

Article

Hybrid Destination-Based Jamming and Opportunistic Scheduling with Optimal Power Allocation to Secure Multiuser Untrusted Relay Networks

Fan Ding * and Yongming Zhou

School of Physics and Electromechanical Engineering, Shaoguan University, Shaoguan 512005, China; gzyyzym@hotmail.com

* Correspondence: dingfsgu@sgu.edu.cn; Tel.: +86-0751-8120144

Received: 7 March 2018; Accepted: 2 April 2018; Published: 9 April 2018



Abstract: In this paper, we investigate secure communication for a dual-hop multiuser relay network, where a source communication with N ($N \ge 1$) destinations via an untrusted variable gains relay. To exploit multiuser diversity while protecting source's confidential message, we first propose a joint destination-based jamming and opportunistic scheduling (DJOS) scheme. Then, we derive closed-form approximated and asymptotic expressions of the secrecy outage probability (SOP) for the considered system with DJOS. Furthermore, we determine an asymptotical optimal power allocation (OPA), which minimizes the asymptotic SOP, to further improve the secrecy performance. Our analytical results show that the achievable secrecy diversity order in terms of SOP with fixed power allocation is $\min(1, \frac{N}{2})$, whereas, with OPA, the achievable secrecy diversity order can be improved up to $\min(1, \frac{2N}{N+2})$. This interesting result reveals that OPA can improve the secrecy diversity order of 1 cannot be achieved when N = 1, thus leaving some space for OPA to improve the diversity order. Nevertheless, for $N \ge 2$, the effect of OPA is to increase the secrecy array gain rather than the secrecy diversity order since full diversity order 1 has been achieved by the OS scheme. Finally, simulation results are presented to validate our analysis.

Keywords: amplify-and-forward; secrecy outage probability; destination-based jamming; multiuser untrusted relay network; opportunistic scheduling

1. Introduction

1.1. Background

Recently, the applications of physical layer security (PLS) techniques in cooperative relaying networks have gained considerable attention. In particular, there are extensive works aimed at enhancing the secrecy performance of cooperative relaying networks by exploiting various PLS approaches, such as diversity techniques and/or cooperative jamming. Specifically, diversity techniques, such as multiple-input multiple-output (MIMO) [1], cooperative diversity (i.e., cooperative relaying) [2], and multiuser diversity [3,4], aim at increasing the capacity of the main channel while degrading that of the wiretap channel. As such, the system security can be significantly improved. On the other hand, cooperative jamming (CJ) [5–10], which exploits artificial noise to confuse external eavesdroppers, can reduce the leakage rate to the eavesdroppers to improve the system security. In particular, in CJ, artificial noise can be sent from a friendly jammer [5], the source [6,10], the relay [7], or the destination [8–10]. Furthermore, more recent works have been devoted to further enhance the PLS by combining diversity strategies and/or CJ scheme [11]. Besides, power allocation technique was also investigated in [12,13] to further improve the secrecy performance.



1.2. Related Works

Common to the aforementioned works is that all relays are assumed to be trusted, and the eavesdroppers are external nodes. Another feasible scenario is that relay(s) might belong to a heterogeneous network with a different security clearance. In this context, the relay(s) can be untrusted, and it is desirable to keep confidential messages from the untrusted relay(s), despite the help of the relay(s)' [14-16]. The research on untrusted relay networks was pioneered by He and Yener [16]. A destination-based jamming (DJ) scheme was proposed in [16] to realize positive secrecy rate in dual-hop relay networks with an untrusted amplify-and-forward (AF) relay. Due to its excellent performance, several works focused on analyzing the performance of DJ in various untrusted relay channels, including the ergodic secrecy capacity (SEC) [17–21], and the secrecy outage probability (SOP) [22–26]. Although these works have proven that secure transmission is feasible in untrusted AF relay networks with DJ, it is worth noting that the existence of untrusted relay(s) brings fundamental changes to the system (secure) capacity and outage performance, as compared to the conventional AF channels with trusted relay(s). More specifically, in [17,18], the authors proved that the SEC of multi-untrusted AF networks degrades as the number of untrusted relay increases, which is in contrast with conventional AF networks with multiple trusted relays. On the other hand, as an alternative secrecy criterion, the SOP of AF networks with DJ was recently investigated for the single-untrusted-relay case [22] and the multi-untrusted-relay case [26]. Their analysis showed that the existence of relay's eavesdropping resulted in a smaller (secrecy) diversity order in terms of SOP. In particular, in [26], the asymptotic SOP expression of multi-untrusted-relay networks with variable gain relaying (VGR) was derived, from which the secrecy diversity order in terms of SOP was shown to be limited to one, rather than the relay number M achieved in conventional trusted AF networks. However, this conclusion only holds for "moderate" number of relays scenario as presented by Theorems 3 and 4 in [26]. This can be attributed to the key approximation based on the law of large numbers (i.e., larger value of M) in [26]. Moreover, Figure 8 in [26] showed that the slop of the simulated SOP curve for M = 3 is actually smaller than that of the asymptotic SOP whose diversity order is 1. Therefore, both the derivation method and the conclusion in [26] cannot be directly extended to the case of small number of relays, especially for the typical single-relay case M = 1. In [22], the SOP of fixed-gain relaying (FGR) for the typical M = 1 case was obtained in an integral form. However, we cannot directly obtain the secrecy diversity order from the integral form of SOP in [22] (a diversity order of 1/2 in terms of SOP can be conjectured from the simulation in Figure 1 in [22] for the single-relay case). Motivated by this key observation, recent work [24] explicitly proved that obtained secrecy diversity order in the single-user and single-untrusted-relay scenario with FGR was limited to 1/2.

To alleviate the impact of untrusted relay, optimal power allocation (OPA) can be used to improve the secrecy performance [21,27–29]. For DJ-based untrusted AF relay networks, where the source and destinations were equipped with large-scale antennas while the untrusted relay was equipped with a single antenna, an OPA scheme was proposed to maximize the instantaneous secure rate (ISR) [27]. Similarly, OPA was investigated in [28] for maximizing the ISR of large-scale antenna system with single-antenna untrusted relay. The authors in [21] considered a DJ-based MIMO untrusted relay system and proposed an iterative power allocation algorithm to jointly design the source, relay, and destination precoding for maximizing the achievable ISR. Very recently, an OPA scheme was proposed in [29] to maximize the ISR in energy harvesting relay network. Noting that all these works focused on maximizing the ISR with OPaA.

1.3. Motivation and Contributions

A major limitation of the aforementioned works [17–23,25–29] is that most were limited to single user scenario, and, thus, the impact of multiuser diversity (MUD) on system secrecy performance has not been considered. In fact, very little work on the secure communication in multiuser relay networks has been reported. In [30], the authors investigated the secure issue in multiuser relay

networks, where the undesired users who were not selected for data reception was treated as potential eavesdroppers. An optimal user selection scheme was proposed for the considered system, which was optimal in the sense of maximizing the secrecy rate. Still, the relay in [30] was assumed to be trusted. In recent work [24], the authors focused on the multiuser untrusted relay networks with FGR and proposed a novel joint destination-based jamming and opportunistic scheduling scheme to improve the system SOP. In particular, the results in [24] explicitly revealed that the proposed scheme can improve the secrecy diversity order from 1/2 in single-user networks up to full secrecy diversity order of 1 in multiuser relay networks. However, OPA between the source and the destination still has not been considered. To the best of our knowledge, no work has yet analyzed the utilization of OPA strategy to minimize the SOP of DJ-based multiuser untrusted relay networks.

In this paper, we aim to enhance the security of a multiuser untrusted AF relay network without expending additional resources. Based on the joint destination-based jamming and opportunistic scheduling (DJOS) scheme in [24], we optimize the power allocation between the source and the destination between source and destination under a total power constraint to further improve the secrecy outage performance. Unlike the previous work in [24], where FGR protocol is employed at the relay, we consider VGR protocol in this paper because VGR achieves better performance than FGR in general. Note that the main channel (source-relay-destination) and the wiretap channel (source-relay) in untrusted relay networks are intuitively correlated with each other, which makes the analysis for deriving the closed-form SOP expression difficult by mathematical treatment. Moreover, compared to the FGR scheme as in [24], the SOP of multiuser untrusted relay networks with VGR scheme is more difficult to analyze. In this regard, it is not easily tractable to get the exact closed-form SOP expressions of VGR scheme, even for the single-user untrusted relay scenario. To tackle this problem, on the premise of large signal-to-noise ratio (SNR), we resort to a number of approximations to obtain the SOP expressions in closed-form.

Compared to closely previous related works [24] and [26], our main contributions are summarized as follows:

- To harvest the MUD while satisfying the security constraint, we propose to apply the DJOS scheme in the considered multiuser untrusted AF relay networks with VGR. Under Rayleigh fading channels, we first derive a new closed-form approximated SOP expression for the considered system with DJOS. Note that an analytical SOP expression for multiple untrusted relay networks with VGR scheme has already derived in [26]. However, as we explained before, both the derivation method and the conclusion in [26] cannot be directly extended to the single-user and single-untrusted-relay case which has been included and studied in this paper.
- To gain further insights, we then present the asymptotic SOP expression and prove that the achievable secrecy order is min(1, N/2), where *N* denotes the number of destinations (users) (In this paper, the diversity order only mathematically indicates the curve slope of the outage performance metric studied at high SNRs. Prior works [8,20,24,26] have confirmed that the (secrecy) diversity order behavior in terms of SOP in cooperative relaying networks with security requirement is very different from the diversity order behavior in terms of connection outage probability (COP) in scenarios without security requirement). That is, for the single-user network (N = 1), the achievable secrecy diversity order in terms of SOP is 1/2, while with DJOS, the secrecy diversity order of 1. Thus, MUD has been harvested by the OS strategy. It is worth noting that our rigorous mathematical analyses explicitly show that the obtained secrecy diversity order for the the typical single-untrusted-relay network with VGR is actually 1/2, rather than 1 as revealed in the multi-untrusted-relay case [26]. Therefore, our theoretical analysis on the single-untrusted-relay network supplements and complements the results in [26].
- Finally, we propose an asymptotically OPA scheme to minimize the asymptotic SOP. Interestingly, with the proposed OPA scheme, we find that the system secrecy diversity order can be improved from min $(1, \frac{N}{2})$ (without OPA) to min $(1, \frac{2N}{N+2})$. This conclusion provides some new

findings that allow us to understand the impact of power allocation on the SOP performance. Specifically, for the N = 1 case, our OPA scheme can help to improve the secrecy diversity order from 1/2 up to 2/3. It is well-known that the application of OPA in conventional trusted relay networks can only help to improve the array gain rather than the diversity gain/order [31]. This is because full diversity order of 1 is already obtained there even without OPA. However, our work explicitly show that, in the untrusted relay case, the effect of OPA is to increase the secrecy diversity order. It is intuitive that the diversity order. Moreover, when $N \ge 2$, we prove that OPA does not affect the secrecy diversity order. This is because full secrecy diversity order of 1 is already obtained there even without OPA. However, our work explicitly show that, in the untrusted relay case, the effect of OPA is to increase the secrecy diversity order. It is intuitive that the diversity order. Moreover, when $N \ge 2$, we prove that OPA does not affect the secrecy diversity order. This is because full secrecy diversity order of 1 is already obtained by the OS scheme even without OPA. However, as we will show in Section 5, the effect of OPA is to increase the secrecy array gain and hence significantly reduces the SOP.

The rest of this paper is organized as follows. Section 2 presents the system model and the DJOS scheme. Section 3 analyzes the tight approximated secrecy outage probability, as well as the high-SNR asymptotic secrecy outage probability. Section 4 studies the optimal power allocation, which minimizes the secrecy outage probability. Section 5 presents numerical and simulation results to verify our theoretical analysis. Finally, Section 6 concludes the paper.

2. System Model

As shown in Figure 1, we consider a downlink cooperative cellular network where one source *S* communicates with *N* destination users D_n (n = 1, ..., N) via the help of an untrusted AF relay *R*. Each node is equipped with a single antenna and operates in a time-division half-duplex mode. It is assumed that all channels are reciprocal and quasi-static over each transmission. Moreover, no direct links exists between the source and the destinations, due to the long distance or significant obstacle [17,18,20,22,26]. In this setting, although *S* has to rely on *R* to transmit its information, it does not trust *R* and would like to keep its confidential information secret from *R*. This model can find application in many practical scenarios such as renting a satellite relay from a third party to forward source's confidential information [20].



Figure 1. System Model for the multiuser untrusted AF relay networks with joint destination-based jamming and opportunistic scheduling (DJOS).

To achieve both the benefits of MUD and DJ schemes, we apply the DJOS scheme in [24] for the considered multiuser untrusted relay network. Specifically, before each data transmission, only the "best" destination out of the *N* candidates is selected to access the channel, using a specific security optimal opportunistic scheduling (OS) strategy whose details will be given later. As will be demonstrated later, MUD can be obtained by the proposed user scheduling strategy. After this, a two-phase transmission starts. In particular, the DJ approach is adopted in Phase 1 to prevent

eavesdropping at the untrusted relay *R*. Note that this DJ-based two-phase transmission is similar to the physical layer network coding (PNC) or analog network coding (ANC) as illustrated in [32,33], respectively. (It is well-known that both PNC and ANC can achieve full diversity order of 1 in terms of COP [34]. In this context, the (secrecy) diversity order deterioration in single-user AF network with DJ, as demonstrated in Section 4, is not due to the application of DJ in untrusted AF networks.) The data transmission process is detailed as follows.

In Phase 1, *S* transmits x_s with power αP and at the same time, the *n*th destination (i.e., D_n) transmits a Gaussian interference signal $x_{d,n}$ with power $(1 - \alpha)P$ to the relay. Here, *P* denotes a fixed total transmission power budget (*P* also denotes the system SNR herein) and $\alpha \in (0, 1)$ is the power allocation ratio [17]. Hence, the superimposed signal received at *R* is given by

$$y_R = \sqrt{\alpha P} h_1 x_s + \sqrt{(1-\alpha)P} h_{2,n} x_{d,n} + n_R, \tag{1}$$

where $h_1 \sim C\mathcal{N}(0, \lambda_1^{-1})$ and $h_{2,n} \sim C\mathcal{N}(0, \lambda_{2,n}^{-1})$ denote the instantaneous channel coefficient of $S \to R$ and $R \to D_n$ links, respectively, and $n_R \sim C\mathcal{N}(0, 1)$ is additive white Gaussian noise (AWGN) at the relay. Then, under Rayleigh fading channels, $|h_1|^2$ and $|h_{2,n}|^2$ are independent exponential random variables with parameters λ_1 and $\lambda_{2,n}$, respectively. Moreover, we assume that all the users are located in close proximity to each other with $\lambda_{2,n} = \lambda_2$ for simplicity. Based on Equation (1), the received signal-to-interference-plus-noise ratio (SINR) at the relay *R* is given by

$$\gamma_R = \frac{\alpha P |h_1|^2}{(1-\alpha)P |h_{2,n}|^2 + 1}.$$
(2)

In Phase 2, *R* simply amplifies the received signal y_R with a scaling gain applied, denoted by G, and then retransmits it to D_n . The received signal at D_n is written as

$$y_{D_n} = h_{2,n} \mathcal{G}(\sqrt{\alpha P} h_1 x_s + \sqrt{(1-\alpha)P} h_{2,n} x_{d,n} + n_R) + n_{D_n},$$
(3)

where $n_{D_n} \sim C\mathcal{N}(0,1)$ is AWGN at D_n . Since $x_{d,n}$ is the transmitted signal of D_n in the first phase, D_n can subtract the term $h_{2,n} \mathcal{G}\sqrt{(1-\alpha)P}h_{2,n}x_{d,n}$ from y_{D_n} and decodes the source message based on the remainder signal $\widetilde{y_{D_n}}$, which is given by

$$\widetilde{y_{D_n}} = h_{2,n} \mathcal{G}(\sqrt{\alpha} P h_1 x_s + n_R) + n_{D_n}.$$
(4)

When a variable gain relay is employed, the variable-gain relaying factor is selected as $\mathcal{G} = \sqrt{\frac{P}{\alpha P |h_1|^2 + (1-\alpha)P |h_{2,n}|^2 + 1}}$. Plugging the expression of \mathcal{G} into $\widetilde{y_{D_n}}$ and after some algebraic manipulations, we can express the SINR at D_n as

$$\gamma_{D_n} = \frac{\alpha P |h_1|^2 \times P |h_{2,n}|^2}{\alpha P |h_1|^2 + (2 - \alpha) P |h_{2,n}|^2 + 1}$$
(5)

According to Equations (2) and (5), the achievable instantaneous secrecy rate at the *n*th destination D_n is calculated by [26]

$$C_{S,n} = \left[\frac{1}{2}\log(1+\gamma_{D_n}) - \frac{1}{2}\log(1+\gamma_R)\right]^+ \\ = \left[\frac{1}{2}\log\left(\frac{1+\frac{\alpha P|h_1|^2 \cdot P|h_{2,n}|^2}{\alpha P|h_1|^2 + (2-\alpha)P|h_{2,n}|^2 + 1}}{1+\frac{\alpha P|h_1|^2}{(1-\alpha)P|h_{2,n}|^2 + 1}}\right)\right]^+,$$
(6)

where $[x]^+ = \max\{0, x\}.$

3. Opportunistic Scheduling Scheme

We now describe the opportunistic scheduling scheme, which aims at exploiting the multiuser diversity inherent in the considered multiuser relay networks as well as guaranteeing the system to achieve the optimal secrecy performance. In this regard, the user scheduling criterion is to select such a destination/user D_{n^*} that satisfies

$$n^* = \arg\max_{1 \le n \le N} C_{S,n}.$$
(7)

In this criterion, at a time, only the destination with the highest instantaneous secrecy rate out of *N* destinations is scheduled for transmitting jamming signal in Phase 1 and receiving the relay's signal in Phase 2. Furthermore, it is not difficult to verify that the instantaneous secrecy rate $C_{S,n}$ in Equation (6) is an increasing function of $|h_{2,n}|^2$, so a user maximizing the instantaneous secrecy rate is identical to a user with the largest instantaneous channel gain of the second hop. Thus, the scheduling policy in Equation (7) can be formulated equivalently as

$$h_M = \max_{1 \le n \le N} |h_{2,n}|^2, \tag{8}$$

where h_M denotes the instantaneous channel gain of the scheduled destination D_n^* .

It should be noted that Equation (8) reveals that the opportunistic scheduling strategy in conventional multiuser relay networks without security requirement [35] can be applied directly in the multiuser untrusted relay networks. Specifically, the scheduling scheme presented in Equation (8) is implemented at the relay, which is assumed to have perfect knowledge of the relay-destination links of all the *N* destinations (This is a common assumption in multiuser relay networks [35–37]. In practice, the channel state informations (CSIs) of the links can be estimated at the relay by employing reciprocity to estimate forward channels from the reverse channels. Generally speaking, the CSI estimation could be very accurate if the training period is sufficiently long [36]). At the beginning of each scheduling period, the relay broadcasts a destination synchronization message, which contains the synchronization information and the pilot signaling transmission order. Then, the relay identifies and selects the strongest user. Finally, the relay feeds back the index of the strongest user to the source.

The relay has perfect channel state information (CSI) of each link.

4. Secrecy Outage Performance Analysis

In this section, we will derive an analytical expression for the SOP with large transmit power first. Then, we provide an high-SNR asymptotic SOP expression to characterize the asymptotic secrecy outage performance of the system, i.e., secrecy diversity order and secrecy array gain. Finally, based on the asymptotic SOP expression, we determine an asymptotic power allocation to further boost the system secrecy performance.

4.1. Approximated Secrecy Outage Probability

SOP is defined as the probability that the instantaneous secrecy rate is less than a given target secrecy rate $R_s > 0$ [26]. Mathematically, according to Equations (6) and (8), the SOP can be formulated as

$$P_{sop} = \Pr\left\{C_{S,M} < R_{S}\right\}$$

$$= \Pr\left\{\frac{1 + \frac{\alpha P |h_{1}|^{2} \cdot P |h_{M}|^{2}}{\alpha P |h_{1}|^{2} + (2-\alpha) P |h_{M}|^{2} + 1}}{1 + \frac{\alpha P |h_{1}|^{2}}{(1-\alpha) P |h_{M}|^{2} + 1}} < 2^{2R_{S}}\right\}.$$
(9)

Unfortunately, it is not easily tractable to get exact closed-form expression of Equation (9). To tackle this, we resort to some approximations to facilitate our analysis. First, we apply the

well-known and widely used inequality $\frac{xy}{1+x+y} < \frac{xy}{x+y} \leq \min(x,y)$ to tightly upper bound γ_D as $\gamma_D < P \min\{\frac{\alpha}{2-\alpha}|h_1|^2, |h_M|^2\}$. Moreover, to guarantee the secure transmission, we consider the worst-case, where the noise at the relay is zero. Note that this assumption is reasonable when SNR is high and it further facilitates the analysis, which is also taken into considered in [27]. That is, we have $\gamma_R \approx \frac{\alpha |h_1|^2}{(1-\alpha)|h_M|^2}$ in high SNR regime. Then, the system SOP with selected destination D_n^* in Equation (9) can be approximated as follows

$$P_{sop} \approx \Pr\left\{\frac{1 + P\min\left\{\frac{\alpha}{2-\alpha}|h_1|^2, |h_M|^2\right\}}{1 + \frac{\alpha|h_1|^2}{(1-\alpha)|h_M|^2}} < 2^{2R_s}\right\}.$$
(10)

In the following theorem, we provide an analytical expression for P_{sop} in Equation (10).

Theorem 1. The secrecy outage probability of the multiuser untrusted relay networks with DJOS can be approximately expressed by:

$$P_{sop} \approx 1 - J_1 + J_2,\tag{11}$$

where J_1 and J_2 are, respectively, given by

$$J_{1} = \sum_{n=1}^{N} {\binom{N}{n}} (-1)^{n-1} \frac{\lambda_{2}n}{P} e^{-\frac{\lambda_{1}\theta_{1} + \lambda_{2}\theta_{0}n}{P}} \sum_{j=0}^{\infty} \frac{(-1)^{j}Q'}{j!} \left(\frac{\lambda_{1}\theta_{0}\theta_{1}}{Q'P}\right)^{j} E_{j}\left(\frac{Q'\lambda_{2}n}{P}\right),$$
(12)

$$J_{2} = \sum_{n=1}^{N} {\binom{N}{n}} (-1)^{n-1} \lambda_{2} n \sqrt{\frac{\theta_{2} \pi}{4\lambda_{1} P}} e^{\frac{\theta_{2}}{4\lambda_{1} P} \left(\lambda_{2} n - \frac{\lambda_{1} Q'}{\theta_{2}}\right)^{2}} \operatorname{erfc}\left(\left(\lambda_{2} n - \frac{\lambda_{1} Q'}{\theta_{2}}\right) \sqrt{\frac{\theta_{2}}{4\lambda_{1} P}} + \frac{Q' + \theta_{0}}{\sqrt{\theta_{2} P/\lambda_{1}}}\right), \quad (13)$$

with $Q = 2^{2R_s}$, Q' = Q - 1, $\theta_0 = \frac{Q(2-\alpha)}{1-\alpha}$, $\theta_1 = \frac{(Q-1)(2-\alpha)}{\alpha}$, and $\theta_2 = \frac{\alpha Q}{1-\alpha}$. Moreover, $E_n(x) = \int_1^{\infty} \frac{e^{-xt}}{t^n} dt$ in Equation (12) is the exponential integral function and $\operatorname{erfc}(\cdot)$ in Equation (13) is the complementary error function [38].

Proof of Theorem 1. Please see Appendix A for the proof. \Box

4.2. Asymptotic Secrecy Outage Probability

In the following, we introduce simple expression for the asymptotic SOP in the high SNR regimes, which is useful in demonstrating the system secrecy diversity order and secrecy array gain.

Theorem 2. The asymptotic high-SNR SOP of the considered system is given by

$$P_{sop} \approx \begin{cases} \frac{\varpi}{P} + \frac{Au}{B\sqrt{P}} - \frac{A^2u^2}{2BP}(1+\omega) &, N = 1\\ \sum_{n=1}^{\lfloor \frac{N}{2} \rfloor} \frac{(-1)^{n+1}}{n!} \left(\frac{\lambda_1\theta_1}{P}\right)^n + \frac{\Theta(N)u^N}{P^{\frac{N}{2}}} &, N \ge 2, \end{cases}$$
(14)

where A = 1.98, B = 1.135, $u = \lambda_2 \sqrt{\frac{\theta_2}{4\lambda_1}}$, $\omega = \frac{\lambda_1 (Q' + 2\theta_0)}{\lambda_2 \theta_2}$, and $\omega = \lambda_1 \theta_1 + \lambda_2 \theta_0 + \lambda_2 Q'$. In (14), when N is an odd number, $\Theta(N) = \frac{AN!}{B(\frac{N}{2} - \frac{1}{2})!}$, while when N is an even number, $\Theta(N) = \frac{A^2 N!}{2B(\frac{N}{2} - 1)!}$. Besides, $\lfloor \cdot \rfloor$ in Equation (14) represents the rounding-down operation.

Proof of Theorem 2. Please see Appendix B for the proof. \Box

Equation (14) implies that the achievable secrecy diversity order and the secrecy array gain of the considered system, for a fixed power allocation (FPA) factor α , can be respectively written as

$$G_d^{FPA} = \min\left(1, \frac{N}{2}\right) = \begin{cases} 1/2 , N = 1 \\ 1 , N \ge 2 \end{cases}$$
(15)

$$G_{c}^{FPA} = \begin{cases} (\frac{A\lambda_{2}\sqrt{\theta_{2}}}{2B})^{-2} , & N = 1\\ (\lambda_{1}\theta_{1} + \frac{A^{2}\lambda_{2}^{2}\theta_{2}}{4B\lambda_{1}})^{-1} , & N = 2\\ (\lambda_{1}\theta_{1})^{-1} , & N > 3 \end{cases}$$
(16)

Remark 1. Recall that, when the relay is trusted, full diversity of 1 can be achieved for the single-user scenario (N = 1) and the diversity order for multiuser scenario $(N \ge 2)$ is unaffected by opportunistic scheduling (OS) [35]. However, when the relay is untrusted, those observations no longer exist.

First, when N = 1, as it is revealed in Equation (15), the AF system with untrusted variable gain relay achieves a secrecy diversity order of $\frac{1}{2}$ in terms of SOP, which is in contrast to full diversity order of 1 in terms of connection outage probability (COP) achieved in trusted AF systems [35]. This result reveals that the existence of relay's eavesdropping will cause some loss of the diversity order (as clarified in Section 2, it is not the application of DJ in untrusted AF networks that results in such a diversity order loss). Intuitively, the diversity order difference between COP and SOP lies in discrepancy between their definitions. Specifically, the concept of SOP jointly characterizes the security and reliability performance, while the COP only evaluate the reliability performance. When the relay is untrusted, the diversity loss becomes the price to satisfy the system secrecy requirement, i.e., avoiding source information intercepted by the untrusted relay. Mathematically, according to Equation (A9) in Appendix A, the external condition $X > \frac{P}{\theta_2}Y^2 - \frac{Q'}{\theta_2}Y$ in J_2 of Equation (A9) will result in a diversity order of 1/2, presenting the probability of not achieving perfect secrecy (i.e., there is some information leakage to untrusted relay R) in single untrusted VGR system.

Furthermore, for the multiuser AF networks (i.e., $N \ge 2$) with OS, the diversity order has been improved from 1/2 up to 1, which implies that the loss of diversity order can be compensated by the OS approach. In particular, the results in Equations (15) and (16) demonstrate the performance gains of employing OS in multiuser untrusted AF relay networks, which is harvested in form of security outage performance improvement, i.e., increased secrecy diversity gain as well as secrecy array gain.

Remark 2. Besides, we can see from Equation (16), although the effect of OS is to increase the array gain as the number of destinations N increases, the array gain becomes saturated, when N increases to a certain extent (i.e., $N \ge 3$). This is because, as N increases, the link quality between the relay and the scheduled user becomes much better than that of the source-relay link. In such case, the secrecy performance will be primarily limited by the quality of the source-relay link. Moreover, while it is generally known that further increasing N leads to array gain saturation (noting that this array gain saturated phenomenon is ubiquitous in conventional trusted multiuser relaying networks when $N \ge 2$ (see [35,39] and references therein)) [35,39] when N = 2 in no secrecy constraint scenario, our results in Equation (16) demonstrate that the array gain enhancement in secrecy constraint scenario is marginal when $N \ge 3$.

4.3. Asymptotic Optimal Power Allocation

We investigate the optimum power allocation in this subsection. For analytical tractability, we choose the asymptotic SOP in Equation (14) as a target function, and, hence, the optimum power allocation aims to minimize the asymptotic SOP by optimally allocating power between the source and the scheduled destination under a total power constraint of *P*. The asymptotic optimal power ratio α^* is presented in the following lemma.

Theorem 3. For sufficiently large SNR (i.e., $P \to \infty$), the asymptotic optimal power allocation factor α^* that minimizes SOP is given by:

$$\alpha^* \approx \frac{1}{1 + \Xi(N)^2 P^{\frac{2-N}{2+N}}},\tag{17}$$

where $\Xi(N) = \left(\frac{N\Theta(N)\beta_2^N}{2\beta_1}\right)^{\frac{1}{N+2}}$ with $\beta_1 = 2\lambda_1 Q'$ and $\beta_2 = \frac{\lambda_2}{2}\sqrt{\frac{Q}{\lambda_1}}$. With the asymptotical OPA derived in Equation (17), the corresponding minimum SOP is given by

$$P_{sop}(\alpha^*) \approx \frac{\beta_1}{2P} + \left(\beta_1 \Xi(N)^2 + \Theta(N) \left(\frac{\beta_2}{\Xi(N)}\right)^N\right) \frac{1}{P^{\frac{2N}{N+2}}}.$$
(18)

As can be observed by Equation (18), the secrecy diversity and array gains of the system with OPA are, respectively, given by

$$G_d^{OPA} = \min\left(1, \frac{2N}{N+2}\right) = \begin{cases} 2/3, N = 1\\ 1, N \ge 2 \end{cases}$$
 (19)

and

$$G_{c}^{OPA} = \begin{cases} \left(\frac{\beta_{2}\Theta(1)}{\Xi(1)}\right)^{-\frac{3}{2}} , N = 1\\ \left(\frac{\beta_{1}}{2} + \beta_{1}\Xi(2)^{2} + \Theta(2)\left(\frac{\beta_{2}}{\Xi(2)}\right)^{2}\right)^{-1} , N = 2\\ \left(\frac{\beta_{1}}{2}\right)^{-1} , N \ge 3. \end{cases}$$
(20)

Proof of Theorem 3. Please see Appendix C. \Box

Remark 3. Note that, in trusted relay systems, OPA scheme does not affect the diversity order, rather it increase only the array gain [31]. Nevertheless, as revealed in Equation (19), the OPA scheme has an impact on the diversity gain of single-user (N = 1) untrusted relay systems. Specifically, by using our proposed OPA scheme, the obtained diversity order can be improved from 1/2 up to 2/3. Thus, significantly secrecy performance improvement can be achieved, as shown in Section 5. Moreover, for multiuser scenario (N \ge 2), the result in Equation (20) confirms that OPA has no impact on the diversity gain due to bottleneck of the source-relay link. Nevertheless, by inspecting Equation (20), we observe that the effect of OPA is to increase the secrecy array gain.

5. Numerical Results and Discussions

In this section, we present some numerical and simulation results to verify our previous theoretical analysis. The simulation results are obtained by performing 5×10^6 random channel realizations. Moreover, the analytical curves obtained by Equation (12) is truncated by the first five terms.

Figure 2 shows the system SOP versus *P* for different values of *N*. The curves are plotted for $\alpha = 0.5$, $\lambda_1 = 0.5$ and $\lambda_2 = 1$. We can see that the analytical approximate SOP results are very close to the simulation results even at low SNR regions, and the asymptotic values match well with the simulations at high SNR regimes. In Figure 2, the achievable secure diversity order of the considered system can be verified to be equal to min(1, N/2). As a result, we can see that the MUD gain is harvested in the form of decreased SOP and increased secrecy diversity order, as *N* increases from 1 to 2. Furthermore, we observe that increasing *N* from 2 to 3 leads to a moderate performance enhancement. This is because, when $N \ge 2$, opportunistic scheduling has no effect on the secrecy diversity order but improves the secrecy array gain. However, as revealed in Equation (16), increasing *N* beyond 3 does not provide an additional array gain. Thus, we can that the curves for N = 3, 4 ($N \ge 3$) overlap each other at sufficiently high SNR. This observation is also demonstrated in Figure 3, from which we can see that the secrecy outage behavior in high SNR regime is stabilized over *N* or λ_2 when $N \ge 3$, while it is only dependent on λ_1 , thus validating the result in Equation (16). However,

for N = 1, 2, we can see in Figure 3 that the secrecy outage performance is determined by both hops, as revealed in Equation (16).



Figure 2. Secrecy outage probability versus *P* for $R_s = 0.1$, $\alpha = 0.5$, $\lambda_1 = 0.5$ and $\lambda_2 = 1$.



Figure 3. The impact of user number *N* and channel gains (λ_1 , λ_2) on the secrecy outage probability when $R_s = 0.1$, $\alpha = 0.5$, P = 40 dB.

Assuming that $\lambda_1 = \lambda_2 = 1$, Figure 4 provides comparisons between the optimal power allocation factor α^* via exhaustive search (minimizing the simulation results of the SOP) and α^* provided by the closed-form expression in Equation (17).

It is clear that the optimal power allocations obtained via exhaustive search match well with those via analytical results, especially in the high SNR region. Moreover, as predicted in Equation (17), we observe that α^* is monotonically decreasing and increasing in *P* for N = 1 and $N \ge 3$, respectively, while α^* tends to be a constant (i.e., $\alpha^* \approx 0.5$ for the considered setting) regardless of *P* for N = 2.

With the α^* obtain in Figure 4, we proceed to compare our proposed OPA scheme with the traditional equal PA (EPA) scheme, i.e., $\alpha = 0.5$, as shown in Figure 5. This figure confirms that the OPA scheme has an obvious SNR advantage over the EPA scheme. For instance, when N = 1 and $P_{out} = 10^{-3}$, OPA provides a significant performance gain as high as 12 dB compared to EPA. This is because the secrecy diversity order is improved from 1/2 (with EPA) to 2/3 (wit OPA). When $N \ge 2$, OPA brings marginal benefits to the array gain. This is because, due to the bottleneck of the first hop, both OPA and EPA schemes achieve the same secrecy diversity order of 1. In particular, the advantage of OPA over EPA in the secrecy outage performance diminishes when $N \ge 3$, as explicitly indicated by the array gain expression in Equation (20).



Figure 4. Comparison between optimal power allocation α^* via exhaustive search and analytical results when $R_s = 0.5$, $\lambda_1 = \lambda_2 = 1$.



Figure 5. SOP comparison: OPA versus EPA, when $R_s = 0.5$, $\lambda_1 = \lambda_2 = 1$.

6. Conclusions

In this paper, we study the secrecy outage probability (SOP) of multiuser relay networks with an untrusted variable-gain relay. The joint destination-based jamming and opportunistic scheduling (DJOS) scheme is employed to harvest multiuser diversity and satisfying security requirement. The performance of the system is evaluated by deriving the SOP approximation as well as its asymptotic expression in closed-form. Analysis of the secrecy diversity order and the impact of number of users provides valuable insights into practical system designs. In particular, we demonstrate that the diversity order loss in single-user untrusted AF networks can be fully compensated by the opportunistic scheduling strategy. Moreover, optimal power allocation (OPA) that minimizes the asymptotic SOP is studied. We prove that OPA can result in a significant performance improvement compared to the conventional equal power allocation scheme without expending external resources.

Acknowledgments: This work was supported by the Key Project of Shaoguan University of China under Grants No. SZ2017KJ08 and No. SZ2016KJ08, and by the Science and Technology Program of Shaoguan City of China under Grant No. SK20157202.

Author Contributions: Fan Ding proposed the original idea and conducted the mathematical analysis. Yongming Zhou provided technical review of the analysis and contributed to the revision of the manuscript. All authors contributed to the write-up of the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Proof of Theorem 1

To simplify notation, we define $X = |h_1|^2$, $Y = |h_M|^2$. Then, we can rewrite Equation (10) as follows

$$P_{sop} \approx \Pr\left\{\frac{1 + P\min\left\{\frac{\alpha}{2-\alpha}X,Y\right\}}{1 + \frac{\alpha X}{(1-\alpha)Y}} < Q\right\}.$$
(A1)

Considering two cases, i.e., $\frac{\alpha X}{2-\alpha} \leq Y$ and $\frac{\alpha X}{2-\alpha} > Y$, and performing some algebraic manipulations, we obtain

$$P_{sop} \approx \underbrace{\Pr\left\{\left(\frac{\alpha P}{2-\alpha} - \frac{Q\alpha}{(1-\alpha)Y}\right) X < Q-1, X \le \frac{2-\alpha}{\alpha}Y\right\}}_{I_1} + \underbrace{\Pr\left\{X > \frac{P(1-\alpha)}{\alpha Q}\left(Y^2 - \frac{Q-1}{P}Y\right), X > \frac{2-\alpha}{\alpha}Y\right\}}_{I_2}.$$
(A2)

Since the first condition $\left(\frac{\alpha P}{2-\alpha} - \frac{Q\alpha}{(1-\alpha)Y}\right) X < Q - 1$ of I_1 in Equation (A2) is always satisfied for $Y < \frac{Q(2-\alpha)}{P(1-\alpha)}$, I_1 can be divided into the following two parts:

$$I_{1} = \Pr\left\{X \leq \frac{2-\alpha}{\alpha}Y, Y \leq \frac{Q(2-\alpha)}{P(1-\alpha)}\right\} + \Pr\left\{X < \min\left(f(Y), \frac{2-\alpha}{\alpha}Y\right), Y > \frac{Q(2-\alpha)}{P(1-\alpha)}\right\},$$
(A3)

where $f(Y) = (Q-1) / \left(\frac{\alpha P}{2-\alpha} - \frac{Q\alpha}{(1-\alpha)Y} \right)$. Moreover, it can be shown that

$$\min\left(f(\mathbf{Y}), \frac{2-\alpha}{\alpha}\mathbf{Y}\right) = \begin{cases} \frac{2-\alpha}{\alpha}\mathbf{Y}, & \frac{Q(2-\alpha)}{P(1-\alpha)} < \mathbf{Y} \le \frac{Q-1}{P} + \frac{Q(2-\alpha)}{P(1-\alpha)}\\ f(\mathbf{Y}), & \mathbf{Y} > \frac{Q-1}{P} + \frac{Q(2-\alpha)}{P(1-\alpha)}. \end{cases}$$
(A4)

For convenience, let $\theta_0 = \frac{Q(2-\alpha)}{1-\alpha}$, $\theta_1 = \frac{(Q-1)(2-\alpha)}{\alpha}$ and Q' = Q-1. Then, substituting Equation (A4) into Equation (A3) yields

$$I_{1} = \Pr\left\{Y \leq \frac{Q' + \theta_{0}}{P}, X \leq \frac{2 - \alpha}{\alpha}Y\right\}$$

+
$$\Pr\left\{Y > \frac{Q' + \theta_{0}}{P}, X < f(Y) = \frac{\theta_{1}Y}{PY - \theta_{0}}\right\}.$$
 (A5)

Similarly, I_2 in Equation (A2) can be rewritten as

$$I_2 = \Pr\left\{X > \max\left(g(Y), \frac{2-\alpha}{\alpha}Y\right)\right\}.$$
 (A6)

where $g(Y) = \frac{P(1-\alpha)}{\alpha Q} \left(Y^2 - \frac{Q'}{P}Y\right)$. It can be deduced that

$$\max\left(g(Y), \frac{2-\alpha}{\alpha}Y\right) = \begin{cases} \frac{2-\alpha}{\alpha}Y, & 0 < Y \leq \frac{Q'+\theta_0}{P}\\ g(Y), & Y > \frac{Q'+\theta_0}{P} \end{cases}.$$
 (A7)

Denoting $\theta_2 = \frac{\alpha Q}{1-\alpha}$ and substituting Equation (A7) into Equation (A6) yields

$$I_{2} = \Pr\left\{Y \leq \frac{Q' + \theta_{0}}{P}, X > \frac{2 - \alpha}{\alpha}Y\right\} + \Pr\left\{Y > \frac{Q' + \theta_{0}}{P}, X > \frac{P}{\theta_{2}}Y^{2} - \frac{Q'}{\theta_{2}}Y\right\}.$$
(A8)

Substituting Equations (A5) and (A8) into Equation (A2), and after some involved simplifications, we arrive at

$$P_{sop} \approx 1 - \underbrace{\Pr\left\{Y \ge \frac{Q' + \theta_0}{P}, X \ge \frac{\theta_1 Y}{PY - \theta_0}\right\}}_{J_1} + \underbrace{\Pr\left\{Y \ge \frac{Q' + \theta_0}{P}, X > \frac{P}{\theta_2}Y^2 - \frac{Q'}{\theta_2}Y\right\}}_{J_2}$$
(A9)

In the following, we will use Equation (A9) to derive the approximate SOP expression in closed-form, which will significantly reduce the computational complexity, as compared to solve Equations (A5) and (A8) separately. More importantly, this simplification will greatly reduce the complexity in the asymptotic analysis for the SOP in high SNR regions. For Rayleigh fading, X and Y are independent random variables with the probability density functions (PDFs) given, respectively, by $f_X(x) = \lambda_1 e^{-\lambda_1 x}$ and $f_Y(y) = \sum_{n=1}^N {\binom{N}{n}} (-1)^{n-1} \lambda_2 n e^{-\lambda_2 n y}$. In the following, we focus on deriving the exact expressions of J_1 and J_2 in Equation (A9), respectively.

Appendix A.1. Derivation of J_1 in Equation (12):

Since X and Y are independent exponential random variables, J_1 in Equation (A9) can be calculated by:

$$J_{1} = \sum_{n=1}^{N} {\binom{N}{n}} (-1)^{n-1} \lambda_{2} n \int_{\frac{Q-1+\theta_{0}}{P}}^{\infty} e^{-\lambda_{2} n y - \frac{\lambda_{1} \theta_{1} y}{Py-\theta_{0}}} dy$$

$$\stackrel{(a)}{=} \sum_{n=1}^{N} {\binom{N}{n}} (-1)^{n-1} \frac{\lambda_{2} n}{P} e^{-\frac{\lambda_{2} \theta_{0} n+\lambda_{1} \theta_{1}}{P}} \int_{\frac{Q'}{P}}^{\infty} e^{-\frac{\lambda_{2} n}{P} t - \frac{\lambda_{1} \theta_{0} \theta_{1}}{Pt}} dt,$$
(A10)

where Step (a) is obtained by making the change of variable $t = Py - \theta_0$ within the integral. Then, after using the Taylor series expression for $e^{-\frac{\lambda_1 \theta_0 \theta_1}{Pt}}$ in Equation (A10), and along with the help of Equation 5.1.4 in [38], we get J_1 as in Equation (12).

Appendix A.2. Derivation of J_2 in Equation (13):

Similarly, we can evaluate J_2 in Equation (A9) as

$$J_{2} = \sum_{n=1}^{N} \binom{N}{n} (-1)^{n-1} \lambda_{2n} \int_{\frac{Q'+\theta_{0}}{P}}^{\infty} e^{-\lambda_{2}ny - \frac{\lambda_{1}P}{\theta_{2}} \left(y^{2} - \frac{Q'}{P}y\right)} dy$$

$$= \sum_{n=1}^{N} \binom{N}{n} (-1)^{n-1} \lambda_{2n} e^{\frac{\theta_{2}}{4\lambda_{1}P} \left(\lambda_{2}n - \frac{\lambda_{1}Q'}{\theta_{2}}\right)^{2}}$$

$$\times \int_{\frac{Q'+\theta_{0}}{P}}^{\infty} e^{-\frac{\lambda_{1}P}{\theta_{2}} \left(y + \frac{\theta_{2}}{2\lambda_{1}P} \left(\lambda_{2}n - \frac{\lambda_{1}Q'}{\theta_{2}}\right)\right)^{2}} dy.$$
(A11)

By setting $y + \frac{\theta_2}{2\lambda_1 P} \left(\lambda_2 n - \frac{\lambda_1(Q-1)}{\theta_2}\right) = t$, using Equation 3.322.1 in [38], and then after some mathematical manipulations, we get J_2 as presented in Equation (13).

Appendix B. Proof of Theorem 2

To proceed, we put forth the following three properties for the sums of binomial coefficients, which play key roles in our derivation. Specifically, with the binomial theorem and the help of Equation 0.154 in [38], it is not difficult to obtain the following three properties for the sums of binomial coefficients:

$$\sum_{n=1}^{N} \binom{N}{n} (-1)^{n-1} (n+a)^k = \begin{cases} a^k & , \ 1 \le k < N \\ a^N + (-1)^{N-1} N! & , \ k = N \end{cases}$$
(A12)

$$\sum_{n=1}^{N} \binom{N}{n} (-1)^{n-1} (n+a)^{k} n^{j} = \begin{cases} 0, & 1 \le k+j < N, j \ge 1 \\ (-1)^{N-1} N!, & k+j = N \end{cases}$$
(A13)

$$\sum_{n=1}^{N} \binom{N}{n} (-1)^{n-1} n(n+a)^{k} (n+a)^{j} = \begin{cases} 0, & 1 \le k+j+1 \le N-1 \\ (-1)^{N-1} N!, & k+j+1 = N. \end{cases}$$
(A14)

As shown in Equation (11), the SOP can be expressed as $P_{sop} = 1 - J_1 + J_2$. In the following, the asymptotic studies of J_1 in Equation (12) and J_2 in Equation (13) are carried out individually.

Appendix B.1. Asymptotic analysis of J_1 in Equation (12)

By applying series expansion of exponential functions, J_1 in Equation (12) can be rewritten as follows:

$$J_{1} = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \frac{(-1)^{i+j} \lambda_{2} (\lambda_{1} \theta_{1} + \lambda_{2} \theta_{0})^{i} (\lambda_{1} \theta_{0} \theta_{1})^{j}}{i! j! Q^{j-1} P^{i+j+1}}$$

$$\times \sum_{n=1}^{N} \binom{N}{n} (-1)^{n-1} \mathbb{E}_{n} \left(\frac{Q' \lambda_{2} n}{P}\right).$$
(A15)

To facilitate the asymptotic analysis, we further separate J_1 in Equation (A15) into a sum of three terms, i.e., $J_1 = J_{11} + J_{12} + J_{13}$, where J_{1i} , i = 1, 2, 3 are defined as follows.

Specifically, when i = 0, j = 0, we have

$$J_{11} = \sum_{n=1}^{N} \binom{N}{n} (-1)^{n-1} \frac{\lambda_2 n Q'}{P} \mathbf{E}_0 \left(\frac{\lambda_2 Q' n}{P}\right).$$
(A16)

When $j = 0, i \ge 1$, we have

$$J_{12} = \sum_{i=1}^{\infty} \frac{(-1)^i \lambda_2 Q'}{i! P^{i+1}} \sum_{n=1}^N \binom{N}{n} (-1)^{n-1} n$$

$$\times (\lambda_2 \theta_0 n + \lambda_1 \theta_1)^i \mathcal{E}_0 \left(\frac{\lambda_2 Q' n}{P}\right).$$
(A17)

When $i \ge 0, j \ge 1$, we have

$$J_{13} = \sum_{i=0}^{\infty} \sum_{j=1}^{\infty} \frac{(-1)^{i+j} (\lambda_1 \theta_0 \theta_1)^j \lambda_2}{i! j! Q'^{j-1} P^{i+j+1}} \sum_{n=1}^N \binom{N}{n} (-1)^{n-1} \times (\lambda_2 \theta_0 n + \lambda_1 \theta_1)^i \mathcal{E}_j \left(\frac{\lambda_2 Q' n}{P}\right).$$
(A18)

(i) For J_{11} , using the fact that $E_0(z) = e^{-z}/z$ and the Taylor series expression of exponential function within $E_0(z)$: $\exp(-z) = \sum_{r=0}^{\infty} (-1)^r z^r / r!$, J_{11} can be approximated as

$$J_{11} = 1 + \sum_{r=1}^{\infty} \frac{(-1)^r (\lambda_2 Q')^r}{r! P^r} \sum_{n=1}^N \binom{N}{n} (-1)^{n-1} n^r$$

$$\stackrel{(a)}{\approx} 1 - \frac{(\lambda_2 Q')^N}{P^N},$$
(A19)

where Step (a) is carried out by using Equation (A12) and discarding the higher order terms of P^{-N} in the first equation of Equation (A19).

(ii) For J_{12} , taking the similar steps as the approximation for J_{11} , we can rewrite J_{12} as follows

$$J_{12} = \sum_{i=1}^{\infty} \frac{(-1)^{i} (\lambda_{2}\theta_{0})^{i}}{i!P^{i+1}} \sum_{n=1}^{N} \binom{N}{n} (-1)^{n-1} \left(n + \frac{\lambda_{1}\theta_{1}}{\lambda_{2}\theta_{0}}\right)^{i} + \sum_{i=1}^{\infty} \sum_{r=1}^{\infty} \frac{(-1)^{i+r} (\lambda_{2}\theta_{0})^{i} (\lambda_{2}Q')^{r}}{i!r!P^{i+r}} \sum_{n=1}^{N} \binom{N}{n} (-1)^{n-1} \left(n + \frac{\lambda_{1}\theta_{1}}{\lambda_{2}\theta_{0}}\right)^{i} n^{r}.$$
(A20)

Applying the properties in Equations (A12) and (A13) for the first and the second terms of Equation (A20), respectively, and discarding the higher order terms with $P^{-(N+1)}$, we can approximated J_{12} as follows

$$J_{12} \approx \sum_{i=1}^{N} \frac{(-1)^{i} (\lambda_{1} \theta_{1})^{i}}{i! P^{i}} - \frac{(\lambda_{2} \theta_{0} + \lambda_{2} (Q-1))^{N}}{P^{N}}.$$
 (A21)

(iii) For J_{13} , consider the following infinite series expansions: $E_j(z)$ can be expanded as $E_j(z) = \frac{(-1)^{j-1}z^{j-1}}{(j-1)!} [\varphi(j) - \ln(z)] - \sum_{k=0, k \neq j-1}^{\infty} \frac{(-z)^k}{(k-j+1)k!}$ for $j \ge 1$ [40], and $\ln(x) = \sum_{r=1}^{\infty} (-1)^{k-1} (x-1)^k / k$ for 0 < x < 1, where $\varphi(\cdot)$ is the digmama function [38]. Then, we can expand J_{13} as follows

$$J_{13} = \sum_{i=0}^{\infty} \sum_{j=1}^{\infty} \frac{(-1)^{i+j} (\lambda_1 \theta_1)^j (\lambda_2 \theta_0)^{i+j} \varphi(j)}{i! j! (j-1!) P^{i+j+1}} \\ \times \sum_{n=1}^{N} {N \choose n} (-1)^{n-1} (n + \frac{\lambda_1 \theta_1}{\lambda_2 \theta_0})^i n^j \\ - \sum_{i=0}^{\infty} \sum_{j=1}^{\infty} \sum_{r=1}^{\infty} \sum_{s=0}^{r} {r \choose s} \frac{(-1)^{i+2j+2r-s} (\lambda_1 \theta_1)^j}{i! j! (j-1)! r} \\ \times \frac{(\lambda_2 \theta_0)^{i+j} (\lambda_2 Q')^{s-1}}{P^{i+j+s+1}} \sum_{n=1}^{N} {N \choose n} (-1)^{n-1} (n + \frac{\lambda_1 \theta_1}{\lambda_2 \theta_0})^i n^{j+s} \\ - \sum_{i=0}^{\infty} \sum_{j=1}^{\infty} \sum_{\substack{k=0, \\ k\neq j-1}}^{\infty} \frac{(-1)^{i+j+k} (\lambda_1 \theta_1)^j (\lambda_2 \theta_0)^{i+j}}{i! j! k! (k-j+1) P^{i+j+k+1}} \\ \times \sum_{n=1}^{N} {N \choose n} (-1)^{n-1} (n + \frac{\lambda_1 \theta_1}{\lambda_2 \theta_0})^i n^{k+1}.$$
(A22)

Compared with the expression of J_{13} in Equation (A18), the expanded form of J_{13} shown in Equation (A22) is more complicated. However, with the help of Equation (A22), we can easily determine the highest order of J_{13} . Specifically, utilizing the properties in Equations (A12) and (A13) again, we can conclude that all three terms in Equation (A22) are at the order of $P^{-(N+1)}$ at high SNR regimes and hence the following conclusion can be obtained

$$J_{13} \to P^{-(N+1)}$$
. (A23)

Finally, combining Equations (A19), (A21) and (A23), J_1 in Equation (12) can be approximated as follows:

$$J_1 \approx 1 + \sum_{i=1}^{N} \frac{(-1)^i (\lambda_1 \theta_1)^i}{i! P^i} - \frac{\lambda_2^N ({Q'}^N + (\theta_0 + Q')^N)}{P^N}.$$
 (A24)

Appendix B.2. Asymptotic analysis of J_2 in Equation (13)

For ease of exposition, let $u = \lambda_2 \sqrt{\frac{\theta_2}{4\lambda_1}}$, $v = \frac{\lambda_1 Q'}{\lambda_2 \theta_2}$, and $\omega = \frac{\lambda_1 (Q' + 2\theta_0)}{\lambda_2 \theta_2}$. Then, we rewrite Equation (13) as

$$J_{2} = \sum_{n=1}^{N} {\binom{N}{n}} (-1)^{n-1} \frac{n\sqrt{\pi u}}{\sqrt{P}} e^{\frac{u^{2}}{P}(n-v)^{2}} \operatorname{erfc}\left(\frac{u}{\sqrt{P}}(n+\omega)\right).$$
(A25)

Using the tight approximation $\operatorname{efrc}(x) \approx \frac{(1-e^{-Ax})e^{-x^2}}{B\sqrt{\pi x}}$ [41] with A = 1.98, B = 1.135, and by applying series expansion of exponential functions, we get $\operatorname{efrc}(x) \approx \frac{A(1-\frac{Ax}{2})}{B\sqrt{\pi}}$. Using this approximation for $\operatorname{erfc}(x)$ and the series expansion of $e^{\frac{u^2}{P}(n-v)^2}$ in Equation (A25), J_2 in Equation (A25) can be approximated, after some careful manipulations, as

$$J_2 = J_{21} - J_{22}, \tag{A26}$$

where

$$J_{21} = \frac{A}{B} \sum_{i=0}^{\infty} \frac{u^{2i+1}}{i!P^{i+1/2}} \sum_{n=1}^{N} \binom{N}{n} (-1)^{n-1} n(n-v)^{2i},$$
(A27)

$$J_{22} = \frac{A^2}{2B} \sum_{i=0}^{\infty} \frac{u^{2i+2}}{i!P^{i+1}} \sum_{n=1}^{N} \binom{N}{n} (-1)^{n-1} n(n+!)(n-v)^{2i}.$$
 (A28)

For N = 1, we have

$$J_2 \stackrel{(a)}{\approx} \frac{Au}{B\sqrt{P}} - \frac{A^2 u^2}{2BP} (1+\omega), \tag{A29}$$

where Step (a) is carried out by substituting i = 0 into the expressions for J_{21} and J_{22} , respectively, and then discarding the higher order terms of P^{-1} .

For $N \ge 2$, we should consider two cases: (1) N is an odd number; and (2) N is an even number. First, consider the case when N is an even number. Utilizing the properties in Equations (A12) and (A13), we can see that the dominant factor in J_{21} is the term with $i = \frac{N-1}{2}$, which implies $J_{21} \rightarrow P^{-\frac{N+1}{2}}$. On the other hand, when N is an odd number, the dominant factor of J_{21} is at the order of $P^{-\frac{N}{2}}$. Noting these facts, we can asymptotically express J_{21} as follows:

$$J_{21} \approx \begin{cases} \frac{A(-1)^{N-1}N!u^{N}}{B(\frac{N}{2}-\frac{1}{2})!P^{\frac{N}{2}}}, & N \text{ is an odd number} \\ \\ \frac{1}{P^{\frac{N}{2}+\frac{1}{2}}} + o(\frac{1}{P^{\frac{N}{2}+\frac{1}{2}}}), & N \text{ is an even number.} \end{cases}$$
(A30)

Similarly, using Equation (A14), we can approximate J_{22} as follows

$$J_{22} \approx \begin{cases} \frac{1}{p^{\frac{N}{2}+1}} + o(\frac{1}{p^{\frac{N}{2}+1}}), & N \text{ is an odd number} \\ \\ \frac{A^{2}(-1)^{N-1}N!u^{N}}{2B(\frac{N}{2}-1)!p^{\frac{N}{2}}}, & N \text{ is an even number.} \end{cases}$$
(A31)

Combining Equations (A30) and (A31), and discarding the higher order terms of $P^{-\frac{N}{2}}$, the asymptotic expression of J_2 for $N \ge 2$ can be obtained as

$$J_{2} \approx \begin{cases} \frac{A(-1)^{N-1}N!u^{N}}{B\left(\frac{N}{2}-\frac{1}{2}\right)!P^{\frac{N}{2}}}, & N \text{ is an odd number} \\ \\ \frac{A^{2}(-1)^{N-1}N!u^{N}}{2B\left(\frac{N}{2}-1\right)!P^{\frac{N}{2}}}, & N \text{ is an even number.} \end{cases}$$
(A32)

Finally, substituting Equations (A24), (A29) and (A32) into Equation (11), we can obtain the asymptotic SOP expression as in Equation (14).

Appendix C. Proof of Theorem 3

By applying the change of variable $\alpha = \frac{1}{1+t^2}$ ($t \ge 0$) and after performing some manipulations, we rewrite Equation (14) as

$$P_{sop}(t) \approx \begin{cases} \frac{\beta_1}{P} t^2 + \left(\frac{\beta_2}{\sqrt{P}}\right)^N \frac{\Theta(N)}{t^N} + \frac{\Delta_1}{P} \frac{1}{t^2} + \frac{\Delta_2}{P} &, N = 1\\ \frac{\beta_1}{P} t^2 + \left(\frac{\beta_2}{\sqrt{P}}\right)^N \frac{\Theta(N)}{t^N} + \frac{\beta_1}{2P} &, N = 2,3\\ \frac{\beta_1}{P} t^2 + \left(\frac{\beta_2}{\sqrt{P}}\right)^N \frac{\Theta(N)}{t^N} + \frac{\beta_1}{2P} + \sum_{n=2}^{\lfloor \frac{N}{2} \rfloor} \frac{(-1)^{n+1}}{n!} \left(\frac{\beta_1}{2P}\right)^n (2t^2 + 1)^n , N \ge 4 \end{cases}$$
(A33)

where $\Delta_1 = Q\lambda_2 \left(1 - \frac{A^2\lambda_2}{8B\lambda_1} - \frac{A^2}{4B}\right)$ and $\Delta_2 = \lambda_2 Q + (\lambda_2 - \lambda_1) Q' + \frac{A^2\lambda_2}{8B} (\lambda_2 Q - (3Q - 1))$. Unfortunately, it is still difficult to obtain a closed-form solution for the optimal value of *t*, i.e., *t*^{*},

that minimizes the asymptotic SOP in Equation (A33). Rather than resort to the numerical method to obtain t^* , we present a simple closed-form suboptimal solution for t^* (i.e., α^*) in the following. To do this, we further simplify the asymptotic SOP in Equation (A33) as follows:

$$P_{sop}(t) \approx \frac{\beta_1}{P} t^2 + \Theta(N) \left(\frac{\beta_2}{\sqrt{P}}\right)^N \frac{1}{t^N} + \frac{\xi}{P}, \text{ for } N \ge 1,$$
(A34)

where $\xi = \Delta_2$ for N = 1, otherwise, $\xi = \beta_1/2$ (i.e., for $N \ge 2$). The rationality for Equation (A34) runs as follows.

We notice from Equation (A33) that $P_{sop}(t) \stackrel{P \to \infty}{\approx} \frac{\Theta(1)\beta_2}{\sqrt{P}} \frac{1}{t}$ for N = 1, which decreases monotonically with *t*. In this context, to minimize $P_{sop}(t)$ for N = 1 in Equation (A33), we should let $t^* \to \infty$ (i.e., $\alpha^* \to 0$), which implies

$$\lim_{\substack{P \to \infty \\ *^2 \to \infty}} \frac{\frac{\Delta_1}{P} \frac{1}{t^{*2}}}{\frac{\beta_1}{P} t^{*2}} = \lim_{t^* \to \infty} \frac{\Delta_1}{\beta_1 t^{*4}} = 0.$$
(A35)

Equation (A35) demonstrates that, when solving the the optimal value of t (t^*) to minimize the SOP of N = 1 in Equation (A33), the third term $\frac{\Delta_1}{P} \frac{1}{t^2}$ in Equation (A33) has little impact on t^* as compared to the first term $\frac{\beta_1}{P}t^2$ when $P \to \infty$, thus it can be ignored. Similarly, when $N \ge 4$, we notice from Equation (A33) that $P_{sop}(t) \approx \frac{\beta_1}{2P}t^2 + \frac{\beta_1}{2P}$, which increase monotonically with t. Therefore, we have $t^* \to 0$ (i.e., $\alpha^* \to 1$), which is also verified in Figure 4. Therefore, the fourth term in Equation (A33) with $N \ge 4$, i.e., $\sum_{n=2}^{\lfloor \frac{N}{2} \rfloor} \frac{(-1)^{n+1}}{n!} \left(\frac{\beta_1}{2P}\right)^n (2t^2 + 1)^n$ can be ignored as compared to the first term and the second term in Equation (A33) with $N \ge 4$. With the above facts, the SOP in Equation (A33) can be further simplified by an unified form, as shown in Equation (A34).

In the following, we use Equation (A34) to determine the asymptotic OPA. Since the term ξ in Equation (A34) is not a function of t, it is sufficient to minimize the following function G(t) to optimize the asymptotic SOP

$$G(t) = \frac{\beta_1}{P} t^2 + \Theta(N) \left(\frac{\beta_2}{\sqrt{P}}\right)^N \frac{1}{t^N}.$$
(A36)

By setting the first order derivation of Equation (A36) as zero, i.e., $\frac{\partial G(t)}{\partial t} = \frac{2\beta_1}{P}t - \left(\frac{\beta_2}{\sqrt{P}}\right)^N \frac{N\Theta[N]}{t^{N+1}} = 0$, we get $t^* = \Xi[N]P^{\frac{2-N}{2(2+N)}}$, where $\Xi[N]$ is given in Equation (17). Using $\alpha = \frac{1}{1+t^2}$, we can obtain the closed-form expression for α^* as in Equation (17). Moreover, substituting Equation (17) into Equation (A33), and performing algebraic manipulations, the asymptotical minimum SOP can be derived as in Equation (18).

References

- Koyluoglu, O.O.; Koksal, C.E.; Gamal, H.E. On secrecy capacity scaling in wireless networks. *IEEE Trans. Inf. Theory* 2012, 58, 3000–3015.
- 2. Ding, Z.; Leung, K.K.; Goeckel, D.L.; Towsley, D. On the application of cooperative transmission to secrecy communications. *IEEE J. Sel. Areas Commun.* **2012**, *30*, 359–368.

- 3. Fan, L.; Yang, N.; Duong, T.Q.; Elkashlan, M.; Karagiannidis, G.K. Exploiting Direct Links for Physical Layer Security in Multiuser Multirelay Networks. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 3856–3867.
- 4. Hoang, T.M.; Duong, T.Q.; Suraweera, H.A. Cooperative beamforming and user selection for improving the security of relay-aided systems. *IEEE Trans. Wirel. Commun.* **2015**, *63*, 5039–5051.
- 5. Krikidis, I.; Thompson, J.S.; McLaughlin, S. Relay selection for secure cooperative networks with jamming. *IEEE Trans. Wirel. Commun.* **2009**, *8*, 5003–5011.
- 6. Huang, J.; Swindlehurst, A.L. Cooperative jamming for secure communications in MIMO relay networks. *IEEE Signal Process. Lett.* **2011**, *59*, 4871–4884.
- 7. Dong, L.; Han, Z.; Petropulu, A.; Poor, H.V. Improving wireless physical layer security via cooperating relays. *IEEE Trans. Signal Process.* **2010**, *58*, 1875–1888.
- 8. Ding, Z.; Leung, K.K.; Goeckel, D.L. Opportunistic relaying for secrecy communications: Cooperative jamming vs. relay chatting. *IEEE Trans. Wirel. Commun.* **2011**, *10*, 1725–1729.
- 9. Liu, Y.; Li, J.; Petropulu, A.P. Destination assisted cooperative jamming for wireless physical-layer security. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 682–694.
- 10. Deng, H.; Wang, H.M.; Guo, W. Secrecy transmission with a helper: To relay or to jam. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 293–307.
- 11. Wang, H.M.; Luo, M.; Xia, X.G. Joint cooperative beamforming and jamming to secure AF relay systems with individual power constraint and no eavesdropper's CSI. *IEEE Signal Process. Lett.* **2013**, *20*, 39–42.
- 12. Wang, C.; Wang, H.M.; Xia, X.G. Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks. *IEEE Trans. Wirel. Commun.* **2015**, *14*, 589–605.
- 13. Park, K.; Wang, T.; Alouini, M. On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 1741–1750.
- 14. Jeong, C.; Kim, I.M.; Kim, D.I. Joint secure beamforming design at the source and the relay for an amplify-and-forward MIMO untrusted relay system. *IEEE Trans. Signal Process.* **2012**, *60*, 310–325.
- 15. Mo, J.; Tao, M.; Liu, Y. Secure beamforming for MIMO two-way communications with an untrusted relay. *IEEE Signal Process. Lett.* **2014**, *62*, 2185–2199.
- 16. He, X.; Yener, A. Cooperation with an untrusted relay: A secrecy perspective. *IEEE Trans. Inf. Theory* **2014**, *56*, 3807–3827.
- 17. Sun, L.; Zhang, T.; Li, Y.; Niu, H. Performance study of two-hop amplify-and-forward systems with untrustworthy relay nodes. *IEEE Trans. Veh. Technol.* **2012**, *61*, 3801–3807.
- 18. Ju, M.C.; Kim, D.H.; Hwang, K.S. Opportunistic transmission of nonregenerative network with untrusted relay. *IEEE Trans. Veh. Technol.* **2015**, *64*, 2703–2709.
- 19. Hu, H.; Gao, Z.; Liao, X. Secure Communications in CIoT Networks with a Wireless Energy Harvesting Untrusted Relay. *Sensors* 2017, *17*, 2023.
- 20. Zhang, S.; Fan, L.; Peng, M.; Vincent Pooret, H. Near-optimal modulo-and-forward scheme for the untrusted relay channel. *IEEE Trans. Inf. Theory* **2016**, *62*, 2545–2556.
- 21. Xiong, J.; Cheng, L.; Ma, D. Destination aided cooperative jamming for dual-hop amplify-and-forward MIMO untrusted relay systems. *IEEE Trans. Veh. Technol.* **2016**, *65*, 7274–7284.
- 22. Huang, J.; Mukherjee, A.; Swindlehurst, A.L. Secure communication via an untrusted non-regenerative relay in fading channels. *IEEE Trans. Signal Process.* **2013**, *61*, 2536–2550.
- 23. Wang, W.; Teh, K.C.; Li, K.H. Relay Selection for Secure Successive AF Relaying Networks With Untrusted Nodes. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 2466–2476.
- 24. Ding, F.; Wang, H.; Zhang, S. Multiuser untrusted relay networks with joint cooperative jamming and opportunistic scheduling under perfect and outdated CSI. *Electron. Lett.* **2016**, *52*, 1925–1927.
- 25. Kalamkar, S.S.; Banerjee, A. Secure communication via a wireless energy harvesting untrusted relay. *IEEE Trans. Veh. Technol.* **2017**, *66*, 2199–2213.
- 26. Kim, J.B.; Lim, J.; Cioff, J.M. Capacity scaling and diversity order for secure cooperative relaying with untrustworthy relays. *IEEE Trans. Wirel. Commun.* **2015**, *14*, 3866–3876.
- 27. Wang, L.; Elkashlan, M.; Huang, J.; Tran, N.H.; Duong, T.Q. Secure transmission with optimal power allocation in untrusted relay networks. *IEEE Wirel. Commun. Lett.* **2014**, *3*, 289–292.
- 28. Kuhestani, A.; Mohammadi, A.; Noori, M. Optimal power allocation to improve secrecy performance of non-regenerative cooperative systems using an untrusted relay. *IET Commun.* **2016**, *10*, 962–968.

- 29. Yao, R.; Xu, F.; Mekkawy, T. Optimised power allocation to maximise secure rate in energy harvesting relay network. *Electron. Lett.* **2016**, *52*, 1879–1881.
- Kim, S.I.; Kim, I.M.; Heo, J. Secure transmission for multiuser relay networks. *IEEE Trans. Wirel. Commun.* 2015, 14, 3724–3737.
- 31. Ikki, S.S.; Aissa, S. A study of optimization problem for amplify-and-forward relaying over Weibull fading channels with multiple antennas. *IEEE Commun. Lett.* **2011**, *15*, 1148–1151.
- 32. Zhang, S.; Liew, S.; Lam, P. Hot topic: Physical-layer network coding. In Proceedings of the ACM Mobicom, Dresden, Germany, 23–29 September 2006; pp. 1–5.
- 33. Popovski, P.; Yomo, H. Wireless network coding by amplify-and-forward for bi-directional traffic flows. *IEEE Commun. Lett.* **2007**, *11*, 16–18.
- 34. Liu, P.; Kim, I.M. Performance analysis of bidirectional communication protocols based on decode-and-forward relaying. *IEEE Trans. Commun.* **2010**, *58*, 2683–2696.
- 35. Yang, N.; Elkashlan, M.; Yuan, J. Outage probability of multiuser relay networks in Nakagami-m fading channels. *IEEE Trans. Veh. Technol.* **2010**, *59*, 2120–2132.
- 36. Singh, K.; Gupta, A.; Ratnarajah, T.; Ku, M.-L. A General Approach Toward Green Resource Allocation in Relay-Assisted Multiuser Communication Networks. *IEEE Trans. Wirel. Commun.* **2018**, *17*, 848–862.
- 37. Singh, K.; Gupta, A.; Ratnarajah, T. QoS-driven resource allocation and EE-balancing for multiuser two-way amplify-and-forward relay networks. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 3189–3204.
- Gradshteyn, I.S.; Ryzhik, I.M. Table of Integrals, Series, and Products, 7th ed.; Academic Press: New York, NY, USA, 2007.
- 39. Hemachandra, K.T.; Beaulieu, N.C. Outage analysis of opportunistic scheduling in dual-hop multiuser relay networks in the presence of interference. *IEEE Trans. Commun.* **2013**, *61*, 1786–1796.
- 40. Abramowitz, M.; Stegun, I.A. *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, 7th ed.; Dover: Mineola, NY, USA, 1972.
- 41. Karagiannidis, G.K.; Lioumpas, A.S. An improved approximation for the Gaussian Q-function. *IEEE Commun. Lett.* **2007**, *11*, 644–646.



© 2018 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).