electronics

MDPI

Article

Secrecy and Throughput Performance of Cooperative Cognitive Decode-and-Forward Relaying Vehicular Networks with Direct Links and Poisson Distributed Eavesdroppers

Fan Wang [1], Cuiran Li [1,*], Jianli Xie [1], Lin Su [1], Yadan Liu [2,*] and Shaoyi Du [3]

[1] School of Electronic and Information Engineering, Lanzhou Jiaotong University, Lanzhou 730070, China; wangfan@lzjtu.edu.cn (F.W.); xiejl@mail.lzjtu.cn (J.X.); 12221856@stu.lzjtu.edu.cn (L.S.)
[2] School of Physics and Mechanical and Electrical Engineering, Longyan University, Longyan 364012, China
[3] Institute of Artificial Intelligence and Robotics, College of Artificial Intelligence, Xi'an Jiaotong University, Xi'an 710049, China; dushaoyi@xjtu.edu.cn
* Correspondence: licr@mail.lzjtu.cn (C.L.); 82009061@lyun.edu.cn (Y.L.)

Abstract: Cooperative communication and cognitive radio can effectively improve spectrum utilization, coverage range, and system throughput of vehicular networks, whereas they also incur several security issues and wiretapping attacks. Thus, security and threat detection are vitally important for such networks. This paper investigates the secrecy and throughput performance of an underlay cooperative cognitive vehicular network, where a pair of secondary vehicles communicate through a direct link and the assistance of a decode-and-forward (DF) secondary relay in the presence of Poisson-distributed colluding eavesdroppers and under an interference constraint set by the primary receiver. Considering mixed Rayleigh and double-Rayleigh fading channels, we design a realistic relaying transmission scheme and derive the closed-form expressions of secrecy and throughput performance, such as the secrecy outage probability (SOP), the connection outage probability (COP), the secrecy and connection outage probability (SCOP), and the overall secrecy throughput, for traditional and proposed schemes, respectively. An asymptotic analysis is further presented in the high signal-to-noise ratio (SNR) regime. Numerical results illustrate the impacts of network parameters on secrecy and throughput and reveal that the advantages of the proposed scheme are closely related to the channel gain of the relay link compared to the direct link.

Keywords: cooperative cognitive vehicular networks; physical-layer security; throughput; secrecy outage probability

Citation: Wang, F.; Li, C.; Xie, J.; Su, L.; Liu, Y.; Du, S. Secrecy and Throughput Performance of Cooperative Cognitive Decode-and-Forward Relaying Vehicular Networks with Direct Links and Poisson Distributed Eavesdroppers. *Electronics* **2024**, *13*, 777. https://doi.org/10.3390/electronics13040777

Academic Editors: Jianji Wang and Meng Yang

Received: 22 December 2023
Revised: 4 February 2024
Accepted: 8 February 2024
Published: 16 February 2024

1. Introduction

1.1. Background and Motivation

With the enormous number of cars and growing application of fifth-generation (5G) communication technologies, the Internet of Vehicles (IoV) has become one of the critical wireless networks and aims to establish and maintain a reliable and intelligent transportation system by connecting pedestrians and vehicles along with roadside units (RSUs). A vehicular ad hoc network (VANET), as a key component of the IoV, is envisaged and deployed to facilitate traffic management by enhancing passenger safety, providing entertainment information, etc. There are mainly three communication modes in the VANET, i.e., vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and hybrid vehicle communication (HVC), including both V2V and V2I. Due to the mobility of vehicles and limited coverage of RSU, V2V and V2I links are intermittently connected and disconnected, causing many problems such as unreliability, continual handoff, and low throughput. Cooperative communication, which provides diversity gain by introducing relays, has been proven to be an effective compensation technology and has been widely used and analyzed in the VANET [1–3].

On the other hand, with the ever-growing demands of vehicular wireless services, the problem of spectrum scarcity in vehicular networks has become more serious [4]. In order to alleviate this problem and pursue green communication, cognitive radio (CR) has been introduced as a promising technology to address the conflict between spectrum scarcity and spectrum underutilization. In CR networks, unlicensed secondary users (SUs) are allowed to dynamically access the licensed spectrum with the requirement of not interfering with the primary users (PUs). In general, according to the different spectrum access strategies, there are mainly two paradigms of CR networks, i.e., overlay CR and underlay CR; the former allows SUs to transmit data by sensing the spectrum holes of PUs, and the latter enables SUs to utilize the licensed spectrum simultaneously with PUs while guaranteeing the interference at PUs does not exceed the acceptable threshold. Comprehensively, coupling CR with cooperative vehicular networks can be an effective and efficient solution for better spectrum utilization, connectivity, and reliability [5].

However, every coin has two sides. The introduction of CR is not without drawbacks. In the underlay CR, the coexistence of licensed and unlicensed users on the same network leads to several security issues and privacy attacks, such as eavesdropping over a wiretap channel shown in Figure 1. This not only makes the network structure more complex by introducing additional interference links between secondary transmitters (SU-Tx) and primary receivers (PU-Rx) and bringing the dependence in channel gains of the instantaneous end-to-end signal-to-noise ratio (SNR) at the destination and eavesdroppers (E), but also throws up various new information security challenges for such vehicular networks. Existing security solutions mainly include key-based cryptographic techniques and physical-layer security (PLS) techniques. PLS has gained wider research interest because it "smartly" utilizes the inherent characteristics of the physical channel to realize keyless secure transmissions, and it can be easily integrated into the prevailing security infrastructure through signal design and physical layer resource allocation [5]. Furthermore, security issues are very prominent in cooperative vehicular networks because confidential information is broadcast twice, i.e., by the source and relays. Thus, it is much more important to study the PLS in cooperative cognitive vehicular networks [6].

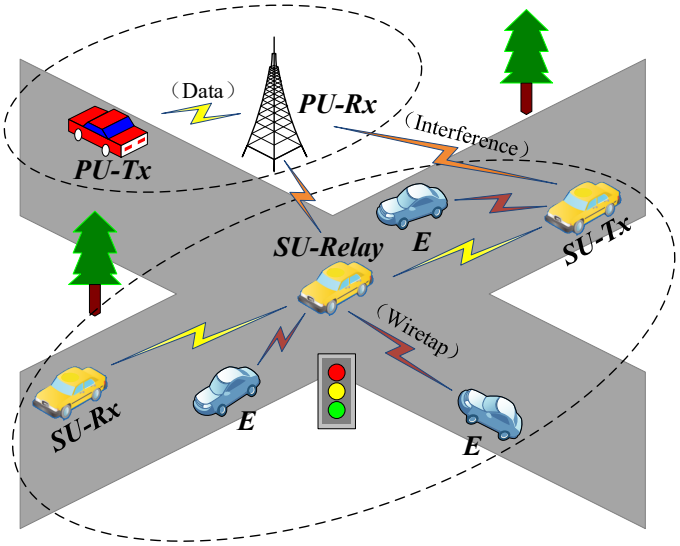


Figure 1. Cooperative underlay CR vehicular networks with wiretap channels.

On the other hand, throughput, as a crucial performance index, directly affects and reflects the system's performance and quality of service (QoS). How to improve throughput to meet the quality of experience (QoE) is a long-standing research hotspot in wireless communication networks, especially in the era of 5G and beyond communication networks that promise high speed, low latency, reliable connectivity, and seamless integration of various complex heterogeneous networks to provide a truly digital world [7]. Therefore,

inspired by the above, exploiting PLS to analyze the secrecy and throughput performance of cooperative underlay CR vehicular networks is the main focus of this paper.

1.2. Related Work

Owing to the merits of PLS, the secrecy performance of wireless networks has been widely studied in previous works. As the originator, Wyner laid the theoretical foundation for the study of PLS by establishing a three-node wiretap channel model and proposing the information-theoretic notion of secrecy in [8]. Based on Wyner's model, a great deal of work has been proposed. For instance, Ref. [9] studied the average secrecy capacity and secrecy outage probability (SOP) under three different conditions when the main and wiretap channels experience independent log-normal, correlated log-normal, and independent composite fading, respectively. Considering both single-antenna and multiple-antenna-aided transmission scenarios, Ref. [10] investigated the PLS of non-orthogonal multiple access (NOMA) in large-scale networks by invoking stochastic geometry.

Furthermore, the PLS of cooperative networks [6,11,12] or CR networks [13–15] have been well analyzed. Specifically, Ref. [6] proposed a relay selection strategy to improve the secure connection probability in a decentralized wireless network with randomly distributed relays and eavesdroppers. Ref. [11] presented two PLS transmission schemes and examined their achievable secrecy performance for multi-user multi-relay networks intercepted by a passive eavesdropper. In terms of CR networks, considering two different interference power constraint scenarios, Ref. [13] derived the closed-form analytical expressions of SOP for an underlay CR sensor network with an external energy harvesting (EH)-based eavesdropper. By modeling a CR network with multiple eavesdroppers for the Internet of Things (IoT) over k-μ fading channels, Ref. [14] developed the minimum limit values of SOP and the probability of strictly positive secrecy capacity (SPSC). In order to achieve secure transmission in a CR network in the presence of randomly distributed eavesdroppers, Ref. [15] designed four transmission protocols and comprehensively analyzed multiple performance factors, including delay, security, reliability, and throughput, for each protocol.

Based on the aforementioned work, of particular interest is the PLS in cooperative cognitive relaying networks, which has been extensively studied in Refs. [16–20]. Over Rayleigh fading channels, Ref. [16] evaluated and asymptotically analyzed the intercept and outage probability of a decode-and-forward (DF) relaying underlay CR network where an eavesdropper tapped the second hop. By deriving closed-form and asymptotic expressions for SOP over Nakagami-m fading channels, Ref. [17] investigated the PLS of a dual-hop underlay uplink CR network assisted by a multi-antenna relay and overheard by M multi-antenna eavesdroppers. Refs. [18–20] studied the PLS with outdated channel state information (CSI) for cooperative cognitive relaying networks. However, all the above work always confines itself to the assumption that nodes are stationary and channels between them are always modeled as Rayleigh, Nakagami-m, or Rician fading.

Recently, vehicular communication networks, which were formed because of the advancements in the development of automatically connected vehicles with embedded sensors, have promised a plethora of mobile world applications, e.g., intelligent transportation systems (ITS), environment monitoring, infotainment services, etc. [6]. It makes mobility performance indispensable and must be considered. In the mobile communication scenarios, however, classical Rayleigh or Nakagami-m fading channels become inadequate, and the double-Rayleigh or double Nakagami-m channels have proven to be more appropriate in characterizing the V2V links according to both the field measurements and theoretical analyses [21,22].

Motivated by this, a quantity of work [5,7,17,23–30] has been proposed. For example, Refs. [5,23] studied the secrecy performance of an underlay cooperative cognitive amplify-and-forward (AF) relaying vehicular network and drew the conclusion that the presence of eavesdroppers causes an irreducible error floor and hence reduces the secrecy diversity order by deriving tight lower bounds and asymptotic expressions of SOP. Further,

assuming a situation where the eavesdropper takes advantage of both the relay and direct link, the secrecy performance was analyzed in [7,24]. Ref. [25] investigated the secrecy performance of a cooperative vehicular relaying network in the presence of an interference source and proposed a power allocation model to reduce the SOP of the source and relay transmission powers. In addition, some new technologies have been introduced to improve secrecy performance, such as beamforming [27,28], cooperative jammers [17,29,30], and reconfigurable intelligent surfaces (RIS) [31–34], especially RIS, which is considered one of the critical 6G technologies for its outstanding advantages in energy efficiency, adaptability, interference management, signal control, and, notably, secrecy performance.

In summary, there are some drawbacks to the current research:

1. For simplicity, some ideal assumptions have always been made. For instance, many studies, such as [5,24,35,36], assumed that the direct link between SU-Tx and its receiver (SU-Rx) is unavailable because of the severe shadowing or path loss, and the direct link between SU-Tx and E is also neglected since E is far away from SU-Tx and outside the transmission range of the first hop. It is unrealistic because vehicles are moving, and the direct links can be available when the receiver (SU-Rx or E) moves close to SU-Tx and does not experience severe fading or shadowing. Also, direct links can affect both legitimate and wiretap transmissions [7], so the impact of direct links should not be ignored for secure transmission in such networks;
2. In terms of wiretap channels, many papers [5,7,25] have focused on the perfect CSI or single eavesdropper, while there is always a potentially large number of passive eavesdroppers who deliberately conceal their CSI or location information from legitimate users in practical scenarios. Therefore, it is necessary to model the location set of eavesdroppers as a stochastic process following some distributions [37,38]. However, it has been rarely discussed for secrecy analysis in such networks.
3. Most work has studied the PLS of cooperative cognitive vehicular networks in the AF relaying protocol, such as [5,7,23,24], but only a few studies have focused on the DF protocol, such as [39]. It is understandable because AF can provide lower latency and complexity, which is crucial for real-time IoV networks. However, meanwhile, AF worsens the legitimate channels because of its non-regenerative principle, where the relay directly amplifies and forwards the received signals without decoding, causing the accumulation of noise and a decrease in system performance. This is not conducive to communication data with high reliability requirements, such as passenger privacy, security information, etc. By comparison, DF is more suitable for some communication environments with relaxed latency but strict reliability requirements because it can eliminate the impact of fading on the first hop by decoding and regenerating the received signal [25,40]. Refs. [41–43] have also studied the gain between AF and DF; for instance, Ref. [41] concluded that from a diversity–multiplexing tradeoff (DMT) perspective, DF is strictly optimal over a certain range of the multiplexing gains, but the DMT of AF is offset by a constant term depending on the quality of CSI of the source-destination link only. Furthermore, Ref. [43] has proven that a hybrid decode–amplify–forward (HDAF) relaying protocol can achieve greater secure rate gain with the help of interfering nodes. Therefore, it is also necessary to study the applicability of DF in such networks.

To the best of the authors' knowledge, there is no existing work that studied the PLS of cooperative underlay CR vehicular networks by simultaneously considering the above-mentioned 1, 2, and 3. Therefore, we mainly analyze the secrecy and throughput performance of such DF relaying networks with direct links and Poisson-distributed colluding eavesdroppers. Table 1 presents the comparison between our work and some existing works to clearly highlight the contributions of this paper.

Table 1. Comparison of proposed work with related research.

Context	This Work	[5]	[7]	[17]	[24]	[39]
Cooperative Cognitive Vehicular Networks	Yes	Yes	Yes	No	No	Yes
Relaying Protocol	DF	AF	AF	DF	DF	DF
Direct link SU-Tx and SU-Rx	Yes	No	Yes	No	No	No
Direct link SU-Tx and E	Yes	No	Yes	Yes	No	No
Performance Analysis	PLS, Throughput	PLS	PLS	PLS	PLS	PLS
Eavesdropping Nodes	Multiple	Single	Single	Multiple	Single	Multiple
Fading Scenario	Rayleigh and Double-Rayleigh	Rayleigh and Double-Rayleigh	Rayleigh and Double-Rayleigh	Nakagami-*m*	Nakagami-*m* and Double Nakagami-*m*	Nakagami-*m*

1.3. Approach and Contributions

Motivated by the aforementioned work, we investigate the secrecy and throughput performance of cooperative underlay CR vehicular networks where a mobile SU-Tx communicates with a mobile SU-Rx assisted by a mobile DF-based secondary relay (SU-Relay) while under the constraint of a stationary PU-Rx. In addition, multiple colluding eavesdroppers whose location set is modeled as a homogeneous Poisson point process (HPPP) exist in the network to overhear the confidential information. In reality, the direct links, including SU-Tx between SU-Rx and SU-Tx between E, are also considered in this paper. Our major contributions are summarized as follows:

1. Considering realistic traffic conditions, this paper establishes a more practical cognitive vehicular system model that not only considers secondary direct links and randomly distributed eavesdroppers but also adopts mixed Rayleigh and double-Rayleigh fading channels to characterize V2V and V2I links. Moreover, a DF relaying transmission scheme is proposed to provide theoretical supplements for existing AF works;
2. According to the proposed system model, this paper derives the approximate expressions of the distribution functions of SNR for the traditional direct transmission scheme and the proposed relaying transmission scheme, respectively. We further deduce the closed-form expressions of the secrecy and throughput performance for each scheme and conduct an asymptotic analysis in the high SNR regime;
3. Designing numerical simulations, this paper verifies our theoretical findings and discusses the performance comparison of the two schemes, the impact of network parameters on security and throughput performance, and the relationship between the maximum secrecy throughput and the optimal relay position in order to provide useful design insights for relay networks with security constraints.

The rest of this paper is organized as follows: Section 2 presents the system model and a complete description of the proposed relay transmission scheme. Section 3 basically obtains the distribution functions of one-hop SNR and performance analysis for the direct transmission scheme. In Section 4, we analyze the distribution functions of two-hop SNR and system performance for the proposed scheme and further present an asymptotic SOP and COP analysis in the high SNR regime. Numerical simulation results are provided in Section 5, and the conclusions are finally put forward in Section 6.

2. System Model and Scheme Description

2.1. System and Channel Models

As shown in Figure 2, we consider a cooperative cognitive mobile network that consists of a primary transmitter–receiver pair (PU-Tx and PU-Rx) and a secondary cooperative network comprising a SU-Tx (S), a SU-Relay (R), a SU-Rx (D), and multiple movable eavesdroppers E_j ($j = 1, 2, \ldots$). The network works in the underlay mode, which allows the licensed spectrum of the primary network to be shared by secondary users to communicate confidential information but requires that the instantaneous interference power at PU-Rx from secondary senders (both S and R) be limited below the maximum tolerable interference threshold I_0. It is worth mentioning that such a system model has theoretical correlations in many popular communication systems, such as cognitive radio sensor networks, cognitive IoT networks, spectrum-sharing heterogeneous cooperative vehicular networks, etc.

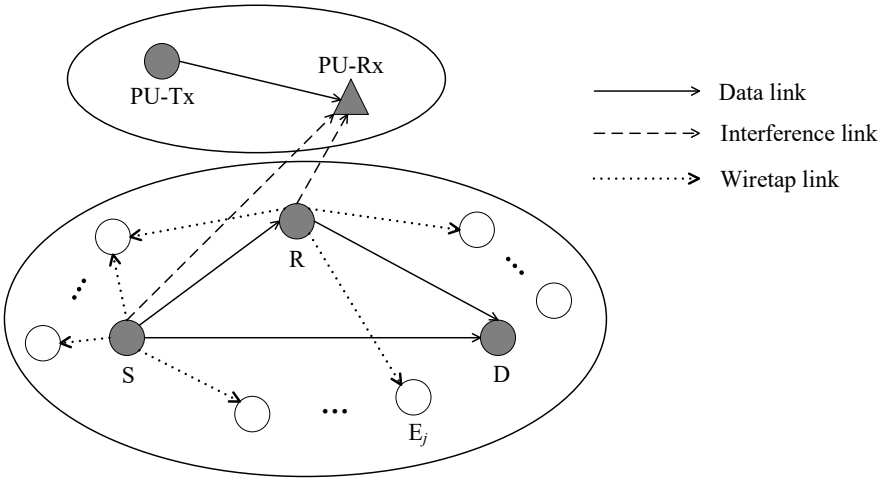


Figure 2. The proposed system model.

In reality, we assume that eavesdroppers are randomly distributed in the secondary network, and the HPPP model with density λ_E is adopted to characterize this stochastic process. Compared to deterministic models, the spatial HPPP model has the advantage of introducing total randomness for the node deployment and being tractable in performance analysis only by requiring the node density. Some important results about wireless networks with PPP-based randomly distributed nodes have been obtained in [37].

In this model, each node has a single antenna and operates in a half-duplex manner. We further assume that the receiver (including PU-Rx, R, D, and E) has the perfect CSI, but the availability of CSI at the transmitter (including PU-Tx, S, and R) is different due to the different capabilities of the receiving terminals. Specifically, we consider a scenario where the PU-Rx is a cellular base station (BS) that is capable of instantaneous CSI to all transmitters, while D, which is always a mobile vehicle, is not capable of full CSI feedback. This assumption meets the fact that the PU-Rx feeds back to both S and R with the instantaneous channel gain to enable them to adjust transmit power to satisfy the interference constraint. Realistically, eavesdroppers are assumed to be totally passive, such that their CSI is not revealed to S and R.

In terms of channel models, we assume all channels are quasi-static and subject to independent and non-identically distributed (i.ni.d.) fading. Moreover, because of the mobile nature of S, R, and D, and the stationary nature of PU-Rx, the V2V channels, i.e., S $\rightarrow$ D, S $\rightarrow$ R, and R $\rightarrow$ D, are assumed to experience the double-Rayleigh fading [44,45], while the V2I links, such as S $\rightarrow$ PU and R $\rightarrow$ PU, are modeled as Rayleigh fading [46,47]. It is worth noting that multiple movable eavesdroppers can be regarded as a single eavesdropper, denoted as E, with multiple distributed antennas for the reason that colluding eavesdroppers can exchange information with each other [6], so the channels related to eavesdroppers, i.e., S $\rightarrow$ E and R $\rightarrow$ E, can also be modeled as the Rayleigh channel [15]. In

particular, the channel coefficients h_{ij} for $\{ij\} \in \{SP, RP, SE, RE\}$ are independent complex Gaussian random variables having zero mean and variance Ω_{ij}, i.e., $h_{ij} \sim CN(0, \Omega_{ij})$. $\Omega_{ij} \propto d_{ij}^{-\varepsilon}$, where d_{ij} is the distance between i and j, ε is the path loss factor, and thus the channel gain $|h_{ij}|^2$ is an exponential random variable, and its probability density function (PDF) and cumulative distribution function (CDF) are given as:

$$f_{|h_{ij}|^2}(x) = \frac{1}{\Omega_{ij}} e^{-\frac{x}{\Omega_{ij}}}, \quad x > 0 \tag{1}$$

$$F_{|h_{ij}|^2}(x) = 1 - e^{-\frac{x}{\Omega_{ij}}}, \quad x > 0 \tag{2}$$

On the other hand, the channel coefficients h_k for $\{k\} \in \{SD, SR, RD\}$ can be modeled as the product of $h_{k,1}$ and $h_{k,2}$, where $h_{k,i} \sim CN(0, \Omega_{k,i})$ and assuming $\Omega_{k,1} = \Omega_{k,2} = \Omega_k$. The PDF and CDF of the channel gain $|h_k|^2$ are, respectively, given as:

$$f_{|h_k|^2}(x) = \frac{2}{\Omega_k^2} \mathcal{K}_0\left(\frac{2\sqrt{x}}{\Omega_k}\right), \quad x > 0 \tag{3}$$

$$F_{|h_k|^2}(x) = 1 - \frac{2\sqrt{x}}{\Omega_k} \mathcal{K}_1\left(\frac{2\sqrt{x}}{\Omega_k}\right), \quad x > 0 \tag{4}$$

where $\mathcal{K}_v(\cdot)$ denotes the v-th order modified Bessel function of the second kind [5]. The additive white Gaussian noise (AWGN) for each link is modeled as $CN(0, N_0)$. The above PDFs and CDFs will be used for the subsequent performance analysis.

2.2. Transmission Scheme

In this section, we provide a complete description of the proposed relaying transmission (RT) scheme. It is worth noting that, unlike transmission schemes in [5,6,15,25], where the communication from S to D must be accomplished via R in two hops, the fastest transmission from S to D in our RT scheme can be completed in one hop by considering the availability of the direct S-D link.

Specifically, in the first time slot, S broadcasts a unit confidential message x_s to R and D; the transmission is completed if D decodes x_s correctly. Otherwise, D requests retransmission in the second time slot. Due to the working principle of the DF relaying protocol, R regenerates and retransmits x_s to D if it has correctly decoded x_s in the first time slot. Otherwise, retransmission can only be executed by S. Note that x_s from both S and R will impose interference on PU and be overheard by E during the whole process. The proposed scheme is presented in Table 2.

Table 2. The proposed relaying transmission scheme.

First Time Slot	Second Time Slot	
S → PU-Rx (Interference)	(only when D decodes with error)	
S → R and D (Data)	If R has decoded correctly	R → PU-Rx (Interference) R → D (Data) R → E (Wiretap)
S → E (Wiretap)	If R has decoded incorrectly	S → PU-Rx (Interference) S → D (Data) S → E (Wiretap)

In terms of secure encoding, secondary senders (S and R) use the widely adopted wiretap code [8] to encode x_s. We denote $\mathbb{C}(R_B, R_S)$ as the set of all possible Wyner codes, where R_B is the codeword transmission rate, R_S is the confidential information rate and $R_B > R_S$. We assume R_B and R_S are constants, as the design of the rate parameter is

beyond the scope of this paper. It is obvious that the rate difference $R_B - R_S$ reflects the cost of securing the message against eavesdropping.

3. Performance Analysis of the Direct Transmission Scheme

In this section, we first analyze the distribution functions of the instantaneous equivalent SNR for each receiver under the direct transmission (DT) scheme and then further study the secrecy and throughput performance of this scheme.

3.1. The PDFs and CDFs of SNR

The so-called DT scheme refers to the transmission without relaying, i.e., whether D decodes the message correctly or not, the data transmission must be completed in one hop. The instantaneous equivalent end-to-end SNR of receivers (both D and E_j) can be represented as:

$$\gamma_{SD} = \frac{P_S|h_{SD}|^2}{N_0}, \quad \gamma_{SE_j} = \frac{P_S\left|h_{SE_j}\right|^2}{N_0} \tag{5}$$

where P_S is the transmit power of S, and it must be adjusted to $P_S = \frac{I_0}{|h_{SP}|^2}$ in order to satisfy the instantaneous interference constraint I_0 at PU-Rx. Denoting Φ_E as the location set of eavesdroppers, (5) can be rewritten as:

$$\gamma_{SD} = \rho\frac{|h_{SD}|^2}{|h_{SP}|^2} \tag{6}$$

$$\gamma_{SE} = \rho\sum_{E_j\in\Phi_E}\frac{\left|h_{SE_j}\right|^2}{|h_{SP}|^2} = \rho\frac{Z_{\Phi_E}}{|h_{SP}|^2} \tag{7}$$

where $\rho \triangleq \frac{I_0}{N_0}$ and $Z_{\Phi_E} \triangleq \sum_{E_j\in\Phi_E}\left|h_{SE_j}\right|^2$. The CDFs of γ_{SD} and γ_{SE} can be calculated as:

$$\begin{aligned} F_{\gamma_{SD}}(x) &= \Pr\{\gamma_{SD} < x\} = \Pr\left\{|h_{SD}|^2 < \tfrac{|h_{SP}|^2 x}{\rho}\right\} \\ &= \int_0^\infty F_{|h_{SD}|^2}\left(\tfrac{xy}{\rho}\right) f_{|h_{SP}|^2}(y)dy \end{aligned} \tag{8}$$

substituting (1) and (4), applying the substitution $\sqrt{y} = t$ and the fact that $\int_0^\infty f_{|h_{SP}|^2}(y)dy = 1$, we can rewrite (8) as:

$$F_{\gamma_{SD}}(x) = 1 - \frac{4\sqrt{\frac{x}{\rho}}}{\Omega_{SD}\Omega_{SP}}\int_0^\infty t^2\cdot\mathcal{K}_1\left(\frac{2\sqrt{\frac{x}{\rho}}\cdot t}{\Omega_{SD}}\right)\cdot e^{-\frac{t^2}{\Omega_{SP}}}dt \tag{9}$$

using $\int_0^\infty x^\mu\mathcal{K}_v(\beta x)e^{-\alpha x^2}dx = \frac{1}{2}\alpha^{-\frac{\mu}{2}}\frac{1}{\beta}\Gamma\left(\frac{1+v+\mu}{2}\right)\Gamma\left(\frac{1-v+\mu}{2}\right)e^{\frac{\beta^2}{8\alpha}}\mathcal{W}_{-\frac{\mu}{2},\frac{v}{2}}\left(\frac{\beta^2}{4\alpha}\right)$ ([48], Equation (6.631.3)), where $\Gamma(x) = \int_0^\infty e^{-t}t^{x-1}dt$ is the Gamma function [49]. We can obtain the final expression as follows:

$$F_{\gamma_{SD}}(x) = 1 - e^{\frac{kx}{2}}\mathcal{W}_{-1,\frac{1}{2}}(kx) \tag{10}$$

where $k \triangleq \frac{\Omega_{SP}}{\rho\Omega_{SD}^2}$, $\mathcal{W}_{v,\mu}(\cdot)$ denotes the Whittaker-W function ([50], Equation (9.220.4)). Furthermore, by using $\frac{\partial\mathcal{W}_{v,\mu}(x)}{\partial x} = \left(\frac{1}{2} - \frac{v}{x}\right)\mathcal{W}_{v,\mu}(x) - \frac{\mathcal{W}_{v+1,\mu}(x)}{x}$ ([49], Equation (07.45.20.0005.01)), the PDF of γ_{SD} can be calculated as follows:

$$f_{\gamma_{SD}}(x) = -ke^{\frac{kx}{2}}\mathcal{W}_{-1,\frac{1}{2}}(kx) - \frac{1}{x}e^{\frac{kx}{2}}\mathcal{W}_{-1,\frac{1}{2}}(kx) + \frac{1}{x}e^{\frac{kx}{2}}\mathcal{W}_{0,\frac{1}{2}}(kx) \tag{11}$$

On the other hand, the CDF of γ_{SE} can be calculated as follows:

$$F_{\gamma_{SE}}(x) = \Pr\{\gamma_{SE} < x\} = \Pr\left\{\rho\frac{Z_{\Phi_E}}{|h_{SP}|^2} < x\right\} = \Pr\left\{|h_{SP}|^2 > \rho\frac{Z_{\Phi_E}}{x}\right\} \tag{12}$$

substituting (1), and the final expression is:

$$\begin{aligned} F_{\gamma_{SE}}(x) &= \int_0^\infty \int_{\rho\frac{z}{x}}^\infty \left[\frac{1}{\Omega_{SP}} e^{-\frac{y}{\Omega_{SP}}}\right] \cdot f_{Z_{\Phi_E}}(z) dy dz \\ &= \int_0^\infty f_{Z_{\Phi_E}}(z) \cdot e^{-\frac{\rho}{\Omega_{SP}x} z} dz \\ &= \mathcal{L}_{Z_{\Phi_E}}(s) \end{aligned} \tag{13}$$

where $s \triangleq \frac{\rho}{\Omega_{SP}x}$, and $\mathcal{L}_{Z_{\Phi_E}}(\cdot)$ denotes the Laplace transform of Z_{Φ_E}. As given in [15]:

$$\mathcal{L}_{Z_{\Phi_E}}(s) = \exp\left(-2\pi\lambda_E s^{2/\varepsilon}/\varepsilon\Gamma\left(1-\frac{2}{\varepsilon}\right)\Gamma\left(\frac{2}{\varepsilon}\right)\right) \tag{14}$$

3.2. Secrecy and Throughput Performance Analysis

Based on Section 3.1, we further evaluate the secrecy and throughput performance by adopting outage-based metrics related to security and reliability instead of using the widely used outage probability of secrecy capacity [51], i.e., $p_{out} = \Pr\{\max[C_D - C_E, 0] < R_S\}$, which cannot differentiate outages caused by either information leakage to eavesdroppers (security) or unreliable reception at the receiver (reliability). Specifically, we denote the secrecy outage probability (SOP) and the connection outage probability (COP) to represent two kinds of outage events under the fixed-rate wiretap code. Furthermore, in order to comprehensively reflect the system performance of having a secure and reliable transmission, the secrecy and connection outage probability (SCOP) is defined. Finally, the overall secrecy throughput is measured based on the SCOP.

- SOP represents the probability that a secrecy outage event happens when the secure transmission cannot be guaranteed, which is given by [52] as follows:

$$p_{so}^{DT} = \Pr\{C_{SE} > R_B - R_S\} \tag{15}$$

where $C_{SE} = \log_2(1+\gamma_{SE})$ denotes the wiretap channel capacity. (15) can be rewritten as follows:

$$\begin{aligned} p_{so}^{DT} &= \Pr\{\log_2(1+\gamma_{SE}) > R_B - R_S\} \\ &= \Pr\left\{\gamma_{SE} > 2^{(R_B - R_S)} - 1\right\} \end{aligned} \tag{16}$$

substituting (13) into (16), SOP can be obtained as follows:

$$p_{so}^{DT} = 1 - \mathcal{L}_{Z_{\Phi_E}}\left(\frac{\rho}{\Omega_{SP}\left[2^{(R_B - R_S)} - 1\right]}\right) \tag{17}$$

- COP represents the probability that a connection outage event happens when the message cannot be decoded at the intended receiver correctly, which can be expressed as follows:

$$p_{co}^{DT} = \Pr\{C_{SD} < R_B\} \tag{18}$$

where $C_{SD} = \log_2(1+\gamma_{SD})$ denotes the wiretap channel capacity. (18) can be rewritten as follows:

$$\begin{aligned} p_{co}^{DT} &= \Pr\{\log_2(1+\gamma_{SD}) < R_B\} \\ &= \Pr\left\{\gamma_{SD} < 2^{R_B} - 1\right\} \end{aligned} \tag{19}$$

substituting (10) into (19), COP can be derived as follows:

$$p_{co}^{DT} = 1 - e^{\frac{k(2^{R_B}-1)}{2}} \mathcal{W}_{-1,\frac{1}{2}}\left[k\left(2^{R_B}-1\right)\right] \tag{20}$$

by using $e^{z/2}\mathcal{W}_{v,\mu}(z) = \frac{1}{\Gamma\left(\frac{1}{2}-\mu-v\right)\Gamma\left(\mu-v+\frac{1}{2}\right)} G_{1,2}^{2,1}\left(z\middle|\begin{matrix} v+1 \\ \mu+\frac{1}{2},\frac{1}{2}-\mu \end{matrix}\right)$ ([49], Equation (07.45.26.0005.01)), where $G_{p,q}^{m,n}\left(z\middle|\begin{matrix} a_1,\cdots,a_n,a_{n+1},\cdots,a_p \\ b_1,\cdots,b_m,b_{m+1},\cdots,b_q \end{matrix}\right)$ is the Meijer-*G* function [49], (20) can be further expressed as follows:

$$p_{co}^{DT} = 1 - G_{1,2}^{2,1}\left(k\left(2^{R_B}-1\right)\Big|_{1,0}^{0}\right) \tag{21}$$

- SCOP represents the probability that either the secrecy outage or the connection outage happens, which can comprehensively reflect the joint performance of security and reliability. SCOP can be given as:

$$p_{sco}^{DT} = 1 - \Pr\{C_{SE} \le R_B - R_S,\ C_{SD} \ge R_B\} \tag{22}$$

It is worth noting that the calculation of (22) is tedious and intractable due to the mutual correlation between security (γ_{SE}) and reliability (γ_{SD}). We assume that the SOP and COP are independent, which is reasonable in CR networks with fixed transmit power [15], so (22) can be simplified as:

$$p_{sco}^{DT} = 1 - \left(1 - p_{so}^{DT}\right)\left(1 - p_{co}^{DT}\right) \tag{23}$$

substituting (17) and (20), SCOP can be derived as:

$$p_{sco}^{DT} = 1 - \mathcal{L}_{Z_{\Phi_E}}\left(\frac{\rho}{\Omega_{SP}\left[2^{(R_B-R_S)}-1\right]}\right) G_{1,2}^{2,1}\left(k\left(2^{R_B}-1\right)\Big|_{1,0}^{0}\right) \tag{24}$$

- Secrecy throughput quantifies the achievable average secrecy rate at which the message can be transmitted securely and reliably to D, which is given as:

$$\eta^{DT} = \left(1 - p_{sco}^{DT}\right) R_S \tag{25}$$

substituting (24), secrecy throughput can be finally obtained as:

$$\eta^{DT} = R_S \cdot \mathcal{L}_{Z_{\Phi_E}}\left(\frac{\rho}{\Omega_{SP}\left[2^{(R_B-R_S)}-1\right]}\right) G_{1,2}^{2,1}\left(k\left(2^{R_B}-1\right)\Big|_{1,0}^{0}\right) \tag{26}$$

Remark 1. *From (17) and (21), it is worth noting that the SOP is an increasing function of λ_E and ρ, while is a decreasing function of Ω_{SP} and $(R_B - R_S)$. Conversely, the COP, which is independent of λ_E, is an increasing function of Ω_{SP} and R_B, while is a decreasing function of ρ. This implies that a large λ_E is harmful to reducing the SOP and SCOP but has no effect on the COP in the secondary network. On the other hand, it can be inferred from (24) and (26) that the SCOP and secrecy throughput of the DT scheme are closely related to the network parameters, including ρ, Ω_{SP}, Ω_{SD}, and $(R_B - R_S)$.*

4. Performance Analysis of the Relaying Transmission Scheme

This section first analyzes the CDFs of the instantaneous equivalent SNR at D and E after two-hop transmission under the proposed relaying transmission (RT) scheme, and the secrecy and throughput performance are then studied based on them. Finally, an asymptotic SOP and COP analysis is presented in the high SNR regime.

4.1. The CDFs of SNR

Unlike the DT scheme with only one hop, the proposed RT scheme involves two-hop transmission, and the SNR analysis of each receiver (D and E) needs to be discussed based on the decoding situation of R. For simplicity, we consider that S and R have the same codebook and code rate. D utilizes the maximal ratio combining (MRC) technique, and E only decodes the signal with a higher SNR in two hops, i.e., E uses the selection combining (SC) technique.

According to Section 2.2, if D decodes x_s with error but R successfully, the retransmission is executed by R in the next hop. Based on the DF forwarding strategy, the instantaneous equivalent SNR at D and E is:

$$\gamma_D = \gamma_{SD} + \gamma_{SRD} = \gamma_{SD} + \min\left\{\gamma_{SR}^{(1)}, \gamma_{RD}^{(2)}\right\} \tag{27}$$

$$\gamma_E = \max\left\{\gamma_{SE}^{(1)}, \gamma_{RE}^{(2)}\right\} \tag{28}$$

where $\gamma_{ij}^{(n)}$ represents the SNR of the link *i*-*j* at the *n*-th hop. They can be further expressed as:

$$\gamma_{SR}^{(1)} = \rho\frac{|h_{SR}|^2}{|h_{SP}|^2}, \gamma_{RD}^{(2)} = \rho\frac{|h_{RD}|^2}{|h_{RP}|^2} \tag{29}$$

$$\gamma_{SE}^{(1)} = \rho\frac{Z_{\Phi_E}}{|h_{SP}|^2}, \gamma_{RE}^{(2)} = \rho\frac{Z'_{\Phi_E}}{|h_{RP}|^2} \tag{30}$$

where $Z'_{\Phi_E} \triangleq \sum_{E_k \in \Phi_E} |h_{RE_k}|^2$. According to $F_{\gamma_{SRD}}(x) = F_{\gamma_{SR}^{(1)}}(x) + F_{\gamma_{RD}^{(2)}}(x) - F_{\gamma_{SR}^{(1)}}(x)F_{\gamma_{RD}^{(2)}}(x)$ [53] and the fact that $\gamma_{SR}^{(1)}$ and $\gamma_{RD}^{(2)}$ follow the same distribution as γ_{SD} in (10), the CDF of γ_{SRD} can be calculated as follows:

$$F_{\gamma_{SRD}}(x) = 1 - e^{\frac{(k_1+k_2)x}{2}}\mathcal{W}_{-1,\frac{1}{2}}(k_1x)\mathcal{W}_{-1,\frac{1}{2}}(k_2x) \tag{31}$$

where $k_1 \triangleq \frac{\Omega_{SP}}{\rho\Omega_{SR}^2}$, $k_2 \triangleq \frac{\Omega_{RP}}{\rho\Omega_{RD}^2}$. We can further express the CDF of γ_D as:

$$\begin{aligned} F_{\gamma_D}(z) &= \Pr\{\gamma_{SD} + \gamma_{SRD} < z\} = \Pr\{\gamma_{SRD} < z - \gamma_{SD}\} \\ &= \int_0^\infty F_{\gamma_{SRD}}(z-x) f_{\gamma_{SD}}(x)dx \end{aligned} \tag{32}$$

with the aid of the $F_{\gamma_{SRD}}(x)$ in (31), the $f_{\gamma_{SD}}(x)$ in (11), (32) can be rewritten as follows:

$$\begin{aligned} F_{\gamma_D}(z) = 1 &+ k\int_0^\infty e^{\frac{kx}{2}}\mathcal{W}_{-1,\frac{1}{2}}(kx)e^{\frac{(k_1+k_2)(z-x)}{2}}\mathcal{W}_{-1,\frac{1}{2}}[k_1(z-x)]\mathcal{W}_{-1,\frac{1}{2}}[k_2(z-x)]dx \\ &+ \int_0^\infty \tfrac{1}{x}e^{\frac{kx}{2}}\mathcal{W}_{-1,\frac{1}{2}}(kx)e^{\frac{(k_1+k_2)(z-x)}{2}}\mathcal{W}_{-1,\frac{1}{2}}[k_1(z-x)]\mathcal{W}_{-1,\frac{1}{2}}[k_2(z-x)]dx \\ &- \int_0^\infty \tfrac{1}{x}e^{\frac{kx}{2}}\mathcal{W}_{0,\frac{1}{2}}(kx)e^{\frac{(k_1+k_2)(z-x)}{2}}\mathcal{W}_{-1,\frac{1}{2}}[k_1(z-x)]\mathcal{W}_{-1,\frac{1}{2}}[k_2(z-x)]dx \end{aligned} \tag{33}$$

similar to the substitution from (20) to (21), it can be rewritten as:

$$\begin{aligned} F_{\gamma_D}(z) = 1 &+ k\int_0^\infty G_{1,2}^{2,1}\left(kx\big|_{1,0}^{0}\right)G_{1,2}^{2,1}\left[k_1(z-x)\big|_{1,0}^{0}\right]G_{1,2}^{2,1}\left[k_2(z-x)\big|_{1,0}^{0}\right]dx \\ &+ \int_0^\infty \tfrac{1}{x}G_{1,2}^{2,1}\left(kx\big|_{1,0}^{0}\right)G_{1,2}^{2,1}\left[k_1(z-x)\big|_{1,0}^{0}\right]G_{1,2}^{2,1}\left[k_2(z-x)\big|_{1,0}^{0}\right]dx \\ &- \int_0^\infty \tfrac{1}{x}G_{1,2}^{2,1}\left(kx\big|_{1,0}^{1}\right)G_{1,2}^{2,1}\left[k_1(z-x)\big|_{1,0}^{0}\right]G_{1,2}^{2,1}\left[k_2(z-x)\big|_{1,0}^{0}\right]dx \end{aligned} \tag{34}$$

according to ([49], Equation (07.34.21.0081.01)), (34) can be further evaluated as follows:

$$F_{\gamma_D}(z) = 1 + G_{2,1:1,2:1,2}^{1,2:2,1:2,1}\left(\begin{matrix} -1,0 \\ 0 \end{matrix} \middle| \begin{matrix} 0 \\ 1,0 \end{matrix} \middle| \begin{matrix} 0 \\ 1,0 \end{matrix} \middle| \begin{matrix} \frac{k_1 z}{k} \\ \end{matrix} \middle| \begin{matrix} \frac{k_2 z}{k} \\ \end{matrix} \right) + G_{2,1:1,2:1,2}^{1,2:2,1:2,1}\left(\begin{matrix} 0,1 \\ 1 \end{matrix} \middle| \begin{matrix} 0 \\ 1,0 \end{matrix} \middle| \begin{matrix} 0 \\ 1,0 \end{matrix} \middle| \begin{matrix} \frac{k_1 z}{k} \\ \end{matrix} \middle| \begin{matrix} \frac{k_2 z}{k} \\ \end{matrix} \right) - G_{2,1:1,2:1,2}^{1,2:2,1:2,1}\left(\begin{matrix} 0,1 \\ 0 \end{matrix} \middle| \begin{matrix} 0 \\ 1,0 \end{matrix} \middle| \begin{matrix} 0 \\ 1,0 \end{matrix} \middle| \begin{matrix} \frac{k_1 z}{k} \\ \end{matrix} \middle| \begin{matrix} \frac{k_2 z}{k} \\ \end{matrix} \right) \tag{35}$$

On the other hand, according to $F_{\gamma_E}(x) = F_{\gamma_{SE}^{(1)}}(x) F_{\gamma_{RE}^{(2)}}(x)$ [53] and $F_{\gamma_{SE}}(x)$ in (13), the CDF of γ_E can be obtained as:

$$F_{\gamma_E}(x) = \mathcal{L}_{Z_{\Phi_E}}\left(\frac{\rho}{\Omega_{SP} x}\right) \cdot \mathcal{L}_{Z'_{\Phi_E}}\left(\frac{\rho}{\Omega_{RP} x}\right) \tag{36}$$

In particular, if both D and R decode x_s incorrectly, the retransmission can only be executed by S in the second hop. In this situation, the SNRs of D and E become as follows:

$$\gamma_D = 2\gamma_{SD}, \gamma_E = 2\gamma_{SE} \tag{37}$$

and their CDFs are simplified as:

$$F_{\gamma_D}(x) = 1 - e^{kx}\left[\mathcal{W}_{-1,\frac{1}{2}}(kx)\right]^2 \tag{38}$$

$$F_{\gamma_E}(x) = \left[\mathcal{L}_{Z_{\Phi_E}}\left(\frac{\rho}{\Omega_{SP} x}\right)\right]^2 \tag{39}$$

4.2. Secrecy and Throughput Performance Analysis

Based on the CDFs obtained in Section 4.1, we further evaluate the secrecy and throughput performance of the proposed RT scheme.

- SOP: referring to (15), SOP can be expressed as:

$$p_{so}^{RT} = \Pr\{\log_2(1+\gamma_E) > R_B - R_S\} = \Pr\left\{\gamma_E > 2^{(R_B - R_S)} - 1\right\} \tag{40}$$

according to the different decoding situations of R and substituting (36) and (39), (40) expands as:

$$p_{so}^{RT} = \begin{cases} 1 - \mathcal{L}_{Z_{\Phi_E}}\left(\frac{\rho}{\Omega_{SP}\left[2^{(R_B - R_S)} - 1\right]}\right) \mathcal{L}_{Z'_{\Phi_E}}\left(\frac{\rho}{\Omega_{RP}\left[2^{(R_B - R_S)} - 1\right]}\right), (1 - p'_{co}) \\ 1 - \left[\mathcal{L}_{Z_{\Phi_E}}\left(\frac{\rho}{\Omega_{SP}\left[2^{(R_B - R_S)} - 1\right]}\right)\right]^2, p'_{co} \end{cases} \tag{41}$$

where p'_{co} is the probability that R cannot decode the message correctly, i.e., the COP of R, which can be calculated by referring to (18):

$$p'_{co} = \Pr\left\{\log_2\left(1 + \gamma_{SR}^{(1)}\right) < R_B\right\} = \Pr\left\{\gamma_{SR}^{(1)} < 2^{R_B} - 1\right\} \tag{42}$$

referring to the CDF of γ_{SD} in (10), p'_{co} can be expressed as:

$$\begin{aligned} p'_{co} &= 1 - e^{\frac{k_1(2^{R_B}-1)}{2}} \mathcal{W}_{-1,\frac{1}{2}}\left[k_1\left(2^{R_B} - 1\right)\right] \\ &= 1 - G_{1,2}^{2,1}\left(k_1\left(2^{R_B} - 1\right)\Big|_{1,0}^{0}\right) \end{aligned} \tag{43}$$

Thus, the average SOP $\overline{p_{so}^{RT}}$ can be obtained by using the expectation formula $E[x] = \sum_{i=1}^{n} x_i p_i$.

- COP: referring to (18), COP can be expressed as:

$$p_{co}^{RT} = \Pr\{\log_2(1+\gamma_D) < R_B\} = \Pr\left\{\gamma_D < 2^{R_B} - 1\right\} \tag{44}$$

similarly, substituting (35) and (38), (44) expands as (45), and the average COP $\overline{p_{co}^{RT}}$ can be obtained by calculating its expectation.

$$p_{co}^{RT} = \begin{cases} 1 + G_{2,1:1,2:1,2}^{1,2:2,1:2,1}\left(\begin{array}{c|c|c|l} -1,0 & 0 & 0 & |k_4(2^{R_B}-1)\,|k_5(2^{R_B}-1) \\ 0 & 1,0 & 1,0 & \end{array} \right) \\ \quad + G_{2,1:1,2:1,2}^{1,2:2,1:2,1}\left(\begin{array}{c|c|c|l} 0,1 & 0 & 0 & |k_4(2^{R_B}-1)\,|k_5(2^{R_B}-1) \\ 1 & 1,0 & 1,0 & \end{array} \right) \\ \quad - G_{2,1:1,2:1,2}^{1,2:2,1:2,1}\left(\begin{array}{c|c|c|l} 0,1 & 0 & 0 & |k_4(2^{R_B}-1)\,|k_5(2^{R_B}-1) \\ 0 & 1,0 & 1,0 & \end{array} \right), & (1-p'_{co}) \\ 1 - e^{k(2^{R_B}-1)}\left\{\mathcal{W}_{-1,\frac{1}{2}}\left[k(2^{R_B}-1)\right]\right\}^2, & p'_{co} \end{cases} \tag{45}$$

where $k_4 = \frac{k_1}{k} = \frac{\Omega_{SD}^2}{\Omega_{SR}^2}$, $k_5 = \frac{k_2}{k} = \frac{\Omega_{RP}\Omega_{SD}^2}{\Omega_{SP}\Omega_{RD}^2}$.

- SCOP: referring to (23), the average SCOP can be expressed as:

$$\overline{p_{sco}^{RT}} = 1 - \left(1 - \overline{p_{so}^{RT}}\right)\left(1 - \overline{p_{co}^{RT}}\right) \tag{46}$$

- Secrecy throughput: referring to (25) and the principle of the RT scheme, the average secrecy throughput is expressed according to the total probability theorem:

$$\overline{\eta^{RT}} = \left(1 - p_{co}^{DT}\right)\eta^{DT} + p_{co}^{DT}\left(1 - \overline{p_{sco}^{RT}}\right)R_S \tag{47}$$

Remark 2. *From (41) and (45), it can be found that the SOP and COP of the proposed RT scheme become more complex due to the cooperation of secondary relays. Specifically, except for the network parameters involved in the DT scheme, the SOP of the proposed RT scheme deeply depends on the values of Ω_{SP} and Ω_{RP}, in other words, $\frac{\Omega_{RP}}{\Omega_{SP}}$. Furthermore, the COP is not only related to $\frac{\Omega_{RP}}{\Omega_{SP}}$, but also highly to $\frac{\Omega_{SD}^2}{\Omega_{SR}^2}$ and $\frac{\Omega_{SD}^2}{\Omega_{RD}^2}$. It means that the advantages of the proposed RT scheme are totally decided by the channel gain of the relay link compared to the direct link, which further reflects the importance of optimal relay selection.*

4.3. Asymptotic Analysis

We present asymptotic SOP and COP performance analysis in the high SNR regime ($\rho \to \infty$). It is worth noting that when $\rho \to \infty$, $p'_{co} \simeq 0$, which means the secondary relay must be able to successfully decode the received message and retransmit it in the second time slot. Substituting $p'_{co} \simeq 0$ into (41), it can be easily found that:

$$\widetilde{p}_{so-UB}^{RT} \simeq 1 \tag{48}$$

which implies that when $\rho \to \infty$, there exists an upper bound for SOP. Specially, an infinite maximum tolerable interference threshold I_0 means there is no limit to the transmission power of the secondary transmitters; a secrecy outage event must happen so that secure transmission cannot be guaranteed since the SNR of both legitimate links and wiretap links is improved simultaneously.

Unlike SOP, it can be discovered by substituting $p'_{co} \simeq 0$ into (45) that:

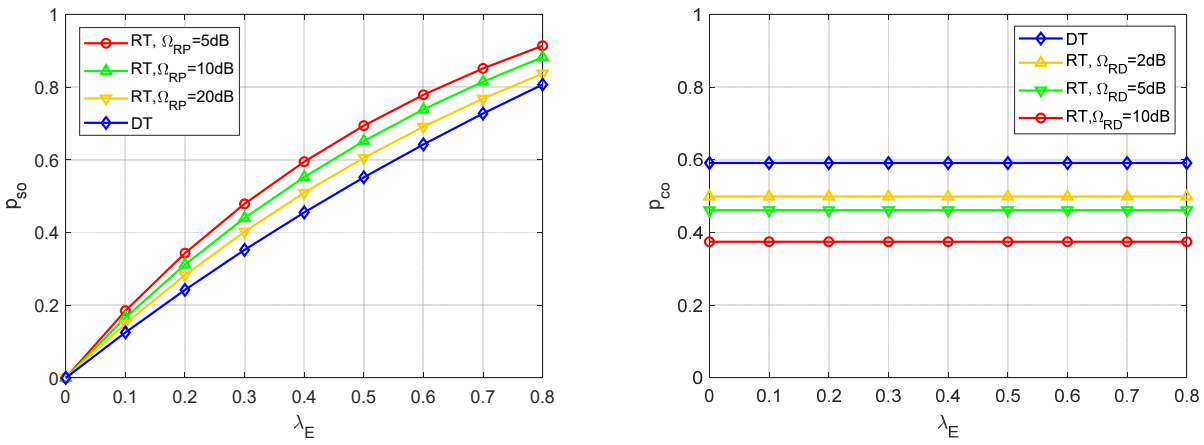
$$\begin{aligned}\widetilde{p}^{RT}_{co-LB} \simeq 1 &+ G^{1,2:2,1:2,1}_{2,1:1,2:1,2}\left(\begin{array}{c|c|c} -1,0 & 0 & 0 \\ 0 & 1,0 & 1,0 \end{array} \middle| k_4\left(2^{R_B}-1\right) \middle| k_5\left(2^{R_B}-1\right) \right) \\ &+ G^{1,2:2,1:2,1}_{2,1:1,2:1,2}\left(\begin{array}{c|c|c} 0,1 & 0 & 0 \\ 1 & 1,0 & 1,0 \end{array} \middle| k_4\left(2^{R_B}-1\right) \middle| k_5\left(2^{R_B}-1\right) \right) \\ &- G^{1,2:2,1:2,1}_{2,1:1,2:1,2}\left(\begin{array}{c|c|c} 0,1 & 0 & 0 \\ 0 & 1,0 & 1,0 \end{array} \middle| k_4\left(2^{R_B}-1\right) \middle| k_5\left(2^{R_B}-1\right) \right)\end{aligned} \tag{49}$$

From (49), it can be found that there exists a lower bound for the asymptotic COP in the high ρ region, and this lower bound is closely related to the ratio of channel gain between the direct link and relay link.

5. Simulations

In this section, we first show the numerical comparison and asymptotic analysis for the aforementioned transmission schemes, i.e., the DT and RT schemes. Then, the interaction and effect of different network parameters on security and reliability performance are present. Finally, we reveal the relationship between the maximum secrecy throughput and the optimal relay location. The channel parameter is assumed to be $\varepsilon = 4$. It is worth noting that we use Ω_{ij} to reflect the distance d_{ij}, the larger Ω_{ij}, the better average $|h_{ij}|^2$, and hence the closer d_{ij}. Similarly, ρ is adopted to comprehensively reflect the ratio of interference threshold I_0 and noise power N_0.

Figure 3 depicts the impact of the eavesdropper density λ_E on SOP (p_{so}) and COP (p_{co}) for fixed values of $\rho = 10$ dB, $\Omega_{SP} = 10$ dB, $\Omega_{SD} = \Omega_{SR} = 5$ dB, $R_B = 3$ bps/Hz, $R_S = 1$ bps/Hz. It can be first seen from Figure 3 that no matter the DT or RT scheme, SOP increases while COP remains constant with λ_E increases; this is consistent with Remark 1. It is reasonable because the larger λ_E, the better wiretap channel quality enhances the ability to eavesdrop on confidential information, p_{so} therefore increases as increasing λ_E. However, COP, which represents the outage probability that D cannot decode the confidential information correctly, i.e., the reliability performance, is independent of the eavesdropper density λ_E, and hence p_{co} keeps unchanged as λ_E increases.



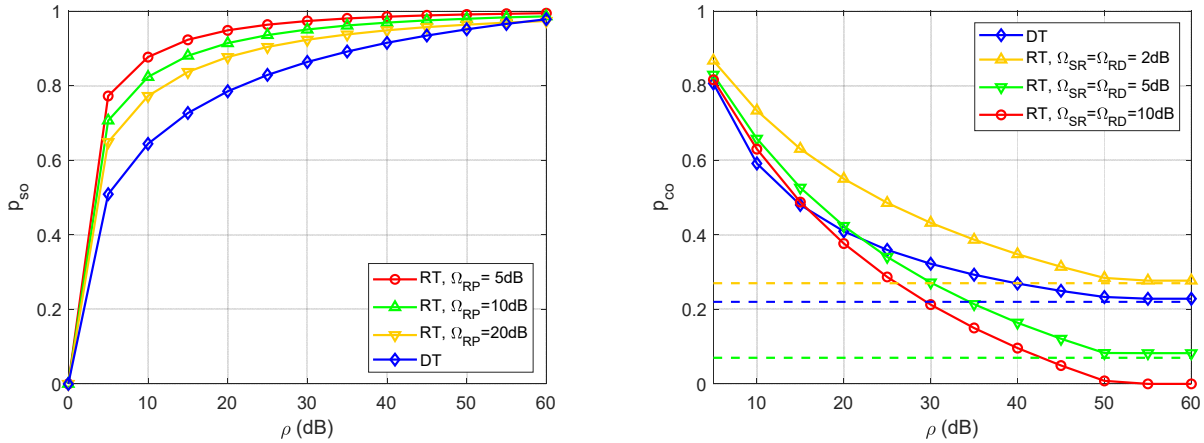
(**a**) SOP versus λ_E (**b**) COP versus λ_E

Figure 3. Impacts of eavesdropper density λ_E on SOP and COP.

Further, we can observe from Figure 3 that the SOP of the DT scheme outperforms that of the RT scheme, especially in a smaller Ω_{RP}. However, in terms of COP, the RT scheme surpasses the DT, especially in a larger Ω_{RD}. The former is because the presence of relays strengthens the wiretap link capacity, and smaller Ω_{RP} results in a better channel quality of R-E link, and hence, a worse security performance will be induced. At the same time, the latter is because the introduction of relays brings diversity to D for successful decoding.

Furthermore, an increasing Ω_{RD} can improve the quality of the R-D channel and enhance the ability of D to decode information, resulting in better reliability performance. It can be concluded from Figure 3 that the introduction of relays is a double-edged sword, which not only improves reliability performance but also deteriorates security performance. As the comment made in [7] identifies, in this case, even E is able to extract the benefits of increased transmit SNR along with D.

Figure 4 further depicts the impact of ρ on SOP and COP for fixed values of $\lambda_E = 0.3$, $\Omega_{SP} = 10$ dB, $\Omega_{SD} = 5$ dB, $R_B = 3$ bps/Hz, $R_S = 1$ bps/Hz. It can be observed from Figure 4 that the asymptotic results (the dotted lines) are in good agreement with the exact results in a high SNR regime. Moreover, Figure 4a reflects the same conclusion as in Figure 3a because SOP is the increasing function of both λ_E and ρ. Figure 4b illustrates the fact that the better the channel gain of the secondary relay (Ω_{SR} and Ω_{RD}), the lower the COP, i.e., the better the reliability performance can be achieved by the proposed RT scheme, especially when the channel gain is better than that of the direct link. It is also consistent with the insight given in Remark 2.



(**a**) SOP versus ρ (**b**) COP versus ρ

Figure 4. Impacts of ρ on SOP and COP.

We then show the effect of different network parameters on the security and reliability performance. Figure 5 plots the SCOP, i.e., p_{sco} versus ρ, for various values of R_B and R_S, when $\lambda_E = 0.3$, $\Omega_{SP} = \Omega_{RP} = 10$ dB, $\Omega_{SR} = \Omega_{RD} = 5$ dB, $\Omega_{SD} = 2$ dB. From Figure 5, we can see that p_{sco} decreases with the increase of ρ. It is because the larger the ρ, the more relaxed the interference constraint on the secondary transmitters, the higher the secondary transmit power can be achieved, and hence, the secure and reliable transmission performance is improved. Moreover, it can be observed from Figure 5 that the SCOP increases with the increase of $R_B - R_S$, which is because a higher power will be required to compensate for the greater cost of secure transmission.

Figure 6 illustrates the impact of the primary receiver (assuming $\Omega_{SP} = \Omega_{RP}$) on SCOP for various values of ρ, when $\lambda_E = 0.3$, $\Omega_{SR} = \Omega_{RD} = 10$ dB, $\Omega_{SD} = 5$ dB, $R_B = 3$ bps/Hz, $R_S = 1$ bps/Hz. It is seen from Figure 6 that p_{sco} increases with the increase of Ω_{SP} (Ω_{RP}), which is owing to the reason that a larger value of Ω_{SP} (Ω_{RP}) imposes a stronger power constraint from the PU receiver to the secondary transmitters (both S and R), causing a lower secondary transmit power (P_S and P_R), thereby degrading the SCOP performance. Moreover, we can find that the SCOP curves exhibit a secrecy floor phenomenon, irrespective of ρ, as reported in [7].

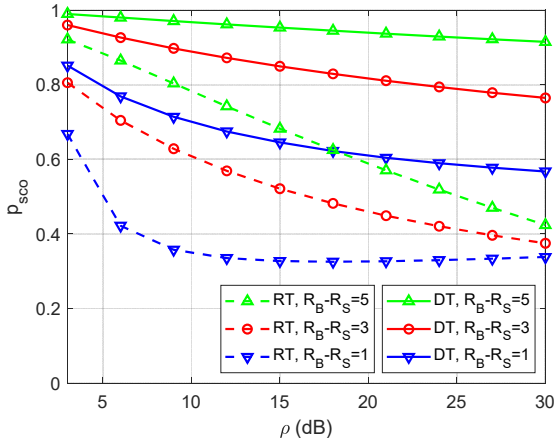


Figure 5. SCOP versus ρ.

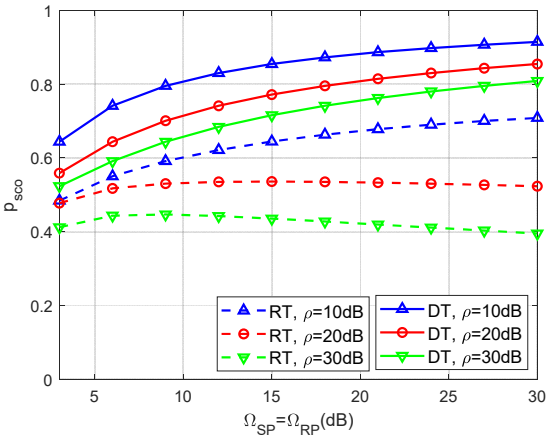


Figure 6. Impact of PU receiver on SCOP.

In Figure 7, we demonstrate the effect of the average channel gain of the direct link, i.e., Ω_{SD}, on the SCOP performance for $\lambda_E = 0.3$, $\rho = 10$ dB, $\Omega_{SP} = \Omega_{RP} = 10$ dB, $R_B = 3$ bps/Hz, $R_S = 1$ bps/Hz. We can observe from Figure 7 that SCOP improves with the increase of Ω_{SD}, which is due to the truth that a larger Ω_{SD} brings a better channel capacity of the legitimate direct S-D link. Furthermore, it can be seen that SCOP decreases as Ω_{RD} increases, especially when both Ω_{RD} and Ω_{SR} improve, such as the curve at $\Omega_{SR} = \Omega_{RD} = 30$ dB, a better SCOP performance can be achieved. This is because the diversity gain depends on the strength of channels pertaining to relays. Therefore, it can be concluded that a secure and reliable transmission will be guaranteed as the channel quality of either/both S-D and R-D (S-R) links increases.

Figure 8 presents the plot of the secrecy throughput, i.e., η, as a function of q_R for different values of λ_E when $\rho = 10$ dB, $\Omega_{SP} = \Omega_{RP} = 10$ dB, $\Omega_{SD} = 5$ dB, $R_B = 3$ bps/Hz, $R_S = 1$ bps/Hz. In this case, we assume a normalized two-dimensional network topology for numerical discussion, and the coordinates of S, R, D, and PU-Rx are $(0,0)$, $(q_R,0)$, $(1,0)$ and $(0,1)$, respectively. It can be first seen from Figure 8 that both schemes achieve a higher secrecy throughput at a smaller λ_E, which is in coherence with the conclusion drawn in Figure 3. Then, we can clearly observe that the closer the relay position is to the midpoint of the distance between S and D, i.e., $q_R = 0.5$, in the RT scheme, the higher secrecy throughput can be obtained. That is, we can graphically evaluate the optimal relay location for maximum secrecy throughput at the midpoint of the communication distance, which provides theoretical guidance and is aligned with the findings reported in [2,4,22]. However, the secrecy throughput of the DT scheme remains constant because it is independent of q_R.

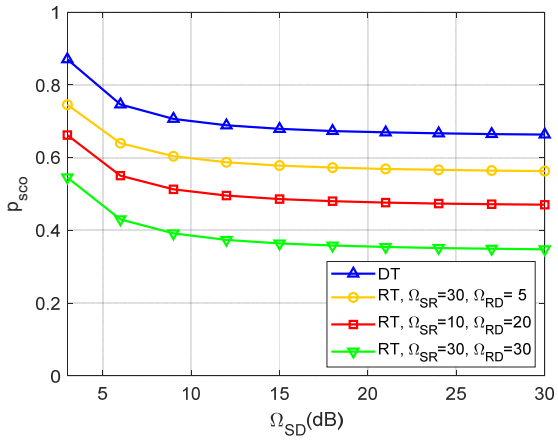


Figure 7. Impact of Ω_{SD} on the SCOP.

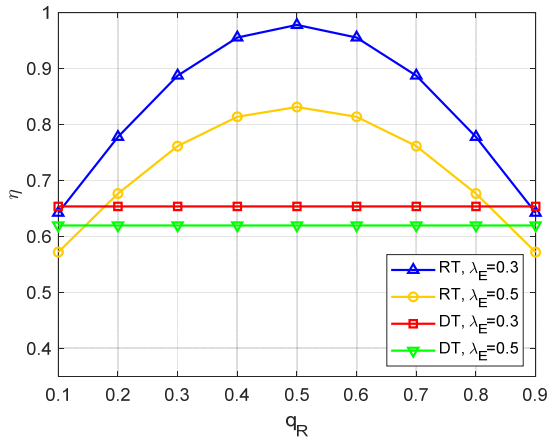


Figure 8. Impact of relay location on throughput.

6. Conclusions

This paper investigated the secrecy and throughput performance of an underlay cognitive vehicular relaying network, wherein a pair of vehicle nodes communicate with each other through a direct link and the help of a secondary DF relay in the presence of multiple movable HPPP-distributed eavesdroppers. Considering Rayleigh fading for V2I links and double-Rayleigh fading for V2V links, we derived expressions of the distribution functions of SNR for the traditional DT scheme and proposed RT scheme, respectively. The closed-form expressions of system performance, including SOP, COP, SCOP, and secrecy throughput, are deduced, and an asymptotic analysis is further conducted. Finally, we verified our analytical results via numerical simulations, revealed the effect of network parameters on secrecy and throughput performance, and showed the channel conditions under which the proposed relaying scheme outperforms the traditional direct schemes.

Future work will focus on the study of preventing and mitigating malicious eavesdropping by employing some advanced technologies, such as cooperative jamming and artificial noise, in such vehicular networks.

Author Contributions: Conceptualization, F.W. and C.L.; methodology, J.X.; software, L.S.; validation, Y.L.; resources, S.D. All authors have read and agreed to the published version of the manuscript.

Funding: This work was partially supported by the National Natural Science Foundation of China (62161016) and the Young Scholars Science Foundation of Lanzhou Jiaotong University (2021005).

Data Availability Statement: The datasets generated and analyzed during the current study are available from the corresponding author upon request.

Acknowledgments: We are truly grateful to the anonymous referees for their constructive comments on our paper.

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

References

1. Xu, L.; Huang, L.; Cao, C.; Wang, H.; Li, Y.; Gulliver, T.A. Outage performance of mobile V2V cooperative networks. *Phys. Commun.* **2019**, *34*, 295–300. [CrossRef]
2. Li, S.; Wang, F.; Gaber, J.; Chang, X. Throughput and energy efficiency of cooperative ARQ strategies for VANETs based on hybrid vehicle communication mode. *IEEE Access* **2020**, *8*, 114287–114304. [CrossRef]
3. Ngo, F.J.M.A. Performance analysis of cooperative V2V and V2I communications under correlated fading. *IEEE Trans. Intell. Transp.* **2020**, *21*, 3476–3484.
4. Feng, J.; Yu, F.R.; Pei, Q.; Chu, X.; Du, J.; Zhu, L. Cooperative computation offloading and resource allocation for blockchain-enabled mobile-edge computing: A deep reinforcement learning approach. *IEEE Int. Things J.* **2020**, *7*, 6214–6228. [CrossRef]
5. Suneel, Y.; Anshul, P. On the secrecy performance of cooperative cognitive vehicular relay networks. In Proceedings of the IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), BITS Pilani, Goa, India, 16–19 December 2019.
6. Cai, C.X.; Cai, Y.M.; Zhou, X.Y.; Yang, W.W.; Yang, W.D. When does relay transmission give a more secure connection in wireless Ad Hoc networks? *IEEE. Trans. Inf. Foren. Sec.* **2014**, *9*, 624–632. [CrossRef]
7. Anshul, P.; Suneel, Y.; Dinh-Thuan, D.; Rupak, K. Secrecy performance of cooperative cognitive AF relaying networks with direct links over mixed Rayleigh and double-Rayleigh fading channels. *IEEE Trans. Veh. Technol.* **2020**, *69*, 15095–15112.
8. Wyner, A.D. The wire-tap channel. *Bell Labs. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
9. Pan, G.F.; Tang, C.Q.; Zhang, X.; Li, T.T.; Weng, Y.; Chen, Y.F. Physical-layer security over non-small-scale fading channels. *IEEE Trans. Veh. Technol.* **2016**, *65*, 1326–1339. [CrossRef]
10. Liu, Y.; Qin, Z.; Elkashlan, M.; Gao, Y.; Hanzo, L. Enhancing the physical layer security of non-orthogonal multiple access in large-scale networks. *IEEE Trans. Wirel. Commun.* **2017**, *16*, 1656–1672. [CrossRef]
11. Fan, L.; Yang, N.; Duong, T. Exploiting direct links for physical layer security in multi-user multi-relay networks. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 3856–3867. [CrossRef]
12. Zhao, H.; Pan, G. Analysis of secure communications for a DF and RF relaying SIMO system with Gauss errors. *Sci. Sin-Inf.* **2016**, *46*, 350–360. [CrossRef]
13. Sun, A.; Liang, T.; Li, B. Secrecy performance analysis of cognitive sensor radio networks with an EH-based eavesdropper. *Sensors* **2017**, *17*, 1026. [CrossRef]
14. Li, J.; Zhao, H.; Johnson, M. Secrecy performance analysis of a cognitive network for IoT over k-μ channels. *Wirel. Commun. Mob. Com.* **2021**, *6*, 1–12. [CrossRef]
15. Xu, X.M.; He, B.A.; Yang, W.W.; Zhou, X.Y.; Cai, Y.M. Secure transmission design for cognitive radio networks with Poisson distributed eavesdroppers. *IEEE. Trans. Inf. Foren. Sec.* **2016**, *11*, 373–387. [CrossRef]
16. Chopra, K.; Bose, R.; Joshi, A. Secrecy performance of threshold-based decode-and-forward cooperative cognitive radio network. *IET Commun.* **2017**, *11*, 1396–1406. [CrossRef]
17. Mounia, B.; Faissal, E.B.; Mohamed-Slim, A. A PHY layer security analysis of uplink cooperative jamming-based underlay CRNs with multi-eavesdroppers. *IEEE Trans. Cogn. Commun.* **2020**, *6*, 704–717.
18. Zhang, T.; Cai, Y.M.; Huang, Y.Z.; Duong, T.Q.; Yang, W.W. Secure transmission in cognitive MIMO Relaying networks with outdated channel state information. *IEEE Access* **2016**, *4*, 8212–8224. [CrossRef]
19. Yang, Q.Q.; Ding, J.; Hu, A.G. Secrecy outage performance analysis of DF cognitive relay network with co-channel interference. *Wirel. Pers. Commun.* **2019**, *107*, 549–564. [CrossRef]
20. Zhang, J.; Pan, X.; Zhuang, Y. Secrecy performance for underlay cognitive multi-relaying MISO-RF/SIMO-FSO networks with outdated CSI. *Phys. Commun.* **2021**, *48*, 1–12. [CrossRef]
21. Salo, J.; El-Sallabi, H.M.; Vainikainen, P. Statistical analysis of the multiple scattering radio channel. *IEEE Trans. Antenn. Propag.* **2006**, *54*, 3114–3124. [CrossRef]
22. Nguyen, S.Q.; Kong, H.Y. Outage probability analysis in dual-hop vehicular networks with the assistance of multiple access points and vehicle nodes. *Wirel. Pers. Commun.* **2016**, *87*, 1175–1190. [CrossRef]
23. Pandey, A.; Yadav, S. Physical layer security in cooperative AF relaying networks with direct links over mixed Rayleigh and double-Rayleigh fading channels. *IET Commun.* **2018**, *67*, 10615–10630. [CrossRef]
24. Pandey, A.; Yadav, S. Physical layer security in cooperative amplify-and-forward relay networks over mixed Nakagami-m and double Nakagami-m fading channels: Performance evaluation and optimization. *IET Commun.* **2020**, *14*, 95–104. [CrossRef]
25. Mohamed, G.A.; Ahmed, H.A.; Mohammed, A. Secrecy performance and power allocation for cooperative vehicular relaying networks in the presence of interference. In Proceedings of the International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 20–22 February 2023.
26. Serdar, Z.A.; Erdogan, E. Secrecy outage probability of inter-vehicular cognitive radio networks. *Int. J. Commun. Syst.* **2020**, *33*, 1–11.

27. Hu, C.; Li, Q.; Yang, L.; Qin, J. Joint power allocation and collaborative beamforming for physical layer security in underlay CR NOMA relay systems. *Phys. Commun.* **2021**, *48*, 1–11. [CrossRef]
28. Li, Q.; Yang, Y.; Ma, W.K.; Lin, M.; Ge, J.; Lin, J. Robust cooperative beamforming and artificial noise design for physical-layer secrecy in AF multi-antenna multi-relay networks. *IEEE Trans. Signal. Proces.* **2014**, *63*, 206–220. [CrossRef]
29. Mensi, N.; Rawat, D.B.; Balti, E. PLS for V2I communications using friendly jammer and double kappa-mu shadowed fading. In Proceedings of the IEEE International Conference on Communications (ICC), Montreal, QC, Canada, 14–23 June 2021.
30. Xie, P.; Zhang, J.; Xing, M.; Zhang, L.; Wu, G. Aided opportunistic jammer selection for secrecy improvement in underlay cognitive radio networks. *Wirel. Pers. Commun.* **2019**, *107*, 1–20. [CrossRef]
31. Ghadi, F.R.; Kaveh, M.; Martín, D. Performance analysis of RIS/STAR-IOS-aided V2V NOMA/OMA communications over composite fading channels. *arXiv* **2023**, arXiv:2309.07738. [CrossRef]
32. Yang, L.; Yang, J.; Xie, W.; Hasna, M.O.; Tsiftsis, T.; Di Renzo, M. Secrecy performance analysis of RIS-aided wireless communication systems. *IEEE Trans. Veh. Technol.* **2020**, *69*, 12296–12300. [CrossRef]
33. Kaveh, M.; Yan, Z.; Jäntti, R. Secrecy performance analysis of RIS-aided smart grid communications. *IEEE Trans. Industr. Inform.* **2023**, 1–13. [CrossRef]
34. Wei, L.; Wang, K.; Pan, C.; Elkashlan, M. Secrecy performance analysis of RIS-aided communication system with randomly flying eavesdroppers. *IEEE Wireless Commun. Lett.* **2022**, *11*, 2240–2244. [CrossRef]
35. Saad, W.; Shokair, M.; Ibraheem, S.M. On the security of relay assisted cognitive radio networks in the presence of primary transceiver network. *Wirel. Pers. Commun.* **2019**, *104*, 949–977. [CrossRef]
36. Zhao, R.; Yuan, Y.; Fan, L.; He, Y. Secrecy performance analysis of cognitive decode-and-forward relay networks in Nakagami-m fading channels. *IEEE Trans. Commun.* **2017**, *65*, 549–563. [CrossRef]
37. Pinto, P.C.; Barros, J.; Win, M.Z. Secure communication in stochastic wireless networks—Part I: Connectivity. *IEEE Trans. Inf. Foren. Sec.* **2012**, *7*, 125–138. [CrossRef]
38. Pinto, P.C.; Barros, J.; Win, M.Z. Secure communication in stochastic wireless networks—Part II: Maximum rate and collusion. *IEEE Trans. Inf. Foren. Sec.* **2012**, *7*, 139–147. [CrossRef]
39. Ji, B.; Han, Y.; Li, P. Research on secure transmission performance of electric vehicles under Nakagami-m channel. *IEEE Trans. Intell. Transp. Syst.* **2020**, *22*, 1881–1891. [CrossRef]
40. Zhang, J.; Pan, G. Secrecy outage analysis with Kth best relay selection in dual-hop inter-vehicle communication systems. *Int. J. Electron. Commun.* **2017**, *71*, 139–144. [CrossRef]
41. Kim, T.T.; Poor, H.V. On the diversity gain of AF and DF relaying with noisy CSI at the source transmitter. *IEEE Trans. Inf. Theory* **2009**, *55*, 5064–5073. [CrossRef]
42. Lai, L.; Gamal, H.E. The relay–eavesdropper channel: Cooperation for secrecy. *IEEE Trans. Inf. Theory* **2008**, *54*, 4005–4019. [CrossRef]
43. Gurrala, K.K.; Das, S. Performance study of hybrid decode–amplify–forward (HDAF) relaying scheme for physical layer security in wireless cooperative network. *Int. J. Commun. Syst.* **2017**, *30*, e3182. [CrossRef]
44. Li, Z.; Jia, L.; Li, F. Outage performance analysis in relay-assisted inter-vehicular communications over double-Rayleigh fading channels. *IEEE Int. Conf. Commun. Mobile Comput.* **2010**, *2*, 266–270.
45. Nguyen, B.C.; Hoang, T.M.; Dung, L.T. Performance analysis of vehicle-to-vehicle communication with full-duplex amplify-and-forward relay over double-Rayleigh fading channels. *Veh. Commun.* **2019**, *19*, 100166. [CrossRef]
46. Sklar, B. Rayleigh fading channels in mobile digital communication systems. I. Characterization. *IEEE Commun. Mag.* **1997**, *35*, 90–100. [CrossRef]
47. Islam, M.R.; Hamouda, W. Performance of cooperative ad-hoc networks in Rayleigh fading channels. In Proceedings of the IEEE Vehicular Technology Conference, Montreal, QC, Canada, 25–28 September 2006; pp. 1–4.
48. Prudnikov, A.P.; Brychkov, Y.A.; Marichev, O.I. *Integrals and Series. Volume 2: Special Functions*; Gordon and Breach Science Publishers: Philadelphia, PA, USA, 1992.
49. The Wolfram Functions Site. Available online: http://functions.wolfram.com/ (accessed on 14 February 2024).
50. Gradshteyn, I.S.; Ryzhik, I.M. *Table of Integrals, Series, and Products*, 6th ed.; Academic Press: New York, NY, USA, 2000.
51. Bloch, M.; Barros, J.; Rodrigues, M.R.D.; McLaughlin, S.W. Wireless information-theoretic security. *IEEE Trans. Inf. Theory* **2008**, *54*, 2515–2534. [CrossRef]
52. He, B.; Zhou, X. Secure on-off transmission design with channel estimation errors. *IEEE Trans. Inf. Foren. Sec.* **2013**, *8*, 1923–1936. [CrossRef]
53. Papoulis, A.; Pillai, S.U. *Probability, Random Variables, and Stochastic Processes*, 4th ed.; McGraw-Hill Book Co.: New York, NY, USA, 2001.