6) into (14), the SNR at $\mathcal{R}$ can be obtained as

$$\gamma_{\mathcal{R}} = \frac{P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{R}}|^2 + P_{\mathcal{S}_2}|h_{\mathcal{S}_2\mathcal{R}}|^2}{P_{TJ}|h_{\mathcal{J}\mathcal{R}}|^2 + N_0} = \frac{P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{R}}|^2 + P_{\mathcal{S}_2}|h_{\mathcal{S}_2\mathcal{R}}|^2}{\beta^{-1}(P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{J}}|^2 + P_{\mathcal{S}_2}|h_{\mathcal{S}_2\mathcal{J}}|^2)|h_{\mathcal{J}\mathcal{R}}|^2 + N_0}, \quad (15)$$

Finally, $\mathcal{R}$ broadcasts the amplified version of the received signal, $x_{\mathcal{R}} = Gy_{\mathcal{R}}$, with the amplification factor of

$$G = \sqrt{\frac{P_{TR}}{P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{R}}|^2 + P_{\mathcal{S}_2}|h_{\mathcal{S}_2\mathcal{R}}|^2 + P_{TJ}|h_{\mathcal{J}\mathcal{R}}|^2 + N_0}}. \quad (16)$$

Moreover, by using (14) and (16), the received signal at $\mathcal{S}_2$ can be expressed as

$$\begin{aligned} y'_{\mathcal{S}_2} &= x_{\mathcal{R}}h_{\mathcal{R}\mathcal{S}_2} + n_{\mathcal{S}_2} \\ &= \sqrt{P_{\mathcal{S}_1}}Gh_{\mathcal{S}_1\mathcal{R}}h_{\mathcal{R}\mathcal{S}_2}x_{\mathcal{S}_1} + \sqrt{P_{\mathcal{S}_2}}Gh_{\mathcal{S}_2\mathcal{R}}h_{\mathcal{R}\mathcal{S}_2}x_{\mathcal{S}_2} \\ &\quad + \sqrt{P_{TJ}}Gh_{\mathcal{J}\mathcal{R}}h_{\mathcal{R}\mathcal{S}_2}x_{\mathcal{J}} + Gh_{\mathcal{R}\mathcal{S}_2}n_{\mathcal{R}} + n_{\mathcal{S}_2}, \end{aligned} \quad (17)$$

Since the jamming signal in FJ scenario is fully known at the sources, as well as the CSI of the links $\mathcal{S}_1$–$\mathcal{R}$, $\mathcal{S}_2$–$\mathcal{R}$, and $\mathcal{R}$–$\mathcal{J}$, $\mathcal{S}_2$ can eliminate the jamming signal and its own self-interference from (17), which simplifies as

$$y_{\mathcal{S}_2} = \sqrt{P_{\mathcal{S}_1}}Gh_{\mathcal{S}_1\mathcal{R}}h_{\mathcal{R}\mathcal{S}_2}x_{\mathcal{S}_1} + Gh_{\mathcal{R}\mathcal{S}_2}n_{\mathcal{R}} + n_{\mathcal{S}_2}. \quad (18)$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2018.2848648, IEEE Transactions on Vehicular Technology

Substituting (16) into (18), and then using P_{TJ} given by (6), the received instantaneous end-to-end SNR at $\mathcal{S}_2$ is given by

$$\gamma_{\mathcal{S}_2}=\frac{P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{R}}|^2|h_{\mathcal{R}\mathcal{S}_2}|^2}{N_0|h_{\mathcal{R}\mathcal{S}_2}|^2+\frac{N_0\left(P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{J}}|^2+P_{\mathcal{S}_2}|h_{\mathcal{S}_2\mathcal{J}}|^2\right)|h_{\mathcal{J}\mathcal{R}}|^2}{P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{R}}|^2+P_{\mathcal{S}_2}|h_{\mathcal{S}_2\mathcal{R}}|^2}+N_0\beta+\epsilon}, \tag{19}$$

Similarly, the received SNR at $\mathcal{S}_1$ is obtained as

$$\gamma_{\mathcal{S}_1}=\frac{P_{\mathcal{S}_2}|h_{\mathcal{S}_2\mathcal{R}}|^2|h_{\mathcal{R}\mathcal{S}_1}|^2}{N_0|h_{\mathcal{R}\mathcal{S}_1}|^2+\frac{N_0\left(P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{J}}|^2+P_{\mathcal{S}_2}|h_{\mathcal{S}_2\mathcal{J}}|^2\right)|h_{\mathcal{J}\mathcal{R}}|^2}{P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{R}}|^2+P_{\mathcal{S}_2}|h_{\mathcal{S}_2\mathcal{R}}|^2}+N_0\beta+\epsilon}. \tag{20}$$

3) Gaussian Noise Jamming: For GNJ, the received SNR at $\mathcal{R}$ is the same as the FJ. However, in this scenario, since the jamming signal is not available at both $\mathcal{S}_1$ and $\mathcal{S}_2$, the term related to the jamming signal $x_{\mathcal{J}}$ in (17) is considered as a noise-like interference. Consequently, after self-interference cancellation, the received signal-to-interference-plus-noise ratio (SINR) at $\mathcal{S}_2$ can be computed as

$$\gamma_{\mathcal{S}_2}=\frac{P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{R}}|^2|h_{\mathcal{R}\mathcal{S}_2}|^2}{\left(P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{J}}|^2+P_{\mathcal{S}_2}|h_{\mathcal{S}_2\mathcal{J}}|^2\right)\left(\beta^{-1}|h_{\mathcal{R}\mathcal{S}_2}|^2+\delta\right)|h_{\mathcal{J}\mathcal{R}}|^2+N_0|h_{\mathcal{R}\mathcal{S}_2}|^2+N_0\beta+\epsilon}, \tag{21}$$

where $\delta \triangleq \frac{N_0}{P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{R}}|^2+P_{\mathcal{S}_2}|h_{\mathcal{S}_2\mathcal{R}}|^2}$. A similar expression can be obtained for $\gamma_{\mathcal{S}_1}$ by changing $\mathcal{S}_2$ with $\mathcal{S}_1$ in (21).

To make the further analysis tractable, we consider the high SNR assumption for all the scenarios by replacing $\epsilon = 0$ in Eqs. (12), (13) and (19)-(21).

IV. Ergodic Secrecy Sum Rate Analysis

In this section, we first derive closed-form expressions for the power outage probability at the helping nodes to take into account the fact that the EH may fail at either $\mathcal{R}$ or $\mathcal{J}$. Then, we analytically obtain new closed-form lower-bound expressions for the ESSR of WoJ, FJ, and GNJ.

We assume the helping nodes only utilize the wireless EH for data transmission. As such, the received power at either $\mathcal{R}$ or $\mathcal{J}$, should be greater than the minimum required power for the activation of their EH circuitry [19], unless they maintain inactive as we assume the helping nodes only utilize the wireless EH technology and have no other power resources. This phenomenon is characterized by the power outage probability, and denoted by P_{po}. In this section, we first derive closed-form expressions for the power outage probability at $\mathcal{R}$ ($P_{po}^{\mathcal{R}}$), and $\mathcal{J}$ ($P_{po}^{\mathcal{J}}$). As such, the probability of power outage for the helper node $\mathcal{K}$, where $\mathcal{K} \in \{\mathcal{R}, \mathcal{J}\}$ is defined precisely as

$$P_{po}^{\mathcal{K}} = \Pr\{P_{\mathcal{K}} < \Theta\}, \tag{22}$$

in which the analytical expression for $P_{po}^{\mathcal{K}}$ is obtained in Proposition 1.

Proposition 1. *The power outage probability at the helper node $\mathcal{K}$, where $\mathcal{K} \in \{\mathcal{R}, \mathcal{J}\}$ is given by*

$$P_{po}^{\mathcal{K}} = \begin{cases} 1 - \frac{\bar{\gamma}_{\mathcal{S}_2\mathcal{K}}}{\bar{\gamma}_{\mathcal{S}_2\mathcal{K}}-\bar{\gamma}_{\mathcal{S}_1\mathcal{K}}}\exp(-\frac{\Theta}{\bar{\gamma}_{\mathcal{S}_2\mathcal{K}}}) \\ \quad - \frac{\bar{\gamma}_{\mathcal{S}_1\mathcal{K}}}{\bar{\gamma}_{\mathcal{S}_1\mathcal{K}}-\bar{\gamma}_{\mathcal{S}_2\mathcal{K}}}\exp(-\frac{\Theta}{\bar{\gamma}_{\mathcal{S}_1\mathcal{K}}}), & \bar{\gamma}_{\mathcal{S}_1\mathcal{K}} \neq \bar{\gamma}_{\mathcal{S}_2\mathcal{K}} \\ \Upsilon(2, \frac{\Theta}{\bar{\gamma}_{\mathcal{S}_1\mathcal{K}}}), & \bar{\gamma}_{\mathcal{S}_1\mathcal{K}} = \bar{\gamma}_{\mathcal{S}_2\mathcal{K}} \end{cases} \tag{23}$$

where $\bar{\gamma}_{\mathcal{S}_1\mathcal{K}} \triangleq P_{\mathcal{S}_1}\mu_{\mathcal{S}_1\mathcal{K}}$, $\bar{\gamma}_{\mathcal{S}_2\mathcal{K}} \triangleq P_{\mathcal{S}_2}\mu_{\mathcal{S}_2\mathcal{K}}$, and $\Upsilon(s,x) = \int_0^x t^{(s-1)}\mathrm{e}^{-t}dt$ is the lower incomplete Gamma function [33].

Proof. See Appendix A. ∎

In principle, the ergodic secrecy rate determines the rate below which any average secure transmission is accessible [1]. Since we assume the MUD is performed at the untrusted relay to decode both the signals $x_{\mathcal{S}_1}$ and $x_{\mathcal{S}_2}$, the integrated secrecy rate of the communication network is considered as [14]. Therefore, the instantaneous secrecy sum rate R_{Sec} is evaluated by

$$R_{Sec} = \left[I_{\mathcal{S}_1} + I_{\mathcal{S}_2} - I_{\mathcal{R}}\right]^+, \tag{24}$$

where for $K \in \{\mathcal{S}_1, \mathcal{R}, \mathcal{S}_2\}$

$$I_K = \frac{(1-\alpha)}{2}\log_2(1+\gamma_K), \tag{25}$$

By combining (24) and (25), R_{Sec} can be rewritten as

$$R_{Sec} = \left[\frac{(1-\alpha)}{2}\log_2\frac{(1+\gamma_{\mathcal{S}_1})(1+\gamma_{\mathcal{S}_2})}{(1+\gamma_{\mathcal{R}})}\right]^+, \tag{26}$$

where $[x]^+ = \max(x, 0)$ and the pre-log factor $\frac{1-\alpha}{2}$ is due to the efficient time of information exchange between the two sources. Moreover, $\gamma_{\mathcal{S}_1}$, $\gamma_{\mathcal{S}_2}$, and $\gamma_{\mathcal{R}}$ are the received SNR at $\mathcal{S}_1$, $\mathcal{S}_2$, and $\mathcal{R}$, respectively. We note that by taking average over R_{Sec} given by (26), one can obtain the ESSR as

$$\bar{R}_{Sec} = \mathbb{E}\{R_{Sec}\}. \tag{27}$$

In the following, we proceed to derive the ESSR of the WoJ, FJ, and GNJ scenarios.

A. Without Jamming

In this scenario, $\mathcal{R}$ may experience power outage due to bad channel conditions. Hence, the ESSR of WoJ can be stated as

$$\bar{R}_{Sec}^{WoJ} = (1 - P_{po}^{\mathcal{R}})\bar{R}_{Act}^{WoJ}, \tag{28}$$

where the exact expression of $\bar{R}_{Act}^{WoJ}$ is obtained by substituting (8), (12), and (13) into (27) as

$$\bar{R}_{Act}^{WoJ} = \int_0^\infty\int_0^\infty R_{sec}(x,y)f_X(x)f_Y(y)dxdy, \tag{29}$$

where $X=|h_{\mathcal{S}_1\mathcal{R}}|^2$ and $Y=|h_{\mathcal{S}_2\mathcal{R}}|^2$ are defined in (29).

The corresponding lower-bound expression for $\bar{R}_{Act}^{WoJ}$ can be analytically formulated as

$$\bar{R}_{LB}^{WoJ} = \frac{1-\alpha}{2\ln(2)}\left[\widehat{I}_1 + \widehat{I}_2 - I_3\right]^+, \tag{30}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2018.2848648, IEEE Transactions on Vehicular Technology

where

$$\widehat{I}_{1(2)}=\ln\Bigg[1+\exp\Bigg(-2\Phi+\ln\Bigg(\frac{\bar{\gamma}_{\mathcal{S}_{1(2)}\mathcal{R}}\mu_{\mathcal{R}\mathcal{S}_{2(1)}}}{\beta N_0}\Bigg)+\exp\big(\frac{\beta}{\mu_{\mathcal{R}\mathcal{S}_{2(1)}}}\big)\mathrm{Ei}\big(-\frac{\beta}{\mu_{\mathcal{R}\mathcal{S}_{2(1)}}}\big)\Bigg)\Bigg], \quad (31)$$

where $\Phi\approx 0.577215$ is the Euler's constant [34], and $\mathrm{Ei}(x)=-\int_{-x}^{\infty}\frac{\exp(-t)}{t}dt$ is the exponential integral [33]. Furthermore, the term I_3 is given by

$$I_3=\frac{\bar{\gamma}_{\mathcal{S}_1\mathcal{R}}}{\bar{\gamma}_{\mathcal{S}_2\mathcal{R}}-\bar{\gamma}_{\mathcal{S}_1\mathcal{R}}}\exp\left(\frac{N_0}{\bar{\gamma}_{\mathcal{S}_1\mathcal{R}}}\right)\mathrm{Ei}\left(-\frac{N_0}{\bar{\gamma}_{\mathcal{S}_1\mathcal{R}}}\right)+\frac{\bar{\gamma}_{\mathcal{S}_2\mathcal{R}}}{\bar{\gamma}_{\mathcal{S}_1\mathcal{R}}-\bar{\gamma}_{\mathcal{S}_2\mathcal{R}}}\exp\left(\frac{N_0}{\bar{\gamma}_{\mathcal{S}_2\mathcal{R}}}\right)\mathrm{Ei}\left(-\frac{N_0}{\bar{\gamma}_{\mathcal{S}_2\mathcal{R}}}\right). \quad (32)$$

Proof. See Appendix B. ∎

B. Friendly Jamming

By considering this fact that the power outage may occur at either $\mathcal{R}$ or $\mathcal{J}$, the ESSR for FJ can be written as

$$\bar{R}_{Sec}^{FJ}=P_{po}^{\mathcal{J}}\bar{R}_{Sec}^{WoJ}+(1-P_{po}^{\mathcal{R}})(1-P_{po}^{\mathcal{J}})\bar{R}_{Act}^{FJ}. \quad (33)$$

We mention that the exact ESSR expression for FJ assuming all the nodes are active, $\bar{R}_{Act}^{FJ}$, can be written as

$$\bar{R}_{Act}^{FJ}=\int_0^{\infty}\int_0^{\infty}\int_0^{\infty}\int_0^{\infty}\int_0^{\infty}R_{sec}(x,y,z,w,u)\times f_X(x)f_Y(y)f_Z(z)f_U(u)f_W(w)dxdydzdudw, \quad (34)$$

where we define $X=|h_{\mathcal{S}_1\mathcal{R}}|^2$, $Y=|h_{\mathcal{S}_2\mathcal{R}}|^2$, $Z=|h_{\mathcal{S}_1\mathcal{J}}|^2$, $W=|h_{\mathcal{S}_2\mathcal{J}}|^2$, and $U=|h_{\mathcal{R}\mathcal{J}}|^2$ in the RVs of $\gamma_{\mathcal{R}}$, $\gamma_{\mathcal{S}_2}$, and $\gamma_{\mathcal{S}_1}$, which are respectively given by (15), (19), and (20).

Although the multiple integral expression in (34) can be evaluated numerically, a closed-form expression is not straightforward to obtain. As such, we proceed by deriving a new compact lower-bound expression for $\bar{R}_{Act}^{FJ}$ in Proposition 2.

Proposition 2. *The lower-bound expression for the ESSR of FJ scenario when both the helpers maintain active ($\bar{R}_{LB}^{FJ}$) can be expressed as*

$$\bar{R}_{LB}^{FJ}=\frac{1-\alpha}{2\ln(2)}\left[\mathcal{L}_1+\mathcal{L}_2-\mathcal{L}_3\right]^{+}, \quad (35)$$

where

$$\mathcal{L}_1\geq\ln\left(1+\frac{\exp\Big[-2\Phi+\ln\big(P_{\mathcal{S}_1}\mu_{\mathcal{S}_1\mathcal{R}}\mu_{\mathcal{S}_2\mathcal{R}}\big)\Big]}{N_0\Big[\mu_{\mathcal{R}\mathcal{S}_2}+\beta+\mu_{\mathcal{J}\mathcal{R}}\frac{P_{\mathcal{S}_1}\mu_{\mathcal{S}_1\mathcal{J}}+P_{\mathcal{S}_2}\mu_{\mathcal{S}_2\mathcal{J}}}{P_{\mathcal{S}_1}\mu_{\mathcal{S}_1\mathcal{R}}-P_{\mathcal{S}_2}\mu_{\mathcal{S}_2\mathcal{R}}}\ln\frac{P_{\mathcal{S}_1}\mu_{\mathcal{S}_1\mathcal{R}}}{P_{\mathcal{S}_2}\mu_{\mathcal{S}_2\mathcal{R}}}\Big]}\right). \quad (36)$$

$$\mathcal{L}_2\geq\ln\left(1+\frac{\exp\Big[-2\Phi+\ln\big(P_{\mathcal{S}_2}\mu_{\mathcal{S}_2\mathcal{R}}\mu_{\mathcal{S}_1\mathcal{R}}\big)\Big]}{N_0\Big[\mu_{\mathcal{R}\mathcal{S}_1}+\beta+\mu_{\mathcal{J}\mathcal{R}}\frac{P_{\mathcal{S}_1}\mu_{\mathcal{S}_1\mathcal{J}}+P_{\mathcal{S}_2}\mu_{\mathcal{S}_2\mathcal{J}}}{P_{\mathcal{S}_1}\mu_{\mathcal{S}_1\mathcal{R}}-P_{\mathcal{S}_2}\mu_{\mathcal{S}_2\mathcal{R}}}\ln\frac{P_{\mathcal{S}_1}\mu_{\mathcal{S}_1\mathcal{R}}}{P_{\mathcal{S}_2}\mu_{\mathcal{S}_2\mathcal{R}}}\Big]}\right). \quad (37)$$

and

$$\mathcal{L}_3\leq\ln\Big(1+\mathcal{A}_0\Big[\mathcal{F}(\mathcal{A}_1)-\mathcal{F}(\mathcal{A}_2)\Big]\Big), \quad (38)$$

where

$$\mathcal{A}_0=\frac{2\beta\left(P_{\mathcal{S}_1}\mu_{\mathcal{S}_1\mathcal{R}}+P_{\mathcal{S}_2}\mu_{\mathcal{S}_2\mathcal{R}}\right)}{(P_{\mathcal{S}_2}\mu_{\mathcal{S}_2\mathcal{J}}-P_{\mathcal{S}_1}\mu_{\mathcal{S}_1\mathcal{J}})\mu_{\mathcal{R}\mathcal{J}}}, \quad (39)$$

and

$$\mathcal{A}_1=\sqrt{\frac{4\beta N_0}{P_{\mathcal{S}_1}\mu_{\mathcal{S}_1\mathcal{J}}\mu_{\mathcal{R}\mathcal{J}}}}, \qquad \mathcal{A}_2=\sqrt{\frac{4\beta N_0}{P_{\mathcal{S}_2}\mu_{\mathcal{S}_2\mathcal{J}}\mu_{\mathcal{R}\mathcal{J}}}}, \quad (40)$$

and, also for $m\in\{1,2\}$

$$\mathcal{F}(\mathcal{A}_m)=-2\sum_{n=1}^{\infty}\sum_{i=1}^{n}\Lambda(1,n,i)\left(\frac{9}{2}\frac{\Gamma(n-\frac{3}{4})\Gamma(n+\frac{3}{2})}{\Gamma(n-\frac{1}{2})\Gamma(n+\frac{5}{2})}+2\right)\times\mathcal{A}_m^{i-2}\begin{cases}\Big((-1)^k\Big[\mathrm{ci}(\mathcal{A}_m)\cos(\mathcal{A}_m)+\mathrm{si}(\mathcal{A}_m)\sin(\mathcal{A}_m)\Big]\\ +\frac{1}{\mathcal{A}_m^{2k-2}}\sum_{j=1}^{k-1}(2k-2j-1)!(-\mathcal{A}_m^2)^{j-1}\Big), & i=2k\\ \Big((-1)^k\Big[\mathrm{ci}(\mathcal{A}_m)\sin(\mathcal{A}_m)-\mathrm{si}(\mathcal{A}_m)\cos(\mathcal{A}_m)\Big]\\ +\frac{1}{\mathcal{A}_m^{2k-1}}\sum_{j=1}^{k}(2k-2j)!(-\mathcal{A}_m^2)^{2j-1}\Big), & i=2k+1\end{cases} \quad (41)$$

where

$$\Lambda(1,n,i)=-\frac{(-2)^i\sqrt{\pi}\mathrm{L}(i,n)}{\sqrt{\pi}\Gamma(n+1)(4n^2-1)}, \quad (42)$$

where $\mathrm{L}(i,n)=\binom{n-1}{i-1}\frac{n!}{i!}$ *for* $n,i>0$ *represents the Lah numbers (e.g. [35]),* $\Gamma(\cdot)$ *is Gamma function. Also,* $\mathrm{ci}(x)$ *and* $\mathrm{si}(x)$ *are the Sine and Cosine integrals, i.e.,* $\mathrm{si}(x)=-\int_x^{\infty}\frac{\sin(t)}{t}\mathrm{d}t$ *and* $\mathrm{ci}(x)=-\int_x^{\infty}\frac{\cos(t)}{t}\mathrm{d}t$*, respectively.*

Proof. See Appendix C. ∎

As shown in the numerical results, the novel lower-bound expression given by (35) is significantly tight, especially in the moderate-to-high SNR regime.

C. Gaussian Noise Jamming

The ESSR of GNJ scenario can be obtained following the same procedure done for FJ scenario. We must only add the term $\beta^{-1}\big(P_{\mathcal{S}_1}\mu_{\mathcal{S}_1\mathcal{J}}+P_{\mathcal{S}_2}\mu_{\mathcal{S}_2\mathcal{J}}\big)\mu_{\mathcal{R}\mathcal{S}_i}\mu_{\mathcal{J}\mathcal{R}}$, for $i\in\{1,2\}$, to the denominator of rational functions in (36) and (37), respectively.

V. Asymptotic Ergodic Secrecy Sum Rate Analysis

In this section, we obtain the asymptotic ESSR when the transmit SNR of each node goes to infinity by deriving the high SNR slope in bits/s/Hz (S_∞) and the high SNR power offset in 3 dB units (L_∞), which are defined respectively as

$$S_\infty=\lim_{\rho\to\infty}\frac{\bar{R}_{Sec}^{\infty}}{\log_2\rho} \quad\text{and}\quad L_\infty=\lim_{\rho\to\infty}\big(\log_2\rho-\frac{\bar{R}_{Sec}^{\infty}}{S_\infty}\big), \quad (43)$$

where

$$\bar{R}_{Sec}^{\infty}=S_\infty(\log_2\rho-L_\infty), \quad (44)$$

is the general asymptotic form of the ESSR performance [25].

For the ease of presentation, we assume that $P_{\mathcal{S}_1}$ and $P_{\mathcal{S}_2}$ grow large with $P_{\mathcal{S}_1}=\xi P_{\mathcal{S}_2}$ for some fixed ratio $0<\xi<\infty$. Furthermore, we define $\rho=\frac{P_{\mathcal{S}_2}}{N_0}$ as the transmit SNR by $\mathcal{S}_2$.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2018.2848648, IEEE Transactions on Vehicular Technology

1) Without Jamming: In the high SNR regime with $\rho \to \infty$ and based on (8), (12), and (13), we conclude that $\ln(1+\gamma_{\mathcal{S}_i}) \approx \ln(\gamma_{\mathcal{S}_i})$ for $i \in \{1,2\}$, and $\ln(1+\gamma_{\mathcal{R}}) \approx \ln(\gamma_{\mathcal{R}})$. As such,

$$\begin{aligned}\mathcal{Y}_1 &\approx \mathbb{E}\{\ln(\gamma_{\mathcal{S}_1})\} = \mathbb{E}\Big\{\ln(\frac{\xi\rho XY}{X+\beta})\Big\}\\ &= \ln(\xi\rho) + \mathbb{E}\Big\{\ln(XY)\Big\} - \mathbb{E}\Big\{\ln(X+\beta)\Big\}, \quad (45)\end{aligned}$$

$$\begin{aligned}\mathcal{Y}_2 &\approx \mathbb{E}\{\ln(\gamma_{\mathcal{S}_2})\} = \mathbb{E}\Big\{\ln(\frac{\rho XY}{Y+\beta})\Big\}\\ &= \ln(\rho) + \mathbb{E}\Big\{\ln(XY)\Big\} - \mathbb{E}\Big\{\ln(Y+\beta)\Big\}, \quad (46)\end{aligned}$$

$$\begin{aligned}\mathcal{Y}_3 &\approx \mathbb{E}\{\ln(\gamma_{\mathcal{R}})\} = \mathbb{E}\Big\{\ln(\xi\rho X + \rho Y)\Big\}\\ &= \ln(\xi\rho) + \mathbb{E}\Big\{\ln(X+\frac{1}{\xi}Y)\Big\}, \quad (47)\end{aligned}$$

where the terms $\mathbb{E}\{\ln(XY)\}$, $\mathbb{E}\{\ln(X+C)\}$ and $\mathbb{E}\{\ln(X+CY)\}$ can be evaluated using the lemma mentioned below.

Lemma 1. *Let C be a strictly positive constant, and X and Y be two different exponential RVs with means of m_x and m_y, respectively. Therefore, we have the following results.*

1) $\mathbb{E}\{\ln X\} = \ln(m_x) - \Phi,$
2) $\mathbb{E}\{\ln(X+C)\} = \ln(C) - e^{\frac{C}{m_x}}\mathrm{Ei}(-\frac{C}{m_x})$
3) $\mathbb{E}\{\ln(X+CY)\} = \frac{Cm_xm_y}{m_x - Cm_y} \times \Big[\frac{\Phi+\ln(m_x)}{m_x} - \frac{\Phi+\ln(Cm_y)}{Cm_y}\Big].$

Proof. This lemma can be proved using [34, Eq. (4.331.1)] for expression 1, using [34, Eq. (4.337.1)] for expression 2, and using [34, Eq. (4.352.2)] for expression 3. ∎

Applying Lemma 1 to (45), (46), and (47), and then substituting them into (27), the closed-form expression for the asymptotic ESSR of the WoJ, can be obtained as

$$\begin{aligned}\bar{R}_{Sec}^{WoJ,\infty} &= \big(1-P_{po}^{\mathcal{R}}\big)\bar{R}_{Act}^{WoJ,\infty}\\ &= \big(1-P_{po}^{\mathcal{R}}\big)\frac{1-\alpha}{2\ln 2}\Bigg(\ln(\rho) + 2\ln\Big(\frac{m_xm_y}{\beta}\Big)\\ &- 4\Phi + e^{\frac{\beta}{m_x}}\mathrm{Ei}\Big(-\frac{\beta}{m_x}\Big) + e^{\frac{\beta}{m_y}}\mathrm{Ei}\Big(-\frac{\beta}{m_y}\Big)\\ &- \frac{m_xm_y}{\xi m_x - m_y}\Big[\frac{\Phi+\ln(m_x)}{m_x} - \frac{\xi\Phi+\xi\ln(\frac{m_y}{\xi})}{m_y}\Big]\Bigg). \quad (48)\end{aligned}$$

By substituting (48) into (43), we arrive at the high SNR slope and the high SNR power offset respectively, as

$$S_{\infty}^{WoJ} = (1-P_{po}^{\mathcal{R}})\frac{1-\alpha}{2}. \quad (49)$$

and

$$\begin{aligned}L_{\infty}^{WoJ} &= \frac{1}{\ln 2}\Bigg(4\Phi - e^{\frac{\beta}{m_x}}\mathrm{Ei}(-\frac{\beta}{m_x}) - e^{\frac{\beta}{m_y}}\mathrm{Ei}(-\frac{\beta}{m_y})\\ &+ \frac{m_xm_y}{\xi m_x - m_y}\Big[\frac{\Phi+\ln(m_x)}{m_x} - \frac{\xi\Phi+\xi\ln(\frac{m_y}{\xi})}{m_y}\Big]\Bigg)\\ &- 2\log_2(\frac{m_xm_y}{\beta}). \quad (50)\end{aligned}$$

2) Friendly Jamming: The asymptotic ESSR for the FJ scenario becomes as

$$\bar{R}_{Sec}^{FJ,\infty} = P_{po}^{\mathcal{J}}\bar{R}_{Sec}^{WoJ,\infty} + (1-P_{po}^{\mathcal{R}})(1-P_{po}^{\mathcal{J}})\bar{R}_{Act}^{FJ,\infty}, \quad (51)$$

where $\bar{R}_{Act,\infty}^{FJ}$ in (51), can be expressed as

$$\bar{R}_{Act}^{FJ,\infty} = \frac{1-\alpha}{2\ln 2}\Big[\underbrace{\mathbb{E}\Big\{\ln(\gamma_{\mathcal{S}_1})\Big\}}_{\mathcal{J}_1} + \underbrace{\mathbb{E}\Big\{\ln(\gamma_{\mathcal{S}_2})\Big\}}_{\mathcal{J}_2} - \underbrace{\mathbb{E}\Big\{\ln(\gamma_R)\Big\}}_{\mathcal{J}_3}\Big], \quad (52)$$

where using (20), (19) and (15), the terms $\mathcal{J}_1$, $\mathcal{J}_2$ and $\mathcal{J}_3$ are derived as follows:

$$\begin{aligned}\mathcal{J}_1 &= \mathbb{E}\Bigg\{\ln\Big(\frac{\rho XY}{X + \frac{\xi Z+W}{\xi X+Y}U + \beta}\Big)\Bigg\}\\ &= \mathbb{E}\Big\{\ln(\rho XY)\Big\} - \mathbb{E}\Big\{\ln\Big(X + \frac{\xi Z+W}{\xi X+Y}U + \beta\Big)\Big\}\\ &\overset{(a)}{\geq} \ln(\rho) + \mathbb{E}\Big\{\ln(XY)\Big\} - \ln\Big(\mathbb{E}\Big\{X + \frac{\xi Z+W}{\xi X+Y}U + \beta\Big\}\Big)\\ &\overset{(b)}{=} \ln(\rho) + \ln(m_xm_y) - 2\Phi\\ &- \ln\Big[\beta + m_x + \frac{\xi m_z + m_w}{\xi m_x - m_y}m_u\ln(\frac{\xi m_x}{m_y})\Big], \quad (53)\end{aligned}$$

where (a) follows from Jensen's inequality, and (b) follows from using Lemma 1. Similar to $\mathcal{J}_1$, we obtain $\mathcal{J}_2$ as

$$\begin{aligned}\mathcal{J}_2 &\geq \ln(\rho) + \ln(\xi m_xm_y) - 2\Phi\\ &- \ln\Big[\beta + m_y + \frac{\xi m_z + m_w}{\xi m_x - m_y}m_u\ln(\frac{\xi m_x}{m_y})\Big]. \quad (54)\end{aligned}$$

Ultimately, the term $\mathcal{J}_3$ is derived as

$$\begin{aligned}\mathcal{J}_3 &= \mathbb{E}\Bigg\{\ln\Big(\frac{X+\frac{1}{\xi}Y}{\frac{1}{\beta}(Z+\frac{1}{\xi}W)U+\epsilon}\Big)\Bigg\}\\ &\overset{(a)}{\approx} \mathbb{E}\Big\{\ln(X+\frac{1}{\xi}Y)\Big\} - \mathbb{E}\Big\{\ln(Z+\frac{1}{\xi}W)\Big\}\\ &- \mathbb{E}\Big\{\ln(U)\Big\} + \ln\beta\\ &\overset{(b)}{=} \frac{\frac{1}{\xi}m_xm_y}{m_x - \frac{1}{\xi}m_y}\Big[\frac{\Phi+\ln(m_x)}{m_x} - \frac{\Phi+\ln(\frac{m_y}{\xi})}{\frac{1}{\xi}m_y}\Big]\\ &- \frac{\frac{1}{\xi}m_zm_w}{m_x - \frac{1}{\xi}m_w}\Big[\frac{\Phi+\ln(m_z)}{m_z} - \frac{\Phi+\ln(\frac{m_w}{\xi})}{\frac{1}{\xi}m_w}\Big]\\ &+ \ln\big(\frac{\beta}{m_u}\big) + \Phi, \quad (55)\end{aligned}$$

where (a) follows from setting $\epsilon = 0$; this means that the untrusted relay is considered as an ideal eavesdropper with the capability of noise cancellation such that from a security

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2018.2848648, IEEE Transactions on Vehicular Technology

perspective this corresponds to the maximum interception by the eavesdropper and is the worst case assumption [36]. Furthermore, (b) follows from Lemma 1. Consequently, substituting (53)-(55) into (52), and then using (51) and (43), the high SNR slope for the FJ, is given by

$$S_{\infty}^{FJ} = P_{po}^{\mathcal{J}} S_{\infty}^{WoJ} + (1 - P_{po}^{\mathcal{R}})(1 - P_{po}^{\mathcal{J}}) S_{\infty}^{FJ,Act}, \quad (56)$$

where by plugging (52) into (43), the expression $S_{\infty}^{FJ,Act}$ can be expressed as

$$S_{\infty}^{FJ,Act} = (1 - \alpha). \quad (57)$$

Ultimately, substituting (57) into (56), and then after simple manipulations results in

$$S_{\infty}^{FJ} = (1 - P_{po}^{\mathcal{R}})(1 - \frac{P_{po}^{\mathcal{J}}}{2})(1 - \alpha). \quad (58)$$

Finally, for the calculation of the high SNR power offset for the FJ, plugging (51) into (43) results in

$$L_{\infty}^{FJ} = \lim_{\rho \to \infty} \left(\log_2 \rho - \left[\frac{P_{po}^{\mathcal{J}} \bar{R}_{Act}^{WoJ,\infty} + (1 - P_{po}^{\mathcal{J}}) \bar{R}_{Act}^{FJ,\infty}}{(1 - \frac{P_{po}^{\mathcal{J}}}{2})(1 - \alpha)} \right] \right). \quad (59)$$

Now, we consider two special cases 1) jammer is always active, i.e., $P_{po}^{\mathcal{J}} = 0$, which is an ideal case maximizing L_{∞}^{FJ}, 2) Jammer is off, $P_{po}^{\mathcal{J}} = 1$, which is also an artificial case but minimizing L_{∞}^{FJ}. we delve into such computations to acquire a deep engineering insight to these criteria. To this end, if $P_{po}^{\mathcal{J}} = 0$, then

$$\begin{aligned} L_{\infty}^{FJ,Act} = \frac{1}{2\ln 2} \Bigg(& \ln \frac{\beta}{\xi m_x^2 m_y^2 m_u} + 5\Phi \\ & + \ln \left[\beta + m_x + \frac{\xi m_z + m_w}{\xi m_x - m_y} m_u \ln(\frac{\xi m_x}{m_y}) \right] \\ & + \ln \left[\beta + m_y + \frac{\xi m_z + m_w}{\xi m_x - m_y} m_u \ln(\frac{\xi m_x}{m_y}) \right] \\ & + \frac{\frac{1}{\xi} m_x m_y}{m_x - \frac{1}{\xi} m_y} \left[\frac{\Phi + \ln(m_x)}{m_x} - \frac{\Phi + \ln(\frac{m_y}{\xi})}{\frac{1}{\xi} m_y} \right] \\ & - \frac{\frac{1}{\xi} m_z m_w}{m_z - \frac{1}{\xi} m_w} \left[\frac{\Phi + \ln(m_z)}{m_z} - \frac{\Phi + \ln(\frac{m_w}{\xi})}{\frac{1}{\xi} m_w} \right] \Bigg), \end{aligned} \quad (60)$$

and if $P_{po}^{\mathcal{J}} = 1$, which also means that there is no jammer in the scenario, accordingly, $L_{\infty}^{FJ,min}$ is equal to L_{∞}^{WoJ} as (50).

Remark 2: By comparing (49) and (58), we can obtain $\frac{S_{\infty}^{FJ}}{S_{\infty}^{WoJ}} = 2(1 - \frac{P_{po}^{\mathcal{J}}}{2})$. This result expresses that the FJ scenario can achieve more high SNR slope compared to the WoJ when a jammer with low threshold to activate the EH circuitry is exploited. Specifically, when $\mathcal{J}$ is always active, FJ achieves twice as the high SNR slope as WoJ. Furthermore, based on (58) which precisely specifies that the power outage at the external jammer has less impact to the high SNR slope rate compared to the power outage at the relay, therefore we can elicit this fact that the jammer's EH component structure can be relatively simple than the relay's.

3) Gaussian Noise Jamming: In this scenario, the asymptotic ESSR can be obtained as (51), but by replacing both the expressions $\mathcal{J}_1$ and $\mathcal{J}_2$ indicated in (52) with the expressions respectively, given by

$$\begin{aligned} \tilde{\mathcal{J}}_1 \geq & \ln(\rho) + \ln(m_x m_y) - 2\Phi \\ & - \ln \Bigg[\beta + m_x + m_u(\xi m_z + m_w) \\ & \left(\frac{\rho m_x}{\beta} + \frac{\ln(\xi m_x) - \ln(m_y)}{\xi m_x - m_y} \right) \Bigg], \end{aligned} \quad (61)$$

and

$$\begin{aligned} \tilde{\mathcal{J}}_2 \geq & \ln(\rho) + \ln(\xi m_x m_y) - 2\Phi \\ & - \ln \Bigg[\beta + m_y + m_u(\xi m_z + m_w) \\ & \left(\frac{\rho m_y}{\beta} + \frac{\ln(\xi m_x) - \ln(m_y)}{\xi m_x - m_y} \right) \Bigg]. \end{aligned} \quad (62)$$

The alternative term for $\bar{R}_{Act,\infty}^{FJ}$ in (51) is given by

$$\bar{R}_{Act}^{GNJ,\infty} = \frac{1 - \alpha}{2 \ln 2} \left[\ln \left(\frac{\beta^2}{m_x m_y} \right) - \mathcal{J}_3 \right]. \quad (63)$$

Following the similar approach to the FJ in regards of the asymptotic ESSR, the high SNR slope for GNJ can be expressed as

$$S_{\infty}^{GNJ} = P_{po}^{\mathcal{J}} S_{\infty}^{WoJ} + (1 - P_{po}^{\mathcal{R}})(1 - P_{po}^{\mathcal{J}}) S_{\infty}^{GNJ,Act}, \quad (64)$$

in which the term $S_{\infty}^{GNJ,Act}$, can be obtained as

$$S_{\infty}^{GNJ,Act} = \lim_{\rho \to \infty} \frac{1 - \alpha}{2 \ln 2} \left[\frac{2 \ln \rho - \ln(\frac{\rho^2 m_x m_y}{\beta^2})}{\log_2 \rho} \right] \overset{(a)}{=} 0, \quad (65)$$

where (a) follows from applying L'Hospital's rule to evaluate the limit in the above expression. Finally, substituting (49) and (65) into (64) results in

$$S_{\infty}^{GNJ} = P_{po}^{\mathcal{J}}(1 - P_{po}^{\mathcal{R}}) \frac{1 - \alpha}{2}. \quad (66)$$

At this point, we shift our focus to derive the high SNR power offset for the GNJ. Accordingly, by using (66) and (43), we express L_{∞}^{GNJ} as

$$L_{\infty}^{GNJ} = \lim_{\rho \to \infty} \left[\log_2 \rho - \left(\frac{P_{po}^{\mathcal{J}} \bar{R}_{Act}^{WoJ,\infty} + (1 - P_{po}^{\mathcal{J}}) \bar{R}_{Act}^{GNJ,\infty}}{P_{po}^{\mathcal{J}}(1 - \frac{P_{po}^{\mathcal{J}}}{2})(\frac{1 - \alpha}{2})} \right) \right]. \quad (67)$$

By substituting (48) and (63) into (67), and after tedious manipulations, we can obtain that $L_{\infty}^{GNJ} = \infty$, which can also be concluded intuitively based on the result in (65).

VI. Numerical Results and Discussions

In this section, we provide some numerical examples to verify the accuracy of the provided expressions. Furthermore, we reveal the impact of different system parameters on the ESSR. Two competitive counterparts, the one-way communication [24] and the two-way CR aided approach [17] are used as benchmarks to highlight the secrecy performance of the proposed FJ. In the simulations, unless otherwise stated, we set the system parameters as given in Table I.

A. Transmit SNR

Fig. 3 plots the ESSR versus transmit SNR for WoJ, FJ, GNJ, and the one-way communication, as well as the CR

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2018.2848648, IEEE Transactions on Vehicular Technology

TABLE I
SYSTEM PARAMETERS

Parameter	Value	Unit	Description
$P_{\mathcal{S}_1}$	10	dBW	transmit power by $\mathcal{S}_1$
$P_{\mathcal{S}_2}$	10	dBW	transmit power by $\mathcal{S}_2$
η	0.7	-	energy conversion efficiency factor
Θ	0	dBm	minimum EH circuitry threshold
N_0	-10	dBm	noise power
$d_{\mathcal{S}_1\mathcal{R}}$	d=3	m	$\mathcal{S}_1 \leftrightarrow \mathcal{R}$ distance
$d_{\mathcal{S}_2\mathcal{R}}$	d=3	m	$\mathcal{S}_2 \leftrightarrow \mathcal{R}$ distance
d_{S_1J}	d=3	m	$\mathcal{S}_1 \leftrightarrow \mathcal{J}$ distance
d_{S_2J}	d=3	m	$\mathcal{S}_2 \leftrightarrow \mathcal{R}$ distance
d_{RJ}	d=3	m	$\mathcal{R} \leftrightarrow \mathcal{J}$ distance
κ	2.7	-	path loss exponent
μ_{ij}	$d_{ij}^{-\kappa}$	-	mean channel power gain

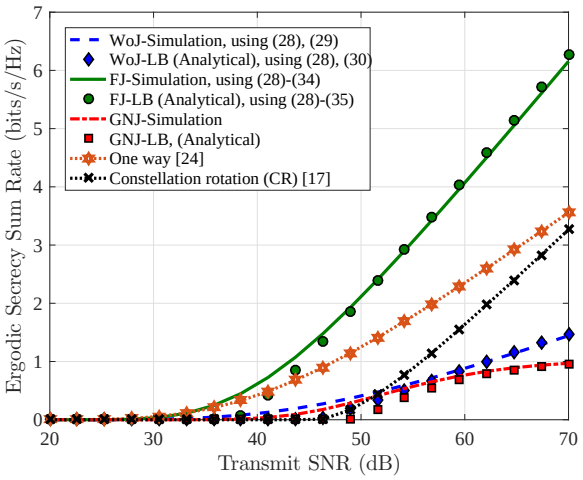


Fig. 3. ESSR versus transmit SNR for the proposed two-way WoJ, FJ, GNJ, and the one-way communication, as well as the CR approach.

scheme. From Fig. 3, we observe that the exact numerical expressions for the ESSR of WoJ, given by (28), (29), and for the ESSR of FJ, given by (33), (34) are well-approximated in the high SNR regime by the closed-form lower-bound expressions in (28), (35) and (33), (35), respectively. As can be seen from Fig. 3, only the ESSR of GNJ is limited a secrecy rate ceiling when the transmit SNR goes beyond a specific threshold, i.e., as predicted before and we observe from Fig. 3. Particularly, the high SNR slop rate for the GNJ scheme is near to zero. That is caused by the fact that although increasing the transmit SNR degrades the received SINR at the relay by augmenting the jamming signal, it also has a detrimental impact on the received SINR at the sources as they can not eliminate the unknown jamming signal. These two contradictory results bring up a saturation region as can be seen from Fig. 3. We can also find from Fig. 3 that in the high SNR regime, the proposed two-way FJ substantially outperforms all of its competent counterparts, e.g., in SNR = 50 dB, the ESSR of FJ provides approximately 1 bit/s/Hz more than the one-way transmission scenario even under the assumption of SUD relaying, and is more than twice as much

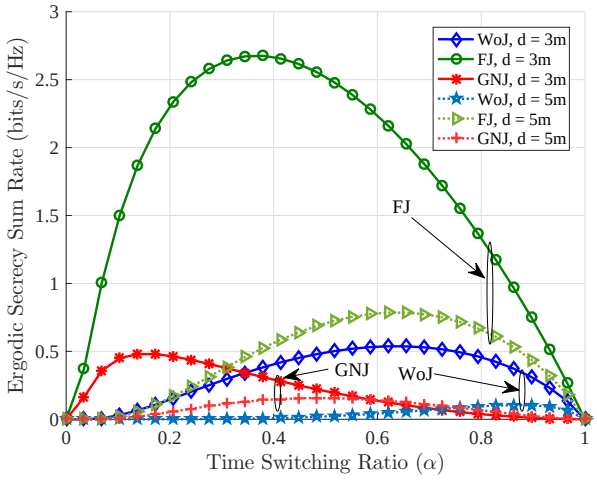


Fig. 4. ESSR versus TS ratio for WoJ, FJ, and GNJ.

the other two-way benchmarks are. Evidently, from Fig. 3, the high SNR slope of the curve corresponding to the proposed two-way FJ is twice as much as the slope of the WoJ scenario as we pointed out this result via the mathematical analysis in Remark 2. The last but not least point we need to mention here is that the conventional one-way communication and the CR approaches achieve higher secrecy data rate comparing with WoJ and GNJ in middle-to-high range of SNR, i.e., above SNR = 50 dB, as can be seen from Fig. 3. This observation once again corroborates the idea that how our proposed FJ can dramatically boost the secrecy performance of the system.

B. Time Switching Ratio (α)

Fig. 4 shows that the ESSR is a quasi-concave function with respect to the TS ratio. For the given system parameters, the maximum ESSR are obtained at the optimum points $\alpha_{opt}^{WoJ} = 0.63$, $\alpha_{opt}^{FJ} = 0.36$, and $\alpha_{opt}^{GNJ} = 0.14$. This finding reveals the importance of TS ratio which should be taken into account in the system design. This observation says that the secrecy performance of the network is highly dependent on both the jamming strategies (WoJ, FJ, or GNJ) and the TS ratio. If the TS ratio is too low, the harvested energy at the relay (and the jammer) may be too low and then, power outage may occur or the received SNR at the sources may be too low. On the other hand, if the TS ratio is too high, insufficient time is dedicated for the relay to broadcast the information signal and hence, the received instantaneous SNR at the receivers may be too low. As a consequence, the reliable communication is influenced. As such, there is a trade-off between a secure transmission and a reliable communication. We consider this issue in our future works. Furthermore, Fig. 4 depicts the impact of distance between the network nodes on the ESSR performance. We assume that all the nodes, except the two sources, are located in equal distances from each other denoted by d. One interesting result from Fig. 4 is that the nodes distance and TS ratio are two proportional parameters subject to the maximum achievable ESSR, i.e., extending the network scale to $d = 5$m, the maximum ESSR

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2018.2848648, IEEE Transactions on Vehicular Technology

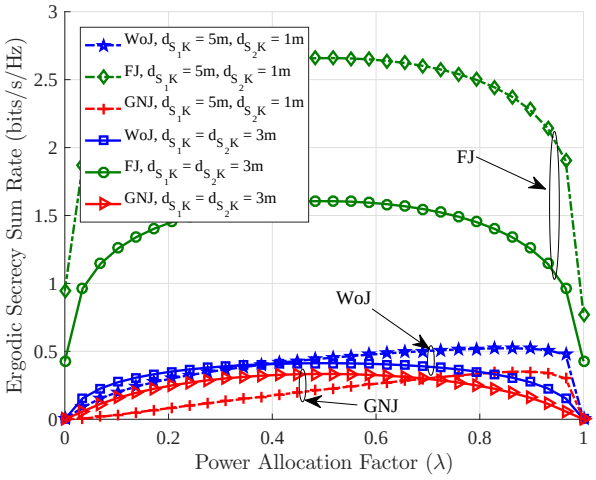


Fig. 5. ESSR versus power allocation factor for the WoJ, FJ, and GNJ scenarios with respect to the distance of the untrusted relay to the sources. We set $d_{\mathcal{S}_1\mathcal{K}} = 3,5m$, $d_{\mathcal{S}_2\mathcal{K}} = 3,1m$, and $d_{\mathcal{J}\mathcal{R}} = 1.5m$. Also, $\mathcal{K}$ represents either $\mathcal{R}$ or $\mathcal{J}$.

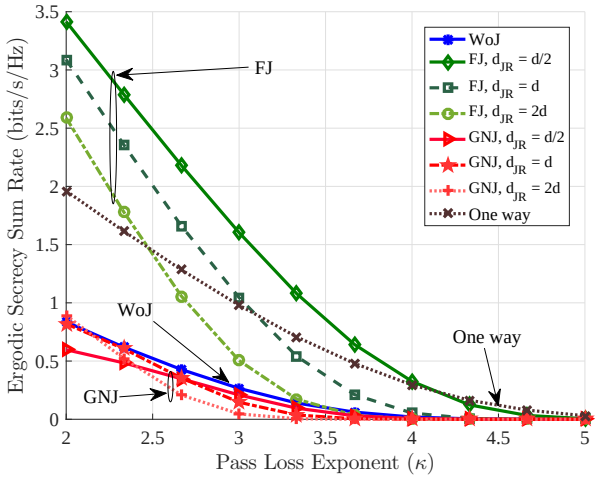


Fig. 6. ESSR versus the environmental path loss exponent (κ).

for all the scenarios is achievable if more time is dedicated to EH than data relaying. This result is reasonable owning to the fact that by extending the network scale, the path loss phenomenon reduces the received SNR at the relay and the jammer. Therefore, more time should be allocated for EH.

C. Power Allocation Factor (λ)

We provide Fig. 5 to observe the impact of power allocation factor and the relay position with respect to the communication nodes on the achievable ESSR of the two-way WoJ, FJ, GNJ scenarios. Let define the power allocation factor λ $(0 < \lambda < 1)$ such that $P_{\mathcal{S}_1} = \lambda P$ and $P_{\mathcal{S}_2} = (1-\lambda)P$. We can observe from Fig. 5 that for all of the transmission scenarios except the FJ, when the helper nodes are close to either of the communication sources, little amount of the power budget should be allocated to that node to maximize the ESSR. For FJ, regardless of sources distance to the helpers, approximately equal power allocation, i.e., $\lambda \approx 0.5$ is required to maximize the ESSR as can be seen from Fig. 5. It should be pointed out that for the two-way FJ scenario, due to the symmetry of the legitimate nodes' placement, the more closer the source to the untrusted relay should transmit with the less power to provide the higher ESSR. Interestingly, we find that the ESSR performance provided by the GNJ pales in comparison to the WoJ for any power distribution. This observation indicates employing a jammer with unknown jamming signal at the sources, adversely impact on the communication secrecy.

D. Path Loss Exponent (κ)

We plot Fig. 6 to illustrate the impact of path loss exponent on the secrecy rate with different $\mathcal{J}$-to-$\mathcal{R}$ distances. When the environmental path loss increases, all the relaying scenarios incontrovertibly suffer from a decline in the ESSR. However, our proposed two-way FJ significantly outperforms the WoJ, GNJ, and one-way communication scenarios. Although, as $\mathcal{J}$'s distance to $\mathcal{R}$ increases, the ESSR of FJ decreases, we can see that the FJ still presents significantly better ESSR in contrast to the WoJ and GNJ scenarios either in urban (small κ) or in suburban (large κ) areas. Furthermore, from another point of view we can draw a conclusion from Fig. 6 that by intelligently choosing the optimal jammer from a group of jammers, e.g., a jammer with low $\mathcal{J}$-to-$\mathcal{R}$ distance, the proposed FJ scenario can clearly achieve higher secrecy rate compared to the one-way communication. In addition, we interestingly find that the WoJ scenario outperforms the GNJ. This new result highlights that employing an external jammer with unknown jamming signal brings almost no improvement in terms of the secrecy performance.

VII. Conclusions

We proposed a wireless-powered two-way cooperative network wherein the two sources communicate via a wireless-powered untrusted relay. To enhance the secrecy performance, we employed an external jammer which is also wirelessly charged by the two sources. By adopting the time switching (TS) protocol at the untrusted relay and jammer, we investigated the ergodic secrecy sum rate (ESSR) criterion for the without jamming (WoJ), friendly jamming (FJ), and Gaussian noise jamming (GNJ) scenarios. New tight lower-bound expressions were derived for the ESSR and the asymptotic ESSR analysis to obtain the high SNR slope and the high SNR power offset for the jamming-based scenarios were also presented. Numerical examples revealed the priority of the proposed two-way FJ compared with the WoJ, GNJ, traditional one-way communication and constellation rotation (CR) aided approaches. Furthermore, several engineering insights were presented regarding the impact of different system parameters such as the TS ratio, power allocation factor, path loss exponent, and nodes distance on the ESSR performance. Our results in this paper gathered new insights to design the high rate energy harvesting based networks for D2D communications as a part of the 5th generation wireless communication networks.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2018.2848648, IEEE Transactions on Vehicular Technology

APPENDIX A

For the wirelessly powered nodes, $\mathcal{R}$ and $\mathcal{J}$, the power outage probability can be written as

$$P_{po}^{\mathcal{K}} = \Pr\{P_{\mathcal{K}} < \Theta\}, \tag{68}$$

where substituting (1) or (4) into (22), one can rewrite (68) as

$$P_{po}^{\mathcal{K}} = \Pr\{P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{K}}|^2 + P_{\mathcal{S}_2}|h_{\mathcal{S}_2\mathcal{K}}|^2 < \Theta\}. \tag{69}$$

To evaluate $P_{po}^{\mathcal{K}}$, we first present the following useful lemma.

Lemma 2. *Let $S = X + Y$ be a new RV such that X and Y are two exponential RVs with scale parameters m_x and m_y, respectively. The PDF and the cumulative distribution function (CDF) of S are as follows*

$$f_S(s) = \begin{cases} -\frac{\mathrm{e}^{\frac{s}{m_x}} - \mathrm{e}^{\frac{s}{m_y}}}{m_x - m_y}\mathrm{e}^{-\frac{s(m_x+m_y)}{m_x m_y}}, & m_x \neq m_y \\ \frac{s}{m^2}\mathrm{e}^{-\frac{s}{m}}, & m_x = m_y \end{cases} \tag{70}$$

and

$$F_S(s) = \begin{cases} 1 - \frac{m_x}{m_x - m_y}\mathrm{e}^{(-\frac{s}{m_x})} - \frac{m_y}{m_y - m_x}\mathrm{e}^{-\frac{s}{m_y}}, & m_x \neq m_y \\ \Upsilon(2, \frac{s}{m_x}), & m_x = m_y \end{cases} \tag{71}$$

where $\Upsilon(s, x) = \int_0^x t^{(s-1)}\mathrm{e}^{-t}dt$ is the lower incomplete Gamma function [33]. Note that both (70) *and* (71) *are subjected to the condition $s > 0$.*

Proof. We commence from evaluating the PDF of S as

$$\begin{aligned} f_S(s) &= \int f_{XY}(x, s-x)dx \\ &\overset{(a)}{=} \int f_X(x) f_Y(s-x)dx \\ &= \frac{1}{m_x m_y} e^{-\frac{s}{m_y}} \int_0^s e^{(\frac{1}{m_y} - \frac{1}{m_x})x} dx, \end{aligned} \tag{72}$$

where (a) follows from the fact that two RVs X and Y are independent. Finally, evaluating the integral in (72) yields the expression as in (70), and using the fact that $F_S(s) = \int_0^s f_S(x)\mathrm{dx}$, (71) is also obtained. ∎

Using Lemma 2 and considering $X = P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{K}}|^2$ and $Y = P_{\mathcal{S}_2}|h_{\mathcal{S}_2\mathcal{K}}|^2$ (which are two exponential RVs with means equal to m_x and m_y, respectively) we arrive at $P_{po}^{\mathcal{K}}$ in (23) as we know $\Pr\{X + Y < \Theta_{\mathcal{K}}\} = F_S(\Theta_{\mathcal{K}})$.

APPENDIX B

In the following, we proceed to evaluate the terms I_1, I_2 and I_3, respectively. We commence from I_1 as follows

$$\begin{aligned} I_1 &= \mathbb{E}\left\{\ln(1 + \gamma_{\mathcal{S}_2})\right\} = \mathbb{E}\left\{\ln(1 + \frac{RS}{S+1})\right\} \\ &\overset{(a)}{\geq} \ln\left(1 + \exp\left(\mathbb{E}\left\{\ln\left(\frac{RS}{S+1}\right)\right\}\right)\right) \\ &= \ln\left(1 + \exp\left(\overbrace{\mathbb{E}\left\{\ln\left[RS\right]\right\}}^{\varphi_1} - \overbrace{\mathbb{E}\left\{\ln\left[S+1\right]\right\}}^{\varphi_2}\right)\right) \\ &\triangleq \widehat{I}_1, \end{aligned} \tag{73}$$

where $R = \frac{P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{R}}|^2}{N_0}$ and $S = \frac{2\eta\alpha|h_{RS_2}|^2}{1-\alpha}$. Furthermore, (a) follows from the fact that $\ln\left(1+\exp(x)\right)$ is a convex function of x, since its second derivative is $\frac{1}{(1+\exp(x))^2} > 0$, hence, we can apply Jensen's inequality. It is worth pointing out that the results in [37] express that this lower-bound is sufficiently tight. Using [34, Eq. (4.352.1)] and [34, Eq. (4.331.2)], φ_1 and φ_2 can be calculated, respectively as

$$\varphi_1 = -2\Phi + \ln\left(m_R m_S\right), \tag{74}$$

and

$$\varphi_2 = -\exp(\frac{1}{m_S})\mathrm{Ei}\left(-\frac{1}{m_S}\right). \tag{75}$$

Note that the averages of R and S are equal to $m_R = \frac{P_{\mathcal{S}_1}\mu_{\mathcal{S}_1\mathcal{R}}}{N_0}$ and $m_S = \frac{2\eta\alpha\mu_{RS_2}}{1-\alpha}$, respectively. The term $\widehat{I}_2$ is obtained similar to (73) by replacing $m_R = \frac{P_{\mathcal{S}_2}\mu_{\mathcal{S}_2\mathcal{R}}}{N_0}$ and $m_S = \frac{2\eta\alpha\mu_{RS_1}}{1-\alpha}$.

Now, attention is shifted to calculate I_3 as follows

$$\begin{aligned} I_3 &= \mathbb{E}\left\{\ln\left(1 + \gamma_R\right)\right\} \\ &= \int_0^\infty \ln(1+\xi) f_{\gamma_{\mathcal{R}}}(\xi)\, d\xi \\ &\overset{(a)}{=} \frac{m_x}{m_y - m_x}\exp\left(\frac{1}{m_x}\right)\mathrm{Ei}\left(-\frac{1}{m_x}\right) \\ &\quad + \frac{m_y}{m_x - m_y}\exp\left(\frac{1}{m_y}\right)\mathrm{Ei}\left(-\frac{1}{m_y}\right), \end{aligned} \tag{76}$$

where $m_x = \frac{P_{\mathcal{S}_1}\mu_{\mathcal{S}_1\mathcal{R}}}{N_0}$ and $m_y = \frac{P_{\mathcal{S}_2}\mu_{\mathcal{S}_2\mathcal{R}}}{N_0}$, and (a) follows from substituting the PDF of γ_R given by (70) and using [34, Eq. (4.352.1)].

APPENDIX C

The lower-bound expression for the ESSR of FJ scenario when all the nodes are active ($\bar{R}_{LB}^{FJ}$) can be obtained as follows

$$\begin{aligned} \bar{R}_{Act}^{FJ} &= \mathbb{E}\left\{\frac{(1-\alpha)}{2}\left[\log_2\frac{(1+\gamma_{\mathcal{S}_2})(1+\gamma_{\mathcal{S}_1})}{(1+\gamma_{\mathcal{R}})}\right]^+\right\} \\ &\overset{(a)}{\geq} \Bigg[\frac{1-\alpha}{2\ln(2)}\Bigg(\underbrace{\mathbb{E}\left\{\ln\left(1+\gamma_{\mathcal{S}_2}\right)\right\}}_{\mathcal{L}_1} + \underbrace{\mathbb{E}\left\{\ln\left(1+\gamma_{\mathcal{S}_1}\right)\right\}}_{\mathcal{L}_2} \\ &\quad - \underbrace{\mathbb{E}\left\{\ln\left(1+\gamma_{\mathcal{R}}\right)\right\}}_{\mathcal{L}_3}\Bigg)\Bigg]^+ \triangleq \bar{R}_{LB}^{FJ}, \end{aligned} \tag{77}$$

where inequality (a) follows from the fact that $\mathbb{E}\{\max(X, Y)\} \geq \max(\mathbb{E}\{X\}, \mathbb{E}\{Y\})$ [33]. Moreover, for calculating the part $\mathcal{L}_1$, we first present the following lemma.

Lemma 3. *Let $Z = \frac{M}{N}$ be an arbitrary RV. According to these facts that 1) $\ln(1+x) = \ln(1+\exp(\ln(x)))$, and 2) $\ln(1+\exp(\ln(x)))$ is a convex function with respect to $\ln(x)$, and then applying Jensen's inequality, we can find a tight lower-bound as follows:*

$$\mathbb{E}\Big\{\ln(1+Z)\Big\} \geq \ln\Big(1 + \exp\Big[\mathbb{E}\big\{\ln M\big\} - \mathbb{E}\big\{\ln N\big\}\Big]\Big), \tag{78}$$

Now, by defining $\gamma_{\mathcal{S}_2} \triangleq \frac{M}{N}$ in which M and N represent the numerator and denominator of $\gamma_{\mathcal{S}_2}$, respectively, and then

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2018.2848648, IEEE Transactions on Vehicular Technology

applying Lemma 3, we can write

$$\mathbb{E}\Big\{\ln(1+\gamma_{\mathcal{S}_2})\Big\}\geq\ln\left(1+\exp\Big[\mathbb{E}\{\ln M\}+\mathbb{E}\{\ln\frac{1}{N}\}\Big]\right)\overset{(a)}{\geq}\ln\left(1+\exp\Big[\underbrace{\mathbb{E}\{\ln M\}}_{\mathcal{K}_1}\Big]\times\underbrace{\frac{1}{\mathbb{E}\{N\}}}_{\mathcal{K}_2}\right),\quad(79)$$

where inequality (a) follows from the facts that 1) both the functions $\ln(\cdot)$ and $\exp(\cdot)$ are monotone functions 2) the function $\ln(\frac{1}{x})$ is convex for $x>0$, Therefore, applying Jensen's inequality results in $\mathbb{E}\{\ln\frac{1}{N}\}\geq\ln(\frac{1}{\mathbb{E}\{N\}})$. To obtain $\mathcal{K}_1$, we can further write as

$$\mathcal{K}_1=\mathbb{E}\Big\{\ln\left(P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{R}}|^2|h_{\mathcal{S}_2\mathcal{R}}|^2\right)\Big\}=-2\Phi-\ln\left(\frac{1}{\bar{\gamma}_{\mathcal{S}_1\mathcal{R}}\mu_{\mathcal{S}_2\mathcal{R}}}\right),\quad(80)$$

where (80) follows from Lemma 1. Furthermore, the term $\mathcal{K}_2$ is obtained as

$$\mathcal{K}_2=\mathbb{E}\left\{N_0\Big(|h_{\mathcal{R}\mathcal{S}_2}|^2+\frac{\left(P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{J}}|^2+P_{\mathcal{S}_2}|h_{\mathcal{S}_2\mathcal{J}}|^2\right)|h_{\mathcal{J}\mathcal{R}}|^2}{P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{R}}|^2+P_{\mathcal{S}_2}|h_{\mathcal{S}_2\mathcal{R}}|^2}+\beta\Big)\right\}\overset{(a)}{=}N_0\left[\mu_{\mathcal{R}\mathcal{S}_2}+\beta+\mu_{\mathcal{J}\mathcal{R}}\frac{\bar{\gamma}_{\mathcal{S}_1\mathcal{J}}+\bar{\gamma}_{\mathcal{S}_2\mathcal{J}}}{\bar{\gamma}_{\mathcal{S}_1\mathcal{R}}-\bar{\gamma}_{\mathcal{S}_2\mathcal{R}}}\ln\frac{\bar{\gamma}_{\mathcal{S}_1\mathcal{R}}}{\bar{\gamma}_{\mathcal{S}_2\mathcal{R}}}\right],\quad(81)$$

where (a) follows from the independency of RVs, and using the lemma below.

Lemma 4. *For two exponential RVs X and Y with the rate parameters λ_x and λ_y, respectively, the new RV $Z=\frac{1}{X+Y}$ with $\lambda_x\neq\lambda_y$ has the following distribution properties*

$$f_Z(z)=\frac{\lambda_x\lambda_y}{z^2(\lambda_x-\lambda_y)}\left(-\mathrm{e}^{-\frac{\lambda_x}{z}}+\mathrm{e}^{-\frac{\lambda_y}{z}}\right),\quad(82)$$

$$F_Z(z)=\frac{1}{\lambda_x-\lambda_y}\left(\lambda_x\,\mathrm{e}^{\frac{\lambda_x}{z}}-\lambda_y\,\mathrm{e}^{\frac{\lambda_y}{z}}\right)\mathrm{e}^{-\frac{\lambda_x+\lambda_y}{z}}.\quad(83)$$

Moreover, to evaluate $\mathbb{E}\Big\{\frac{1}{X+Y}\Big\}$ one can write as

$$\mathbb{E}\{Z\}=\int_0^\infty zf_Z(z)dz\overset{(a)}{=}\int_0^\infty(1-F_z(z))dz=\frac{\lambda_y\lambda_x}{\lambda_y-\lambda_x}\ln\left(\frac{\lambda_y}{\lambda_x}\right),\quad(84)$$

where (a) simply follows from integration by part.

Finally, the part $\mathcal{L}_1$ is bounded from below by

$$\mathcal{L}_1\geq\ln\left(1+\exp(\mathcal{K}_1)/\mathcal{K}_2\right).\quad(85)$$

Following the similar steps, $\mathcal{L}_2$ can also be derived, but by simply exchanging the roles of $P_{\mathcal{S}_1}$ and $\mu_{\mathcal{S}_1\mathcal{R}}$ with $P_{\mathcal{S}_2}$ and $\mu_{\mathcal{S}_2\mathcal{R}}$, respectively.

Finally, we try to find an upper bound for the term $\mathcal{L}_3$ to satisfy the original inequality as well as to find a very tight lower-bound expression for $\bar{R}_{sec}$ which is our primary purpose. To this end, we use the inequality $\mathbb{E}\{\ln(1+x)\}\leq\ln(1+\mathbb{E}\{x\})$ from which $\ln(1+x)$ is a concave function with respect of x. By defining $X=P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{R}}|^2/N_0$, $Y=P_{\mathcal{S}_2}|h_{\mathcal{S}_2\mathcal{R}}|^2/N_0$, $Z=\frac{P_{\mathcal{S}_1}|h_{\mathcal{S}_1\mathcal{J}}|^2}{\beta N_0}$, $W=\frac{P_{\mathcal{S}_2}|h_{\mathcal{S}_2\mathcal{J}}|^2}{\beta N_0}$, and $U=|h_{\mathcal{R}\mathcal{J}}|^2$ as RVs with exponential distribution and means $m_x=P_{\mathcal{S}_1}\mu_{\mathcal{S}_1\mathcal{R}}/N_0$, $m_y=P_{\mathcal{S}_2}\mu_{\mathcal{S}_2\mathcal{R}}/N_0$, $m_z=\frac{P_{\mathcal{S}_1}\mu_{\mathcal{S}_1\mathcal{J}}}{\beta N_0}$, $m_w=\frac{P_{\mathcal{S}_2}\mu_{\mathcal{S}_2\mathcal{J}}}{\beta N_0}$, and $m_u=\mu_{\mathcal{R}\mathcal{J}}$, we can express

$$\begin{aligned}\mathcal{L}_3&=\mathbb{E}\Big\{\ln(1+\gamma_R)\Big\}\\&=\mathbb{E}\left\{\ln\Big(1+\frac{X+Y}{(Z+W)U+1}\Big)\right\}\\&\leq\ln\left(1+\mathbb{E}\Big\{\frac{X+Y}{(Z+W)U+1}\Big\}\right)\\&=\ln\left(1+\frac{2(m_x+m_y)}{(m_w-m_z)m_u}\Big[\mathcal{F}_1-\mathcal{F}_2\Big]\right),\end{aligned}\quad(86)$$

where $\mathcal{F}_1$ and $\mathcal{F}_2$ follow from Appendix D.

APPENDIX D

Lemma 5. *For two independent RVs U (exponential RV with mean equal to m_u) and S (Summation of two independent exponential RVs, i.e., $S=Z+W$ with the PDF and the CDF given in Lemma 2), the new RV $Q=\frac{1}{SU+1}$ has the following distribution properties*

$$f_Q(q)=\begin{cases}\frac{2\left[K_0\left(\frac{2\sqrt{\frac{1}{q}-1}}{\sqrt{m_wm_u}}\right)-K_0\left(\frac{2\sqrt{\frac{1}{q}-1}}{\sqrt{m_zm_u}}\right)\right]}{q^2(m_w-m_z)m_u}, & 0<q\leq1\\ 0, & o.w.\end{cases}\quad(87)$$

and then, for $q\in(0,1]$ we have

$$F_Q(q)=1+\frac{2m_z}{m_u(m_w-m_z)}\sqrt{\frac{m_u(1-q)}{m_zq}}K_1\Big(\frac{2\sqrt{1-q}}{\sqrt{m_zm_uq}}\Big)-\frac{2m_w}{m_u(m_w-m_z)}\sqrt{\frac{m_u(1-q)}{m_wq}}K_1\Big(\frac{2\sqrt{1-q}}{\sqrt{m_wm_uq}}\Big).\quad(88)$$

Proof. Let commence from the definition of CDF

$$\begin{aligned}F_Q(q)&=\Pr\Big\{Q\leq q\Big\}\\&=\mathbb{E}_u\Big\{\Pr\big\{S\leq\frac{1-q}{qu}\Big|U=u\big\}\Big\}\\&=\mathbb{E}_u\Big\{F_S(\frac{1-q}{qu})\Big\}\\&\overset{(a)}{=}\int_0^\infty\left(1+\frac{m_z}{m_w-m_z}\exp(-\frac{1-q}{m_zqu})-\frac{m_w}{m_w-m_z}\exp(-\frac{1-q}{m_wqu})\right)\frac{\exp(\frac{-u}{m_u})}{m_u}du,\end{aligned}\quad(89)$$

where (a) follows from Appendix A. Also, the last equality can be further calculated using [34, Eq. (3.471.9)] with

$$\int_0^\infty x^{\nu-1}\exp(-\alpha x-\frac{\beta}{x})\mathrm{d}x=2\left(\frac{\beta}{\alpha}\right)^{\frac{\nu}{2}}K_\nu\left(2\sqrt{\alpha\beta}\right),\quad(90)$$

where $K_\nu(\cdot)$ is the modified Bessel function of the second kind and ν-th order. Finally, after simple manipulations as well as using the fact that $\mathbb{E}\{X\}=\int_0^\infty(1-F_X(x))dx$, we

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2018.2848648, IEEE Transactions on Vehicular Technology

can evaluate $\mathbb{E}\{Q\}$ as

$$\begin{aligned}\mathbb{E}\{Q\}&=\int_0^\infty q f_Q(q)\mathrm{d}q\\&=\int_0^1 \frac{2\left[K_0\Big(\frac{2\sqrt{\frac{1}{q}-1}}{\sqrt{m_w m_u}}\Big)-K_0\Big(\frac{2\sqrt{\frac{1}{q}-1}}{\sqrt{m_z m_u}}\Big)\right]}{q(m_w-m_z)m_u}\mathrm{d}q\\&=\frac{2}{(m_w-m_z)m_u}\\&\times\Bigg[\underbrace{\int_0^1\frac{K_0\Big(\frac{2\sqrt{\frac{1}{q}-1}}{\sqrt{m_w m_u}}\Big)}{q}\mathrm{d}q}_{\mathcal{F}_1}-\underbrace{\int_0^1\frac{K_0\Big(\frac{2\sqrt{\frac{1}{q}-1}}{\sqrt{m_z m_u}}\Big)}{q}\mathrm{d}q}_{\mathcal{F}_2}\Bigg].\end{aligned}\quad(91)$$

Now, due to symmetry of the integrals in the last equation, we only compute the first term $\mathcal{F}_1$ as

$$\mathcal{F}_1=\int_0^1\frac{K_0\Big(C_1\sqrt{\frac{1}{q}-1}\Big)}{q}\mathrm{d}q,\quad(92)$$

where C_1 is defined as $C_1=\frac{2}{\sqrt{m_w m_u}}$. To proceed further, we employ an equivalent definition, i.e., an infinite series of modified Bessel functions of the second kind and ν-th order, with $\nu>0$, as introduced in [38]

$$\mathrm{K}_\nu(\beta x)=\exp(-\beta x)\sum_{n=0}^{\infty}\sum_{i=0}^{n}\Lambda(\nu,n,i)(\beta x)^{i-\nu},\quad(93)$$

where

$$\Lambda(\nu,n,i)=\frac{(-1)^i\sqrt{\pi}\Gamma(2\nu)\Gamma(n-\nu+\frac{1}{2})\mathrm{L}(n,i)}{2^{\nu-i}\Gamma(\frac{1}{2}-\nu)\Gamma(n+\nu+\frac{1}{2})n!}.\quad(94)$$

However, we cannot directly apply the expression in (93) to calculate the integral in (92) since in our case, we have $\nu=0$. Therefore, using the equality $\mathrm{K}_{\nu-2}(\beta x)=\mathrm{K}_\nu(\beta x)-\frac{2(\nu-1)}{\beta x}\mathrm{K}_{\nu-1}(\beta x)$ [38] when $\nu=2$, we can rewrite $\mathrm{K}_0(\beta x)$ as

$$\mathrm{K}_0(\beta x)=\exp(-\beta x)\sum_{n=0}^{\infty}\sum_{i=0}^{n}\Lambda(1,n,i)(g(n)-2)(\beta x)^{i-2},\quad(95)$$

where [3]

$$g(n)=\frac{\Lambda(2,n,i)}{\Lambda(1,n,i)}=-\frac{9}{2}\frac{\Gamma(n-\frac{3}{4})\Gamma(n+\frac{3}{2})}{\Gamma(n-\frac{1}{2})\Gamma(n+\frac{5}{2})}.\quad(96)$$

Substituting (95) in (92), and after some manipulations, one can represent (92) as

$$\begin{aligned}\mathcal{F}_1&=\sum_{n=1}^{\infty}\sum_{i=1}^{n}\Lambda(1,n,i)(g(n)-2)C_1^{i-2}\\&\times\int_0^1\frac{\exp(-C_1(\frac{1-q}{q}))(\sqrt{\frac{1-q}{q}})^{i-2}}{q}\mathrm{d}q\\&\overset{(a)}{=}2\int_0^\infty\frac{\exp(-C_1u)u^{i-1}}{u^2+1}\mathrm{d}u,\end{aligned}\quad(97)$$

where (a) follows from taking the axillary variable $u=\sqrt{\frac{1-q}{q}}$. Using [34, Eq. (3.356.1)] and [34, Eq. (3.356.2)] we ultimately obtain the required expression for $\mathcal{F}_{1,2}$ as

$$\begin{aligned}\mathcal{F}_{1,2}(x)=&-\sum_{n=1}^{\infty}\sum_{i=1}^{n}\Lambda(1,n,i)\left(9\frac{\Gamma(n-\frac{3}{4})\Gamma(n+\frac{3}{2})}{\Gamma(n-\frac{1}{2})\Gamma(n+\frac{5}{2})}+4\right)\\&\times x^{i-2}\begin{cases}(-1)^k\Big[\mathrm{ci}(x)\cos(x)+\mathrm{si}(x)\sin(x)\Big]\\+\frac{1}{x^{2k-2}}\sum_{j=1}^{k-1}(2k-2j-1)!(-x^2)^{j-1}, & i=2k\\(-1)^k\Big[\mathrm{ci}(x)\sin(x)-\mathrm{si}(x)\cos(x)\Big]\\+\frac{1}{x^{2k-1}}\sum_{j=1}^{k}(2k-2j)!(-x^2)^{2j-1}, & i=2k+1\end{cases}\end{aligned}\quad(98)$$

It should be clearly noted that $\mathcal{F}_{1,2}(C_1)=\mathcal{F}_1$, and $\mathcal{F}_{1,2}(C_2)=\mathcal{F}_2$, which $C_2=\frac{2}{\sqrt{m_z m_u}}$. ■

ACKNOWLEDGMENT

The authors would like to thank Dr. Phee Lep Yeoh for the constructive comments to improve the paper and indispensable collaboration that led to our joint prior work.

REFERENCES

[1] A. Yenner and S. Ulukus, "Wireless physical-layer security: lessons learned from information theory," *Proc. IEEE*, vol. 103, no. 10, pp. 1814-1825, Sep. 2015.

[2] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20-27, Apr. 2015.

[3] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. L- Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: state of the art and beyond," *IEEE Commun. Mag.*, pp. 2-9, Dec. 2015.

[4] Y. Oohama, "Coding for relay channels with confidential messages," *in Proc. Inf. Theory Workshop*, 2001, pp. 87-89.

[5] Z. Han, N. Marina, M. Debbah, and A. Hjorungnes, "Physical layer security game: Interaction between source, eavesdropper and friendly jammer," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, pp. 452907-1 452907-10, Mar. 2009.

[6] D. Fang, N. Yang, M. Elkashlan, P. L. Yeoh, and J. Yuan, "Cooperative jamming protocols in two-Hop amplify-and- forward wiretap channels," *in Proc. IEEE ICC*, Budapest, Hungary, pp. 2188-2192, Nov. 2013.

[7] L. Wang, Y. Cai, Y. Zou, W. Yang and L. Hanzo, "Joint relay and jammer selection improves the physical layer security in the face of CSI feedback delays," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6259-6274, Aug. 2016.

[8] K. Wang, L. Yuan, T. Miyazaki, S. Guo and Y. Sun, "Anti-eavesdropping with selfish jamming in wireless networks: A bertrand game approach," *IEEE Trans. Veh. Technol.*, vol. 66, no. 7, pp. 6268-6279, July 2017.

[9] X. He and A. Yener, "Two-hop secure communication using an untrusted relay: A case for cooperative jamming," *in Proc. IEEE Globecom*, New Orleans, LA, pp. 15, Dec. 2008.

[10] L. Wang, M. Elkashlan, J. Huang, N. H. Tran, and T. Q. Duong, "Secure transmission with optimal power allocation in untrusted relay networks," *IEEE Wireless Commun. Lett.*, vol. 3, no. 3, pp. 289-292, Jun. 2014.

[11] A. Kuhestani, A. Mohammadi and M. Noori, "Optimal power allocation to improve secrecy performance of non-regenerative cooperative systems using an untrusted relay," *IET Commun.*, vol. 10, no. 8, pp. 962-968, May. 2016.

[12] J.-B. Kim, J. Lim, and J. Cioffi, "Capacity scaling and diversity order for secure cooperative relaying with untrustworthy relays," *IEEE Trans. Wireless Commun.*, vol. 14, no. 7, pp. 38663876, July 2015.

[13] A. Kuhestani, A. Mohammadi, and M. Mohammadi, "Joint relay selection and power allocation in large-scale MIMO systems with untrusted relays and passive Eavesdroppers," *IEEE Trans. Inf. Forensics Security*., vol. 13 no. 2 pp. 341 - 355, Feb. 2018.

[3] Note that for the evaluation of the coefficients, $\Lambda(\nu,n,i)$, following results are fruitful: $L(0,0)=1$, $L(n,0)=0$, $L(n,1)=n!$ for positive values of n. In addition, for Gamma function $\Gamma(\frac{1}{2})=\sqrt{\pi}$, $\Gamma(-\frac{1}{2})=-2\sqrt{\pi}$, $\Gamma(1)=1$, and $\Gamma(x+1)=x\Gamma(x)$.

[14] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Trans. Veh. Technol.*, vol. 61, no. 8, pp. 3693-3704, Oct. 2012.

[15] J. Mo, M. Tao, Y. Liu, and R. Wang, "Secure beamforming for MIMO two-way communications with an untrusted relay," *IEEE Trans. Signal Process.*, vol. 62, no. 9, May. 2014.

[16] J. Huang, A. L. Swindlehurst, "Joint transmit design and node selection for one-way and two-way untrusted relay channels," *Asilomar Conference on Signals, Systems and Computers*, pp. 1555-1559, Nov. 2013.

[17] H. Xu, L. Sun, P. Ren and Q. Du, "Securing two-way cooperative systems with an untrusted relay: a constellation-rotation aided approach," *in IEEE Commun. Let.*, vol. 19, no. 12, pp. 2270-2273, Dec. 2015.

[18] A. Kuhestani, P. L. Yeoh, and A. Mohammadi, "Optimal power allocation and secrecy sum rate in two-way untrusted relaying," *in Proc. IEEE Globecom*, Singapore, Dec. 2017.

[19] M. L. Ku, W. Li, Y. Chen and K. J. Ray Liu, "Advances in energy harvesting communications: past, present, and future challenges," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1384-1412, Second Quarter 2016.

[20] P. Grover and A. Sahai, "Shannon meets Tesla: Wireless information and power transfer," *in Proc. IEEE ISIT*, pp. 23632367, Jun. 2010.

[21] A. A. Nasir, X. Zhou, S. Durrani, and R. A. Kennedy, "Wireless-powered relays in cooperative communications: Time-switching relaying protocols and throughput analysis," *IEEE Trans. Commun.*, vol. 63, no. 5, pp. 1607-1622, May. 2015.

[22] H. Al-Hraishawi and G. A. Aruma Baduge, "Wireless energy harvesting in cognitive massive MIMO systems with underlay spectrum sharing," *IEEE Wireless Commun. Lett.*, vol. 6, no. 1, pp. 134-137, Feb. 2017.

[23] W. Liu, X. Zhou, S. Durrani and P. Popovski, "Secure communication with a wireless-powered friendly jammer," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 401-415, Jan. 2016.

[24] S. S. Kalamkar and A. Banerjee, "Secure communication via a wireless energy harvesting untrusted relay," *IEEE Trans. Veh. Tech.*, vol. 66, no. 3, pp. 2199-2213, March 2017.

[25] A. Lozano, A. Tulino, and S. Verdu, "High-SNR power offset in multiantenna communication," *IEEE Trans. Inf. Theory*, vol. 51, no. 12, pp. 4134-4151, Dec. 2005.

[26] G. Amarasuriya, E. G. Larsson and H. V. Poor, "Wireless information and power transfer in multi-way massive MIMO relay networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 6, pp. 3837-3855, June 2016.

[27] Y. Zou, X. Wang, W. Shen, and L. Hanzo, "Security versus reliability analysis of opportunistic relaying," *IEEE Trans. Veh. Tech.*, vol. 63, no. 6, pp. 2653-2661, Jul. 2014.

[28] A. Kuhestani, A. Mohammadi and P. L. Yeoh, "Optimal power allocation and secrecy sum rate in two-way untrusted relaying networks with an external jammer," *IEEE Trans. Commun.*, doi: 10.1109/TCOMM.2018.2802951.

[29] M. Zhang, Y. Liu, and R. Zhang, "Artificial noise aided secrecy information and power transfer in OFDMA systems,"*IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 30853096, Apr. 2016.

[30] M. Liu and Y. Liu, "Power allocation for secure SWIPT systems with wireless-powered cooperative jamming," *IEEE Wireless Commun. Lett.*, vol. 21, no. 6, pp. 1353-1356, June 2017.

[31] W. Harrison and S. McLaughlin, "Tandem coding and cryptography on wiretap channels: EXIT chart analysis," *in Proc. IEEE ISIT*, June 2009, pp. 19391943.

[32] W. Harrison, J. Almeida, S. McLaughlin, and J. Barros, "Coding for cryptographic security enhancement using stopping sets," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 575584, Sep. 2011.

[33] A. Papoulis, *Probability, Random Variables, and Stochastic Processes*. New York: McGraw-Hill, 1984.

[34] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. New York: Academic, 2007.

[35] S. Daboul, J. Mangaldan, M. Z. Spivey, and P. J. Taylor. "The Lah Numbers and the nth Derivative of $e^{\frac{1}{x}}$," accessed on Aug. 6, 2012. [Online]. Available: http://math.pugetsound.edu/ mspivey/Exp.pdf

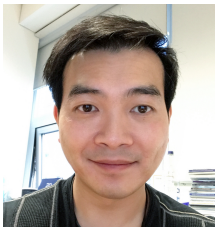
[36] R. H. Y. Louie, Y. Li, H. A. Suraweera, and B. Vucetic, "Performance analysis of beamforming in two hop amplify and forward relay networks with antenna correlation," *IEEE Trans. Wireless Commun.*, vol. 8, no. 6, pp. 3132-3141, June 2009.

[37] L. Wang, H. Q. Ngo, M. Elkashlan, T. Q. Duong and K. K. Wong, "Massive MIMO in spectrum sharing networks: achievable rate and power efficiency," *IEEE Systems Journal*, vol. 11, no. 1, pp. 20-31, March 2017.

[38] M. M. Molu, P. Xiao, M. Khalily, L. Zhang and R. Tafazolli, "A novel equivalent definition of modified Bessel functions for performance analysis of multi-hop wireless communication systems," *IEEE Access*, vol. 5, pp. 7594-7605, 2017.

Milad Tatar Mamaghani was born in Tabriz, Iran, on May 12, 1994. He received the B.Sc. degree in Electrical and Communications Engineering from Amirkabir University of Technology, Tehran, Iran, in 2016. He was awarded as an Exceptional Talent for outstanding performance during his undergraduate studies, and honored to do double major in Control Engineering. From 2016 to 2018, he worked as a research assistant at MMWCL of the Department of Electrical Engineering, Amirkabir University of Technology, Tehran, Iran. He has also served as a Reviewer for IET Communications. His research interests lie in the areas of wireless communications and networking, physical layer security, Internet of Things (IoT), and signal processing.

Ali Kuhestani received his B.Sc. degree in Electrical Engineering from Shiraz University of Technology, Shiraz, Iran, in 2010, his M.Sc. degree in Electrical Engineering from Tarbiat Modares University, Tehran, Iran, in 2012, and his Ph.D. degree in Electrical Engineering from Amirkabir University of Technology, Tehran, Iran, in 2017, with high distinction. He has authored over 15 journals in prestigious publication avenues (e.g., the IEEE and IET) and about 10 papers in major conference proceedings. He also serves as a reviewer for the IEEE transactions/journals and conferences. He is the holder of Iran's National Elites Foundation award for outstanding students in 2017. His research interests include physical-layer security of wireless communications, Internet of Things (IoT), millimeter-wave communication, massive MIMO system and space-time coding.



Kai-Kit Wong (M'01-SM'08-F'16) received the BEng, the MPhil, and the PhD degrees, all in Electrical and Electronic Engineering, from the Hong Kong University of Science and Technology, Hong Kong, in 1996, 1998, and 2001, respectively. After graduation, he took up academic and research positions at the University of Hong Kong, Lucent Technologies, Bell-Labs, Holmdel, the Smart Antennas Research Group of Stanford University, and the University of Hull, UK. He is Chair in Wireless Communications at the Department of Electronic and Electrical Engineering, University College London, UK.

His current research centers around 5G and beyond mobile communications, including topics such as massive MIMO, full-duplex communications, millimetre-wave communications, edge caching and fog networking, physical layer security, wireless power transfer and mobile computing, V2X communications, and of course cognitive radios. There are also a few other unconventional research topics that he has set his heart on, including for example, fluid antenna communications systems, remote ECG detection and etc. He is a co-recipient of the 2013 IEEE Signal Processing Letters Best Paper Award and the 2000 IEEE VTS Japan Chapter Award at the IEEE Vehicular Technology Conference in Japan in 2000, and a few other international best paper awards.

He is Fellow of IEEE and IET and is also on the editorial board of several international journals. He has served as Senior Editor for IEEE Communications Letters since 2012 and also for IEEE Wireless Communications Letters since 2016. He had also previously served as Associate Editor for IEEE Signal Processing Letters from 2009 to 2012 and Editor for IEEE Transactions on Wireless Communications from 2005 to 2011. He was also Guest Editor for IEEE JSAC SI on virtual MIMO in 2013 and currently Guest Editor for IEEE JSAC SI on physical layer security for 5G.