entropy

MDPI

Article

Performance Comparison between Fountain Codes-Based Secure MIMO Protocols with and without Using Non-Orthogonal Multiple Access

Dang The Hung [1], Tran Trung Duy [2], Phuong T. Tran [3,*], Do Quoc Trinh [1] and Tan Hanh [2]

[1] Faculty of Radio-Electronics Engineering, Le Quy Don Technical University, Ha Noi 100000, Vietnam; danghung8384@gmail.com (D.T.H.); trinhdq@mta.edu.vn (D.Q.T.)
[2] Department of Telecommunications, and Department of Information Technology, Posts and Telecommunications Institute of Technology, Ho Chi Minh City 700000, Vietnam; trantrungduy@ptithcm.edu.vn (T.T.D.); tanhanh@ptithcm.edu.vn (T.H.)
[3] Wireless Communications Research Group, Faculty of Electrical and Electronics Engineering, Ton Duc Thang University, Ho Chi Minh City 700000, Vietnam
* Correspondence: tranthanhphuong@tdtu.edu.vn

Received: 13 August 2019; Accepted: 6 October 2019; Published: 9 October 2019

Abstract: In this paper, we propose and evaluate the performance of fountain codes (FCs) based secure transmission protocols in multiple-input-multiple-output (MIMO) wireless systems, in presence of a passive eavesdropper. In the proposed protocols, a source selects its best antenna to transmit fountain encoded packets to a destination that employs selection combining (SC) or maximal ratio combing (MRC) to enhance reliability of the decoding. The transmission is terminated when the destination has a required number of the encoded packets to reconstruct the original data of the source. Similarly, the eavesdropper also has the ability to recover the source data if it can intercept a sufficient number of the encoded packets. To reduce the number of time slots used, the source can employ non-orthogonal multiple access (NOMA) to send two encoded packets to the destination at each time slot. For performance analysis, exact formulas of average number of time slots (TS) and intercept probability (IP) over Rayleigh fading channel are derived and then verified by Monte-Carlo simulations. The results presented that the protocol using NOMA not only reduces TS but also obtains lower IP at medium and high transmit signal-to-noise ratios (SNRs), as compared with the corresponding protocol without using NOMA.

Keywords: physical-layer security; fountain codes; non-orthogonal multiple access; intercept probability

1. Introduction

Secure communication is one of the critical issues of wireless communication systems due to the broadcast nature of wireless channels. Conventionally, cryptographic methods at upper layers are used to obtain wireless security via generating cryptographic keys. However, eavesdroppers can decode the encrypted signals if they are equipped with advanced equipment and have enough time for the decoding operation. In [1–6], the authors introduced a new security method, called physical-layer security (PLS), where characteristics of wireless channels, i.e., distances and channel state information (CSI), can be exploited to ensure confidentiality of the data transmission. To obtain the security in PLS, the secrecy capacity must be greater than zero or the channel capacity of the data link must be better than that of the eavesdropping link. For example, joint transmit and receive diversity methods [7–10] were proposed to enhance secrecy performances for multiple-input-multiple-output (MIMO) secure communication protocols, in terms of secrecy outage probability (SOP) and probability of non-zero secrecy capacity (PNSC). Particularly, the transmitters in [7–10] select the best transmit

antenna (transmit antenna selection (TAS)) to maximize post-processed signal-to-noise ratios (SNRs) obtained at the intended receivers that use maximal ratio combining (MRC) or selection combining (SC). Because the eavesdroppers in [7–10] only obtain the receive diversity with their MRC or SC combiners, the diversity order of the data links can be higher than that of the eavesdropping ones. In [11], the secrecy outage performance of the TAS/MRC method in underlay cognitive radio networks (CRNs) was evaluated. In the underlay spectrum sharing approach, transmit power of the secondary transmitters is limited by a pre-determined interference level so that quality of service (QoS) of the primary network is not harmful. In contrast to [11], the authors in [12] proposed a secure transmission protocol in overlay CRNs. In this system model, a full-duplex secondary transmitter employs TAS/MRC to transmit the secondary data and receive the primary data at the same time. Moreover, it can use an interactive zero forcing beam-forming method to simultaneously broadcast both the primary and secondary data. The protocol proposed in [12] not only enhances the SOP performance for the primary network but also improves throughput of the secondary transmission. Published works [13,14] introduced the PLS schemes in radio frequency energy harvesting (RF-EH) environment. In [13], one multi-antenna base station adopts TAS to send information and energy to one desired receiver and EH receivers, respectively. Since the EH receivers can illegally decode the information of the intended receiver, there exists a trade-off between energy harvested and security of the data transmission. In [14], an energy-limited source harvests the RF energy from a dedicated power beacon for transmitting the data in presence of multiple eavesdroppers. In addition, the source can employ TAS or maximal ratio transmission (MRT) to enhance the secrecy diversity order. Recently, secure transmission approaches for non-orthogonal multiple access (NOMA) systems have been studied. In contrast to conditional transmission techniques, the source using NOMA can send multiple signals to the destinations at the same time, frequency and code. Indeed, the signals that are linearly combined with different transmit power levels are then sent to the destinations which use successive interference cancellation (SIC) to extract the desired signals. In [15], the authors proposed various TAS methods to enhance the secrecy performance for two-user down-link NOMA networks. Reference [16] investigated the SOP performance of a secure NOMA system using max-min TAS method, in presence of non-colluding and colluding eavesdroppers.

Cooperative relaying protocols with efficient relay selection methods [17–19] also provide high secrecy performance for PLS-based wireless networks. The advantages of these schemes are that (i) the data transmission on short hops is more reliable, (ii) the relay selection provides high diversity gain. However, because the source data can be overheard over multiple hops, the channel capacity obtained at the eavesdroppers can be significantly increased by using the MRC combiner [20]. To solve this problem, a randomize-and-forward strategy [20,21] is often employed by the transmitters including the source and the relays to confuse the eavesdroppers. In [22], a secure transmission protocol in a dual-hop MIMO relay system using TAS/MRC over Nakagami-m fading channels was proposed and analyzed. The authors of [23] considered a buffer-aided MIMO cooperative system in the presence of a passive eavesdropper. Particularly, due to lack of the CSI of the eavesdropping channel, a joint transmit antenna and relay selection scheme was proposed to only enhance the quality of the main channel. Published works [24,25] analyzed SOP of dual-hop cooperative underlay CRNs with and without direct link between the secondary source and the secondary destination. In [26], secure communication protocols in multi-hop underlay CRNs were considered. In addition, the authors in [26] introduced an efficient cooperative routing method to enhance the end-to-end secrecy performance, as compared with the traditional mutli-hop transmission one. To further enhance the secrecy performance for cooperative cognitive networks, cooperative jamming (CJ) [27,28] can be used. With CJ, jammers are employed to transmit interference on the eavesdroppers, while the intended receivers can remove the interference from their received signals via cooperation with jammers. However, the implementation of the CJ methods is very complex due to a high synchronization between the jammer and receiver nodes. Moreover, the jamming signals can cause co-channel interference on other wireless devices in the network. In [29], the authors proposed a secure two-way relaying protocol, where two legitimate users

exchange data with each other via the help of amplify-and-forward cooperative relays, with presence of an eavesdropper, and imperfect CSI of the eavesdropping channels. References [30–32] considered secure transmission protocols in RF-EH relay systems, in which the relay nodes have to harvest energy from the RF signals to forward the source data to the destination. In [32], the destination plays a role as a jammer for obtaining positive secrecy rate with presence of the untrusted relay. In [33–35], wireless powered CJ methods are employed to improve the secrecy rate. In these methods, called harvest-to-jam (HJ), the jammer nodes first harvest energy from ambient RF sources and then use the harvested energy to generate noises. References [36,37] investigated the secrecy performance of cooperative NOMA systems with various relay selection methods. In [38], the source performs the jamming operation to enhance the security for dual-hop relaying networks using NOMA. In [39,40], secure NOMA transmission strategies in CRNs were proposed and analyzed. In [41], the trade-off between security and reliability of cooperative cognitive NOMA systems was evaluated via SOP and connection outage probability (COP).

Fountain codes (FCs) or rateless codes [42,43] have gained much attention due to low decoding complexity. In contrast to typical fixed-rate codes, a FC transmitter can generate a limitless stream of fountain encoded packets from a finite number of the source packets. The encoded packets are then continuously sent to the desired receivers until each receiver can receive a sufficient number of the encoded packets for recovering the original data (regardless of which encoded packets are received). Therefore, FCs do not require knowledge of CSI, automatically adapt the channel conditions, and avoid the feedback channel. In [44], the authors proposed a FCs based cooperative relaying network, where energy consumption and transmission time significantly decrease due to mutual information accumulation. Published work [45] presented the advantage of applying FCs on wireless broadcast systems, in terms of transmission efficiency. In [46], a rateless code based spectrum access model in overlay CRNs was proposed. In the scheme proposed in [46], the secondary transmitters help a primary transmitter forward the fountain packets to a primary receiver, and then they can find opportunities to access licensed bands. The authors of [47] considered cooperative relay networks using FCs and RF-EH, where the source and relay nodes use FCs, and hence, the destination can perform the mutual information accumulation and energy accumulation. However, due to broadcast of wireless channels, the eavesdroppers can also receive enough number of the encoded packets for intercepting the original data. Hence, security in FCs based PLS system becomes a critical issue.

1.1. Related Work

Until now, there have been many published works concerned with performance analysis of diversity based secure communication using MIMO techniques, e.g., [7–16], and cooperative relaying methods [17–41]. However, to the best of our knowledge, several existing literatures studying secure transmission protocols using FCs have been reported. The basic idea of the FC-based PLS protocols is that when the intended destination can receive enough encoded packets before the eavesdroppers, the data transmission is successful and secure [48]. In [49], the authors evaluated the intercept probability which is defined as the probability that the eavesdropper can intercept enough coded packets to recover the original data. In [50], the authors proposed a multicast model to attain the wireless security for Internet of Things (IoT) networks using FCs. In [51], the secrecy performance of the FCs aided PLS protocol is significantly enhanced with the TAS and CJ techniques when the transceiver hardware of the destination and the eavesdropper are not perfect. Reference [52] considered a FCs aided relaying network using the CJ method to enhance the transmission secrecy, in terms of quality-of-service violating probability (QVP). In [53], the authors proposed various relay selection and jammer selection methods to enhance both outage performance and IP performance for dual-hop multiple-relay decode-and-forward networks. The authors of [54] proposed a FCs based transmission protocol to secure the source-destination communication. Moreover, a new FC construction method, which opportunistically adapts the coding strategy following outage prediction, is proposed in [54]. In [55], the authors analyzed the security-reliability trade-off for multi-hop low-energy adaptive

clustering hierarchy (LEACH) networks employing FCs and CJ. The authors of [56] proposed a rateless codes-based communication protocol to provide security for wireless systems. In this protocol, a source uses the TAS technique to transmit the encoded packets to a destination, and a cooperative jammer harvests energy from the RF signals of the source and interference sources to generate jamming noises on an eavesdropper.

1.2. Motivations and Contributions

In this paper, we propose a MIMO secure communication system exploiting FCs. In the proposed protocol, a multi-antenna source uses TAS to transmit the encoded packets to a multi-antenna destination in presence of a multi-antenna eavesdropper. The receivers including the destination and the eavesdropper can use the MRC or SC combiner to enhance the reliability of the decoding operation. When a required number of the encoded packets can be obtained by the destination, it sends a feedback to the source for stopping the transmission. Therefore, the security is guaranteed as the eavesdropper cannot sufficiently intercept the encoded packets. The main motivations and contributions of this paper can be summarized as follows:

- In contrast to [48–50,54], in the proposed protocol, all the nodes including the source, the destination and eavesdropper are equipped with multiple antennas and use the MRC or SC technique to combine the received signals. Although the source nodes in [51,56] have multi-antenna and employ TAS to transmit the encoded packets, the destinations in [51,56] are only single-antenna nodes. Moreover, References [52,53,55] considered single-input-single-output (SISO) relaying protocols where all the terminals are deployed with a single antenna.
- In contrast to [48–56], the source in the proposed protocol can employ NOMA to transmit two packets to the destination in each time slot to reduce the number of time slots used. Moreover, reducing the number of time slots also means reducing the delay time and transmit power, which are important metrics of the wireless systems.
- We compare the performance of the proposed protocols in two cases where the source uses NOMA (named NOMA) and does not use NOMA (named Wo-NOMA), in terms of average number of time slots (TS) and intercept probability (IP). The results shows that the FCs based secure transmission protocol exploiting NOMA can decrease both TS and IP, as compared with the corresponding protocol without using NOMA.
- We derive exact expressions of TS and IP for the NOMA and Wo-NOMA protocols over Rayleigh fading channels and realize computer simulations to verify.

The remainder of this paper is organized as follows. The system model of NOMA and Wo-NOMA is described in Section 2. In Section 3, the TS and IP performances of NOMA and Wo-NOMA over Rayleigh fading channel are evaluated. The simulation and theoretical results are shown in Section 4. Finally, this paper is concluded in Section 5.

2. System Model

Figure 1 presents system model of the proposed protocol, where a source node (S) equipped with N_S antennas uses FCs to transmit its data to an N_D-antenna destination (D), in presence of an N_E-antenna passive eavesdropper (E). The original data of the source is divided into L packets which are then encoded by the FC encoder. At each time slot, the source selects its best antenna to transmit two (or one) encoded packets to the destination, which are also received by the eavesdropper. Then, the D and E nodes attempt to decode the encoded packets. To recover the original data, the destination and eavesdropper have to correctly receive at least $N_{\text{req}}^{\text{pkt}}$ encoded packets, where $N_{\text{req}}^{\text{pkt}} = (1+\varepsilon)\,L$, and ε is the decoding overhead which depends on concrete code design [48–56]. After receiving a sufficient number of the encoded packets for reconstructing the original data, the destination sends an ACK message to inform the source, and then the source stops its transmission. In this case, if the

eavesdropper successfully receives at least $N_{\text{req}}^{\text{pkt}}$ encoded packets, it can also recover the original data, and hence the source data is intercepted.

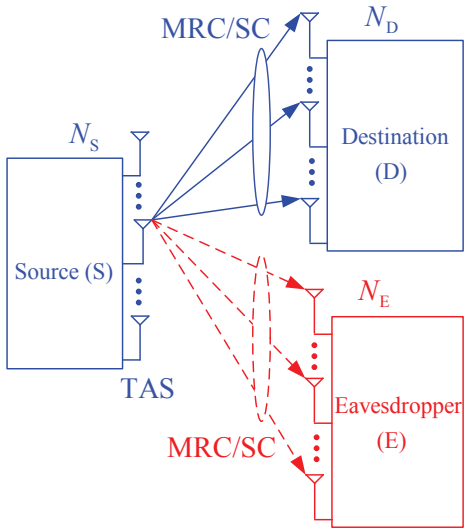

Figure 1. System model of the proposed scheme.

Next, we introduce notations and assumptions used through this paper. Let us denote $h_{\text{S}_m\text{D}_n}$ and $h_{\text{S}_m\text{E}_t}$ as channel coefficients between the m-th antenna of the source and n-th antenna of the destination and between the m-th antenna of the source and t-th antenna of the eavesdropper, respectively, where $m = 1, 2, ..., N_{\text{S}}$, $n = 1, 2, ..., N_{\text{D}}$, $t = 1, 2, ..., N_{\text{E}}$. We assume that all the channels are independent and identically distributed (i.i.d.), block and flat Rayleigh fading, where they keep constant in one time slot but independently changes at other time slots. Therefore, the channel gains $\gamma_{\text{S}_m\text{D}_n} = |h_{\text{S}_m\text{D}_n}|^2$ and $\gamma_{\text{S}_m\text{E}_t} = |h_{\text{S}_m\text{E}_t}|^2$ are exponential random variables (RVs) whose cumulative distribution functions (CDFs) are expressed respectively as [57]:

$$\begin{aligned} F_{\gamma_{\text{S}_m\text{D}_n}}(x) &= 1 - \exp(-\lambda_{\text{SD}} x), \\ F_{\gamma_{\text{S}_m\text{E}_t}}(x) &= 1 - \exp(-\lambda_{\text{SE}} x), \end{aligned} \tag{1}$$

where $\lambda_{\text{SD}} = 1/\mathcal{E}\{\gamma_{\text{S}_m\text{D}_n}\}$ and $\lambda_{\text{SE}} = 1/\mathcal{E}\{\gamma_{\text{S}_m\text{E}_t}\}$, and $\mathcal{E}\{.\}$ is an expected operator.

Therefore, probability density function (PDF) of $\gamma_{\text{S}_m\text{D}_n}$ and $\gamma_{\text{S}_m\text{E}_t}$ can be given respectively as

$$\begin{aligned} f_{\gamma_{\text{S}_m\text{D}_n}}(x) &= \lambda_{\text{SD}} \exp(-\lambda_{\text{SD}} x), \\ f_{\gamma_{\text{S}_m\text{E}_t}}(x) &= \lambda_{\text{SE}} \exp(-\lambda_{\text{SE}} x). \end{aligned} \tag{2}$$

Let N_{TS} denote number of time slots used by the source to transmit the encoded packets to the destination. We denote $N_{\text{D}}^{\text{pkt}}$ and $N_{\text{E}}^{\text{pkt}}$ as number of the encoded packets that the destination and the eavesdropper can successfully receive, respectively.

Function $\lfloor x \rfloor$ gives the greatest integer less than or equal to x, and function $\lceil x \rceil$ gives the smallest integer equal to or greater than x.

2.1. Without Using NOMA (Wo-NOMA)

If the source does not use NOMA, at each time slot, it transmits one encoded packet to the destination. Assume that each encoded packet, e.g., p, includes U symbols, i.e., $p = \{x_1[1], x_1[2], ..., x_1[U]\}$, where $x[u]$ is a symbol of p, and $u = 1, 2, ..., U$. When the source uses the m-th antenna to transmit x_u to the destination, the received signal at the n-th antenna of the destination is expressed as

$$y_{\text{D}}[u] = \sqrt{P} h_{\text{S}_m\text{D}_n} x[u] + n_{\text{D}}[u], \tag{3}$$

where P is transmit power of all the antennas of the source, $n_{\mathrm{D}}[u]$ is additive white Gaussian noise (AWGN) at D. For ease of presentation and analysis, we assume that all the additive noises are modeled as Gaussian RVs with zero mean and variance of σ^2.

From (3), the instantaneous signal-to-noise ratio (SNR) of the $\mathrm{S}_m \to \mathrm{D}_n$ link is given as

$$\psi_{\mathrm{S}_m\mathrm{D}_n} = \frac{P\gamma_{\mathrm{S}_m\mathrm{D}_n}}{\sigma^2} = \Delta\gamma_{\mathrm{S}_m\mathrm{D}_n}, \tag{4}$$

where $\Delta = P/\sigma^2$ is transmit SNR.

When the destination uses the SC technique, the SNR obtained at the output of the combiner can be formulated similarly to Equation (3) of [58] as

$$\psi_{\mathrm{S}_m\mathrm{D}_b} = \max_{n=1,2,\ldots,N_{\mathrm{D}}} \left(\psi_{\mathrm{S}_m\mathrm{D}_n}\right), \tag{5}$$

where b denotes index of the receive antenna at D used to decode $x[u]$, $b \in \{1, 2, \ldots, N_{\mathrm{D}}\}$.

Then, the source selects its best antenna to maximize the instantaneous SNR of the data link (see [51]):

$$\psi_{\mathrm{S}_a\mathrm{D}_b} = \max_{m=1,2,\ldots,N_{\mathrm{S}}} \left(\psi_{\mathrm{S}_m\mathrm{D}_b}\right), \tag{6}$$

where a denotes index of the selected transmit antenna at the source.

Combining (5) and (6), we can rewrite the SNR of the data link as

$$\psi_{\mathrm{D}}^{\mathrm{TAS/SC}} = \max_{m=1,2,\ldots,N_{\mathrm{S}}} \left(\max_{n=1,2,\ldots,N_{\mathrm{D}}} \left(\psi_{\mathrm{S}_m\mathrm{D}_n}\right) \right). \tag{7}$$

For a fair comparison, the eavesdropper also uses the SC combiner for decoding p. Similar to (5), the obtained SNR of the eavesdropping link is computed as

$$\psi_{\mathrm{E}}^{\mathrm{SC}} = \max_{t=1,2,\ldots,N_{\mathrm{E}}} \left(\psi_{\mathrm{S}_a\mathrm{E}_t}\right), \tag{8}$$

where $\psi_{\mathrm{S}_a\mathrm{E}_t} = \Delta\gamma_{\mathrm{S}_a\mathrm{E}_t}$.

If the destination uses MRC, the combined signal at D can be given as

$$\begin{aligned} y_{\mathrm{D}}^{\mathrm{MRC}}[u] &= \sum_{n=1}^{N_{\mathrm{D}}} \frac{\sqrt{P}h^*_{\mathrm{S}_m\mathrm{D}_n}}{\sum\limits_{n=1}^{N_D} P|h_{\mathrm{S}_m\mathrm{D}_n}|^2} y_{\mathrm{D}}[u] \\ &= x[u] + \sum_{n=1}^{N_{\mathrm{D}}} \frac{\sqrt{P}h^*_{\mathrm{S}_m\mathrm{D}_n} n_{\mathrm{D}}[u]}{\sum\limits_{n=1}^{N_D} P|h_{\mathrm{S}_m\mathrm{D}_n}|^2}, \end{aligned} \tag{9}$$

where $h^*_{\mathrm{S}_m\mathrm{D}_n}$ is conjugate of the complex number $h_{\mathrm{S}_m\mathrm{D}_n}$.

From (9), the SNR obtained at D is calculated as

$$\psi_{\mathrm{S}_m\mathrm{D}}^{\mathrm{MRC}} = \sum_{n=1}^{N_{\mathrm{D}}} \Delta|h_{\mathrm{S}_m\mathrm{D}_n}|^2 = \sum_{n=1}^{N_{\mathrm{D}}} \psi_{\mathrm{S}_m\mathrm{D}_n}. \tag{10}$$

Then, the TAS technique is employed to provide the highest SNR for the data link, i.e.,

$$\psi_{\mathrm{D}}^{\mathrm{TAS/MRC}} = \max_{m=1,2,\ldots,N_{\mathrm{S}}} \left(\sum_{n=1}^{N_{\mathrm{D}}} \psi_{\mathrm{S}_m\mathrm{D}_n} \right). \tag{11}$$

Similar to (10), the instantaneous SNR of the eavesdropping link is computed as

$$\psi_{\mathrm{E}}^{\mathrm{MRC}} = \sum_{t=1}^{N_{\mathrm{E}}} \psi_{\mathrm{S}_a\mathrm{E}_t}, \tag{12}$$

where a denotes index of the selected antenna at the source.

Remark 1. *Due to the block fading channel, the instantaneous SNRs of the symbols $x[u]$ are the same for all u. Hence, in (7), (8), (11) and (12), we skip the index u as presenting SNRs of the data and eavesdropping channels. Next, we assume that the encoded packet p can be decoded successfully if the instantaneous SNRs received at the destination and the eavesdropper are higher than a predetermined threshold denoted by γ_{th}, which can be formulated respectively as*

$$\begin{aligned}\rho_{\text{D}} &= \Pr\left(\psi_{\text{D}}^{\text{Y}} \geq \gamma_{\text{th}}\right),\\ \rho_{\text{E}} &= \Pr\left(\psi_{\text{E}}^{\text{Z}} \geq \gamma_{\text{th}}\right),\end{aligned} \tag{13}$$

where $\text{Y} \in \{\text{TAS/SC}, \text{TAS/MRC}\}$ *and* $\text{Z} \in \{\text{SC}, \text{MRC}\}$.

Then, the probabilities that D and E nodes cannot correctly be decoded the encoded packet p are given as $1-\rho_{\text{D}}$ and $1-\rho_{\text{E}}$, respectively.

2.2. Using NOMA

To reduce the number of time slots used to transmit the encoded packets, the source can use NOMA to transmit two encoded packets, e.g., p_1 and p_2, to the destination in one time slot. We can assume that $p_1 = \{x_1[1], x_1[2], ..., x_1[U]\}$ and $p_2 = \{x_2[1], x_2[2], ..., x_2[U]\}$, where $x_1[u]$ and $x_2[u]$ are symbols of p_1 and p_2, respectively, and $u = 1, 2, ..., U$. Indeed, the source linearly combines two signals $x_1[u]$ and $x_2[u]$ [36], i.e., $x_+[u] = \sqrt{a_1 P}x_1[u] + \sqrt{a_2 P}x_2[u]$, and it then sends $x_+[u]$ to the destination, where a_1 and a_2 are power allocation coefficients with $a_1 + a_2 = 1$, $a_1 > a_2 > 0$. Similar to (3), the received signal at D can be expressed as

$$\begin{aligned}y_{\text{D}}[u] &= h_{\text{S}_m\text{D}_n} x_+[u] + n_{\text{D}}[u]\\ &= h_{\text{S}_m\text{D}_n}\left(\sqrt{a_1 P}x_1[u] + \sqrt{a_2 P}x_2[u]\right) + n_{\text{D}}[u].\end{aligned} \tag{14}$$

Follows the SIC principle, the destination first decodes $x_1[u]$ by treating $x_2[u]$ as noise. After successfully decoding $x_1[u]$, D removes the component including $x_1[u]$, i.e., $\sqrt{a_1 P}h_{\text{S}_m\text{D}_n}x_1[u]$, from $y_{\text{D}}[u]$. Then, the signal used to decode $x_2[u]$ can be expressed as (see [36])

$$z_{\text{D}}[u] = \sqrt{a_2 P}h_{\text{S}_m\text{D}_n}x_2[u] + n_{\text{D}}[u]. \tag{15}$$

From (14) and (15), the instantaneous SNRs, with respect to $x_1[u]$ and $x_2[u]$, are given respectively as

$$\psi_{\text{S}_m\text{D}_n}^{x_1[u]} = \frac{a_1 \Delta\gamma_{\text{S}_m\text{D}_n}}{a_2 \Delta\gamma_{\text{S}_m\text{D}_n} + 1}, \psi_{\text{S}_m\text{D}_n}^{x_2[u]} = a_2 \Delta\gamma_{\text{S}_m\text{D}_n}. \tag{16}$$

When the TAS/SC technique is employed, similar to (7), the obtained SNRs of the data link for decoding $x_1[u]$ and $x_2[u]$ can be expressed respectively as

$$\begin{aligned}\psi_{\text{D},1}^{\text{TAS/SC}} &= \frac{a_1 \max\limits_{m=1,2,...,N_{\text{S}}}\left(\max\limits_{n=1,2,...,N_{\text{D}}}\left(\psi_{\text{S}_m\text{D}_n}\right)\right)}{a_2 \max\limits_{m=1,2,...,N_{\text{S}}}\left(\max\limits_{n=1,2,...,N_{\text{D}}}\left(\psi_{\text{S}_m\text{D}_n}\right)\right) + 1},\\ \psi_{\text{D},2}^{\text{TAS/SC}} &= a_2 \max\limits_{m=1,2,...,N_{\text{S}}}\left(\max\limits_{n=1,2,...,N_{\text{D}}}\left(\psi_{\text{S}_m\text{D}_n}\right)\right).\end{aligned} \tag{17}$$

Similarly, the eavesdropper E first decodes $x_1[u]$, and then performs SIC before decoding $x_2[u]$. With the SC combiner, the instantaneous SNRs of the eavesdropping channel used to decode $x_1[u]$ and $x_2[u]$ are given respectively as

$$\psi_{\mathrm{E},1}^{\mathrm{SC}} = \frac{a_1 \max\limits_{t=1,2,\ldots,N_{\mathrm{E}}} \left(\psi_{\mathrm{S}_a\mathrm{E}_t}\right)}{a_2 \max\limits_{t=1,2,\ldots,N_{\mathrm{E}}} \left(\psi_{\mathrm{S}_a\mathrm{E}_t}\right) + 1}, \psi_{\mathrm{E},2}^{\mathrm{SC}} = a_2 \max_{t=1,2,\ldots,N_{\mathrm{E}}} \left(\psi_{\mathrm{S}_a\mathrm{E}_t}\right). \tag{18}$$

In the case that the MRC technique is used, the combined signal at D can be given as

$$\begin{aligned} y_{\mathrm{D},x_1}^{\mathrm{MRC}}[u] &= \sum_{n=1}^{N_{\mathrm{D}}} \frac{\sqrt{a_1 P} h_{\mathrm{S}_m\mathrm{D}_n}^*}{a_1 P \sum\limits_{n=1}^{N_{\mathrm{D}}} |h_{\mathrm{S}_m\mathrm{D}_n}|^2} \left(\sqrt{a_1 P} h_{\mathrm{S}_m\mathrm{D}_n} x_1[u] + \sqrt{a_2 P} h_{\mathrm{S}_m\mathrm{D}_n} x_2[u] + n_{\mathrm{D}}[u]\right) \\ &= x_1[u] + \frac{\sqrt{a_2}}{\sqrt{a_1}} x_2[u] + \sum_{n=1}^{N_{\mathrm{D}}} \frac{\sqrt{a_1 P} h_{\mathrm{S}_m\mathrm{D}_n}^* n_{\mathrm{D}}[u]}{a_1 P \sum\limits_{n=1}^{N_{\mathrm{D}}} |h_{\mathrm{S}_m\mathrm{D}_n}|^2}. \end{aligned} \tag{19}$$

After canceling the components including $x_1[u]$ from the signals received at all the antennas, the destination again uses MRC to decode $x_2[u]$ using the following combined signal:

$$\begin{aligned} y_{\mathrm{D},x_2}^{\mathrm{MRC}}[u] &= \sum_{n=1}^{N_{\mathrm{D}}} \frac{\sqrt{a_2 P} h_{\mathrm{S}_m\mathrm{D}_n}^*}{a_2 P \sum\limits_{n=1}^{N_{\mathrm{D}}} |h_{\mathrm{S}_m\mathrm{D}_n}|^2} \left(\sqrt{a_2 P} h_{\mathrm{S}_m\mathrm{D}_n} x_2[u] + n_{\mathrm{D}}[u]\right) \\ &= x_2[u] + \sum_{n=1}^{N_{\mathrm{D}}} \frac{\sqrt{a_2 P} h_{\mathrm{S}_m\mathrm{D}_n}^* n_{\mathrm{D}}[u]}{a_2 P \sum\limits_{n=1}^{N_{\mathrm{D}}} |h_{\mathrm{S}_m\mathrm{D}_n}|^2}. \end{aligned} \tag{20}$$

From (19) and (20), the obtained SNRs, with respect to $x_1[u]$ and $x_2[u]$, can be expressed respectively as

$$\psi_{\mathrm{S}_m\mathrm{D}}^{x_1[u]} = \frac{a_1 \sum\limits_{n=1}^{N_{\mathrm{D}}} \psi_{\mathrm{S}_m\mathrm{D}_n}}{a_2 \sum\limits_{n=1}^{N_{\mathrm{D}}} \psi_{\mathrm{S}_m\mathrm{D}_n} + 1}, \psi_{\mathrm{S}_m\mathrm{D}}^{x_2[u]} = a_2 \sum_{n=1}^{N_{\mathrm{D}}} \psi_{\mathrm{S}_m\mathrm{D}_n}. \tag{21}$$

Since the source uses TAS to optimize quality of the data link, the obtained SNRs used to decode $x_1[u]$ and $x_2[u]$ can be calculated respectively as

$$\begin{aligned} \psi_{\mathrm{D},1}^{\mathrm{TAS/MRC}} &= \max_{m=1,2,\ldots,N_{\mathrm{S}}} \left(\frac{a_1 \sum\limits_{n=1}^{N_{\mathrm{D}}} \psi_{\mathrm{S}_m\mathrm{D}_n}}{a_2 \sum\limits_{n=1}^{N_{\mathrm{D}}} \psi_{\mathrm{S}_m\mathrm{D}_n} + 1} \right), \\ \psi_{\mathrm{D},2}^{\mathrm{TAS/MRC}} &= \max_{m=1,2,\ldots,N_{\mathrm{S}}} \left(a_2 \sum_{n=1}^{N_{\mathrm{D}}} \psi_{\mathrm{S}_m\mathrm{D}_n} \right). \end{aligned} \tag{22}$$

Similarly, for the eavesdropping channel, the instantaneous SNRs, with respect to $x_1[u]$ and $x_2[u]$, can be formulated respectively as

$$\psi_{\mathrm{E},1}^{\mathrm{MRC}} = \frac{a_1 \sum\limits_{t=1}^{N_{\mathrm{E}}} \psi_{\mathrm{S}_a\mathrm{E}_t}}{a_2 \sum\limits_{n=1}^{N_{\mathrm{E}}} \psi_{\mathrm{S}_a\mathrm{E}_t} + 1}, \psi_{\mathrm{E},2}^{\mathrm{MRC}} = a_2 \sum_{n=1}^{N_{\mathrm{E}}} \psi_{\mathrm{S}_a\mathrm{E}_t}, \tag{23}$$

where the source selects the a-th antenna to transmit data to the destination.

Remark 2. *To further decrease the number of time slots used for the transmission, the source can send more than two encoded packets to the destination at each time slot. However, when more signals are combined by the*

source, the implementation is more complex. Moreover, the fraction of the transmit power allocated to the signals is lower, which can degrade the system performance. For example, let us consider $\psi_{\mathrm{D},1}^{\mathrm{TAS/SC}}$ *in* (17) *which can be approximated as*

$$\psi_{\mathrm{D},1}^{\mathrm{TAS/SC}} \approx \frac{a_1 \max\limits_{m=1,2,..,N_{\mathrm{S}}} \left(\max\limits_{n=1,2,..,N_{\mathrm{D}}} (\psi_{\mathrm{S}_m\mathrm{D}_n}) \right)}{a_2 \max\limits_{m=1,2,..,N_{\mathrm{S}}} \left(\max\limits_{n=1,2,..,N_{\mathrm{D}}} (\psi_{\mathrm{S}_m\mathrm{D}_n}) \right)} = \frac{a_1}{a_2}. \tag{24}$$

It is obvious from (24) *that to obtain high SNR* $\psi_{\mathrm{D},1}^{\mathrm{TAS/SC}}$, a_1 *should be much higher than* a_2, *(or* a_2 *is small). For another example, if the source combines 3 signals using the coefficients* a_1, a_2 *and* a_3, *where* $a_1 > a_2 > a_3$ *and* $a_1 + a_2 + a_3 = 1$, *similarly, we have* $a_1 \text{»} a_2 \text{»} a_3$, *and hence the transmit power allocated to the third signal is very small.*

Remark 3. *It is obvious that to obtain the packet* p_2, *the destination must correctly decode the packet* p_1 *first. If the decoding status of* p_1 *is not successful,* p_2 *cannot also be decoded successfully. Therefore, the probabilities that in one time slot the destination cannot obtain any packet only obtains* p_1, *and obtains* p_1 *and* p_2 *are formulated respectively as*

$$\begin{aligned}
\chi_{\mathrm{D},0} &= \Pr\left(\psi_{\mathrm{D},1}^{\mathrm{Y}} < \gamma_{\mathrm{th}}\right), \\
\chi_{\mathrm{D},1} &= \Pr\left(\psi_{\mathrm{D},1}^{\mathrm{Y}} \geq \gamma_{\mathrm{th}}, \psi_{\mathrm{D},2}^{\mathrm{Y}} < \gamma_{\mathrm{th}}\right), \\
\chi_{\mathrm{D},2} &= \Pr\left(\psi_{\mathrm{D},1}^{\mathrm{Y}} \geq \gamma_{\mathrm{th}}, \psi_{\mathrm{D},2}^{\mathrm{Y}} \geq \gamma_{\mathrm{th}}\right),
\end{aligned} \tag{25}$$

where $\mathrm{Y} \in \{\mathrm{TAS/SC}, \mathrm{TAS/MRC}\}$.

Similarly, the probabilities that the eavesdropper cannot obtain any packet only obtains p_1, and obtains both p_1 and p_2 are formulated respectively as

$$\begin{aligned}
\chi_{\mathrm{E},0} &= \Pr\left(\psi_{\mathrm{E},1}^{\mathrm{Z}} < \gamma_{\mathrm{th}}\right), \\
\chi_{\mathrm{E},1} &= \Pr\left(\psi_{\mathrm{E},1}^{\mathrm{Z}} \geq \gamma_{\mathrm{th}}, \psi_{\mathrm{E},2}^{\mathrm{Z}} < \gamma_{\mathrm{th}}\right), \\
\chi_{\mathrm{E},2} &= \Pr\left(\psi_{\mathrm{E},1}^{\mathrm{Z}} \geq \gamma_{\mathrm{th}}, \psi_{\mathrm{E},2}^{\mathrm{Z}} \geq \gamma_{\mathrm{th}}\right).
\end{aligned} \tag{26}$$

where $\mathrm{Z} \in \{\mathrm{SC}, \mathrm{MRC}\}$.

3. Performance Analysis

In this section, we derive exact expressions of average number of time slots (TS) and intercept probability (IP) of the proposed protocols. At first, the probabilities $\rho_{\mathrm{D}}, \rho_{\mathrm{E}}, \chi_{\mathrm{D},i}$ and $\chi_{\mathrm{E},i}$ $(i = 0, 1, 2)$ are calculated.

3.1. Derivation of ρ_{D} *and* ρ_{E}

- Case 1: The SC combiner is used by D and E

  Combining (1), (7) and (13), we can obtain

$$\begin{aligned}
\rho_{\mathrm{D}} &= 1 - \Pr\left(\max_{m=1,2,\ldots,N_{\mathrm{S}}} \left(\max_{n=1,2,\ldots,N_{\mathrm{D}}} (\psi_{\mathrm{S}_m\mathrm{D}_n}) \right) < \gamma_{\mathrm{th}} \right) \\
&= 1 - \prod_{m=1}^{N_{\mathrm{S}}} \prod_{n=1}^{N_{\mathrm{D}}} F_{\gamma_{\mathrm{S}_m\mathrm{D}_n}} \left(\frac{\gamma_{\mathrm{th}}}{\Delta} \right) \\
&= 1 - \left[1 - \exp\left(-\frac{\lambda_{\mathrm{SD}} \gamma_{\mathrm{th}}}{\Delta} \right) \right]^{N_{\mathrm{S}} N_{\mathrm{D}}}.
\end{aligned} \tag{27}$$

Similarly, combining (1), (8), and (13), the probability ρ_{E} is calculated as

$$\begin{aligned}\rho_{\mathrm{E}} &= 1 - \Pr\left(\max_{t=1,2,\ldots,N_{\mathrm{E}}} (\psi_{\mathrm{S}_a\mathrm{E}_t}) < \gamma_{\mathrm{th}}\right) \\ &= 1 - \left[1 - \exp\left(-\frac{\lambda_{\mathrm{SE}}\gamma_{\mathrm{th}}}{\Delta}\right)\right]^{N_{\mathrm{E}}}. \end{aligned} \tag{28}$$

- Case 2: The MRC combiner is used by D and E

From (1), (11) and (13), the probability ρ_{D} can be formulated as

$$\begin{aligned}\rho_{\mathrm{D}} &= 1 - \Pr\left(\max_{m=1,2,\ldots,N_{\mathrm{S}}} \left(\sum_{n=1}^{N_{\mathrm{D}}} \psi_{\mathrm{S}_m\mathrm{D}_n}\right) < \gamma_{\mathrm{th}}\right) \\ &= 1 - \left[\Pr\left(\sum_{n=1}^{N_{\mathrm{D}}} \psi_{\mathrm{S}_m\mathrm{D}_n} < \gamma_{\mathrm{th}}\right)\right]^{N_{\mathrm{S}}}. \end{aligned} \tag{29}$$

Using CDF of sum of identical and independent exponential RVs [59], we can obtain

$$\rho_{\mathrm{D}} = 1 - \left[1 - \sum_{m=0}^{N_{\mathrm{D}}-1} \frac{1}{m!}\left(\frac{\lambda_{\mathrm{SD}}\gamma_{\mathrm{th}}}{\Delta}\right)^m \exp\left(-\frac{\lambda_{\mathrm{SD}}\gamma_{\mathrm{th}}}{\Delta}\right)\right]^{N_{\mathrm{S}}}. \tag{30}$$

Similarly, we can calculate the probability ρ_{E} in this case as follows:

$$\rho_{\mathrm{E}} = \sum_{t=0}^{N_{\mathrm{E}}-1} \frac{1}{t!}\left(\frac{\lambda_{\mathrm{SE}}\gamma_{\mathrm{th}}}{\Delta}\right)^t \exp\left(-\frac{\lambda_{\mathrm{SE}}\gamma_{\mathrm{th}}}{\Delta}\right). \tag{31}$$

3.2. Derivation of $\chi_{\mathrm{D},i}$ and $\chi_{\mathrm{E},i}$

- Case 1: The SC combiner is used by D and E

At first, we consider $\chi_{\mathrm{D},2}$ combining (17) and (25), we have

$$\begin{aligned}&\chi_{\mathrm{D},2} = \\ &\Pr\left((a_1 - a_2\gamma_{\mathrm{th}}) \max_{m=1,2,\ldots,N_{\mathrm{S}}} \left(\max_{n=1,2,\ldots,N_{\mathrm{D}}} (\psi_{\mathrm{S}_m\mathrm{D}_n})\right) \geq \gamma_{\mathrm{th}}, a_2 \max_{m=1,2,\ldots,N_{\mathrm{S}}} \left(\max_{n=1,2,\ldots,N_{\mathrm{D}}} (\psi_{\mathrm{S}_m\mathrm{D}_n})\right) \geq \gamma_{\mathrm{th}}\right). \end{aligned} \tag{32}$$

We observe from (32) that if $a_1 - a_2\gamma_{\mathrm{th}} \leq 0$, then $\chi_{\mathrm{D},2} = 0$. Otherwise, (32) can be rewritten as

$$\chi_{\mathrm{D},2} = \Pr\left(\max_{m=1,2,\ldots,N_{\mathrm{S}}} \left(\max_{n=1,2,\ldots,N_{\mathrm{D}}} (\gamma_{\mathrm{S}_m\mathrm{D}_n})\right) \geq \mu_1, \max_{m=1,2,\ldots,N_{\mathrm{S}}} \left(\max_{n=1,2,\ldots,N_{\mathrm{D}}} (\gamma_{\mathrm{S}_m\mathrm{D}_n})\right) \geq \mu_2\right), \tag{33}$$

where

$$\mu_1 = \frac{\gamma_{\mathrm{th}}}{(a_1 - a_2\gamma_{\mathrm{th}})\,\Delta}, \mu_2 = \frac{\gamma_{\mathrm{th}}}{a_2\Delta}. \tag{34}$$

Remark 4. *As mentioned in Remark 2, a_1 should be much higher than a_2 so that the obtained SNR $\psi_{\mathrm{D},1}^{\mathrm{TAS/SC}}$ is high enough. Therefore, it can be assumed that $a_1 > (1+\gamma_{\mathrm{th}})a_2$, which yields the following result: $0 < \mu_1 < \mu_2$. Then, the probability $\chi_{\mathrm{D},2}$ is calculated as*

$$\begin{aligned}\chi_{\mathrm{D},2} &= \Pr\left(\max_{m=1,2,\ldots,N_{\mathrm{S}}} \left(\max_{n=1,2,\ldots,N_{\mathrm{D}}} (\gamma_{\mathrm{S}_m\mathrm{D}_n})\right) \geq \mu_2\right) \\ &= 1 - \Pr\left(\max_{m=1,2,\ldots,N_{\mathrm{S}}} \left(\max_{n=1,2,\ldots,N_{\mathrm{D}}} (\gamma_{\mathrm{S}_m\mathrm{D}_n})\right) < \mu_2\right) \\ &= 1 - \left[1 - \exp\left(-\lambda_{\mathrm{SD}}\mu_2\right)\right]^{N_{\mathrm{S}}N_{\mathrm{D}}}. \end{aligned} \tag{35}$$

Next, we can calculate $\chi_{\mathrm{D},0}$ and $\chi_{\mathrm{D},1}$ respectively as

$$\begin{aligned}\chi_{\mathrm{D},0} &= \Pr\left(\max_{m=1,2,\ldots,N_{\mathrm{S}}}\left(\max_{n=1,2,\ldots,N_{\mathrm{D}}}\left(\gamma_{\mathrm{S}_m\mathrm{D}_n}\right)\right) < \mu_1\right)\\ &= \left(1-\exp\left(-\lambda_{\mathrm{SD}}\mu_1\right)\right)^{N_{\mathrm{S}}N_{\mathrm{D}}},\\ \chi_{\mathrm{D},1} &= \Pr\left(\mu_1 \le \max_{m=1,2,\ldots,N_{\mathrm{S}}}\left(\max_{n=1,2,\ldots,N_{\mathrm{D}}}\left(\gamma_{\mathrm{S}_m\mathrm{D}_n}\right)\right) < \mu_2\right)\\ &= \left(1-\exp\left(-\lambda_{\mathrm{SD}}\mu_2\right)\right)^{N_{\mathrm{S}}N_{\mathrm{D}}} - \left(1-\exp\left(-\lambda_{\mathrm{SD}}\mu_1\right)\right)^{N_{\mathrm{S}}N_{\mathrm{D}}}.\end{aligned} \tag{36}$$

Similarly, we can calculate $\chi_{\mathrm{E},0}$, $\chi_{\mathrm{E},1}$, and $\chi_{\mathrm{E},2}$, respectively as

$$\begin{aligned}\chi_{\mathrm{E},0} &= \left(1-\exp\left(-\lambda_{\mathrm{SE}}\mu_1\right)\right)^{N_{\mathrm{E}}},\\ \chi_{\mathrm{E},1} &= \left(1-\exp\left(-\lambda_{\mathrm{SE}}\mu_2\right)\right)^{N_{\mathrm{E}}} - \left(1-\exp\left(-\lambda_{\mathrm{SE}}\mu_1\right)\right)^{N_{\mathrm{E}}},\\ \chi_{\mathrm{E},2} &= 1-\left(1-\exp\left(-\lambda_{\mathrm{SE}}\mu_2\right)\right)^{N_{\mathrm{E}}}.\end{aligned} \tag{37}$$

- Case 2: The MRC combiner is used by D and E

  In this case, it is straightforward to obtain the following results:

$$\begin{aligned}\chi_{\mathrm{D},0} &= \left[1-\sum_{m=0}^{N_{\mathrm{D}}-1}\frac{\left(\lambda_{\mathrm{SD}}\mu_1\right)^m}{m!}\exp\left(-\lambda_{\mathrm{SD}}\mu_1\right)\right]^{N_{\mathrm{S}}},\\ \chi_{\mathrm{D},1} &= \left[1-\sum_{m=0}^{N_{\mathrm{D}}-1}\frac{\left(\lambda_{\mathrm{SD}}\mu_2\right)^m}{m!}\exp\left(-\lambda_{\mathrm{SD}}\mu_2\right)\right]^{N_{\mathrm{S}}} - \left[1-\sum_{m=0}^{N_{\mathrm{D}}-1}\frac{\left(\lambda_{\mathrm{SD}}\mu_1\right)^m}{m!}\exp\left(-\lambda_{\mathrm{SD}}\mu_1\right)\right]^{N_{\mathrm{S}}},\\ \chi_{\mathrm{D},2} &= 1-\left[1-\sum_{m=0}^{N_{\mathrm{D}}-1}\frac{\left(\lambda_{\mathrm{SD}}\mu_2\right)^m}{m!}\exp\left(-\lambda_{\mathrm{SD}}\mu_2\right)\right]^{N_{\mathrm{S}}},\\ \chi_{\mathrm{E},0} &= 1-\sum_{t=0}^{N_{\mathrm{E}}-1}\frac{\left(\lambda_{\mathrm{SE}}\mu_1\right)^t}{t!}\exp\left(-\lambda_{\mathrm{SE}}\mu_1\right),\\ \chi_{\mathrm{E},1} &= \sum_{t=0}^{N_{\mathrm{E}}-1}\frac{\left(\lambda_{\mathrm{SE}}\mu_1\right)^t}{t!}\exp\left(-\lambda_{\mathrm{SE}}\mu_1\right) - \sum_{t=0}^{N_{\mathrm{E}}-1}\frac{\left(\lambda_{\mathrm{SE}}\mu_2\right)^t}{t!}\exp\left(-\lambda_{\mathrm{SE}}\mu_2\right),\\ \chi_{\mathrm{E},2} &= \sum_{t=0}^{N_{\mathrm{E}}-1}\frac{\left(\lambda_{\mathrm{SE}}\mu_2\right)^t}{t!}\exp\left(-\lambda_{\mathrm{SE}}\mu_2\right).\end{aligned} \tag{38}$$

3.3. Average Number of Time Slots (TS)

3.3.1. Without Using NOMA (Wo-NOMA)

The average number of time slots of the Wo-NOMA protocol can be formulated as

$$\mathrm{TS} = \sum_{N_{\mathrm{TS}}=N_{\mathrm{req}}^{\mathrm{pkt}}}^{+\infty} N_{\mathrm{TS}} \times \Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} | N_{\mathrm{TS}}\right), \tag{39}$$

where $\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} | N_{\mathrm{TS}}\right)$ is the probability that the destination obtains $N_{\mathrm{req}}^{\mathrm{pkt}}$ encoded packets after N_{TS} time slots, which follows a negative binomial distribution (see Equation (9) of [60]):

$$\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} | N_{\mathrm{TS}}\right) = C_{N_{\mathrm{TS}}-1}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1}\left(\rho_{\mathrm{D}}\right)^{N_{\mathrm{req}}^{\mathrm{pkt}}}\left(1-\rho_{\mathrm{D}}\right)^{N_{\mathrm{TS}}-N_{\mathrm{req}}^{\mathrm{pkt}}}, \tag{40}$$

and $C_b^a\ (b \ge a)$ denotes the binomial coefficient:

$$C_b^a = \frac{b!}{a!\,(b-a)!}.$$

Equation (40) can be explained as follows. After $(N_{\mathrm{TS}}-1)$ time slots, the destination obtains $N_{\mathrm{req}}^{\mathrm{pkt}}-1$ encoded packets, and it correctly receives one more encoded packet at the N_{TS}-th time slot. In (40), $C_{N_{\mathrm{TS}}-1}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1}$ is number of possible cases can occur when D has $N_{\mathrm{req}}^{\mathrm{pkt}}-1$ encoded packets before the last time slot.

Substituting (40) into (39), and using Equation (8) of [60], we obtain

$$\mathrm{TS}=\frac{N_{\mathrm{req}}^{\mathrm{pkt}}}{\rho_{\mathrm{D}}}. \tag{41}$$

Substituting (27) and (29) into (41), we respectively obtain exact expressions of TS when the SC and MRC combiners are used.

3.3.2. Using NOMA

In this protocol, we formulate the average number of time slots used by the source as

$$\mathrm{TS}=\sum_{N_{\mathrm{TS}}=\left\lceil N_{\mathrm{req}}^{\mathrm{pkt}}/2\right\rceil}^{+\infty}N_{\mathrm{TS}}\times\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}\cup N_{\mathrm{D}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}+1|N_{\mathrm{TS}}\right), \tag{42}$$

where $\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}\cup N_{\mathrm{D}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}+1|N_{\mathrm{TS}}\right)$ is the probability that the destination can obtain $N_{\mathrm{req}}^{\mathrm{pkt}}$ or $N_{\mathrm{req}}^{\mathrm{pkt}}+1$ encoded packets after N_{TS} time slots.

Let us denote T_1 and T_2 as the number of time slots that the destination correctly receives one encoded packet and two encoded packets, respectively. Now, to calculate $\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}\cup N_{\mathrm{D}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}+1|N_{\mathrm{TS}}\right)$, we consider three cases as follows:

- Case 1: After $N_{\mathrm{TS}}-1$ time slots, the destination obtains $N_{\mathrm{req}}^{\mathrm{pkt}}-2$ encoded packets, and at the last time slot, it obtains two encoded packets.

In this case, after the transmission is terminated, the destination has $N_{\mathrm{req}}^{\mathrm{pkt}}$ encoded packets, i.e., $N_{\mathrm{D}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}$ and $\mathrm{T}_1+2\mathrm{T}_2=N_{\mathrm{req}}^{\mathrm{pkt}}$. Moreover, the probability of Case 1 can be calculated as follows:

$$\theta_{\mathrm{D},1}=\sum_{\mathrm{T}_2=1}^{\left\lfloor N_{\mathrm{req}}^{\mathrm{pkt}}/2\right\rfloor}C_{N_{\mathrm{TS}}-1}^{\mathrm{T}_1}C_{N_{\mathrm{TS}}-\mathrm{T}_1-1}^{\mathrm{T}_2-1}(\chi_{\mathrm{D},2})^{\mathrm{T}_2}(\chi_{\mathrm{D},1})^{\mathrm{T}_1}(\chi_{\mathrm{D},0})^{N_{\mathrm{TS}}-\mathrm{T}_2-\mathrm{T}_1}, \tag{43}$$

where $\mathrm{T}_1\leq N_{\mathrm{TS}}-1$, $\mathrm{T}_2\leq N_{\mathrm{TS}}-\mathrm{T}_1$.

- Case 2: After $N_{\mathrm{TS}}-1$ time slots, the destination obtains $N_{\mathrm{req}}^{\mathrm{pkt}}-1$ encoded packets, and at the last time slot, it only obtains one encoded packet.

In Case 2, we also have $N_{\mathrm{D}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}$ and $\mathrm{T}_1+2\mathrm{T}_2=N_{\mathrm{req}}^{\mathrm{pkt}}$. Then, the probability of this event is computed as

$$\theta_{\mathrm{D},2}=\sum_{\mathrm{T}_2=0}^{\left\lfloor N_{\mathrm{req}}^{\mathrm{pkt}}/2\right\rfloor}C_{N_{\mathrm{TS}}-1}^{\mathrm{T}_2}C_{N_{\mathrm{TS}}-\mathrm{T}_2-1}^{\mathrm{T}_1-1}(\chi_{\mathrm{D},2})^{\mathrm{T}_2}(\chi_{\mathrm{D},1})^{\mathrm{T}_1}(\chi_{\mathrm{D},0})^{N_{\mathrm{TS}}-\mathrm{T}_2-\mathrm{T}_1}, \tag{44}$$

where $1\leq\mathrm{T}_1\leq N_{\mathrm{TS}}-\mathrm{T}_2$.

- Case 3: After $N_{\mathrm{TS}}-1$ time slots, the destination obtains $N_{\mathrm{req}}^{\mathrm{pkt}}-1$ encoded packets, and at the last time slot, it obtains two encoded packets.

In this case, the destination can successfully receive $N_{\mathrm{req}}^{\mathrm{pkt}}+1$ encoded packets after N_{TS} time slots: $\mathrm{T}_1+2\mathrm{T}_2=N_{\mathrm{D}}^{\mathrm{pkt}}=N_{\mathrm{req}}^{\mathrm{pkt}}+1$. Therefore, the probability that this event occurs can be calculated exactly as

$$\theta_{\mathrm{D},3} = \sum_{\mathrm{T}_2=1}^{\left\lceil N_{\mathrm{req}}^{\mathrm{pkt}}/2 \right\rceil} C_{N_{\mathrm{TS}}-1}^{\mathrm{T}_1} C_{N_{\mathrm{TS}}-\mathrm{T}_1-1}^{\mathrm{T}_2-1} (\chi_{\mathrm{D},2})^{\mathrm{T}_2} (\chi_{\mathrm{D},1})^{\mathrm{T}_1} (\chi_{\mathrm{D},0})^{N_{\mathrm{TS}}-\mathrm{T}_2-\mathrm{T}_1}, \tag{45}$$

where $\mathrm{T}_1 \leq N_{\mathrm{TS}} - 1$, $\mathrm{T}_2 \leq N_{\mathrm{TS}} - \mathrm{T}_1$.

From (43)–(45), we can obtain an exact expression of $\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} \cup N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} + 1 | N_{\mathrm{TS}}\right)$ by using the following formula:

$$\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} \cup N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} + 1 | N_{\mathrm{TS}}\right) = \theta_{\mathrm{D},1} + \theta_{\mathrm{D},2} + \theta_{\mathrm{D},3}.$$

Then, from (42), we can write the average number of time slots used in the NOMA protocol as follows:

$$\mathrm{TS} = \sum_{N_{\mathrm{TS}}=\left\lceil N_{\mathrm{req}}^{\mathrm{pkt}}/2 \right\rceil}^{+\infty} N_{\mathrm{TS}} \times (\theta_{\mathrm{D},1} + \theta_{\mathrm{D},2} + \theta_{\mathrm{D},3}). \tag{46}$$

Remark 5. *From (41) and (46), we can observe that when the transmit SNR is high enough, i.e., $\Delta \to +\infty$, the values of TS in the Wo-NOMA and NOMA protocols converge to $N_{\mathrm{req}}^{\mathrm{pkt}}$ and $\left\lceil N_{\mathrm{req}}^{\mathrm{pkt}}/2 \right\rceil$, respectively. It is due to the fact that at high Δ regimes, all of the encoded packet(s) can be correctly received by the destination. Therefore, by using NOMA, the proposed protocol can reduce a half of time slots used for transmitting the encoded packets.*

3.4. Intercept Probability (IP)

In this subsection, we calculate the intercept probability of the proposed protocols with and without using NOMA.

3.4.1. Without Using NOMA (Wo-NOMA)

At first, we see that the source data is intercepted if the eavesdropper can sufficiently obtain the number of the encoded packets for recovering the original data before or at the same time with the destination. Mathematically speaking, we can write

$$\mathrm{IP} = \sum_{N_{\mathrm{TS}}^{\mathrm{E}}=N_{\mathrm{req}}^{\mathrm{pkt}}}^{+\infty} \left[\begin{array}{l} \left(\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} | N_{\mathrm{TS}}^{\mathrm{E}}\right) + \Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} < N_{\mathrm{req}}^{\mathrm{pkt}} | N_{\mathrm{TS}}^{\mathrm{E}}\right)\right) \\ \times \Pr\left(N_{\mathrm{E}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} | N_{\mathrm{TS}}^{\mathrm{E}}\right) \end{array} \right], \tag{47}$$

Equation (47) implies that the eavesdropper can obtain $N_{\mathrm{req}}^{\mathrm{pkt}}$ encoded packets after $N_{\mathrm{TS}}^{\mathrm{E}}$ time slots, while the destination can sufficiently receive or not. In (47), $\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} | N_{\mathrm{TS}}^{\mathrm{E}}\right)$ is calculated as in (40), and similarly, $\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} < N_{\mathrm{req}}^{\mathrm{pkt}} | N_{\mathrm{TS}}^{\mathrm{E}}\right)$ is also given as

$$\Pr\left(N_{\mathrm{E}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} | N_{\mathrm{TS}}^{\mathrm{E}}\right) = C_{N_{\mathrm{TS}}^{\mathrm{E}}-1}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1} (\rho_{\mathrm{E}})^{N_{\mathrm{req}}^{\mathrm{pkt}}} (1-\rho_{\mathrm{E}})^{N_{\mathrm{TS}}^{\mathrm{E}}-N_{\mathrm{req}}^{\mathrm{pkt}}}. \tag{48}$$

Considering $\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} < N_{\mathrm{req}}^{\mathrm{pkt}} | N_{\mathrm{TS}}^{\mathrm{E}}\right)$ in (47); this is the probability that the destination cannot sufficiently receive the number of the encoded packets for the data recovery after $N_{\mathrm{TS}}^{\mathrm{E}}$ time slots and is calculated as

$$\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} < N_{\mathrm{req}}^{\mathrm{pkt}} | N_{\mathrm{TS}}^{\mathrm{E}}\right) = \sum_{N_{\mathrm{D}}^{\mathrm{pkt}}=0}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1} C_{N_{\mathrm{TS}}^{\mathrm{E}}}^{N_{\mathrm{D}}^{\mathrm{pkt}}} (\rho_{\mathrm{D}})^{N_{\mathrm{D}}^{\mathrm{pkt}}} (1-\rho_{\mathrm{D}})^{N_{\mathrm{TS}}^{\mathrm{E}}-N_{\mathrm{D}}^{\mathrm{pkt}}}. \tag{49}$$

Remark 6. *When the eavesdropper obtains $N_{\mathrm{req}}^{\mathrm{pkt}}$ encoded packets, it does not decode the encoded packets any more, regardless of whether the source still transmits the encoded packets to the destination. This also means that after having $N_{\mathrm{req}}^{\mathrm{pkt}}$ encoded packets, it stops overhearing the data transmission and starts the data recovery.*

Combining (47)–(49), IP can be exactly calculated as

$$\mathrm{IP} = \sum_{N_{\mathrm{TS}}^{\mathrm{E}}=N_{\mathrm{req}}^{\mathrm{pkt}}}^{+\infty} \left[\begin{array}{l} \left(C_{N_{\mathrm{TS}}^{\mathrm{E}}-1}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1} (\rho_{\mathrm{D}})^{N_{\mathrm{req}}^{\mathrm{pkt}}} (1-\rho_{\mathrm{D}})^{N_{\mathrm{TS}}^{\mathrm{E}}-N_{\mathrm{req}}^{\mathrm{pkt}}} + \sum_{N_{\mathrm{D}}^{\mathrm{pkt}}=0}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1} C_{N_{\mathrm{TS}}^{\mathrm{E}}}^{N_{\mathrm{D}}^{\mathrm{pkt}}} (\rho_{\mathrm{D}})^{N_{\mathrm{D}}^{\mathrm{pkt}}} (1-\rho_{\mathrm{D}})^{N_{\mathrm{TS}}^{\mathrm{E}}-N_{\mathrm{D}}^{\mathrm{pkt}}} \right) \\ \times C_{N_{\mathrm{TS}}^{\mathrm{E}}-1}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1} (\rho_{\mathrm{E}})^{N_{\mathrm{req}}^{\mathrm{pkt}}} (1-\rho_{\mathrm{E}})^{N_{\mathrm{TS}}^{\mathrm{E}}-N_{\mathrm{req}}^{\mathrm{pkt}}} \end{array} \right]. \quad (50)$$

3.4.2. Using NOMA

In this protocol, IP can be formulated as

$$\mathrm{IP} = \sum_{N_{\mathrm{TS}}^{\mathrm{E}}=\left\lceil N_{\mathrm{req}}^{\mathrm{pkt}}/2 \right\rceil}^{+\infty} \left[\begin{array}{l} \left(\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} \cup N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}}+1 | N_{\mathrm{TS}}^{\mathrm{E}} \right) + \Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} < N_{\mathrm{req}}^{\mathrm{pkt}} | N_{\mathrm{TS}}^{\mathrm{E}} \right) \right) \\ \times \Pr\left(N_{\mathrm{E}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} \cup N_{\mathrm{E}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}}+1 | N_{\mathrm{TS}}^{\mathrm{E}} \right) \end{array} \right]. \quad (51)$$

where $\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} \cup N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}}+1 | N_{\mathrm{TS}}^{\mathrm{E}} \right)$ and $\Pr\left(N_{\mathrm{E}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} \cup N_{\mathrm{E}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}}+1 | N_{\mathrm{TS}}^{\mathrm{E}} \right)$ are computed similarly to (43)–(45) as

$$\begin{aligned} \Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} \cup N_{\mathrm{D}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}}+1 | N_{\mathrm{TS}}^{\mathrm{E}} \right) &= \theta_{\mathrm{D},1} + \theta_{\mathrm{D},2} + \theta_{\mathrm{D},3}, \\ \Pr\left(N_{\mathrm{E}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}} \cup N_{\mathrm{E}}^{\mathrm{pkt}} = N_{\mathrm{req}}^{\mathrm{pkt}}+1 | N_{\mathrm{TS}}^{\mathrm{E}} \right) &= \theta_{\mathrm{E},1} + \theta_{\mathrm{E},2} + \theta_{\mathrm{E},3}. \end{aligned} \quad (52)$$

In (52), we note that $\theta_{\mathrm{D},1}$, $\theta_{\mathrm{D},2}$, and $\theta_{\mathrm{D},3}$ are obtained by replacing N_{TS} in (43)–(45) by $N_{\mathrm{TS}}^{\mathrm{E}}$. For $\theta_{\mathrm{E},1}$, $\theta_{\mathrm{E},2}$, and $\theta_{\mathrm{E},3}$, with the same method as deriving $\theta_{\mathrm{D},1}$, $\theta_{\mathrm{D},2}$, $\theta_{\mathrm{D},3}$, we can obtain

$$\begin{aligned} \theta_{\mathrm{E},1} &= \sum_{\mathrm{V}_2=1}^{\left\lfloor N_{\mathrm{req}}^{\mathrm{pkt}}/2 \right\rfloor} C_{N_{\mathrm{TS}}^{\mathrm{E}}-1}^{\mathrm{V}_1} C_{N_{\mathrm{TS}}^{\mathrm{E}}-\mathrm{V}_1-1}^{\mathrm{V}_2-1} (\chi_{\mathrm{E},2})^{\mathrm{V}_2} (\chi_{\mathrm{E},1})^{\mathrm{V}_1} (\chi_{\mathrm{E},0})^{N_{\mathrm{TS}}^{\mathrm{E}}-\mathrm{V}_2-\mathrm{V}_1}, \\ \theta_{\mathrm{E},2} &= \sum_{\mathrm{V}_2=0}^{\left\lfloor N_{\mathrm{req}}^{\mathrm{pkt}}/2 \right\rfloor} C_{N_{\mathrm{TS}}^{\mathrm{E}}-1}^{\mathrm{V}_2} C_{N_{\mathrm{TS}}^{\mathrm{E}}-\mathrm{V}_2-1}^{\mathrm{V}_1-1} (\chi_{\mathrm{E},2})^{\mathrm{V}_2} (\chi_{\mathrm{E},1})^{\mathrm{V}_1} (\chi_{\mathrm{E},0})^{N_{\mathrm{TS}}^{\mathrm{E}}-\mathrm{V}_2-\mathrm{V}_1}, \\ \theta_{\mathrm{E},3} &= \sum_{\mathrm{V}_2=1}^{\left\lceil N_{\mathrm{req}}^{\mathrm{pkt}}/2 \right\rceil} C_{N_{\mathrm{TS}}^{\mathrm{E}}-1}^{\mathrm{V}_1} C_{N_{\mathrm{TS}}^{\mathrm{E}}-\mathrm{V}_1-1}^{\mathrm{V}_2-1} (\chi_{\mathrm{E},2})^{\mathrm{V}_2} (\chi_{\mathrm{E},1})^{\mathrm{V}_1} (\chi_{\mathrm{E},0})^{N_{\mathrm{TS}}^{\mathrm{E}}-\mathrm{V}_2-\mathrm{V}_1}, \end{aligned} \quad (53)$$

where V_1 and V_2 are the number of time slots that the eavesdropper correctly receives one encoded packet and two encoded packets, respectively.

Considering $\Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} < N_{\mathrm{req}}^{\mathrm{pkt}} | N_{\mathrm{TS}}^{\mathrm{E}} \right)$; this is probability that the destination cannot obtain $N_{\mathrm{req}}^{\mathrm{pkt}}$ encoded packets after $N_{\mathrm{TS}}^{\mathrm{E}}$ time slots, and is computed as

$$\begin{aligned} \Pr\left(N_{\mathrm{D}}^{\mathrm{pkt}} < N_{\mathrm{req}}^{\mathrm{pkt}} | N_{\mathrm{TS}}^{\mathrm{E}} \right) &\triangleq \theta_{\mathrm{D},4} \\ &= \sum_{N_{\mathrm{D}}^{\mathrm{pkt}}=0}^{N_{\mathrm{req}}^{\mathrm{pkt}}-1} \sum_{\mathrm{T}_2=0}^{\left\lfloor N_{\mathrm{D}}^{\mathrm{pkt}}/2 \right\rfloor} C_{N_{\mathrm{TS}}^{\mathrm{E}}}^{\mathrm{T}_2} C_{N_{\mathrm{TS}}^{\mathrm{E}}-\mathrm{T}_2}^{\mathrm{T}_1} (\chi_{\mathrm{D},2})^{\mathrm{T}_2} (\chi_{\mathrm{D},1})^{\mathrm{T}_1} (\chi_{\mathrm{D},0})^{N_{\mathrm{TS}}^{\mathrm{E}}-\mathrm{T}_2-\mathrm{T}_1}. \end{aligned} \quad (54)$$

From (51)–(54), IP in the NOMA protocol is written as follows:

$$\mathrm{IP} = \sum_{N_{\mathrm{TS}}^{\mathrm{E}}=\left\lceil N_{\mathrm{req}}^{\mathrm{pkt}}/2 \right\rceil}^{+\infty} [(\theta_{\mathrm{D},1} + \theta_{\mathrm{D},2} + \theta_{\mathrm{D},3} + \theta_{\mathrm{D},4}) \times (\theta_{\mathrm{E},1} + \theta_{\mathrm{E},2} + \theta_{\mathrm{E},3})]. \quad (55)$$

Remark 7. *Equations (50) and (55) exactly express the IP performance of the Wo-NOMA and NOMA protocols. To obtain the IP values, we truncate the infinite series by 500 first terms. Moreover, because (50) and (55) are in closed-form formulas, which can be used efficiently in designing and optimizing the networks.*

4. Simulation Results

In this section, we present simulation results using the Monte-Carlo approach to verify the theoretical results obtained in Section 3 as well as to compare the performances of the proposed protocols with and without using NOMA, in terms of TS and IP. All of the simulation and theoretical results are drawn by MATLAB R2014a software (MathWorks, Natick, MA, USA). For Monte-Carlo simulations, we perform $10^5 - 5 \times 10^6$ trials in which the Rayleigh channel coefficients of the X-Y links are generated by $hXY = 1/sqrt(2 \times LXY) \times (randn(1,1) + j \times randn(1,1))$, where $(\mathrm{X}, \mathrm{Y}) \in \{\mathrm{S}_m, \mathrm{D}_n, \mathrm{E}_t\}$, LXY (or λ_{XY}) is the parameter of the X-Y channel, and $randn(1,1)$ is a MATLAB function which generates Gaussian distributed pseudo-random numbers with zero-mean and unit variance. Then, using the given system parameters (we summarize the system parameters and their value ranges in Table 1), we obtain the simulation results of TS and IP. For the theoretical results, the expressions of TS and IP derived in the previous section are used to present them. As mentioned in Remark 7, the infinite series in the derived formulas are truncated by 500 first terms.

Table 1. System parameters.

System Parameters	Values
Δ	0 (dB)–24 (dB)
N_{S}, N_{D}	1–7
N_{E}	2–4
λ_{SD}	1–5
λ_{SE}	2.5–5
$N_{\mathrm{req}}^{\mathrm{pkt}}$	5–10
γ_{th}	1 and 1.5
a_1, a_2	$\frac{1+\gamma_{\mathrm{th}}}{2+\gamma_{\mathrm{th}}} < a_1 < 1, a_2 = 1 - a_1$

4.1. Average Number of Time Slots (TS)

In Figure 2, we present average number of time slots that the source uses to transmit the encoded packets to the destination as a function of the transmit SNR (Δ) in dB. In this figure, the number of antennas at the source (N_{S}) and the destination (N_{D}) is 1 and 3, respectively, the parameter of the data link (λ_{SD}) is fixed by 2, the required number of the encoded packets for successfully recovering the original data ($N_{\mathrm{req}}^{\mathrm{pkt}}$) is set by 8, and the threshold γ_{th} is set to 1. As mentioned in Remark 4, the value of a_1 has to satisfy the condition: $a_1 > (1 + \gamma_{\mathrm{th}})\, a_2$ or $a_1 > (1 + \gamma_{\mathrm{th}}) \,/\, (2 + \gamma_{\mathrm{th}}) = 2/3$, hence we can select $a_1 = 0.9$ ($a_2 = 0.1$). We can see from Figure 2 that the TS values of the Wo-NOMA and NOMA protocols decrease with the increasing of Δ and are lower when the destination is equipped with the MRC combiner. However, at high Δ regions, the TS values of the Wo-NOMA protocol converge to $N_{\mathrm{req}}^{\mathrm{pkt}}$, while those of the NOMA protocol reach to $N_{\mathrm{req}}^{\mathrm{pkt}}/2$. It is due to the fact that at high transmit SNR, the destination in the NOMA scheme can obtain two encoded packets at each time slot, and hence the source only uses $N_{\mathrm{req}}^{\mathrm{pkt}}/2$ time slots for the data transmission. However, we can observe that the NOMA protocol does not perform well at low Δ values when it uses more time slots than the Wo-NOMA protocol. It is worth noting that the simulation results (Sim) match very well with the theoretical ones (Theory), which verifies our derivations.

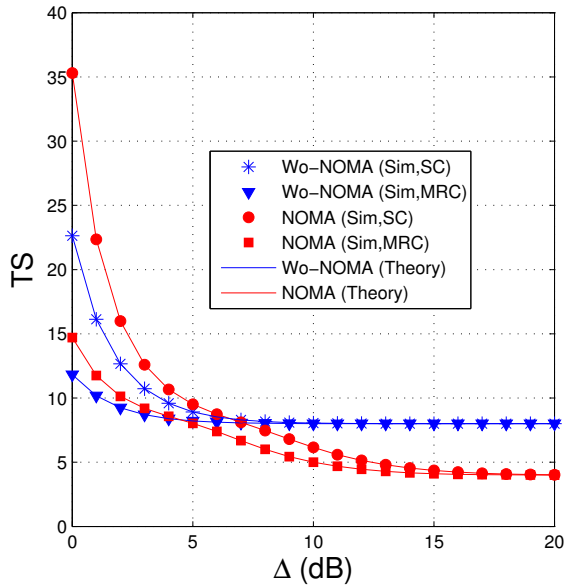

Figure 2. Average number of time slots as a function of Δ (dB) when $N_S = 1$, $N_D = 3$, $\lambda_{SD} = 2$, $N_{req}^{pkt} = 8$, $a_1 = 0.9$, $\gamma_{th} = 1$.

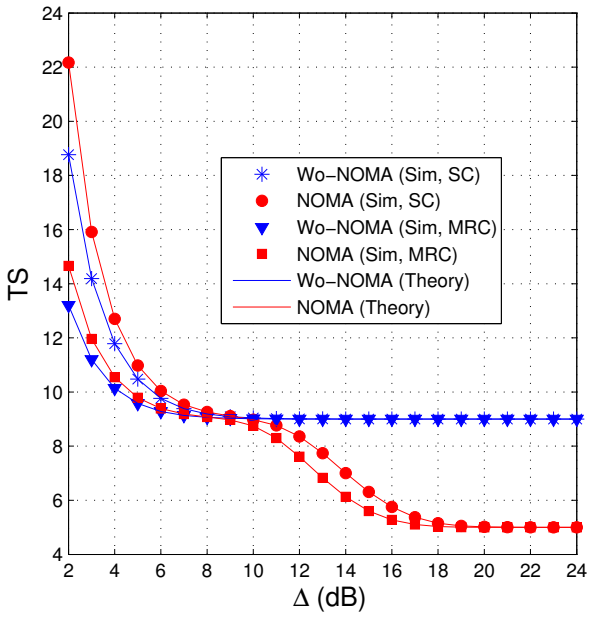

Figure 3. Average number of time slots as a function of Δ (dB) when $N_S = 2$, $N_D = 2$, $\lambda_{SD} = 3$, $N_{req}^{pkt} = 9$, $a_1 = 0.95$, $\gamma_{th} = 1$.

Figure 3 shows similar results to Figure 2, i.e., the performance of the NOMA protocol is better than that of the Wo-NOMA protocol at medium and high transmit SNRs. We also see from Figure 3 that the TS values of Wo-NOMA and NOMA at high Δ regimes converge to N_{req}^{pkt} and $\left\lceil N_{req}^{pkt}/2 \right\rceil$, respectively. In addition, as shown in Figures 2 and 3, the TS performance of Wo-NOMA more rapidly converges than that of NOMA. Again, the simulation results validate the correction of the theoretical ones.

In Figure 4, we fix the total number of antennas at the source and the destination, i.e., $N_S + N_D = 8$, and present TS as a function of N_S. In this figure, the Wo-NOMA protocol almost uses 8 time slots for transmitting the encoded packets, for all N_S. In the NOMA protocol, the average number of time slots significantly varies as changing N_S from 1 to 7. We can see that with the SC technique, the TS

performance of the NOMA protocol is same when the number of antennas at the source is N_S and $8 - N_S$. Moreover, in this case, the value of TS is lowest when $N_S = N_D = 4$. However, in the case where the destination is equipped with MRC, the optimal value of N_S is 2 ($N_D = 6$), and the TS performance is worst as $N_S = 7$. It is due to the fact that the MRC combiner is better than the SC one, and hence more antennas should be allocated to the destination to optimize the TS performance. Finally, it is seen that the TS values of the NOMA scheme with $a_1 = 0.86$ ($a_2 = 0.14$) are lower than those with $a_1 = 0.9$ ($a_2 = 0.1$). This can be explained as follows: Reducing a_2 means that the transmit power of the second signal is lower, which hence decreases the probability that the destination can obtain two encoded packets in each time slot (see $\chi_{D,2}$ in (35) and (38)), as well as increases the average number of the time slots used.

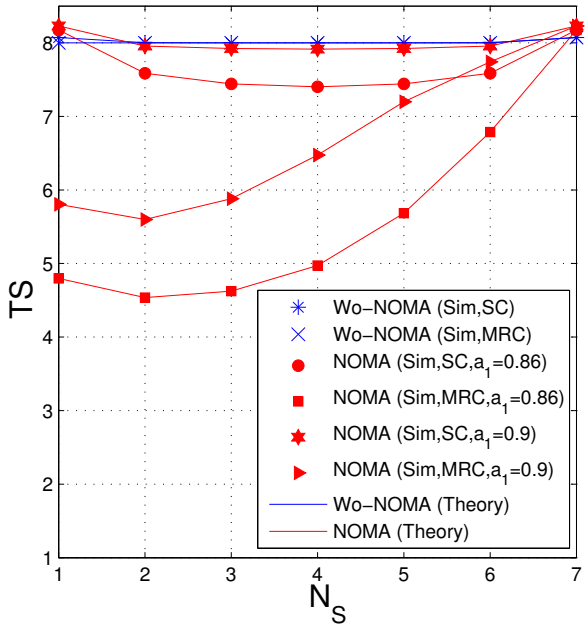

Figure 4. Average number of time slots as a function of N_S when $\Delta = 8$ dB, $N_D + N_S = 8$, $\lambda_{SD} = 3$, $N_{req}^{pkt} = 8$, $\gamma_{th} = 1.5$.

4.2. Intercept Probability (IP)

In Figure 5, we present IP of the proposed protocols as a function of Δ in dB. We can see that IP of the Wo-NOMA and NOMA protocols almost increases as increasing the transmit SNR. It is due to the fact that when the transmit power of the source is high, SNR of the eavesdropping link also increases, which enhances the intercept probability. However, in the NOMA scheme, when Δ belongs to interval of (8 dB, 10 dB), IP slightly decreases with the increasing of Δ, and hence, there exists a high performance gap between Wo-NOMA and NOMA in this interval. Because the intercept probability at the eavesdropper depends on the decoding at the destination and the interference between the signals, the changing of IP in the NOMA protocol, with respect to Δ, is more complex. Indeed, from (17), (18), (22) and (23), it is observed that as Δ increases, the interference from $x_2[u]$ to $x_1[u]$ also increases, which leads to a slow increase of SNR of $x_1[u]$ obtained at the D and E nodes. Because D and E must decode $x_1[u]$ first, the slow increase of SNRs can make IP slightly increase. However, when Δ is high enough, all the encoded packets can be correctly obtained by D and E. In this case, D and E can obtain N_{req}^{pkt} encoded packets at the same time, and hence the IP value converges to 1, as shown in Figure 5. Next, we can observe that when the destination and the eavesdropper use MRC, the IP values of the proposed protocols are higher. It is because the intercept possibility of the eavesdropper is better when it is equipped with MRC. Finally, it is seen that the NOMA protocol obtains better IP performance compared with the Wo-NOMA one.

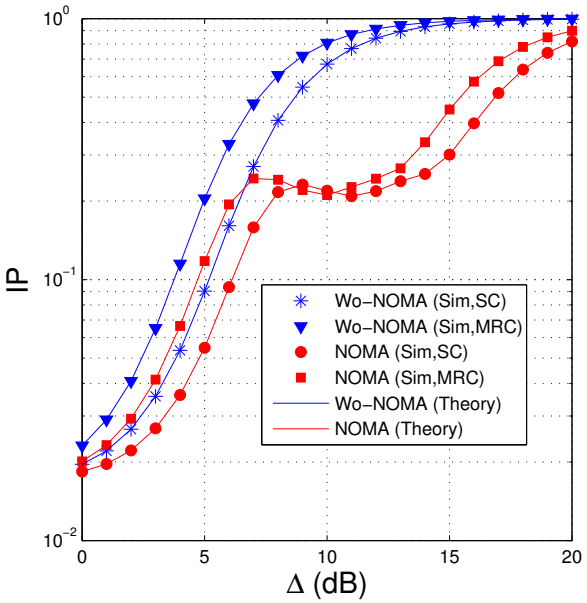

Figure 5. Intercept probability as a function of Δ (dB) when $N_S = 3$, $N_D = 2$, $N_E = 2$, $\lambda_{SD} = 2.5$, $\lambda_{SE} = 2.5$, $N_{req}^{pkt} = 8$, $a_1 = 0.9$, $\gamma_{th} = 1$.

In Figure 6, we investigate the impact of the parameter of the data link (λ_{SD}) on the IP performance. As we can see, IP of the proposed protocols increases as λ_{SD} increases. It is due to the fact that when the quality of the data channel is worse (λ_{SD} is high), the eavesdropper has more opportunity to obtain sufficient number of the encoded packets for recovering the original data. We also see that the IP performance of the Wo-NOMA protocol is worse than that of the NOMA protocol. Similar to Figure 5, the intercept probability of the eavesdropper increases when it uses MRC.

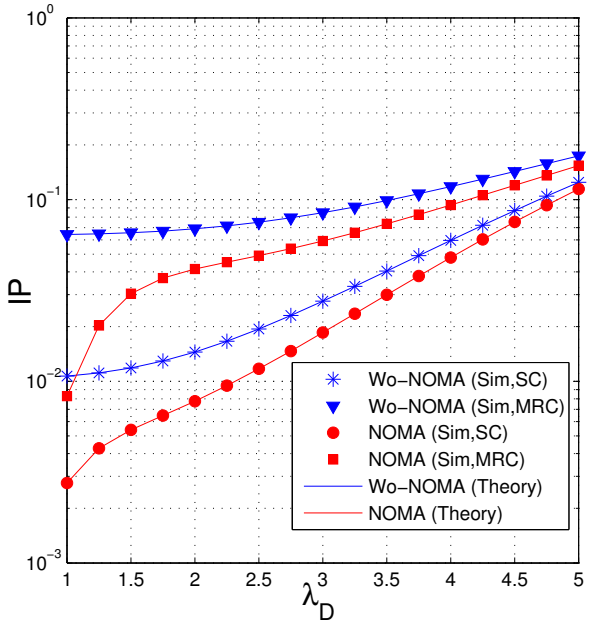

Figure 6. Intercept probability as a function of λ_{SD} when $\Delta = 7$ (dB), $N_S = 2$, $N_D = 2$, $N_E = 2$, $\lambda_{SE} = 5$, $N_{req}^{pkt} = 9$, $a_1 = 0.95$, $\gamma_{th} = 1$.

Figure 7 presents IP as a function of N_S when $N_S + N_D = 8$. Similar to Figure 4, in the case where the D and E nodes use SC, the IP value is lowest when $N_S = N_D = 4$, and when MRC is employed, the optimal value of N_S is 2. It is also seen that the IP performance of the Wo-NOMA protocol slightly varies with the changing of N_S but that of the NOMA protocol significantly varies. Again, the NOMA

protocol obtains better performance compared with the Wo-NOMA one. Moreover, we can see from this figure that when the MRC technique is used by the eavesdropper, the IP performance is not good. Indeed, if the desired value of IP is (below) 0.1, it is seen that both Wo-NOMA and NOMA cannot be practically implemented. In this case, to reduce IP, the source can reduce its transmit power or appropriately design the systems parameters $N_{\text{req}}^{\text{pkt}}$ and a_1 (see Figures 8 and 9 below).

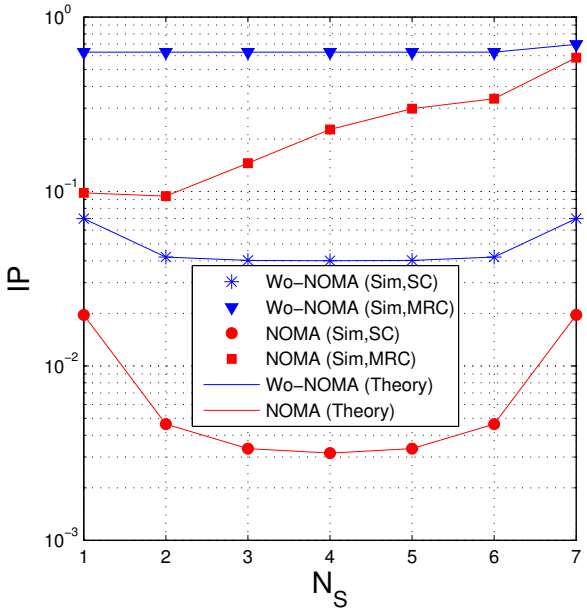

Figure 7. Intercept probability as a function of N_{S} when $\Delta = 5$ (dB), $N_{\text{S}} + N_{\text{D}} = 8$, $N_{\text{E}} = 4$, $\lambda_{\text{SD}} = 2$, $\lambda_{\text{SE}} = 3$, $N_{\text{req}}^{\text{pkt}} = 8$, $a_1 = 0.9$, $\gamma_{\text{th}} = 1.5$.

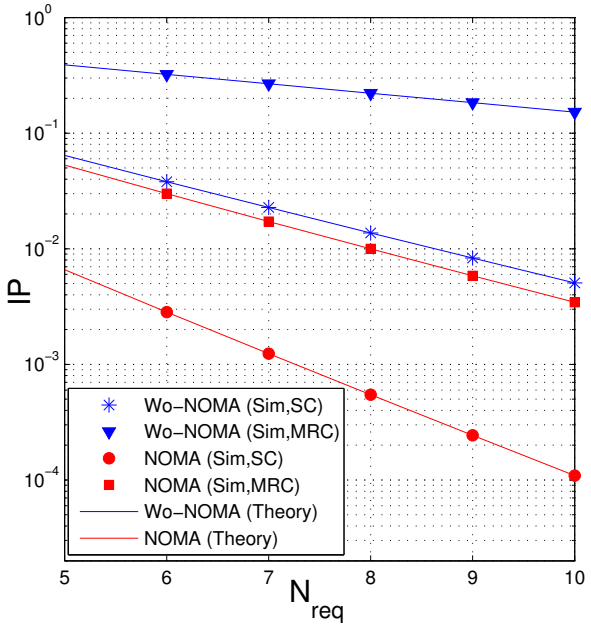

Figure 8. Intercept probability as a function of $N_{\text{req}}^{\text{pkt}}$ when $\Delta = 5$ (dB), $N_{\text{S}} = 3$, $N_{\text{D}} = 3$, $N_{\text{E}} = 3$, $\lambda_{\text{SD}} = 2$, $\lambda_{\text{SE}} = 3$, $a_1 = 0.85$, $\gamma_{\text{th}} = 1.5$.

In Figure 8, we present IP of the proposed protocols as a function of $N_{\text{req}}^{\text{pkt}}$. For ease of observation, we only change $N_{\text{req}}^{\text{pkt}}$ from 5 to 10. We can see that the values of IP decrease as $N_{\text{req}}^{\text{pkt}}$ increases. It is due to the fact that as $N_{\text{req}}^{\text{pkt}}$ is higher, the probability that the destination can obtain $N_{\text{req}}^{\text{pkt}}$ encoded packets before the eavesdropper increases, which hence reduces the intercept probability at the eavesdropper.

The obtained results in this figure can be used to design the considered network. For example, we assume that the D and E nodes are equipped with the MRC combiner, and hence Wo-NOMA cannot be used due to high IP value (higher than 0.1). Instead of Wo-NOMA, the NOMA scheme can be used to obtain higher security for the source data. For another example, assume that the system cannot use NOMA due to limited hardware and processing capacity. In this case, the source in the Wo-NOMA protocol can increase the number of $N_{\text{req}}^{\text{pkt}}$ to reduce IP. However, we note that increasing $N_{\text{req}}^{\text{pkt}}$ does increase the number of time slots and the delay time.

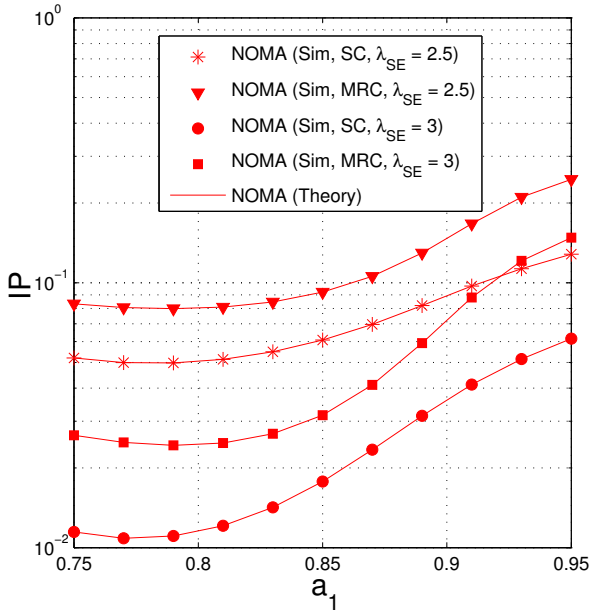

Figure 9. Intercept probability as a function of a_1 when $\Delta = 7.5$ (dB), $N_{\text{S}} = 2$, $N_{\text{D}} = 2$, $N_{\text{E}} = 2$, $\lambda_{\text{SD}} = 2$, $N_{\text{req}}^{\text{pkt}} = 8$, $\gamma_{\text{th}} = 1.5$.

Figure 9 investigates the impact of the fractions of the transmit power (a_1, a_2) on the IP performance of the NOMA protocol by changing a_1, and presenting IP as a function of a_1. Again, from Remark 4, the value of a_1 must be designed so that $a_1 > (1 + \gamma_{\text{th}}) / (2 + \gamma_{\text{th}}) = 0.7143$. Hence, in this figure, we can select the interval of a_1 as $(0.75, 0.95)$. As we can see, there exist optimal values of a_1 at which the IP value is lowest. It is also observed that the IP values are higher as the λ_{SE} decreases because the average channel gain of the eavesdropping is higher.

It is worth noting from Figures 4–9 that the simulation and theoretical results are in a good agreement, which validates the derived formulas of IP.

5. Conclusions

This paper showed that applying the NOMA technique into FCs secure communication protocols not only reduces the number of time slots used but also enhances security. Particularly, the NOMA protocol can reduce by half the number of time slots compared with the Wo-NOMA one. For the secure transmission, IP of the eavesdropper significantly decreases as the source uses NOMA to transmit two encoded packets to the destination at each time slot. For performance illustration, we derived exact expressions of TS and IP, which were validated by computer simulations. The results showed that the performance for the Wo-NOMA and NOMA protocols can be significantly enhanced by increasing or optimally designing the number of antennas at the source and the destination, appropriately selecting the faction of transmit power allocated to the NOMA signals and increasing the number of the encoded packets required for the data recovery.

Author Contributions: The main contributions of D.T.H. and T.T.D. were to create the main ideas and execute performance evaluation by simulations, while the main contributions of P.T.T., D.Q.T., and T.H. were to discuss, create, and advise in regard to the main ideas and performance evaluations.

Funding: This research is funded by Posts and Telecommunications Institute of Technology (PTIT) under grant number 11-HV-2019-RD_VT2.

Acknowledgments: This work was supported by the Domestic PhD Scholarship Programme of Vingroup Innovation Foundation.

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

References

1. Wyner, A.D. The Wire-tap Channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
2. Csiszar, I.; Korner, J. Broadcast Channels with Confidential Messages. *IEEE Trans. Inf. Theory* **1978**, *2*, 339–348. [CrossRef]
3. Liu, R.; Maric, I.; Spasojevic, P.; Yates, R.D. Discrete Memoryless Interference and Broadcast Channels with Conffdential Messages: Secrecy Rate Regions. *IEEE Trans. Inf. Theory* **2008**, *2*, 2493–2507. [CrossRef]
4. Gopala, P.K.; Lai, L.; Gamal, H.E. On the Secrecy Capacity of Fading Channels. *IEEE Trans. Inf. Theory* **2008**, *2*, 4687–4698. [CrossRef]
5. Zhang, J.; Duong, T.Q.; Woods, R.; Marshall, A. Securing Wireless Communications of the Internet of Things from the Physical Layer, An Overview. *Entropy* **2017**, *19*, 420. [CrossRef]
6. Li, G.; Sun, C.; Zhang, J.; Jorswieck, E.; Xiao, B.; Hu, A. Physical Layer Key Generation in 5G and Beyond Wireless Communications: Challenges and Opportunities. *Entropy* **2019**, *21*, 497. [CrossRef]
7. Yang, N.; Yeoh, P.L.; Elkashlan, M.; Schober, R.; Collings, I.B. Transmit Antenna Selection for Security Enhancement in MIMO Wiretap Channels. *IEEE Trans. Commun.* **2013**, *61*, 144–154. [CrossRef]
8. Yang, N.; Suraweera, H.A.; Collings, I.B.; Yuen, C. Physical Layer Security of TAS/MRC with Antenna Correlation. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 254–259. [CrossRef]
9. Xiong, J.; Tang, Y.; Ma, D.; Xiao, P.; Wong, K.-K. Secrecy Performance Analysis for TAS-MRC System with Imperfect Feedback. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 1617–1629. [CrossRef]
10. Yang, L.; Hasna, M.O.; Ansari, I.S. Physical Layer Security for TAS/MRC Systems with and without Co-Channel Interference Over $\eta - \mu$ Fading Channels. *IEEE Trans. Veh. Technol.* **2018**, *67*, 12421–12426. [CrossRef]
11. Zhao, H.; Tan, Y.; Pan G.; Chen, Y.; Yang, N. Secrecy Outage on Transmit Antenna Selection/Maximal Ratio Combining in MIMO Cognitive Radio Networks. *IEEE Trans. Veh. Technol.* **2016**, *65*, 10236–10242. [CrossRef]
12. Li, M.; Huang, Y.; Yin, H.; Wang Y.; Cai, C. Improving the Security and Spectrum Efficiency in Overlay Cognitive Full-Duplex Wireless Networks. *IEEE Access* **2019**, *7*, 68359–68372. [CrossRef]
13. Pan, G.; Lei, H.; Deng, Y.; Fan, L.; Yang, J.; Chen, Y.; Ding, Z. On Secrecy Performance of MISO SWIPT Systems With TAS and Imperfect CSI. *IEEE Commun.* **2016**, *64*, 3831–3843. [CrossRef]
14. 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]
15. Lei, H.; Zhang, J.; Park K.H.; Xu, P.; Ansari, I.S.; Pan, G.; Alomair, B.; Alouini, M.S. On Secure NOMA Systems With Transmit Antenna Selection Schemes. *IEEE Access* **2017**, *5*, 33774–33788. [CrossRef]
16. Lei, H.; Zhang, J.; Park K.H.; Xu, P.; Zhang, Z.; Pan, G.; Alouini, M.S. Secrecy Outage of Max–Min TAS Scheme in MIMO-NOMA Systems. *IEEE Trans. Veh. Technol.* **2018**, *67*, 6981–6990. [CrossRef]
17. Krikidis, I. Opportunistic Relay Selection For Cooperative Networks With Secrecy Constraints. *IET Commun.* **2010**, *4*, 1787–1791. [CrossRef]
18. Zhong, B.; Zhang, Z. Secure Full-Duplex Two-Way Relaying Networks With Optimal Relay Selection. *IEEE Commun. Lett.* **2017**, *21*, 1123–1126. [CrossRef]
19. Kuhestani, A.; Mohammadi, A.; Mohammadi, M. Joint Relay Selection and Power Allocation in Large-Scale MIMO Systems With Untrusted Relays and Passive Eavesdroppers. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 341–355. [CrossRef]
20. Mo, J.; Tao, M.; Liu, Y. Relay Placement for Physical Layer Security: A Secure Connection Perspective. *IEEE Commun. Lett.* **2012**, *16*, 878–881.

21. Yao, J.; Liu, Y. Secrecy Rate Maximization With Outage Constraint in Multihop Relaying Networks. *IEEE Commun. Lett.* **2018**, *22*, 304–307. [CrossRef]
22. Zhao, R.; Lin, H.; He, Y.C.; Chen, D.H.; Huang, Y.; Yang, L. Secrecy Performance of Transmit Antenna Selection for MIMO Relay Systems With Outdated CSI. *IEEE Trans. Commun.* **2018**, *66*, 546–559. [CrossRef]
23. Tang, X.; Cai, Y.; Huang, Y.; Duong, T.Q.; Yang, W.; Yang, W. Secrecy Outage Analysis of Buffer-Aided Cooperative MIMO Relaying Systems. *IEEE Trans. Veh. Technol.* **2018**, *67*, 2035–2048. [CrossRef]
24. Tang, C.; Pan, G.; Li, T. Secrecy Outage Analysis of Underlay Cognitive Radio Unit Over Nakagami-m Fading Channels. *IEEE Wirel. Commun. Lett.* **2014**, *3*, 609–612. [CrossRef]
25. Chakraborty, P.; Prakriya, S. Secrecy Outage Performance of a Cooperative Cognitive Relay Network. *IEEE Commun. Lett.* **2017**, *21*, 326–329. [CrossRef]
26. Tin, P.T.; Hung, D.T.; Tan, N.N.; Duy, T.T.; Voznak, M. Secrecy Performance Enhancement for Underlay Cognitive Radio Networks Employing Cooperative Multi-hop Transmission With and Without Presence of Hardware Impairments. *Entropy* **2019**, *21*, 217. [CrossRef]
27. Liu, Y.; Wang, L.; Tran, T.D.; Elkashlan, M.; Duong, T.Q. Relay Selection for Security Enhancement in Cognitive Relay Networks. *IEEE Wirel. Commun. Lett.* **2015**, *4*, 46–49. [CrossRef]
28. Jia, S.; Zhang, J.; Zhao, H.; Zhang, R. Relay Selection for Improved Security in Cognitive Relay Networks With Jamming. *IEEE Wirel. Commun. Lett.* **2017**, *6*, 662–665. [CrossRef]
29. Sun, C.; Liu, K.; Zheng, D.; Ai, W. Secure Communication for Two-Way Relay Networks with Imperfect CSI. *Entropy* **2017**, *19*, 522. [CrossRef]
30. Chang, S.; Li, J.; Fu, X.; Zhang, L. Energy Harvesting for Physical Layer Security in Cooperative Networks Based on Compressed Sensing. *Entropy* **2017**, *19*, 462. [CrossRef]
31. Kalamkar, S.S.; Banerjee, A. Secure Communication via a Wireless Energy Harvesting Untrusted Relay. *IEEE Trans. Veh. Technol.* **2017**, *66*, 2199–2213. [CrossRef]
32. Yin, C.; Nguyen, H.T.; Kundu, C.; Kaleem, Z.; Emiliano, G.P.; Duong, T.Q. Secure Energy Harvesting Relay Networks With Unreliable Backhaul Connections. *IEEE Access* **2018**, *6*, 12074–12084. [CrossRef]
33. Hoang, T.M.; Duong, T.Q.; Vo, N.S.; Kundu, C. Physical Layer Security in Cooperative Energy Harvesting Networks With a Friendly Jammer. *IEEE Wirel. Commun. Lett.* **2017**, *6*, 174–177. [CrossRef]
34. Zhang, G.; Xu, J.; Wu, Q.; Cui, M.; Li, X.; Lin, F. Wireless Powered Cooperative Jamming for Secure OFDM System. *IEEE Trans. Veh. Technol.* **2018**, *2*, 1331–1346. [CrossRef]
35. Hu, G.; Cai, Y. Analysis and Optimization of Wireless-Powered Cooperative Jamming for Sensor Network Over Nakagami- m Fading Channels. *IEEE Commun. Lett.* **2019**, *23*, 926–929. [CrossRef]
36. Yu, C.; Ko, H.L.; Peng, X.; Xie, W. Secrecy Outage Performance Analysis for Cooperative NOMA Over Nakagami-m Channel. *IEEE Access* **2019**, *7*, 79866–79876. [CrossRef]
37. Wang, Z.; Peng, Z. Secrecy Performance Analysis of Relay Selection in Cooperative NOMA Systems. *IEEE Access* **2019**, *7*, 86274–86287. [CrossRef]
38. Yuan, C.; Tao, X.; Li, N.; Ni, W.; Liu R.P.; Zhang, P. Analysis on Secrecy Capacity of Cooperative Non-Orthogonal Multiple Access With Proactive Jamming. *IEEE Trans. Veh. Technol.* **2019**, *68*, 2682–2696. [CrossRef]
39. Xiang, Z.; Yang W.; Pan G.; Cai Y.; Song Y. Physical Layer Security in Cognitive Radio Inspired NOMA Network. *IEEE J. Sel. Top. Sig. Process.* **2019**, *13*, 700–714. [CrossRef]
40. Huynh, T.P.; Son, P.N., Voznak, M. Secrecy Performance of Underlay Cooperative Cognitive Network Using Non-Orthogonal Multiple Access with Opportunistic Relay Selection. *Symmetry* **2019**, *11*, 385. [CrossRef]
41. Li, B.; Qi, X.; Huang, K.; Fei, Z.; Zhou, F.; Hu, R.Q. Security-Reliability Tradeoff Analysis for Cooperative NOMA in Cognitive Radio Networks. *IEEE Trans. Commun.* **2018**, *67*, 83–96. [CrossRef]
42. MacKay, D. Fountain Codes. *IEE Proc. Commun.* **2005**, *2*, 1331–1346. [CrossRef]
43. Castura, J.; Mao, Y. Rateless Coding over Fading Channels. *IEEE Commun. Lett.* **2006**, *2*, 46–48. [CrossRef]
44. Molisch, A.F.; Mehta, N.B.; Yedidia, J.S.; Zhang, J. Performance of Fountain Codes in Collaborative Relay Networks. *IEEE Trans. Wirel. Commun.* **2007**, *6*, 4108–4119. [CrossRef]
45. Nguyen, H.D.T.; Tran, L.N.; Hong, E.K. On Transmission Efficiency for Wireless Broadcast Using Network Coding and Fountain Codes. *IEEE Commun. Lett.* **2011**, *2*, 569–571. [CrossRef]
46. Duy, T.T.; Kong, H.Y. Secondary Spectrum Access in Cognitive Radio Networks Using Rateless Codes over Rayleigh Fading Channels. *Wirel. Pers. Commun.* **2014**, *2*, 963-978. [CrossRef]

47. Di, X.; Xiong, K.; Fan, P.; Yang, H.C. Simultaneous Wireless Information and Power Transfer in Cooperative Relay Networks With Rateless Codes. *IEEE Trans. Veh. Technol.* **2017**, *66*, 2981–2996. [CrossRef]
48. Niu, H.; Iwai, M.; Sezaki, K.; Sun, L.; Du, Q. Exploiting Fountain Codes for Secure Wireless Delivery. *IEEE Commun. Lett.* **2014**, *2*, 777–780. [CrossRef]
49. Khan, A.S.; Tassi, A.; Chatzigeorgiou, I. Rethinking the Intercept Probability of Random Linear Network Coding. *IEEE Commun. Lett.* **2015**, *19*, 1762–1765. [CrossRef]
50. Du, Q.; Xu, Y.; Li, W.; Song, H. Security Enhancement for Multicast over Internet of Things by Dynamically Constructed Fountain Codes. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 8404219. [CrossRef]
51. Hung, D.T.; Duy, T.T.; Trinh, D.Q.; Bao, V.N.Q. Secrecy Performance Evaluation of TAS Protocol Exploiting Fountain Codes and Cooperative Jamming under Impact of Hardware Impairments. In Proceedings of the 2018 2nd International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom), Ho Chi Minh City, Vietnam, 29–31 January 2018; pp. 164–169.
52. Sun, L.; Ren, P.; Du, Q.; Wang, Y. Fountain-coding Aided Strategy for Secure Cooperative Transmission in Industrial Wireless Sensor Networks. *IEEE Trans. Ind. Inform.* **2016**, *2*, 291–300. [CrossRef]
53. Khan, A.S.; Chatzigeorgiou, I. Opportunistic Relaying and Random Linear Network Coding for Secure and Reliable Communication. *IEEE Trans. Wirel. Commun.* **2018**, *17*, 223–234. [CrossRef]
54. Sun, L.; Xu, H. Fountain-Coding-Based Secure Communications Exploiting Outage Prediction and Limited Feedback. *IEEE Trans. Veh. Technol.* **2019**, *68*, 740–753. [CrossRef]
55. Hung, D.T.; Duy, T.T.; Trinh, D.Q. Security-Reliability Analysis of Multi-hop LEACH Protocol with Fountain Codes and Cooperative Jamming. *EAI Trans. Ind. Netw. .Int. Syst.*, **2019**, *6*, 1–7. [CrossRef]
56. Tin, P.T.; Tan, N.N.; Sang, N.Q.; Duy, T.T.; Phuong, T.T.; Voznak, M. Rateless Codes based Secure Communication Employing Transmit Antenna Selection and Harvest-To-Jam under Joint Effect of Interference and Hardware Impairments. *Entropy* **2019**, *21*, 291–300. [CrossRef]
57. Papoulis, A.; Pillai, S.U. *Probability, Random Variables and Stochastic Processes*, 4th ed.; McGraw-Hill Europe: London, UK, 2002.
58. Qin, D.; Wang, Y.; Zhou, F.; Wong, K.K. Performance Analysis of AF Relaying With Selection Combining in Nakagami-m Fading. *IEEE Syst. J.* **2019**, *13*, 2375–2385. [CrossRef]
59. Amari, S.V.; Misra, R.B. Closed-form Expressions for Distribution of Sum of Exponential Random Variables. *IEEE Trans. Reliab.* **1997**, *46*, 519–522. [CrossRef]
60. Wang, X.; Chen, W.; Cao, Z. A Rateless Coding Based Multi-relay Cooperative Transmission Scheme for Cognitive Radio Networks. In Proceedings of IEEE Global Telecommunications Conference, Honolulu, HI, USA, 30 November–4 December 2009; pp. 164–169.