applied sciences

MDPI

Article

Secure Transmission for Buffer-Aided Relay Networks in the Internet of Things

Chen Wei, Wendong Yang * and Yueming Cai

College of Communications Engineering, Army Engineering University of PLA, Nanjing 210007, China; weichen155@163.com (C.W.); caiym@vip.sina.com (Y.C.)

* Correspondence: ywd1110@163.com

Received: 20 September 2019; Accepted: 21 October 2019; Published: 24 October 2019

Abstract: This paper investigates the secure transmission for buffer-aided relay networks in the Internet of Things (IoT) in the presence of multiple passive eavesdroppers. For security enhancement, we adopt the max-link relay selection policy and propose three secure transmission schemes: (1) non-jamming (NJ); (2) source cooperative jamming (SCJ); and (3) source cooperative jamming with optimal power allocation (SCJ-OPA). Moreover, to analyze the secrecy performance comprehensively, two eavesdropping scenarios, i.e., non-colluding eavesdroppers (NCE) and colluding eavesdroppers (CE) are considered. Based on this, by modeling the dynamic buffer state transition as a Markov chain, we derive the exact closed-form expressions of the secrecy outage probability, the average secrecy throughput, and the end-to-end delay for each schemes. The analytical analysis and simulation shows that the SCJ-OPA scheme achieves similar performance as the NJ scheme when the total transmit power is small. On the other hand, when the transmit power is high, the performance achieved by SCJ-OPA is similar to that of SCJ. Thereby, the SCJ-OPA scheme can achieve better performance across the entire total transmit power, which makes up the defects of NJ and SCJ exactly.

Keywords: buffer-aided relay; physical layer security; Internet of Things (IoT); secrecy performance

1. Introduction

The Internet of things (IoT) serves a crucial architecture in future wireless communication systems, which can connect all things (e.g., mobile devices, sensors, and vehicles) to the Internet and enable these physical devices with sensorial and computing capabilities to cooperate with each other and achieve common goals [1–3]. Numerous fields such as industry, medical and transportation are expected to deploy IoT applications widely [4]. Moreover, due to the resource constraints of IoT devices (e.g., energy and computing capability), relay transmission is seen as a promising solution to solve the problem above in IoT networks, which has attracted great research interest [5–7]. Specifically, in [6], the unmanned aerial vehicle (UAV) was considered as the relay node firstly, and then the outage probability and throughput was investigated in the UAV relay assisted IoT networks enhanced with energy harvesting. In [7], G. Chen et al. considered both half-duplex (HD) and full-duplex (FD) decode-and-forward (DF) relaying schemes in multi-hop IoT networks, whose operating mode was similar to the one in [8], and studied the outage probability of the system with randomly located interferers.

However, since the best link may be not available, the relay has to follow the fixed transmission strategy to transmit the data packet [9]. That is to say, the selected relay receives the data packets from the source node in the first hop and then forwards it to the destination node immediately in the second hop. Recently, equipping data buffer at the relays has drawn considerable attentions due to its ability of offering high performance gains and extra degrees of freedom, which is called "buffer-aided relay" [10–13]. In [12], A. Ikhlef et al. proposed the max-max relay selection (MMRS) scheme for

DF relay networks. In [13], the max-link relay selection scheme was proposed, which could achieve better performance than MMRS by selecting the best link among all the available links. Nowadays, several works have considered applying the buffer-aided relay to IoT for increasing the reliability of communication networks [14–16]. The buffer-aided successive relay selection scheme for energy harvesting IoT networks based on DF and amplify-and-forward (AF) relay is investigated in [15]. In [16], a novel prioritization-based buffer-aided relay selection scheme was proposed, which can seamlessly combine both non-orthogonal multiple access (NOMA) and orthogonal multiple access (OMA) transmission in the IoT.

On the other hand, the broadcast characteristics of the wireless channels makes the wireless networks vulnerable to malicious attacks by illegitimate nodes, which presents a new challenge for the security of data transmission [17,18]. The encryption technique employed at the upper layer is a traditional method against eavesdropping [19]. However, this traditional technique not only imposes extra computational complexity resulted from the secret key management but can also be easily decrypted with the rapid improvement of the calculation level and thus being inappropriate to provide security services for IoT networks especially. Alternatively, physical layer security has been proposed as an effective approach to prevent the eavesdroppers from intercepting the information transmission by exploiting the randomness nature of the wireless channels [20–22]. Inspired by this, lots of research efforts have focused on the security of IoT networks from a physical layer security perspective [23–26]. In [23], the secrecy outage performance was studied for the wireless communication in IoT under eavesdropper collusion. In [24], three different scheduling schemes were designed to perform secure communication in an untrusted-relay-aided IoT uplink transmission. An on-off based multiuser secure transmission scheme was proposed for the heterogeneous IoT downlink networks in [25]. Then, the authors optimized several parameters to maximize the network secrecy throughput. Additionally, P. Huang et al. further examined the maximization of the secrecy sum rate for the downlink IoT systems with a novel relay-aided secure transmission scheme [26]. In recent years, some works have studied the physical layer security of buffer-aided relay networks [27–29]. In [27], G. Chen et al. proposed a novel max-ratio relay selection scheme to enhance the physical layer security for buffer-aided DF networks. For multi-relay multiple-input multiple-output (MIMO) cooperative networks, a buffer-aided joint transmit antenna and relay selection (JTARS) scheme was proposed in [28], and then the expression of the secrecy outage probability in closed-form was derived to assess the impact of different parameters on the secrecy performance. The closed-form expression of the secrecy outage probability was also derived in [29] to understand the secrecy performance of a buffer-aided underlay cognitive relay network. However, the secure transmission of buffer-aided relay network in IoT is an open issue to study. To the best of our knowledge, the design of secure transmission schemes for buffer-aided relay IoT networks has not been examined.

Inspired by these observations above, we investigate the secure transmission for buffer-aided relay IoT networks. To enhance the secrecy performance of the considered system, we adopt the max-link relay selection policy and propose three secure transmission schemes. The main contributions of this paper are summarized as follows:

- We propose three secure transmission schemes, i.e., non-jamming (NJ), source cooperative jamming (SCJ) and source cooperative jamming with optimal power allocation (SCJ-OPA), to enhance the secrecy performance for buffer-aided relay networks in IoT scenarios.
- By modeling the dynamic buffer state transition as a Markov chain, we derive the closed-form expressions of the secrecy outage probability, the average secrecy throughput and the end-to-end delay under the non-colluding eavesdroppers (NCE) and colluding eavesdroppers (CE) scenarios, respectively. Based on these expressions, the impacts of different parameters on the secrecy performance can be evaluated effectively.
- Our findings highlight that although the NJ and the SCJ schemes can achieve good secrecy performance when the total transmit power is small or large, respectively, the SCJ-OPA scheme

outperforms the other two schemes across the whole transmit power range of interest, which can make up the defects of the other two schemes.

Table 1 provides a list of the fundamental symbols throughout this paper. The remainder of the paper is organized as follows. In Section 2, we introduce the considered system model and the relay selection policy. Section 3 presents three transmission schemes. In Section 4, we investigate the several key performance metrics of the system, respectively. Section 5 provides simulation results. Finally, the conclusion is given in Section 6.

Table 1. List of the main notations and parameters.

Symbol	Description	Symbol	Description
M	Number of relay sensors	$(\cdot)^T$	The transpose operation
R_m	The m-th relay sensor	$M_{1,n}$	The number of available links in the first hop
K	Number of eavesdroppers	$M_{2,n}$	The number of available links in the second hop
E_k	The k-th eavesdropper	α	The power allocation factor
L	Buffer size	P_{out}	The overall secrecy outage probability
h_{ab}	The channel coefficient of link $a \to b$	$P_{out,n}$	The secrecy outage probability at state s_n
$\mathbf{h}_{ab}$	The channel vector of link $a \to b$	$\boldsymbol{\pi}$	The stationary probability vector
$E[\cdot]$	The expectation operation	$\boldsymbol{\pi_n}$	The stationary probability vector at state s_n
d_{ab}	The distance between a and b	R_s	The predefined secrecy rate
κ	The path loss factor	γ_{th}	The secrecy outage threshold
C_{ab}	The achievable secrecy rate of link $a \to b$	N	The number of all the buffer states
σ^2	The variance of AWGN	$\mathbf{A}$	The state transition matrix
P_S	The maximum transmit power of S	$\mathbf{A}_{v,n}$	The (v,n)th entry of $\mathbf{A}$
P_R	The maximum transmit power of relay sensor	$\mathbf{I}$	The identity matrix
P_{Total}	The total power	$\mathbf{Q}$	The all-ones matrix
s_n	The n-th buffer state	$\bar{T}$	The average secrecy throughput
$\varphi_n(m)$	The number of data packets in B_m at state s_n	$\bar{D}_{total}$	The average end-to-end delay
$\|\cdot\|$	The Euclidean or L_2 vector norm	$\bar{Q}_m$	The average queuing length at R_m

2. System Model and Relay Selection Policy

2.1. System Model

Let us consider the uplink transmission for the buffer-aided relay network in IoT application, as illustrated in Figure 1, which consists of a source sensor S, a controller D, M half-duplex intermediate relay sensors $\{R_m\}_{m=1}^{M}$ and K passive eavesdroppers $\{E_k\}_{k=1}^{K}$. In the network, all nodes are equipped with a single antenna and each relay is also equipped with a data buffer B_m of finite size L. Note that the data packets in the buffer obey the "first-in-first-out" rule. Therefore, the time that a data packet is transmitted from the relay sensor to the controller depends on the length of the queue. On the other hand, it takes only one time slot to transmit a packet from the source sensor to the relay sensor. Furthermore, the $S \to R$ and $R \to D$ links are referred to as the main channel, and the $S \to E$ and $R \to E$ links are referred to as the wiretap channels. All channels are modeled as the quasi-static flat Rayleigh fading, hence the channel coefficients keep unchanged in the coherent time of the channels [30]. Since the impact of significant path loss, the direct link between S and D is assumed unavailable. That is to say, the source sensor S has to communicate with the controller D via the assistance of multiple intermediate relay sensors [27,31,32].

In this paper, we denote the complex Gaussian random variable h_{ab} as the channel coefficient of link $a \to b$. According to this, the channel gain $|h_{ab}|^2$ can be regarded as an exponentially distributed random variable, which mean it is equal to $E\left[|h_{ab}|^2\right] = 1/\lambda_{ab} = d_{ab}^{-\kappa}$, where $E[\cdot]$ denotes the expectation operation, and d_{ab} and κ represent the distance of the link and the path loss factor, respectively. Specifically, the main channels are assumed independent and identically distributed (i.i.d), i.e., $\lambda_{SR} = \lambda_{RD}$. Besides, due to the energy limitation of the sensors nodes in IoT networks, we consider the total power constraint $P_S + P_R = P_{Total}$, where P_S and P_R represent the maximum transmit power of the source and the relay sensor, and P_{Total} denotes the total power.

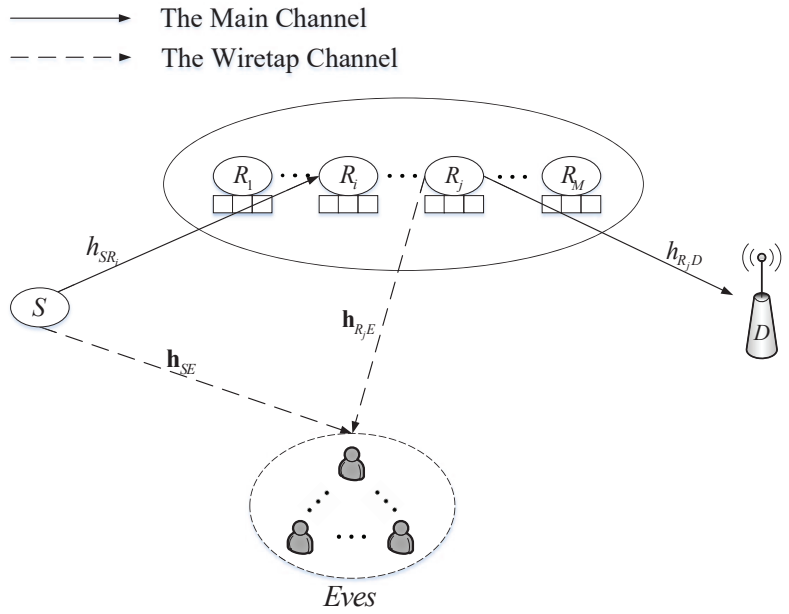

Figure 1. System Model.

2.2. Relay Selection Policy

In this subsection, we investigate the max-link relay selection considering the secrecy constraints [13]. To further probe into this relay selection policy mentioned above, the number of the data packets in each buffer is modeled as a state firstly. We define $s_n = [\varphi_n(1), \varphi_n(2), \cdots, \varphi_n(M)]^T$ as a certain buffer state, where $\varphi_n(m) \in \{0, 1, \cdots, L\}$ $(1 \le m \le M)$ denotes the number of data packets in buffer B_m at state s_n.

For the buffer-aided relay R_m, when its buffer is full or empty, it means that the relay cannot receive or transmit data packet, i.e., $\varphi_n(m) = L$ or $\varphi_n(m) = 0$. According to this, $\phi_{1,n}(m) = 1$ and $\phi_{2,n}(m) = 1$ denote that the relay R_m can be chosen to receive and transmit data packet at state s_n. In other words, the corresponding link is available. On the contrary, $\phi_{1,n}(m) = 0$ and $\phi_{2,n}(m) = 0$ represent the link in the first and second hops corresponding to the relay R_m is not available, respectively. Hence, we have $\phi_{1,n}(m) = \begin{cases} 1 & , \quad \varphi_n(m) \neq L \\ 0 & , \quad \varphi_n(m) = L \end{cases}$ and $\phi_{2,n}(m) = \begin{cases} 1 & , \quad \varphi_n(m) \neq 0 \\ 0 & , \quad \varphi_n(m) = 0 \end{cases}$.

Then, the number of available links at state s_n in the first or the second hops are, respectively, given by

$$M_{1,n} = \sum_{m=1}^{M} \phi_{1,n}(m), \tag{1}$$

$$M_{2,n} = \sum_{m=1}^{M} \phi_{2,n}(m). \tag{2}$$

Based on [13], the relay selection policy can be mathematically expressed as

$$R^* = \arg\max \left\{ \left| h_{SR'_{M_{1,n}}} \right|^2, \left| h_{R''_{M_{2,n}}D} \right|^2 \right\}, \tag{3}$$

where $\left|h_{SR'_{M_{1,n}}}\right|^2 = \max_{\varphi_n(i)\neq L}\left\{\left|h_{SR_i}\right|^2\right\}$ denotes the largest channel gain among $M_{1,n}$ available links in the first hop. Similarly, $\left|h_{R''_{M_{2,n}}D}\right|^2 = \max_{\varphi_n(j)\neq 0}\left\{\left|h_{R_jD}\right|^2\right\}$ is the largest channel gain among $M_{2,n}$ available links in the second hop.

From the above expression, we find that the relay with the strongest channel gain is always selected for data transmission. Specifically, when R^* is selected for reception, it receives and decodes the data packet and the packet can be stored in the buffer B^*. Hence, the number of packets in the buffer B^* increases by one. Similarly, when R^* is chosen for transmission, the controller D receives and decodes the data packet, and the buffer B^* discards the packet. Thereby, the number of the packets correspondingly decreases by one. Furthermore, if the whole communication between the source sensor S and the controller D is not successful, the buffer state will remain unchanged.

3. Transmission Schemes

In this section, a conventional non-jamming scheme and two source cooperative jamming schemes are presented for the considered buffer-aided relay IoT networks.

3.1. NJ Scheme

The total transmission is divided into two hops. In the first hop, the source sensor S sends the signal to the relay sensor while intercepted by K eavesdroppers $\{E_k\}_{k=1}^K$. Hence, the received SNR at R_i and E_k can be, respectively, expressed as

$$\gamma_{SR_i}^{NJ} = \frac{P_{S_1}\left|h_{SR_i}\right|^2}{\sigma^2}, \tag{4}$$

$$\gamma_{SE_k}^{NJ} = \frac{P_{S_1}\left|h_{SE_k}\right|^2}{\sigma^2}, \tag{5}$$

where $P_{S_1} = P_{Total}/2$ denotes the transmit power of the source sensor, which obeys the uniform power allocation for ease of analysis. $\left|h_{SR_i}\right|^2$ and $\left|h_{SE_k}\right|^2$ represent the channel gains of link $S \to R_i$ and $S \to E_k$, σ^2 is the variance of the additive white Gaussian noise (AWGN).

Similar to the first hop, the received SNR at D and E_k can be, respectively, given by

$$\gamma_{R_jD}^{NJ} = \frac{P_{R_1}\left|h_{R_jD}\right|^2}{\sigma^2}, \tag{6}$$

$$\gamma_{R_jE_k}^{NJ} = \frac{P_{R_1}\left|h_{R_jE_k}\right|^2}{\sigma^2}, \tag{7}$$

where $P_{R_1} = P_{Total}/2$ is the transmit power of the selected relay sensor, and $\left|h_{R_jD}\right|^2$ and $\left|h_{R_jE_k}\right|^2$ denote the channel gains of link $R_j \to D$ and $R_j \to E_k$, respectively.

Due to the presence of multiple eavesdroppers, we take both NCE and CE scenarios into account.

In the NCE scenario, the eavesdroppers decode information individually without interactions [33]. Hence, the received signal-to-noise ratio (SNR) at the eavesdroppers of the first and second hops can be, respectively, given by

$$\gamma_{1,NCE}^{NJ} = \max_{1\leq k\leq K}\gamma_{SE_k}^{NJ} = \frac{P_{S_1}\max\limits_{1\leq k\leq K}\left(\left|h_{SE_k}\right|^2\right)}{\sigma^2}, \tag{8}$$

$$\gamma_{2,NCE}^{NJ} = \max_{1\le k\le K} \gamma_{R_jE_k}^{NJ} = \frac{P_{R_1} \max\limits_{1\le k\le K} \left(\left| h_{R_jE_k} \right|^2 \right)}{\sigma^2}. \tag{9}$$

In the CE scenario, all eavesdroppers can exchange the information with each other and adopt the maximal ratio combining (MRC) for enhancing the intercept ability [34,35]. Thus, the instantaneous SNR of the eavesdroppers' channels for the first and second hops are expressed as

$$\gamma_{1,CE}^{NJ} = \sum_{1\le k\le K} \gamma_{SE_k}^{NJ} = \frac{P_{S_1} \left\| \mathbf{h}_{SE} \right\|^2}{\sigma^2}, \tag{10}$$

$$\gamma_{2,CE}^{NJ} = \sum_{1\le k\le K} \gamma_{R_jE_k}^{NJ} = \frac{P_{R_1} \left\| \mathbf{h}_{R_jE} \right\|^2}{\sigma^2}, \tag{11}$$

where $\mathbf{h}_{SE}$ denotes the $K \times 1$ channel vector between the source sensor and the eavesdroppers. Similarly, $\mathbf{h}_{R_jE}$ represents the channel vector between the selected relay sensor and the eavesdroppers.

The NJ scheme is a benchmark invoked for the purpose of comparison, which can also be applicable for the practical application scenario due to it lower complexity.

3.2. SCJ Scheme

In this case, when the second hop is selected, the source sensor can send jamming signals to the eavesdroppers with the transmit power P_{J_2}, which degrades the quality of eavesdroppers' channels effectively without interfering other nodes. Furthermore, due to the total power constraint, we have $P_{S_2} + P_{J_2} + P_{R_2} = P_{Total}$, where P_{S_2} denotes the transmit power of the source sensor when transmitting useful information. Similar to the NJ scheme, the power allocation follows the uniform allocation rule, i.e., $P_{R_2} = P_{Total}/2$, $P_{S_2} = P_{J_2} = P_{Total}/4$.

The first hop of the SCJ scheme is the same as the NJ scheme, hence we have $\gamma_{SR_i}^{SCJ} = P_{S_2} \left| h_{SR_i} \right|^2 / \sigma^2$ and $\gamma_{SE_k}^{SCJ} = P_{S_2} \left| h_{SE_k} \right|^2 / \sigma^2$. In the second hop, the received signal-to-interference-plus-noise-ratio (SINR) at E_k is given by

$$\gamma_{R_jE_k}^{SCJ} = \frac{P_{R_2} \left| h_{R_jE_k} \right|^2}{\sigma^2 + P_{J_2} \left| h_{JE_k} \right|^2}, \tag{12}$$

where $\left| h_{JE_k} \right|^2$ denotes the link of $S \to E_k$ when S acts as a jamming node.

Thus, for the NCE scenario, the received SNR and SINR at the eavesdroppers of the first and second hops can be written as

$$\gamma_{1,NCE}^{SCJ} = \frac{P_{S_2} \max\limits_{1\le k\le K} \left(\left| h_{SE_k} \right|^2 \right)}{\sigma^2}, \tag{13}$$

$$\gamma_{2,NCE}^{SCJ} = \max_{1\le k\le K} \left(\frac{P_{R_2} \left| h_{R_jE_k} \right|^2}{\sigma^2 + P_{J_2} \left| h_{JE_k} \right|^2} \right). \tag{14}$$

For the CE mode, the received SNR and SINR of the eavesdroppers' channel for the first and second hops are given by

$$\gamma_{1,CE}^{SCJ} = \frac{P_{S_2} \left\| \mathbf{h}_{SE} \right\|^2}{\sigma^2}, \tag{15}$$

$$\gamma_{2,CE}^{SCJ} = \frac{P_{R_2} \left\| \mathbf{h}_{R_jE} \right\|^2}{\sigma^2 + P_{J_2} \left\| \mathbf{h}_{JE} \right\|^2}, \tag{16}$$

where $\mathbf{h}_{JE}$ represents the $K \times 1$ channel vector between the source sensor and the eavesdroppers when the source acts as a jamming node.

3.3. SCJ-OPA Scheme

To further enhance the physical layer security for the SCJ scheme, the optimal power allocation operation is employed at the source sensor node under the SCJ-OPA scheme. Similar to the section above, we still assume that $P_{R_3} = P_{Total}/2$. Then, we have $P_{S_3} + P_{J_3} = P_{Total}/2$. Given $P_{S_3} = \alpha P_{Total}/2$ and $P_{J_3} = (1-\alpha) P_{Total}/2$ where $0 < \alpha < 1$ denotes the power allocation factor. We aim to find the optimal power allocation factor to minimize the secrecy outage probability of the considered system. Therefore, the optimization problem can be written as

$$\min_{\substack{\alpha \\ \text{s.t. } 0<\alpha<1}} P_{out}, \tag{17}$$

where P_{out} represents the overall secrecy outage probability of the system. We derive the expression of the secrecy outage probability and solve the optimization in the following section. Moreover, making an appropriate substitution of the parameters, i.e., $P_{S_2} \to P_{S_3}$ and $P_{J_2} \to P_{J_3}$, the received SNR or SINR at the corresponding node under the SCJ-OPA scheme can be obtained easily, hence is omitted.

Now, according to the authors of [36,37], the achievable secrecy rate of the first and second hops can be, respectively, expressed as

$$C^{\star}_{SRE} = \left[\log_2\left(1+\gamma^{\star}_{SR_i}\right) - \log_2\left(1+\gamma^{\star}_{1,E}\right)\right]^{+}, \tag{18}$$

$$C^{\star}_{RDE} = \left[\log_2\left(1+\gamma^{\star}_{R_jD}\right) - \log_2\left(1+\gamma^{\star}_{2,E}\right)\right]^{+}, \tag{19}$$

where $\star \in \{NJ, SCJ, SCJ-OPA\}$, $\gamma^{\star}_{1,E} \in \left\{\gamma^{\star}_{1,NCE}, \gamma^{\star}_{1,CE}\right\}$, $\gamma^{\star}_{2,E} \in \left\{\gamma^{\star}_{2,NCE}, \gamma^{\star}_{2,CE}\right\}$, $[x]^{+} = \max\{0, x\}$.

4. Performance Analysis

4.1. Secrecy Outage Analysis

In this subsection, we investigate the secrecy outage performance of the considered system. According to [13], considering all of the possible states, the secrecy outage probability of the system is given by

$$P^{\star}_{out}(\gamma_{th}) = \sum_{n=1}^{N} \boldsymbol{\pi}^{\star}_{n} P^{\star}_{out,n}(\gamma_{th}), \tag{20}$$

where $N = (L+1)^M$ denotes the total number of states, $\boldsymbol{\pi}^{\star}_{n}$ and $P^{\star}_{out,n}(\gamma_{th})$ denote that when the state is s_n, the corresponding stationary probability and the secrecy outage probability. $\gamma_{th} \triangleq 2^{2R_s}$ represents the secrecy outage threshold. Besides, to make the following analysis traceable, we define $\gamma^{\star}_{E1} = \left(1+\gamma^{\star}_{SR'_{M_{1,n}}}\right) / \left(1+\gamma^{\star}_{1,E}\right)$, $\gamma^{\star}_{E2} = \left(1+\gamma^{\star}_{R''_{M_{2,n}}D}\right) / \left(1+\gamma^{\star}_{2,E}\right)$ and the noise variance is $\sigma^2 = 1$.

4.1.1. NJ Scheme

According to [28], the secrecy outage probability at state s_n under the NJ scheme is given by

$$P^{NJ}_{out,n}(\gamma_{th}) = F_{\gamma^{NJ}_{E1}}(\gamma_{th}) \cdot F_{\gamma^{NJ}_{E2}}(\gamma_{th}). \tag{21}$$

Theorem 1. *The CDF of γ_{E1}^{NJ} under the NCE scenario is given by*

$$F_{\gamma_{E1}^{NJ}}(x) = \sum_{s=0}^{M_{1,n}} \sum_{t=0}^{K-1} \binom{M_{1,n}}{s} \binom{K-1}{t} \frac{(-1)^{s+t} K \lambda_{SE}}{\lambda_{SE}(t+1) + \lambda_{SR} s x} e^{-\frac{\lambda_{SR} s (x-1)}{P_{S_1}}}. \tag{22}$$

Proof of Theorem 1. See Appendix A. □

Theorem 2. *The CDF of γ_{E1}^{NJ} under the CE scenario can be written as*

$$F_{\gamma_{E1}^{NJ}}(x) = \sum_{s=0}^{M_{1,n}} \binom{M_{1,n}}{s} (-1)^s \left(\frac{\lambda_{SE}}{\lambda_{SE} + \lambda_{SR} s x} \right)^K e^{-\frac{\lambda_{SR} s (x-1)}{P_{S_1}}}. \tag{23}$$

Proof of Theorem 2. See Appendix B. □

It is worth noting that, if we replace some parameters, i.e., $M_{1,n} \to M_{2,n}$, $P_{S_1} \to P_{R_1}$, $\lambda_{SR} \to \lambda_{RD}$ and $\lambda_{SE} \to \lambda_{RE}$, we can derive the CDF of γ_{E2}^{NJ} due to the symmetry of the first and second hops.

Next, we proceed with the stationary probability under the NJ scheme $\boldsymbol{\pi}^{NJ}$. Firstly, we denote Ω_n as the set whose states can be transferred from state s_n successfully within one step. Then, according to the authors of [13,38,39], we denote $\mathbf{A}^{NJ} \in \mathbb{R}^{N \times N}$ as the state transition matrix of the Markov chain under the NJ scheme, where the entry $\mathbf{A}_{v,n}^{NJ} = \Pr[T(t+1) = s_v \,|\, T(t) = s_n]$ denotes the transition probability of moving from state s_n to the state s_v, where s_v is an element in set Ω_n.

As can be seen from the relay selection policy, if the packet is not successfully transmitted to the corresponding node, the buffer state keeps unchanged. In other words, the secrecy outage event occurs. On the other hand, when the current state transforms to another state s_v within one step, i.e., $s_v \in \Omega_n$, then the corresponding transmission is successful. From these observations, the entry of $\mathbf{A}^{NJ}$ is given by

$$\mathbf{A}_{v,n}^{NJ} = \begin{cases} P_{out,n}^{NJ}(\gamma_{th}), & s_v = s_n \\ \frac{1 - P_{out,n}^{NJ}(\gamma_{th})}{M_{1,n} + M_{2,n}}, & s_v \in \Omega_n \\ 0, & else \end{cases}. \tag{24}$$

Based on this, we can obtain the stationary probability vector in the following.

Theorem 3. *The stationary probability vector of the NJ scheme is given by*

$$\boldsymbol{\pi}^{NJ} = \left(\mathbf{A}^{NJ} - \mathbf{I} + \mathbf{Q} \right)^{-1} \mathbf{b}, \tag{25}$$

where $\boldsymbol{\pi}^{NJ} = \left[\pi_1^{NJ}, \pi_2^{NJ} \cdots, \pi_N^{NJ} \right]^T$, $\mathbf{b} = (1, 1, \cdots, 1)^T$, $\mathbf{I}$ is the identity matrix and $\mathbf{Q}$ is the all-ones matrix.

Proof of Theorem 3. The proof can be found in [13]. □

Now, by substituting Equations (21) and (25) into Equation (20), the closed-form expression of the secrecy outage probability for the NCE and CE scenarios under the NJ scheme can be easily derived, respectively.

4.1.2. SCJ Scheme

The secrecy outage probability at state s_n under the SCJ scheme can be represented as

$$P_{out,n}^{SCJ}(\gamma_{th}) = F_{\gamma_{E1}^{SCJ}}(\gamma_{th}) \cdot F_{\gamma_{E2}^{SCJ}}(\gamma_{th}). \tag{26}$$

Theorem 4. *The CDF of* γ_{E2}^{SCJ} *under the NCE scenario is given by*

$$F_{\gamma_{E2}^{SCJ}}(x) = K\sum_{s=0}^{M_{2,n}}\sum_{t=0}^{K-1}\binom{M_{2,n}}{s}\binom{K-1}{t}(-1)^{s+t}\beta^t\left[\frac{\lambda_{JE}}{P_{J_2}}I_1(t)+\beta I_2(t)\right]e^{-\frac{\lambda_{RD}s(x-1)}{P_{R_2}}}, \tag{27}$$

where $\beta=\frac{\lambda_{JE}P_{R_2}}{\lambda_{RE}P_{J_2}}$, $\mu(t)=\frac{\lambda_{RD}sx+\lambda_{RE}(t+1)}{P_{R_2}}$, $I_1(t)$ *and* $I_2(t)$ *are given by*

$$I_1(t)=\begin{cases}-e^{\beta\mu(t)}Ei(-\beta\mu(t)), & t=0\\ \sum_{l=1}^{t}\frac{(l-1)!(-\mu(t))^{t-l}}{t!\beta^l}-\frac{(-\mu(t))^t e^{\beta\mu(t)}Ei(-\beta\mu(t))}{t!} & t>0\end{cases}, \tag{28}$$

$$I_2(t)=\sum_{l=1}^{t+1}\frac{(l-1)!(-\mu(t))^{t-l+1}}{(t+1)!\beta^l}-\frac{(-\mu(t))^{t+1}}{(t+1)!}e^{\beta\mu(t)}Ei(-\beta\mu(t)). \tag{29}$$

Proof of Theorem 4. See Appendix C. □

Theorem 5. *The CDF of* γ_{E2}^{SCJ} *under the CE scenario can be presented as*

$$F_{\gamma_{E2}^{SCJ}}(x)=\sum_{s=0}^{M_{2,n}}\binom{M_{2,n}}{s}(-1)^s e^{-\frac{\lambda_{RD}s(x-1)}{P_{R_2}}}\Phi, \tag{30}$$

where Φ *is given by*

$$\Phi=1+\frac{\lambda_{JE}^K}{(K-1)!}e^{\omega\lambda_{JE}}\sum_{t=1}^{K}\sum_{l=0}^{K-1}\binom{K}{t}\binom{K-1}{l}(-\theta)^t(-\omega)^{K-1-l}\Phi_1, \tag{31}$$

with $\theta=\frac{\lambda_{RD}sx}{P_{J_2}\lambda_{RE}}$, $\omega=\theta+\frac{1}{P_{J_2}}$ *and* Φ_1 *can be expressed as*

$$\Phi_1=\begin{cases}\frac{\Gamma(l-t+1,\ \omega\lambda_{JE})}{\lambda_{JE}^{l-t+1}}, & l-t\geq 0\\ -Ei(-\omega\lambda_{JE}), & l-t=-1\\ e^{-\omega\lambda_{JE}}\sum_{v=1}^{t-l-1}\frac{(v-1)!(-\lambda_{JE})^{t-l-1-v}}{(t-l-1)!\omega^v}-\frac{(-\lambda_{JE})^{t-l-1}}{(t-l-1)!}Ei(-\omega\lambda_{JE}), & l-t\leq -2\end{cases}, \tag{32}$$

where $\Gamma(\cdot,\cdot)$ *is the upper incomplete Gamma function [40] (eq. (8.350.2)), and* $Ei(\cdot)$ *is the exponential integral function [40] (eq. (8.211.1)).*

Proof of Theorem 5. See Appendix D. □

Recalling the first hop of the SCJ scheme is the same as the NJ scheme, we can derive $F_{\gamma_{E1}^{SCJ}}$ by making a substitution of some parameters. Furthermore, the stationary probability vector of the SCJ scheme $\boldsymbol{\pi}^{SCJ}=\left(\mathbf{A}^{SCJ}-\mathbf{I}+\mathbf{B}\right)^{-1}\mathbf{b}$ can also be obtained following the similar analysis as in **Theorem 3**. Hence, the secrecy outage probability for the NCE and CE scenarios under the SCJ scheme in closed-form can be derived by substituting Equation (26) and $\boldsymbol{\pi}^{SCJ}$ into Equation (20).

4.1.3. SCJ-OPA Scheme

Since the difference between the SCJ and the SCJ-OPA scheme is that the latter operates the optimal power allocation at the source sensor, making a substitution of the parameters $P_{S_2}\rightarrow P_{S_3}$, $P_{R_2}\rightarrow P_{R_3}$ and $P_{J_2}\rightarrow P_{J_3}$, we can obtain the secrecy outage probability for the NCE and CE scenarios under the SCJ-OPA scheme easily.

However, recalling the closed-form expression and the optimization problem mentioned above, we find that an explicit expression for α is intractable. Instead, considering that the value space of α is limited, thus the optimal result can be obtained by numerical calculations, i.e., the grid-search solution or the straightforward search solution, and the computer complexity is also acceptable.

4.2. Average Secrecy Throughput and End to End Delay

The average secrecy throughput can measure the average rate of the transmitted information which is kept confidential to the eavesdropper. Resorting to the work in [24,41], the average secrecy throughput can be expressed as

$$\bar{T}^{\star} = \frac{R_s}{2}\left(1 - P^{\star}_{out}\left(\gamma_{th}\right)\right), \tag{33}$$

where the factor $1/2$ is because every packet reaches the controller takes two time slots.

Recalling the definition of the secrecy outage probability, the value of $P^{\star}_{out}$ is increased with the increase of R_s. Thus, from Equation (33), we observe that the function of the average secrecy throughput with respect to R_s is a unimodal function. When R_s is small or large, only the lower average secrecy throughput can be obtained. That is to say, there exists an optimal secrecy rate which can maximum the average secrecy throughput of the considered system. The optimization problem can be given by

$$\max_{R_s} \bar{T}^{\star}. \tag{34}$$

Following a similar approach, we find the optimal R_s by utilizing the grid-search or the straightforward search techniques.

In the buffer-aided relay IoT network, the end-to-end delay is the time slots it takes for a data packet to arrive at the controller from the source sensor, which is given by

$$\bar{D}^{\star}_{total} = 1 + \bar{D}^{\star}_{R}, \tag{35}$$

where the term "1" represents the delay at the source sensor. This is because each packet takes only one time slot when it is sent from the source sensor to the relay sensor. $\bar{D}^{\star}_{R}$ denotes the average delay at the intermediate relay sensors. On the other hand, considering the probability of selecting a relay sensor R_m among all M relays is the same, we can obtain $\bar{D}^{\star}_{R_m} = \bar{D}^{\star}_{R}$ and $\bar{T}^{\star}_{m} = \bar{T}^{\star}/M$, where $\bar{D}^{\star}_{R_m}$ denotes the delay at relay R_m, and $\bar{T}^{\star}_{m}$ represents the average secrecy throughput at relay R_m.

Then, we denote $\varphi_n\left(m\right)$ as the queuing length in the buffer of relay R_m at state s_n. Therefore, considering all of the possible states, the average queuing length at R_m can be written as

$$\bar{Q}^{\star}_{m} = \sum_{n=1}^{N} \pi^{\star}_{n} \varphi_n\left(m\right). \tag{36}$$

With the help of the Little's law [42], the average delay at relay R_m is given by

$$\bar{D}^{\star}_{R_m} = \frac{\bar{Q}^{\star}_{m}}{\bar{T}^{\star}_{m}}. \tag{37}$$

Finally, based on the analysis above, the average end-to-end delay can be expressed as

$$\bar{D}^{\star}_{total} = 1 + \frac{2M \sum\limits_{n=1}^{N} \pi^{\star}_{n} \varphi_n\left(m\right)}{R_s\left(1 - P^{\star}_{out}\left(\gamma_{th}\right)\right)}. \tag{38}$$

5. Simulation Analysis

In this section, Monte-Carlo simulation results are presented to validate the theoretical analysis derived in the previous sections for the three transmission schemes. Without loss of generality,

the normalized distance is set as follows: $d_{SR} = d_{RD} = 1$, $d_{SE} = d_{RE} = 2$. The path loss factor κ is set to be 3. From the figures, the theoretical curves are in exact agreement with the simulation results, which verifies the accuracy of our theoretical analysis.

Figure 2 illustrates the secrecy outage probability versus the total transmit power budget P_{Total} for the three proposed transmission schemes. As shown in Figure 2, the secrecy outage probability decreases with the increase of P_{Total} until a secrecy outage performance floor occurs at high transmit power. This is intuitive since both capacities of the main and wiretap channels improve with the increase of the transmit power. Furthermore, we observe that, in both the NCE and CE scenarios, the NJ scheme outperforms the SCJ scheme at the low total transmit power, while the opposite holds in the high total transmit power. For the SCJ-OPA scheme, almost the same performance as the NJ scheme can be obtained at the low transmit power, and, when P_{Total} is large, a similar performance as the SCJ scheme can also be achieved, which indicates that the SCJ-OPA scheme covers the shortages of the NJ and SCJ schemes exactly. In addition, it is worth noting that the secrecy performance of the CE scenario is worse than that of the NCE scenario under the same conditions, which is because that the MRC scheme utilized by the CE mode can enhance the ability of eavesdropping.

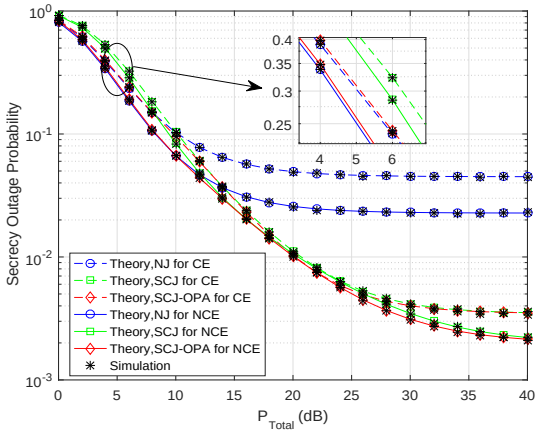

Figure 2. Secrecy outage probability vs. the total transmit power budget P_{Total} for the three proposed transmission schemes when $R_s = 0.6$ (bit/s/Hz), $M = 3$, $L = 2$, $K = 2$.

Figure 3 plots the average secrecy throughput of the three proposed transmission schemes versus the total transmit power budget P_{Total}. It is observed that the average secrecy throughput increases until it converges to a fixed value with the increase of the total transmit power. In addition, we further observe that the NJ and SCJ-OPA schemes outperforms the SCJ scheme in terms of the average secrecy throughput when P_{Total} is not large. At the high P_{Total}, the SCJ and SCJ-OPA schemes achieve better performance than the NJ scheme. In other words, utilizing the SCJ-OPA scheme can improve the secrecy performance of the considered system, especially when the total power is small or large.

Figure 4 investigates the impact of the secrecy rate R_s on the average secrecy throughput for the NCE and CE scenarios, respectively. From these figures, we find that, for both NCE and CE scenarios, the average secrecy throughput first increases with the increase of R_s and then decreases when R_s increases beyond a certain value, which demonstrates the accuracy of the analysis in Section 4.2. Besides, it can be observed that when the total transmit power is small, i.e., $P_{Total} = 10$ dB, the SCJ-OPA scheme obtains a similar average secrecy throughput as the NJ scheme, which are both better than the SCJ scheme. On the other hand, when the total transmit power is large, i.e., $P_{Total} = 20$ dB, the SCJ-OPA and SCJ schemes are superior to the NJ scheme, which is consistent with the previous analysis and simulation.

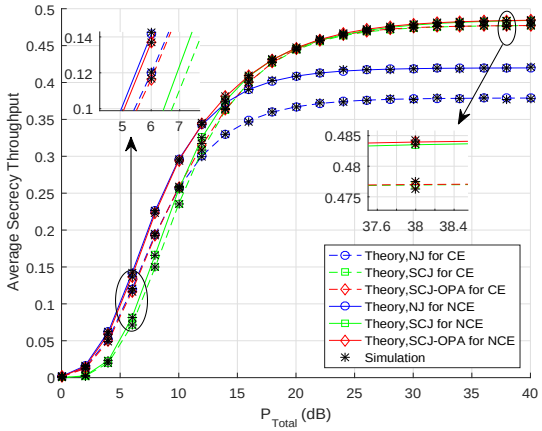

Figure 3. Average Secrecy throughput vs. the total transmit power budget P_{Total} for the three proposed transmission schemes when $R_s = 1$ (bit/s/Hz), $M = L = 2$, $K = 2$.

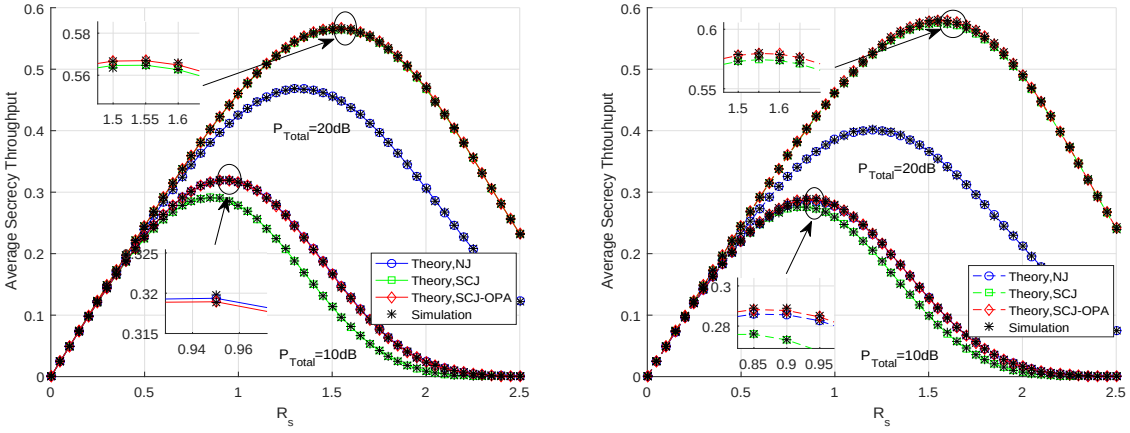

Figure 4. Average Secrecy throughput vs. the secrecy rate R_s for the three proposed transmission schemes under the NCE (**a**) and CE (**b**) scenarios when $M = 2$, $L = 3$, $K = 2$, $P_{Total} = 10, 20$ dB.

Figure 5 presents the end-to-end delay for the three proposed transmission schemes versus the total transmit power budget P_{Total}. As shown in Figure 5, the end-to-end delay is significantly decreased as the P_{Total} increases in both the NCE and CE scenarios. Similarly, when the P_{Total} increases beyond a certain value, the end-to-end delay remains unchanged. That is to say, a performance floor occurs. This is because the secrecy outage probability tends to a fixed value at this moment. Furthermore, we can also observe that the SCJ-OPA scheme achieves better performance in terms of the end-to-end delay than the other two schemes across the entire transmit power range of interest, which indicates the advantage of the SCJ-OPA scheme.

Figure 6 plots the secrecy outage probability versus the buffer size L for the three proposed transmission schemes under the NCE and CE scenarios, respectively. As can be readily observed, as the buffer size increases, the achieved performance approaches the performance floor. Specifically, for both NCE and CE scenarios, the NJ and SCJ-OPA schemes outperform the SCJ scheme when P_{Total} is small. On the contrary, the SCJ and SCJ-OPA schemes are superior to the NJ scheme at the condition of the high transmit power, which matches the simulation above.

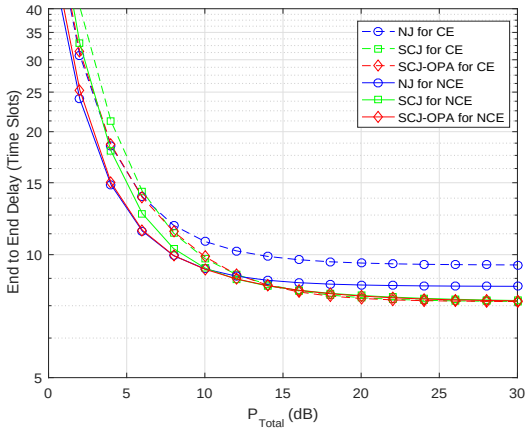

Figure 5. End to end delay vs. the total transmit power budget P_{Total} for the three proposed transmission schemes when $R_s = 0.6$ (bit/s/Hz), $M = L = 2$, $K = 3$.

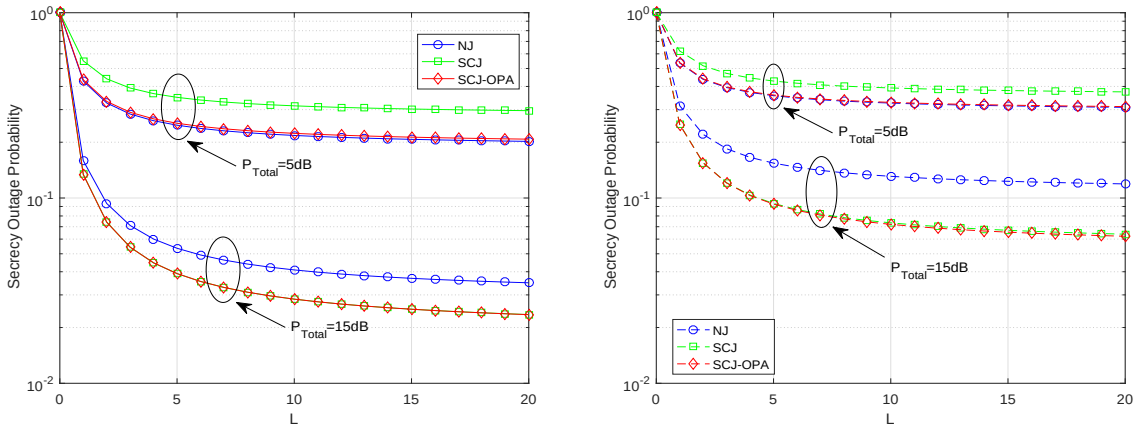

Figure 6. Secrecy outage probability vs. the buffer size L for the three proposed transmission schemes under the NCE (**a**) and CE (**b**) scenarios when $R_s = 0.5$ (bit/s/Hz), $M = 2$, $K = 3$, $P_{Total} = 5, 15$ dB.

Figure 7 shows the impact of the power allocation factor α on the secrecy outage probability for the SCJ-OPA scheme. The curves shown in Figure 7 are calculated by using the grid-search or the straightforward search methods. It is clearly seen that the optimal power allocation factor is decreased with the increase of P_{Total}. That is to say, more power is allocated to transmit the useful information at the source sensor when P_{Total} is not large. This is because, when α is too small, only few packets can be sent from the source sensor to relay sensors in the first hop. Thereby, not enough data packets can be forwarded to the controller. Even if the jamming power is large in the second hop, it cannot improve the secrecy performance of the whole network. On the other hand, with the increase of P_{Total}, the dominant factor that affects the secrecy performance of the considered system changes from the information transmit power to the jamming transmit power at the source sensor, which is the exact reason the optimal power allocation factor becomes smaller gradually.

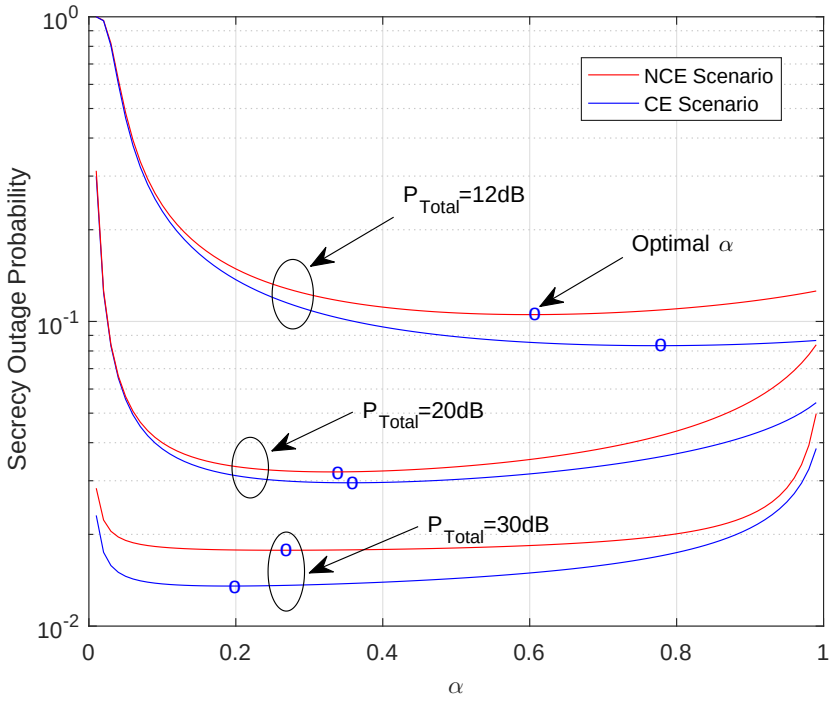

Figure 7. Secrecy outage probability vs. the power allocation factor α for the SCJ-OPA scheme under the NCE and CE scenarios when $R_s = 0.5$ (bit/s/Hz), $M = L = 2$, $K = 2$, and $P_{Total} = 12, 20, 30$ dB.

6. Conclusions

In this paper, we propose three secure transmission schemes for buffer-aided relay networks in IoT. To take full advantage of buffer-aided relay, the max-link relay selection policy is adopted to enhance the secrecy performance by selecting the main link with the best rate. Furthermore, for each schemes, we also derive the exact expressions of the secrecy outage probability, the average secrecy throughput and the end-to-end delay in closed-form by utilizing the Markov chain theory under both the NCE and CE scenarios, respectively, which provides an effective way to evaluate the secrecy performance of each proposed scheme. Our numerical results indicate that, when the total power P_{Total} is small, the performance achieved by the SCJ-OPA scheme is similar to that of the NJ scheme. On the other hand, the SCJ-OPA scheme can also achieve almost identical performance as the SCJ scheme when P_{Total} is high. In other words, the SCJ-OPA scheme achieves better performance across the whole transmit power range of interest than the other two schemes, which is because the factor α can be dynamically allocated under different total transmit power. These results could be useful in the design of buffer-aided relay IoT networks under multiple eavesdroppers scenarios.

Author Contributions: C.W. and W.Y. conceived the model; C.W. performed the simulation results and wrote the paper; and W.Y., Y.C. provided some suggestions and revised the paper.

Funding: This work was supported by the National Natural Science Foundation of China under Grant Nos. 61771487 and 61371122.

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

Appendix A

Let us define $X_1 = \left|h_{SR'_{M_{1,n}}}\right|^2$ and $Y_1 = \max\limits_{1\le k\le K}\left(\left|h_{SE_k}\right|^2\right)$, according to the order statistic, the CDF of γ_{E1}^{NJ} under the NCE scenario can be expressed as

$$F_{\gamma_{E1}^{NJ}}(x) = \Pr\left(\frac{1+P_{S_1}X_1}{1+P_{S_1}Y_1} < x\right) = \int_0^\infty F_{X_1}\left(\frac{x-1}{P_{S_1}} + xy\right) f_{Y_1}(y)\, dy. \tag{A1}$$

According to the relay selection policy and the analysis above, the CDF of X_1 and the PDF of Y_1 are, respectively, expressed as

$$F_{X_1}(x) = \left(1 - e^{-\lambda_{SR}x}\right)^{M_{1,n}}, \tag{A2}$$

$$f_{Y_1}(y) = K\lambda_{SE}\left(1 - e^{-\lambda_{SE}y}\right)^{K-1} e^{-\lambda_{SE}y}. \tag{A3}$$

Then, substituting Equations (A2) and (A3) into Equation (A1) yields the desired result shown in **Theorem 1** by using the binomial theorem [43].

Appendix B

Assuming $Y_2 = \|\mathbf{h}_{SE}\|^2$, the PDF of Y_2 can be presented as [44]

$$f_{Y_2}(y) = \lambda_{SE}^K \frac{y^{K-1}e^{-\lambda_{SE}y}}{(K-1)!}. \tag{A4}$$

Following the similar analysis as Equation (A1), we can derive the CDF of γ_{E1}^{NJ} under the CE scenario, which can be expressed as

$$F_{\gamma_{E1}^{NJ}}(x) = \int_0^\infty F_{X_1}\left(\frac{x-1}{P_{S_1}} + xy\right) f_{Y_2}(y)\, dy. \tag{A5}$$

To this end, substituting Equations (A2) and (A4) into Equation (A5), the CDF of γ_{E1}^{NJ} under the CE scenario can be obtained as Equation (23) after some simple manipulations.

Appendix C

We first define $Z_1 = \max\limits_{1\le k\le K}\left(\frac{P_{R_2}\left|h_{R^*E_k}\right|^2}{1+P_{J_2}\left|h_{JE_k}\right|^2}\right)$, and the CDF of Z_1 can be expressed as

$$F_{Z_1}(z) = \Pr\left[\max_{1\le k\le K}\left(\frac{P_{R_2}\left|h_{R^*E_k}\right|^2}{1+P_{J_2}\left|h_{JE_k}\right|^2}\right) < z\right] = \prod_K \Pr\left(\frac{P_{R_2}\left|h_{R^*E_k}\right|^2}{1+P_{J_2}\left|h_{JE_k}\right|^2} < z\right). \tag{A6}$$

In view of the selection of a relay sensor that is independent of the eavesdroppers' channel, we have the PDF of $\left|h_{R^*E_k}\right|^2$ and $\left|h_{JE_k}\right|^2$ as follows:

$$f_{\left|h_{R^*E_k}\right|^2}(x) = \lambda_{RE}e^{-\lambda_{RE}x}, \tag{A7}$$

and

$$f_{\left|h_{JE_k}\right|^2}(x) = \lambda_{JE}e^{-\lambda_{JE}x}. \tag{A8}$$

By substituting Equations (A7) and (A8) into Equation (A6), the CDF of Z_1 can be easily obtained, which is given by

$$F_{Z_1}(z) = \left(1 - \frac{P_{R_2}\lambda_{JE}}{P_{R_2}\lambda_{JE} + P_{J_2}\lambda_{RE}z}e^{-\frac{\lambda_{RE}z}{P_{R_2}}}\right)^K. \tag{A9}$$

Next, we can derive the PDF of Z_1 by taking the derivative of $F_{Z_1}(z)$ with respect z. We also denote $X_2 = \left| h_{R''_{M_{2,n}} D} \right|^2$ and the CDF of X_2 can be easily derived by making a substitution of some parameters. Following a similar approach, the CDF of γ_{E2}^{SCJ} under the NCE scenario can be given by

$$F_{\gamma_{E2}^{SCJ}}(x) = \Pr\left(\frac{1+X_2}{1+Z_1} < x\right) = \int_0^\infty F_{X_2}(xz+x-1) f_{z_1}(z) dz. \tag{A10}$$

Substituting the CDF of X_2 and the PDF of Z_1 into Equation (A10), and denoting $\beta = \frac{\lambda_{JE} P_{R_2}}{\lambda_{RE} P_{J_2}}$, $\mu(t) = \frac{\lambda_{RD} sx + \lambda_{RE}(t+1)}{P_{R_2}}$, the CDF of γ_{E2}^{SCJ} can be further expressed as

$$\begin{aligned} F_{\gamma_{E2}^{SCJ}}(x) = K \sum_{s=0}^{M_{2,n}} \sum_{t=0}^{K-1} \binom{M_{2,n}}{s} \binom{K-1}{t} (-1)^{s+t} \beta^t \\ \times e^{-\frac{\lambda_{RD} s(x-1)}{P_{R_2}}} \left[\frac{\lambda_{JE}}{P_{J_2}} \underbrace{\int_0^\infty \frac{e^{-\mu(t)y} dy}{(y+\beta)^{t+1}}}_{I_1(t)} + \beta \underbrace{\int_0^\infty \frac{e^{-\mu(t)y} dy}{(y+\beta)^{t+2}}}_{I_2(t)} \right]. \end{aligned} \tag{A11}$$

For item $I_1(t)$, there are two cases to consider, i.e., $t = 0$ and $t > 0$. We can obtain the corresponding terms for two cases according to the equalities [40] (eq. (3.352.4)) and [40] (eq. (3.353.2)), respectively. Similarly, the item $I_2(t)$ can be easily derived when we utilize [40] (eq. (3.353.2)) to solve the corresponding integral. Finally, the desired results in **Theorem 4** can be easily obtained after some mathematical manipulations.

Appendix D

Denoting $Y_3 = \left\| \mathbf{h}_{R^* E} \right\|^2$ and $Z_2 = \left\| \mathbf{h}_{JE} \right\|^2$, the CDF of γ_{E2}^{SCJ} under the CE scenario can be given by

$$\begin{aligned} F_{\gamma_{E2}^{SCJ}}(x) &= \Pr\left(\frac{1 + P_{R_2} X_2}{1 + \frac{P_{R_2} Y_3}{1 + P_{J_2} Z_2}} < x \right) \\ &= \int_0^\infty \int_0^\infty F_{X_2}\left(\frac{x-1}{P_{R_2}} + \frac{xy}{1 + P_{J_2} z} \right) f_{Y_3}(y) \, dy f_{Z_2}(z) \, dz. \end{aligned} \tag{A12}$$

By invoking the PDF of Y_3 and Z_2 and the CDF of X_2 into Equation (A12), we can obtain the expression as follows:

$$\begin{aligned} F_{\gamma_{E2}^{SCJ}}(x) = \sum_{s=0}^{M_{2,n}} \binom{M_{2,n}}{s} (-1)^s e^{-\frac{\lambda_{RD} s(x-1)}{P_{R_2}}} \\ \times \underbrace{\int_0^\infty \underbrace{\int_0^\infty \frac{\lambda_{RE}^K y^{K-1}}{(K-1)!} e^{-\left(\lambda_{RE} + \frac{\lambda_{RD} sx}{1 + P_{J_2} z}\right) y} dy}_{\Lambda} \frac{\lambda_{JE}^K z^{K-1} e^{-\lambda_{JE} z}}{(K-1)!} dz}_{\Phi}. \end{aligned} \tag{A13}$$

Now, by utilizing [40] (eq. (3.351.3)) and the binomial theorem, we have

$$\Lambda = \left(1 - \frac{\theta}{z+\omega}\right)^K = \sum_{t=0}^{K} \binom{K}{t} (-1)^t \left(\frac{\theta}{z+\omega}\right)^t, \tag{A14}$$

where $\theta = \frac{\lambda_{RD} sx}{P_{J_2} \lambda_{RE}}$ and $\omega = \theta + \frac{1}{P_{J_2}}$ for the analysis tractable. Hence, Φ can be further written as

$$\Phi = \sum_{t=0}^{K} \binom{K}{t} (-\theta)^t \frac{\lambda_{JE}^K}{(K-1)!} \underbrace{\int_0^\infty \frac{z^{K-1} e^{-\lambda_{JE} z} dz}{(z+\omega)^t}}_{\Phi_2}. \tag{A15}$$

Obviously, to obtain Φ, we have to calculate Φ_2 first. For the item Φ_2, there are also two cases to consider, i.e., $t = 0$ and $t > 0$. For $t = 0$, with the help of [40] (eq. (3.351.3)), we have $\Phi_2 = (K-1)! \lambda_{JE}^{-K}$, which yields $\Phi = 1$. On the other hand, for $t > 0$, by changing variable $z + \omega = \rho$ and using the binomial theorem, we have

$$\Phi_2 = e^{\omega \lambda_{JE}} \sum_{l=0}^{K-1} \binom{K-1}{l} (-\omega)^{K-1-l} \underbrace{\int_\omega^\infty \rho^{l-t} e^{-\lambda_{JE} \rho} d\rho}_{\Phi_1}. \tag{A16}$$

By utilizing [40] (eq. (3.351.2)), [40] (eq. (3.352.2)) and [40] (eq. (3.353.1)), the item Φ_1 as $t > 0$ can be derived, as shown in Equation (32). Finally, the desired result in **Theorem 5** can be derived by pulling everything together.

References

1. Xu, L.; He, W.; Li, S. Internet of things in industries: A survey. *IEEE Trans. Ind. Inform.* **2014**, *10*, 2233–2243. [CrossRef]
2. Mukherjee, A. Physical-layer security in the Internet of things: Sensing and communication confidentiality under resource constraints. *Proc. IEEE* **2015**, *103*, 1747–1761. [CrossRef]
3. Xu, Q.; Ren, P.; Song, H.; Du, Q. Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations. *IEEE Access* **2016**, *4*, 2840–2853. [CrossRef]
4. Chen, Y.; Han, F.; Yang, Y.; Ma, H.; Han, Y.; Jiang, C.; Lai, H.; Claffey, D.; Safar, Z.; Liu, K. Time-reversal wireless paradigm for green Internet of things: An overview. *IEEE Internet Things J.* **2014**, *1*, 81–98. [CrossRef]
5. Lyu, B.; Yang, Z.; Guo, H.; Tian, F.; Gui, G. Relay cooperation enhanced backscatter communication for Internet-of-things. *IEEE Internet Things J.* **2019**, *6*, 2860–2871. [CrossRef]
6. Ji, B.; Li, Y.; Zhou, B.; Li, C.; Song, K.; Wen, H. Performance analysis of UAV relay assisted IoT communication network enhanced with energy harvesting. *IEEE Access* **2019**, *7*, 38738–38747. [CrossRef]
7. Chen, G.; Coon, J.; Mondal, A.; Allen, B.; Chambers, J. Performance analysis for multi-hop full-duplex IoT networks subject to poisson distributed interferers. *IEEE Internet Things J.* **2019**, *6*, 3467–3479. [CrossRef]
8. Massri, K.; Vitaletti, A.; Vernata, A.; Chatzigiannakis, I. Routing protocols for delay tolerant networks: A reference architecture and a thorough quantitative evaluation. *J. Sens. Actuator Netw.* **2016**, *5*, 6. [CrossRef]
9. Michalopoulos, D.; Karagiannidis, G. Performance analysis of single relay selection in Rayleigh fading. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 3718–3724. [CrossRef]
10. Xia, B.; Fan, Y.; Thompson, J.; Poor, H. Buffering in a three-node relay network. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 4492–4496. [CrossRef]
11. Zlatanov, N.; Schober, R.; Popovski, P. Buffer-aided relaying with adaptive link selection. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 1530–1542. [CrossRef]
12. Ikhlef, A.; Michalopoulos, D.; Schober, R. Max-max relay selection for relays with buffers. *IEEE Trans. Wirel. Commun.* **2012**, *11*, 1124–1135. [CrossRef]
13. Krikidis, I.; Charalambous, T.; Thompson, J. Buffer-aided relay selection for cooperative diversity systems without delay constraints. *IEEE Trans. Wirel. Commun.* **2012**, *11*, 1957–1967. [CrossRef]
14. Nasir, H.; Javaid, N.; Raza, W.; Guizani, M.; Alrajeh, N.; Alabed, M. Virtual-link relay selection scheme for buffer-aided IoT based cooperative relay networks. *IEEE Access* **2018**, *6*, 74648–74659. [CrossRef]
15. Shabbir, G.; Ahmad, J.; Raza, W.; Amin, Y.; Akram, A.; Loo, J.; Tenhunen, H. Buffer-aided successive relay selection scheme for energy harvesting IoT networks. *IEEE Access* **2019**, *7*, 36246–36258. [CrossRef]

16. Alkhawatrah, M.; Gong, Y.; Chen, G.; Lambotharan, S.; Chambers, J. Buffer-aided relay selection for cooperative NOMA in the Internet of things. *IEEE Internet Things J.* **2019**, *6*, 5722–5731. [CrossRef]
17. Mukherjee, A.; Fakoorian, S.; Huang, J.; Swindlehurst, A. Principles of physical layer security in multiuser wireless networks: A survey. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1550–1573. [CrossRef]
18. Zou, Y.; Zhu, J.; Wang, X.; Hanzo, L. A survey on wireless security: Technical challenges, recent advances, and future trends. *Proc. IEEE* **2016**, *104*, 1727–1765. [CrossRef]
19. Bloch, M.; Barros, J.; Rodrigues, M.; Mclaughlin, S. Wireless information-theoretic security. *IEEE Trans. Inf. Theory* **2008**, *54*, 2515–2534. [CrossRef]
20. Liang, Y.; Poor, H.; Shamai, S. Secure communication over fading channels. *IEEE Trans. Inf. Theory* **2008**, *54*, 2470–2492. [CrossRef]
21. Nan, Y.; Wang, L.; Geraci, G.; Elkashlan, M.; Yuan, J.; Renzo, M. Safeguarding 5G wireless communication networks using physical layer security. *IEEE Commun. Mag.* **2015**, *53*, 20–27.
22. Zou, Y.; Zhu, J.; Wang, X.; Leung, V. Improving physical-layer security in wireless communications using diversity techniques. *IEEE Netw.* **2015**, *29*, 42–48. [CrossRef]
23. Zhang, Y.; Shen, Y.; Wang, H.; Yong, J.; Jiang, X. On secure wireless communications for IoT under eavesdropper collusion. *IEEE Trans. Autom. Sci. Eng.* **2016**, *13*, 1281–1293. [CrossRef]
24. Chen, D.; Yang, W.; Hu, J.; Cai, Y.; Tang, X. Energy-efficient secure transmission design for the Internet of things with an untrusted relay. *IEEE Access* **2018**, *6*, 11862–11870. [CrossRef]
25. Hu, J.; Yang, N.; Cai, Y. Secure downlink transmission in the Internet of things: How many antennas are needed?. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 1622–1634. [CrossRef]
26. Huang, P.; Hao, Y.; Lv, T.; Xing, J.; Yang, J.; Mathiopoulos, P. Secure beamforming design in relay-assisted Internet of things. *IEEE Internet Things J.* **2019**, *6*, 6453–6464. [CrossRef]
27. Chen, G.; Tian, Z.; Gong, Y.; Chen, Z.; Chambers, J. Max-ratio relay selection in secure buffer-aided cooperative wireless networks. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 719–729. [CrossRef]
28. Tang, X.; Cai, Y.; Huang, Y.; Duong, T.; Yang, W.; Yang, W. Secrecy outage analysis of buffer-aided cooperative MIMO relaying systems. *IEEE Trans. Veh. Technol.* **2018**, *67*, 2035–2048. [CrossRef]
29. Sun, A.; Liang, T.; Zhang, Y. Performance analysis of secure buffer-aided cognitive radio network. In Proceedings of the 2015 4th IEEE/CIC International Conference on Communications in China (ICCC), Shenzhen, China, 2–4 November 2015; pp. 1–4.
30. Bletsas, A.; Shin, H.; Win, M. Cooperative communications with outage-optimal opportunistic relaying. *IEEE Trans. Wirel. Commun.* **2007**, *6*, 3450–3460. [CrossRef]
31. Chatzigiannakis, I.; Kinalis, A.; Nikoletseas, S. Efficient data propagation strategies in wireless sensor networks using a single mobile sink. *Comput. Commun.* **2008**, *31*, 896–914. [CrossRef]
32. Chatzigiannakis, I.; Kinalis, A.; Nikoletseas, S. Fault-tolerant and efficient data propagation in wireless sensor networks using local, additional network information. *J. Parallel Distrib. Comput.* **2007**, *67*, 456–473. [CrossRef]
33. Zheng, T.; Wang, H.; Yuan, J.; Towsley, D.; Lee, M. Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers. *IEEE Trans. Commun.* **2015**, *63*, 4347–4362. [CrossRef]
34. Zhou, X.; Ganti, R.; Andrews, J. Secure wireless network connectivity with multi-antenna transmission. *IEEE Trans. Wirel. Commun.* **2011**, *10*, 425–430. [CrossRef]
35. Huang, Y.; Zhang, P.; Wu, Q.; Wang, J. Secrecy performance of wireless powered communication networks with multiple eavesdroppers and outdated CSI. *IEEE Access* **2018**, *6*, 33774–33788. [CrossRef]
36. Gopala, P.; Lai, L.; Gamal, H. On the secrecy capacity of fading channels. *IEEE Trans. Inf. Theory* **2008**, *54*, 4687–4698. [CrossRef]
37. Oggier F.; Hassibi, B. The secrecy capacity of the MIMO wiretap channel. *IEEE Trans. Inf. Theory* **2011**, *57*, 4961–4972. [CrossRef]
38. Chatzigiannakis, I.; Nikoletseas, S. Design and analysis of an efficient communication strategy for hierarchical and highly changing ad-hoc mobile networks. *Mob. Netw. Appl.* **2004**, *9*, 319–332. [CrossRef]
39. Chatzigiannakis, I.; Nikoletseas, S.; Spirakis, P. On the average and worst-case efficiency of some new distributed communication and control algorithms for ad-hoc mobile networks. In Proceedings of the 1st ACM Int'l Workshop on Principles of Mobile Computing (POMC'01), Newport, RI, USA, August 2001; pp. 1–19.
40. Gradshteyn, I.; Ryzhik, I. *Table of Integrals, Series, and Products*; Publishing House: San Diego, CA, USA, 2007.

41. Chen, G.; Gong, Y.; Xiao, P.; Tafazolli, R. Dual antenna selection in self-backhauling multiple small cell networks. *IEEE Commun. Lett.* **2016**, *20*, 1611–1614. [CrossRef]
42. Tian, Z.; Gong, Y.; Chen, G.; Chambers, J. Buffer-aided relay selection with reduced packet delay in cooperative networks. *IEEE Trans. Veh. Technol.* **2017**, *66*, 2567–2575. [CrossRef]
43. Coolidge, J.L. The Story of the Binomial Theorem. *Am. Math. Mon.* **1949**, *23*, 147–157. [CrossRef]
44. Afana, A.; Asghari, V.; Ghrayeb, A.; Affes, S. Cooperative relaying in spectrum-sharing systems with beamforming and interference constraints. In Proceedings of the 2012 IEEE 13th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), Cesme, Turkey, 17–20 June 2012; pp. 429–433.