



Article

Multi-Antenna Jammer-Assisted Secure Short Packet Communications in IoT Networks

Dechuan Chen ^{1,2,3} , Jin Li ¹, Jianwei Hu ^{4,*} , Xingang Zhang ⁵ and Shuai Zhang ¹

¹ College of Physics and Electronic Engineering, Nanyang Normal University, Nanyang 473061, China; chenchuan927@163.com (D.C.); lijn_01@163.com (J.L.); nynuzhang@163.com (S.Z.)

² Key Lab of Broadband Wireless Communication and Sensor Network Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

³ Henan Engineering Research Center for Radio Frequency Front End and Antenna of Millimeter Wave Wireless Communication System, Nanyang 473061, China

⁴ National Key Laboratory for Complex Systems Simulation, Beijing 100101, China

⁵ College of Computer Science and Technology, Nanyang Normal University, Nanyang 473061, China; xgzhang999@163.com

* Correspondence: hujianwei1990@yeah.net

Abstract: In this work, we exploit a multi-antenna cooperative jammer to enable secure short packet communications in Internet of Things (IoT) networks. Specifically, we propose three jamming schemes to combat eavesdropping, i.e., the zero forcing beamforming (ZFB) scheme, null-space artificial noise (NAN) scheme, and transmit antenna selection (TAS) scheme. Assuming Rayleigh fading, we derive new closed-form approximations for the secrecy throughput with finite blocklength coding. To gain further insights, we also analyze the asymptotic performance of the secrecy throughput in the case of infinite blocklength. Furthermore, we investigate the optimization problem in terms of maximizing the secrecy throughput with the latency and reliability constraints to determine the optimal blocklength. Simulation results validate the accuracy of the approximations and evaluate the impact of key parameters such as the jamming power and the number of antennas at the jammer on the secrecy throughput.

Keywords: short-packet communications; physical layer security; multi-antenna jammer; secrecy throughput



Citation: Chen, D.; Li, J.; Hu, J.; Zhang, X.; Zhang, S. Multi-Antenna Jammer-Assisted Secure Short Packet Communications in IoT Networks.

Future Internet **2023**, *15*, 320.

<https://doi.org/10.3390/fi15100320>

Academic Editor: Claude Chaudet

Received: 28 August 2023

Revised: 19 September 2023

Accepted: 25 September 2023

Published: 26 September 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The Internet of Things (IoT), which is expected to connect various surrounding physical nodes such as different kinds of controllers and sensors, serves as a crucial architecture for e-health, home automation, smart cities, environmental monitoring, intelligent transportation, etc. [1–3]. Note that enormous amounts of confidential and sensitive information, e.g., financial files, trade secrets, and personal privacy, are exchanged via wireless channels in the IoT networks. For example, e-health contains personal confidential information such as physiological information and real-time location. If this private information is obtained by illegal eavesdroppers, it will result in very serious consequences. Therefore, privacy and security protection are a fundamental requirement in the design of IoT networks [4,5]. Conventionally, security for IoT is addressed by cryptographic techniques. The encryption-based security techniques have inherent high complexity in secret key generation, distribution, and management, which makes it difficult to apply for IoT networks with many resource-constrained sensors and actuators [6–8].

Compared with cryptographic techniques, physical layer security utilizes the inherent randomness of the wireless medium, such as fading, noise, and interference, to guarantee secure information transmission. Since physical layer security does not need the complicated key exchange procedure and provides a low-complexity and effective security solution, it is more favorable for IoT networks [9–12]. The physical layer security performance can be

further enhanced by a jamming strategy. By designing an artificial noise signal, the difference between the quality of the legitimate link and the eavesdropping link can be enlarged, which will lead to a high secrecy rate. In particular, a secure downlink IoT network was considered in [13], where the power allocation between the legitimate signal and the artificial noise signal and the number of transmit antennas were jointly optimized to maximize the network secrecy throughput. A cooperative jammer in [14] sends jamming signals to confuse the eavesdroppers for downlink transmission in IoT networks. The artificial noise sent by the IoT devices was proposed in [15] for secrecy performance enhancement and the sum secrecy rate was maximized, subject to the transmit power constraint. The authors in [16] derived the secrecy outage probability of multihop IoT networks with a cooperative jamming scheme.

The above studies on IoT networks in the context of physical layer security assumed that the coding blocklength is large enough to achieve the secrecy capacity. However, the primary feature of IoT networks is the use of short packet transmissions to reduce communication latency. From [2,5,17,18], we know that the packet length in IoT applications is only a few hundreds bits, e.g., 10–300 bytes of factory automation. In this case, perfect decoding cannot be achieved even when the data rate is below the Shannon capacity. Therefore, the physical layer security based on classic infinite blocklength design cannot be directly adopted to the IoT networks with short packet transmissions. The authors in [19] evaluated the maximal achievable secrecy rate for general wiretap channels under a given information leakage, error probability, and blocklength. Based on this achievable secrecy rate, Reference [20] derived the secrecy throughput of an IoT network in the presence of a multi-antenna eavesdropper. Later, the work in [20] was extended to a wiretap channel with multiple eavesdroppers [21], multiuser multiple-input-multiple-output (MIMO) networks [22], and cognitive IoT networks with a multi-antenna relay [23]. Additionally, Reference [24] considered the relationship between secrecy throughput and secrecy coding under finite blocklength, and provided the optimal code rates and blocklength in terms of maximizing the secrecy throughput. Furthermore, the work [25] proposed some approaches to minimize the total transmit power or maximize the weighted throughput. In addition, the non-orthogonal multiple access (NOMA) technique has been incorporated to design the secure short packet communications schemes [26–28]. However, all these works only considered the secure communications of legitimate parties without an external helper, and most of them neglected the impact of cooperative jamming on the system performance, which may lead to an underestimation of the secrecy performance.

Motivated by the above background, in this paper, we investigate secure short packet communications in an IoT network, where an access point (AP) sends confidential information to a connected actuator in the presence of a cooperative jammer equipped with multiple antennas and an eavesdropper. Specifically, we propose three jamming schemes, i.e., the zero-forcing beamforming (ZFB) scheme, null-space artificial noise (NAN) scheme, and transmit antenna selection (TAS) scheme, for security improvement. The main contributions of our work are summarized as follows.

1. We first derive new closed-form approximations for the secrecy throughput of an IoT network with three different jamming transmission schemes, i.e., the ZFB scheme, NAN scheme, and TAS scheme. To achieve further insights, we also investigate the asymptotic secrecy throughput in the case of infinite blocklength.
2. We present the optimal design for the three different jamming transmission schemes. The blocklength is optimally determined in terms of maximizing the secrecy throughput subject to the constraints on the latency and reliability.
3. The results demonstrate that both the ZFB scheme and the NAN scheme strictly outperform the TAS scheme in terms of secrecy throughput. Moreover, increasing the number of antennas at the jammer provides significant performance gains for the three proposed schemes, which can be used to compensate for the performance loss from short packet transmissions.

The rest of the paper is organized as follows. We describe the system model of an IoT network with a multi-antenna cooperative jammer in Section 2. In Section 3, we present

the analytical expressions of the secrecy throughput and asymptotic secrecy throughput and characterize the maximization of the secrecy throughput. Finally, we give simulation results in Section 4 and conclude this work in Section 5.

2. System Model

We consider an IoT downlink short packet communications system, as shown in Figure 1, which consists of an AP (Alice), a legitimate actuator (Bob), a cooperative jammer, and an eavesdropper (Eve). Similar to [29,30], we assume that all nodes are equipped with a single antenna, except that the jammer has N_j antennas. We also assume that all the involved channels follow quasi-static Rayleigh block fading, such that the channel coefficients keep constant within each transmission block and change independently between different blocks.

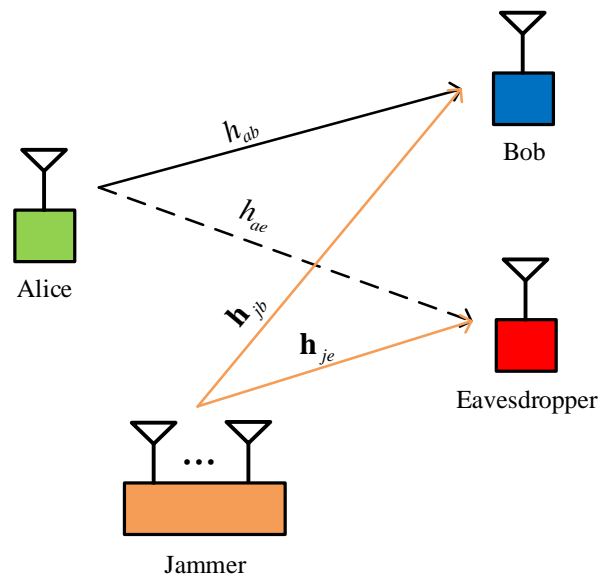


Figure 1. A multi-antenna jammer-assisted secure short packet communications in the presence of an eavesdropper.

To exploit the advantages of both multiple antenna and cooperative jamming techniques, we consider three different secure transmission schemes, i.e., the ZFB scheme, NAN scheme, and TAS scheme. For the ZFB scheme, the jammer aims to maximize the interference at Eve, while avoiding interference to Bob. Thus, the beamforming vector \mathbf{w}_{ZF} is the solution of the following optimization problem:

$$\begin{aligned} \max_{\mathbf{w}_{ZF}} & \quad \left| \mathbf{h}_{je}^{\dagger} \mathbf{w}_{ZF} \right| \\ \text{s.t.} & \quad \left| \mathbf{h}_{jb}^{\dagger} \mathbf{w}_{ZF} \right| = 0 \text{ \& } \|\mathbf{w}_{ZF}\|_F = 1, \end{aligned} \quad (1)$$

where \dagger is the conjugate transpose operator, $\|\cdot\|_F$ is the Frobenius norm, \mathbf{h}_{je} is the $N_j \times 1$ channel vector for the jammer to Eve link with entries following identical and independently distributed (i.i.d.) Rayleigh fading with parameter $\bar{\gamma}_{je}$, and \mathbf{h}_{jb} is the $N_j \times 1$ channel vector for the jammer to Bob link with entries following i.i.d. Rayleigh fading with parameter $\bar{\gamma}_{jb}$. By using projection matrix theory [31], the beamforming vector \mathbf{w}_{ZF} can be expressed as:

$$\mathbf{w}_{ZF} = \frac{\mathbb{N}^{\perp} \mathbf{h}_{je}}{\|\mathbb{N}^{\perp} \mathbf{h}_{je}\|_F}, \quad (2)$$

where $\mathbb{N}^{\perp} = \mathbf{I} - \mathbf{h}_{jb} \left(\mathbf{h}_{jb}^{\dagger} \mathbf{h}_{jb} \right)^{-1} \mathbf{h}_{jb}^{\dagger}$ is the projection idempotent matrix with rank $N_j - 1$. Accordingly, the received signal-to-noise ratios (SNRs) at Bob and Eve of the ZFB scheme, respectively, can be expressed as:

$$\gamma_b^{ZBF} = \frac{P_a}{\sigma^2} |h_{ab}|^2 \quad (3)$$

and

$$\gamma_e^{ZBF} = \frac{P_a |h_{ae}|^2}{P_j \left| \mathbf{h}_{je}^\dagger \mathbf{w}_{ZF} \right|^2 + \sigma^2}, \quad (4)$$

where P_a is the transmit power of Alice, P_j is the transmit power of the jammer, h_{ab} is the Rayleigh channel coefficient for Alice to Bob link with parameter $\bar{\gamma}_{ab}$, h_{ae} is the Rayleigh channel coefficient for Alice to Eve link with parameter $\bar{\gamma}_{ae}$, and σ^2 is the noise variance at each receiver.

For the NAN scheme, the jammer sends artificial noise in the null space of the legitimate channel to guarantee secure communication. Thus, the beamforming matrix at the jammer is designed as $\mathbf{W} = [\mathbf{w}_{jb}, \mathbf{W}_{je}]$, where $\mathbf{w}_{jb} \in \mathbb{C}^{N_j \times 1}$ is a weighted vector used for the jammer to Bob link, and $\mathbf{W}_{je} \in \mathbb{C}^{N_j \times N_j - 1}$ is a weighted matrix for the null space of \mathbf{h}_{jb} , i.e., $\mathbf{h}_{jb} \mathbf{W}_{je} = 0$. As in [29,32], we assume that the transmit power P_j of the jammer is uniformly allocated in the $N_j - 1$ directions. Accordingly, the received SNRs at Bob and Eve of the NAN scheme, respectively, can be expressed as:

$$\gamma_b^{NAN} = \frac{P_a}{\sigma^2} |h_{ab}|^2 \quad (5)$$

and

$$\gamma_e^{NAN} = \frac{P_a |h_{ae}|^2}{\frac{P_j}{N_j - 1} \left\| \mathbf{h}_{je}^\dagger \mathbf{W}_{je} \right\|_F^2 + \sigma^2}. \quad (6)$$

In addition to transmit beamforming, TAS is regarded as another effective method to improve the physical layer security performance. Moreover, TAS is particularly well adapted to systems with computational constraints, since it has two main advantages: low cost and easy implementation. For the TAS scheme, the jammer selects an antenna, which minimizes the interference imposed on Bob, to transmit the jamming signal. Accordingly, the received SNRs at Bob and Eve of the TAS scheme, respectively, can be expressed as:

$$\gamma_b^{TAS} = \frac{P_a |h_{ab}|^2}{P_j \min_{1 \leq i \leq N_j} |h_{jib}|^2 + \sigma^2} \quad (7)$$

and

$$\gamma_e^{TAS} = \frac{P_a |h_{ae}|^2}{P_j |h_{j^*e}|^2 + \sigma^2}, \quad (8)$$

where h_{jib} is the Rayleigh channel coefficient for the i -th antenna of the jammer to Bob link, and h_{j^*e} is the Rayleigh channel coefficient for the selected antenna of the jammer to Eve link.

According to [19], the maximal instantaneous secrecy rate of the IoT downlink short packet communications system with a cooperative jammer for a given information leakage probability δ , decoding error probability ϵ , and blocklength N can be approximated as:

$$R_s^*(N, \epsilon, \delta) = \begin{cases} C_s - \sqrt{\frac{V_x^*}{N}} \frac{Q^{-1}(\epsilon)}{\ln 2} - \sqrt{\frac{V_e^*}{N}} \frac{Q^{-1}(\delta)}{\ln 2}, & \gamma_b^* > \gamma_e^*, \\ 0, & \gamma_b^* \leq \gamma_e^*, \end{cases} \quad (9)$$

where $C_s = \log_2(1 + \gamma_b^*) - \log_2(1 + \gamma_e^*)$ is the secrecy capacity for the infinite number of channel uses, $V_x^* = 1 - (1 + \gamma_x^*)^{-2}$, $x \in \{b, e\}$ is the channel dispersion, $Q^{-1}(\cdot)$ is the inverse Q -function $Q(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} e^{-\frac{t^2}{2}} dt$, and $\star \in \{ZFB, NAN, TAS\}$. For the reader's convenience, we define $\lambda_a = \frac{P_a}{\sigma^2}$ and $\lambda_j = \frac{P_j}{\sigma^2}$.

3. Secrecy Performance Analysis

In this section, we give a comprehensive analysis on the secrecy performance of the three proposed schemes. We first derive closed-form approximations for the secrecy throughput. Then, we analyze the asymptotic secrecy throughput in the case of infinite blocklength to gain further insights. Furthermore, the optimization problem in terms of maximizing the secrecy throughput is investigated under the latency and reliability constraints.

3.1. Secrecy Throughput

The secrecy throughput is the average secrecy rate where confidential messages from Alice are reliably transmitted to Bob under a certain secrecy constraint. Mathematically, it can be expressed as:

$$T = \mathbb{E}_{\gamma_b, \gamma_e} \left(\frac{B}{N} (1 - \epsilon) \right) = \frac{B}{N} (1 - \bar{\epsilon}) \quad (10)$$

where B is the information bits delivered over N channel uses and $\bar{\epsilon} = \mathbb{E}_{\gamma_b, \gamma_e}(\epsilon)$ is the average decoding error probability.

3.1.1. ZFB Scheme

The closed-form expression for the secrecy throughput of the IoT downlink short packet communications system with the ZFB scheme can be approximated as (here, we assume that $N_j \geq 3$; when $N_j \leq 3$, the result can be directly derived by similar procedures):

$$\begin{aligned} T^{ZFB} \approx & \frac{M_1 B}{2N} \sum_{m=1}^{M_2} \left(\frac{\pi}{M_2} \sqrt{1 - t_m^2} e^{-\frac{\omega_m}{\lambda_a \tilde{\gamma}_{ab}}} \left(\frac{e^{-\frac{M_1(t_m+1)}{2\lambda_a \tilde{\gamma}_{ae}}}}{\lambda_a \tilde{\gamma}_{ae} \tilde{\gamma}_{je}^{N_j-1}} \left(\frac{M_1 \lambda_j (t_m+1)}{2\lambda_a \tilde{\gamma}_{ae}} + \frac{1}{\tilde{\gamma}_{je}} \right)^{1-N_j} \right. \right. \\ & + \left. \left. \frac{\lambda_j (N_j-1)}{\lambda_a \tilde{\gamma}_{ae} \tilde{\gamma}_{je}^{N_j-1}} e^{-\frac{M_1(t_m+1)}{2\lambda_a \tilde{\gamma}_{ae}}} \left(\frac{M_1 \lambda_j (t_m+1)}{2\lambda_a \tilde{\gamma}_{ae}} + \frac{1}{\tilde{\gamma}_{je}} \right)^{-N_j} \right) \right) \\ & + \frac{B \lambda_a^{N_j-2} \tilde{\gamma}_{ae}^{N_j-2} e^{-\frac{\omega_1-1}{\lambda_a \tilde{\gamma}_{ab}}}}{N \lambda_j^{N_j-1} \tilde{\gamma}_{je}^{N_j-1}} \left(\sum_{k=1}^{N_j-2} \frac{(k-1)! \lambda_j^k \tilde{\gamma}_{je}^k (-1)^{N_j-2-k} e^{-\frac{M_1 \omega_1}{\lambda_a \tilde{\gamma}_{ab}} - \frac{M_1}{\lambda_a \tilde{\gamma}_{ae}}}}{(N_j-2)! (M_1 \lambda_j \tilde{\gamma}_{je} + \lambda_a \tilde{\gamma}_{ae})^k} \right. \\ & \times \left(\frac{\omega_1}{\lambda_a \tilde{\gamma}_{ab}} + \frac{1}{\lambda_a \tilde{\gamma}_{ae}} \right)^{N_j-2-k} - \frac{(-1)^{N_j-2}}{(N_j-2)!} \left(\frac{\omega_1}{\lambda_a \tilde{\gamma}_{ab}} + \frac{1}{\lambda_a \tilde{\gamma}_{ae}} \right)^{N_j-2} \\ & \times e^{\frac{\omega_1 \tilde{\gamma}_{ae}}{\lambda_j \tilde{\gamma}_{je} \tilde{\gamma}_{ab}} + \frac{1}{\lambda_j \tilde{\gamma}_{je}}} Ei \left(- \left(\frac{\omega_1}{\lambda_a \tilde{\gamma}_{ab}} + \frac{1}{\lambda_a \tilde{\gamma}_{ae}} \right) \left(M_1 + \frac{\lambda_a \tilde{\gamma}_{ae}}{\lambda_j \tilde{\gamma}_{je}} \right) \right) \Bigg) + e^{-\frac{\omega_1-1}{\lambda_a \tilde{\gamma}_{ab}}} \\ & \times \frac{B \lambda_a^{N_j-1} \tilde{\gamma}_{ae}^{N_j-1} (N_j-1) e^{-\frac{\omega_1-1}{\lambda_a \tilde{\gamma}_{ab}}}}{N \lambda_j^{N_j-1} \tilde{\gamma}_{je}^{N_j-1} (N_j-1)!} \left(\sum_{k=1}^{N_j-1} \frac{(k-1)! \lambda_j^k \tilde{\gamma}_{je}^k e^{-\frac{M_1 \omega_1}{\lambda_a \tilde{\gamma}_{ab}} - \frac{M_1}{\lambda_a \tilde{\gamma}_{ae}}}}{(M_1 \lambda_j \tilde{\gamma}_{je} + \lambda_a \tilde{\gamma}_{ae})^k} \right. \\ & \times \left(-\frac{\omega_1}{\lambda_a \tilde{\gamma}_{ab}} - \frac{1}{\lambda_a \tilde{\gamma}_{ae}} \right)^{N_j-1-k} - \left(-\frac{\omega_1}{\lambda_a \tilde{\gamma}_{ab}} - \frac{1}{\lambda_a \tilde{\gamma}_{ae}} \right)^{N_j-1} \\ & \times e^{\frac{\omega_1 \tilde{\gamma}_{ae}}{\lambda_j \tilde{\gamma}_{je} \tilde{\gamma}_{ab}} + \frac{1}{\lambda_j \tilde{\gamma}_{je}}} Ei \left(- \left(\frac{\omega_1}{\lambda_a \tilde{\gamma}_{ab}} + \frac{1}{\lambda_a \tilde{\gamma}_{ae}} \right) \left(M_1 + \frac{\lambda_a \tilde{\gamma}_{ae}}{\lambda_j \tilde{\gamma}_{je}} \right) \right) \Bigg), \quad (11) \end{aligned}$$

where $Ei(\cdot)$ is the exponential integral function and $M_1, M_2, \omega_1, \omega_m$, and t_m are defined in Appendix A.

Proof. See Appendix A. \square

3.1.2. NAN Scheme

The closed-form expression for the secrecy throughput of the IoT downlink short packet communications system with the NAN scheme can be approximated as (here, we assume that $N_j \geq 3$; when $N_j \leq 3$, the result can be directly derived by similar procedures):

$$\begin{aligned}
T^{NAN} \approx & \frac{M_1 B}{2N} \sum_{m=1}^{M_2} \left(\frac{\pi}{M_2} \sqrt{1-t_m^2} e^{-\frac{\omega_m}{\lambda_a \tilde{\gamma}_{ab}}} \left(\left(\frac{M_1 \lambda_j (t_m+1)}{2\lambda_a \tilde{\gamma}_{ae} (N_j-1)} + \frac{1}{\tilde{\gamma}_{je}} \right)^{1-N_j} \right. \right. \\
& \times \frac{e^{-\frac{M_1(t_m+1)}{2\lambda_a \tilde{\gamma}_{ae}}}}{\lambda_a \tilde{\gamma}_{ae} \tilde{\gamma}_{je}^{N_j-1}} + \frac{\lambda_j e^{-\frac{M_1(t_m+1)}{2\lambda_a \tilde{\gamma}_{ae}}}}{\lambda_a \tilde{\gamma}_{ae} \tilde{\gamma}_{je}^{N_j-1}} \left(\frac{M_1 \lambda_j (t_m+1)}{2\lambda_a \tilde{\gamma}_{ae} (N_j-1)} + \frac{1}{\tilde{\gamma}_{je}} \right)^{-N_j} \Bigg) \\
& + \frac{B \lambda_a^{N_j-2} \tilde{\gamma}_{ae}^{N_j-2} e^{-\frac{\omega_1-1}{\lambda_a \tilde{\gamma}_{ab}}}}{N \lambda_j^{N_j-1} \tilde{\gamma}_{je}^{N_j-1}} \left(\sum_{k=1}^{N_j-2} \frac{(N_j-1)^{N_j-1} (k-1)! \lambda_j^k \tilde{\gamma}_{je}^k e^{-\frac{M_1 \omega_1}{\lambda_a \tilde{\gamma}_{ab}} - \frac{M_1}{\lambda_a \tilde{\gamma}_{ae}}}}{(N_j-2)! (M_1 \lambda_j \tilde{\gamma}_{je} + \lambda_a \tilde{\gamma}_{ae} (N_j-1))^k} \right. \\
& \times \left(-\frac{\omega_1}{\lambda_a \tilde{\gamma}_{ab}} - \frac{1}{\lambda_a \tilde{\gamma}_{ae}} \right)^{N_j-2-k} - \frac{e^{\frac{\omega_1 \tilde{\gamma}_{ae} (N_j-1)}{\lambda_j \tilde{\gamma}_{je} \tilde{\gamma}_{ab}} + \frac{N_j-1}{\lambda_j \tilde{\gamma}_{je}}}}{(N_j-2)!} \left(-\frac{\omega_1}{\lambda_a \tilde{\gamma}_{ab}} - \frac{1}{\lambda_a \tilde{\gamma}_{ae}} \right)^{N_j-2} \\
& \times (N_j-1)^{N_j-1} Ei \left(-\left(\frac{\omega_1}{\lambda_a \tilde{\gamma}_{ab}} + \frac{1}{\lambda_a \tilde{\gamma}_{ae}} \right) \left(M_1 + \frac{\lambda_a \tilde{\gamma}_{ae} (N_j-1)}{\lambda_j \tilde{\gamma}_{je}} \right) \right) \Bigg) \\
& + \frac{B \lambda_a^{N_j-1} \tilde{\gamma}_{ae}^{N_j-1} (N_j-1)^{N_j} e^{-\frac{\omega_1-1}{\lambda_a \tilde{\gamma}_{ab}}}}{N \lambda_j^{N_j-1} \tilde{\gamma}_{je}^{N_j-1} (N_j-1)!} \left(\sum_{k=1}^{N_j-1} \frac{(k-1)! \lambda_j^k \tilde{\gamma}_{je}^k (-1)^{N_j-1-k} e^{-\frac{M_1}{\lambda_a \tilde{\gamma}_{ae}}}}{(M_1 \lambda_j \tilde{\gamma}_{je} + \lambda_a \tilde{\gamma}_{ae} (N_j-1))^k} \right. \\
& \times \left(\frac{\omega_1}{\lambda_a \tilde{\gamma}_{ab}} + \frac{1}{\lambda_a \tilde{\gamma}_{ae}} \right)^{N_j-1-k} e^{-\frac{M_1 \omega_1}{\lambda_a \tilde{\gamma}_{ab}}} - \left(-\frac{\omega_1}{\lambda_a \tilde{\gamma}_{ab}} - \frac{1}{\lambda_a \tilde{\gamma}_{ae}} \right)^{N_j-1} e^{\frac{N_j-1}{\lambda_j \tilde{\gamma}_{je}}} \\
& \times e^{\frac{\omega_1 \tilde{\gamma}_{ae} (N_j-1)}{\lambda_j \tilde{\gamma}_{je} \tilde{\gamma}_{ab}}} Ei \left(-\left(\frac{\omega_1}{\lambda_a \tilde{\gamma}_{ab}} + \frac{1}{\lambda_a \tilde{\gamma}_{ae}} \right) \left(M_1 + \frac{\lambda_a \tilde{\gamma}_{ae} (N_j-1)}{\lambda_j \tilde{\gamma}_{je}} \right) \right) \Bigg). \quad (12)
\end{aligned}$$

Proof. Since $\|\mathbf{h}_{je}^\dagger \mathbf{W}_{je}\|_F^2$ is a chi-squared random variable with $2(N_j-1)$ degrees of freedom [33], by following similar steps as the ZFB scheme, we can obtain the desired expression in (12) after some mathematical manipulations. \square

3.1.3. TAS Scheme

The closed-form expression for the secrecy throughput of the IoT downlink short packet communications system with the TAS scheme can be approximated as (here, we assume that $c_1 \neq \frac{\lambda_a \tilde{\gamma}_{ae}}{\lambda_j \tilde{\gamma}_{je}}$; when $c_1 = \frac{\lambda_a \tilde{\gamma}_{ae}}{\lambda_j \tilde{\gamma}_{je}}$, the result can be obtained by similar analysis):

$$\begin{aligned}
T^{TAS} \approx & \frac{M_1 B}{2N} \sum_{m=1}^{M_2} \left(\frac{\pi N_j \lambda_a \tilde{\gamma}_{ab} \sqrt{1-t_m^2} e^{-\frac{\omega_m}{\lambda_a \tilde{\gamma}_{ab}}}}{M_2 \omega_m \lambda_j \tilde{\gamma}_{jb} + M_2 \lambda_a \tilde{\gamma}_{ab} N_j} \left(\frac{2e^{-\frac{M_1(t_m+1)}{2\lambda_a \tilde{\gamma}_{ae}}}}{\lambda_j \tilde{\gamma}_{je} M_1 (t_m+1) + 2\lambda_a \tilde{\gamma}_{ae}} \right. \right. \\
& + \frac{4\lambda_a \tilde{\gamma}_{ae} \lambda_j \tilde{\gamma}_{je} e^{-\frac{M_1(t_m+1)}{2\lambda_a \tilde{\gamma}_{ae}}}}{(\lambda_j \tilde{\gamma}_{je} M_1 (t_m+1) + 2\lambda_a \tilde{\gamma}_{ae})^2} \Bigg) - \frac{B N_j \lambda_a^2 \tilde{\gamma}_{ab} \tilde{\gamma}_{ae} \tilde{\gamma}_{je} e^{-\frac{M_1 \omega_1}{\lambda_a \tilde{\gamma}_{ab}} - \frac{M_1}{\lambda_a \tilde{\gamma}_{ae}} - \frac{\omega_1-1}{\lambda_a \tilde{\gamma}_{ab}}}}{N \omega_1 \tilde{\gamma}_{jb} (M_1 \lambda_j \tilde{\gamma}_{je} + \lambda_a \tilde{\gamma}_{ae})} \\
& \times \frac{1}{\lambda_a \tilde{\gamma}_{ae} - c_1 \lambda_j \tilde{\gamma}_{je}} + \left(\frac{\lambda_a \lambda_j \tilde{\gamma}_{je}}{(\lambda_a \tilde{\gamma}_{ae} - c_1 \lambda_j \tilde{\gamma}_{je})^2} - \frac{\omega_1}{(\lambda_a \tilde{\gamma}_{ae} - c_1 \lambda_j \tilde{\gamma}_{je}) \tilde{\gamma}_{ab}} \right) \\
& \times \frac{B N_j \lambda_a \tilde{\gamma}_{ab} \tilde{\gamma}_{ae}}{N \omega_1 \lambda_j \tilde{\gamma}_{jb}} e^{\frac{\omega_1 \tilde{\gamma}_{ae}}{\lambda_j \tilde{\gamma}_{je} \tilde{\gamma}_{ab}} + \frac{1}{\lambda_j \tilde{\gamma}_{je}}} Ei \left(-\left(\frac{\omega_1}{\lambda_a \tilde{\gamma}_{ab}} + \frac{1}{\lambda_a \tilde{\gamma}_{ae}} \right) \left(M_1 + \frac{\lambda_a \tilde{\gamma}_{ae}}{\lambda_j \tilde{\gamma}_{je}} \right) \right) \\
& \times e^{-\frac{\omega_1-1}{\lambda_a \tilde{\gamma}_{ab}}} - \frac{B N_j \lambda_a \tilde{\gamma}_{ab} \tilde{\gamma}_{ae}}{N \omega_1 \lambda_j \tilde{\gamma}_{jb}} \left(\frac{1}{\lambda_a \tilde{\gamma}_{ae} - c_1 \lambda_j \tilde{\gamma}_{je}} + \frac{\lambda_a \lambda_j \tilde{\gamma}_{je} \tilde{\gamma}_{ae}}{(\lambda_a \tilde{\gamma}_{ae} - c_1 \lambda_j \tilde{\gamma}_{je})^2} \right) \\
& \times e^{\frac{c_1 \omega_1}{\lambda_a \tilde{\gamma}_{ab}} + \frac{c_1}{\lambda_a \tilde{\gamma}_{ae}} - \frac{\omega_1-1}{\lambda_a \tilde{\gamma}_{ab}}} Ei \left(-\frac{\omega_1 (M_1 + c_1)}{\lambda_a \tilde{\gamma}_{ab}} - \frac{M_1 + c_1}{\lambda_a \tilde{\gamma}_{ae}} \right), \quad (13)
\end{aligned}$$

where $c_1 = \frac{(\omega_1-1)\lambda_j\tilde{\gamma}_{jb}+\lambda_a\tilde{\gamma}_{ab}N_j}{\omega_1\lambda_j\tilde{\gamma}_{jb}}$.

Proof. Since $|h_{ji^*e}|^2$ is an exponentially distributed random variable and the probability density function (PDF) of $Z_1 = \min_{1 \leq i \leq N_j} |h_{ji}|^2$ is given by $f_{Z_1}(z) = \frac{N_j}{\tilde{\gamma}_{jb}} e^{-\frac{N_j z}{\tilde{\gamma}_{jb}}}$ [29], by following a similar procedure as the ZFB scheme, we can derive the desired result in (13) after some mathematical manipulations.

The derived analytical results in (11)–(13) provide an efficient means to evaluate the secrecy throughput of the IoT downlink short packet communications system with the three proposed transmission schemes. Moreover, the approximations for the secrecy throughput of finite blocklength will be verified via simulations. \square

3.2. Asymptotic Analysis

In an effort to understand the relationship between infinite blocklength and finite blocklength and gain more physical insights, in this subsection, we look into the asymptotic secrecy throughput under the infinite blocklength regime, i.e., $N \rightarrow \infty$. When $N \rightarrow \infty$, we have $\epsilon \rightarrow 0$ as long as $\gamma_b^* > \gamma_e^*$ from (9). Therefore, the asymptotic secrecy throughput in the case of infinite blocklength can be mathematically expressed as:

$$T_{N \rightarrow \infty}^* = \frac{B}{N} \Pr(\gamma_b^* > \gamma_e^*). \quad (14)$$

Corollary 1. The asymptotic secrecy throughput of the ZFB scheme in the infinite blocklength regime is given by:

$$T_{N \rightarrow \infty}^{ZFB} = B(\Delta_1 + \Delta_2)N^{-1}, \quad (15)$$

where Δ_1 and Δ_2 are given by:

$$\begin{aligned} \Delta_1 = & \frac{\lambda_a^{N_j-2} \tilde{\gamma}_{ae}^{N_j-2}}{\lambda_j^{N_j-1} \tilde{\gamma}_{je}^{N_j-1}} \left(\sum_{k=1}^{N_j-2} \frac{(k-1)! \lambda_j^k \tilde{\gamma}_{je}^k (-1)^{N_j-2-k}}{(N_j-2)! \lambda_a^k \tilde{\gamma}_{ae}^k} \left(\frac{1}{\lambda_a \tilde{\gamma}_{ab}} + \frac{1}{\lambda_a \tilde{\gamma}_{ae}} \right)^{N_j-2-k} \right. \\ & \left. - \frac{e^{\frac{\tilde{\gamma}_{ae}}{\lambda_j \tilde{\gamma}_{je} \tilde{\gamma}_{ab}} + \frac{1}{\lambda_j \tilde{\gamma}_{je}}}}{(N_j-2)!} \left(-\frac{1}{\lambda_a \tilde{\gamma}_{ab}} - \frac{1}{\lambda_a \tilde{\gamma}_{ae}} \right)^{N_j-2} Ei \left(-\frac{\tilde{\gamma}_{ae}}{\lambda_j \tilde{\gamma}_{je} \tilde{\gamma}_{ab}} - \frac{1}{\lambda_j \tilde{\gamma}_{je}} \right) \right) \end{aligned} \quad (16)$$

and

$$\begin{aligned} \Delta_2 = & \frac{\lambda_a^{N_j-1} \tilde{\gamma}_{ae}^{N_j-1} (N_j-1)}{\lambda_j^{N_j-1} \tilde{\gamma}_{je}^{N_j-1}} \left(\sum_{k=1}^{N_j-1} \frac{(k-1)! \lambda_j^k \tilde{\gamma}_{je}^k}{(N_j-1)! \lambda_a^k \tilde{\gamma}_{ae}^k} \left(-\frac{1}{\lambda_a \tilde{\gamma}_{ab}} - \frac{1}{\lambda_a \tilde{\gamma}_{ae}} \right)^{N_j-1-k} \right. \\ & \left. - \frac{e^{\frac{\tilde{\gamma}_{ae}}{\lambda_j \tilde{\gamma}_{je} \tilde{\gamma}_{ab}} + \frac{1}{\lambda_j \tilde{\gamma}_{je}}}}{(N_j-1)!} \left(-\frac{1}{\lambda_a \tilde{\gamma}_{ab}} - \frac{1}{\lambda_a \tilde{\gamma}_{ae}} \right)^{N_j-1} Ei \left(-\frac{\tilde{\gamma}_{ae}}{\lambda_j \tilde{\gamma}_{je} \tilde{\gamma}_{ab}} - \frac{1}{\lambda_j \tilde{\gamma}_{je}} \right) \right). \end{aligned} \quad (17)$$

Corollary 2. The asymptotic secrecy throughput of the NAN scheme in the infinite blocklength regime is given by:

$$T_{N \rightarrow \infty}^{NAN} = B(\Delta_3 + \Delta_4)N^{-1}, \quad (18)$$

where Δ_3 and Δ_4 are given by:

$$\Delta_3 = \frac{\lambda_a^{N_j-2} \tilde{\gamma}_{ae}^{N_j-2} (N_j-1)^{N_j-1}}{\lambda_j^{N_j-1} \tilde{\gamma}_{je}^{N_j-1}} \left(\sum_{k=1}^{N_j-2} \frac{(k-1)! \lambda_j^k \tilde{\gamma}_{je}^k (-1)^{N_j-2-k}}{(N_j-2)! \lambda_a^k \tilde{\gamma}_{ae}^k (N_j-1)^k} \left(\frac{1}{\lambda_a \tilde{\gamma}_{ab}} + \frac{1}{\lambda_a \tilde{\gamma}_{ae}} \right)^{N_j-2-k} \right. \\ \left. - \frac{e^{\frac{\tilde{\gamma}_{ae}(N_j-1)}{\lambda_j \tilde{\gamma}_{je} \tilde{\gamma}_{ab}} + \frac{N_j-1}{\lambda_j \tilde{\gamma}_{je}}}}{(N_j-2)!} \left(-\frac{1}{\lambda_a \tilde{\gamma}_{ab}} - \frac{1}{\lambda_a \tilde{\gamma}_{ae}} \right)^{N_j-2} Ei \left(-\frac{\tilde{\gamma}_{ae}(N_j-1)}{\lambda_j \tilde{\gamma}_{je} \tilde{\gamma}_{ab}} - \frac{N_j-1}{\lambda_j \tilde{\gamma}_{je}} \right) \right) \quad (19)$$

and

$$\Delta_4 = \frac{\lambda_a^{N_j-1} \tilde{\gamma}_{ae}^{N_j-1} (N_j-1)^{N_j}}{\lambda_j^{N_j-1} \tilde{\gamma}_{je}^{N_j-1}} \left(\sum_{k=1}^{N_j-1} \frac{(k-1)! \lambda_j^k \tilde{\gamma}_{je}^k (-1)^{N_j-1-k}}{(N_j-1)! \lambda_a^k \tilde{\gamma}_{ae}^k (N_j-1)^k} \left(\frac{\tilde{\gamma}_{ae} + \tilde{\gamma}_{ab}}{\lambda_a \tilde{\gamma}_{ab} \tilde{\gamma}_{ae}} \right)^{N_j-1-k} \right. \\ \left. - \frac{e^{\frac{\tilde{\gamma}_{ae}(N_j-1)}{\lambda_j \tilde{\gamma}_{je} \tilde{\gamma}_{ab}} + \frac{N_j-1}{\lambda_j \tilde{\gamma}_{je}}}}{(N_j-1)!} \left(-\frac{1}{\lambda_a \tilde{\gamma}_{ab}} - \frac{1}{\lambda_a \tilde{\gamma}_{ae}} \right)^{N_j-1} Ei \left(-\frac{\tilde{\gamma}_{ae}(N_j-1)}{\lambda_j \tilde{\gamma}_{je} \tilde{\gamma}_{ab}} - \frac{N_j-1}{\lambda_j \tilde{\gamma}_{je}} \right) \right). \quad (20)$$

Corollary 3. The asymptotic secrecy throughput of the TAS scheme in the infinite blocklength regime is given by:

$$T_{N \rightarrow \infty}^{TAS} = B(\Delta_5 - \Delta_6 - \Delta_7)N^{-1}, \quad (21)$$

where $\Delta_7 = \frac{N_j \tilde{\gamma}_{ab} \tilde{\gamma}_{je}}{\tilde{\gamma}_{jb} \tilde{\gamma}_{ae} - N_j \tilde{\gamma}_{ab} \tilde{\gamma}_{je}}$ and Δ_5 and Δ_6 are given by:

$$\Delta_5 = \frac{N_j \tilde{\gamma}_{ae} (\lambda_j \tilde{\gamma}_{je} \tilde{\gamma}_{jb} \tilde{\gamma}_{ab} - \tilde{\gamma}_{ae} \tilde{\gamma}_{jb} + \tilde{\gamma}_{ab} \tilde{\gamma}_{je} N_j)}{\lambda_j (\tilde{\gamma}_{ae} \tilde{\gamma}_{jb} - \tilde{\gamma}_{ab} \tilde{\gamma}_{je} N_j)^2} \\ \times e^{\frac{\tilde{\gamma}_{ae}}{\lambda_j \tilde{\gamma}_{je} \tilde{\gamma}_{ab}} + \frac{1}{\lambda_j \tilde{\gamma}_{je}}} Ei \left(-\frac{\tilde{\gamma}_{ae}}{\lambda_j \tilde{\gamma}_{je} \tilde{\gamma}_{ab}} - \frac{1}{\lambda_j \tilde{\gamma}_{je}} \right) \quad (22)$$

and

$$\Delta_6 = \frac{N_j \tilde{\gamma}_{ab} (\tilde{\gamma}_{ae} \tilde{\gamma}_{jb} - \tilde{\gamma}_{ab} \tilde{\gamma}_{je} N_j + \lambda_j \tilde{\gamma}_{je} \tilde{\gamma}_{jb} \tilde{\gamma}_{ae})}{\lambda_j (\tilde{\gamma}_{ae} \tilde{\gamma}_{jb} - \tilde{\gamma}_{ab} \tilde{\gamma}_{je} N_j)^2} \\ \times e^{\frac{N_j}{\lambda_j \tilde{\gamma}_{jb}} + \frac{\tilde{\gamma}_{ab} N_j}{\lambda_j \tilde{\gamma}_{jb} \tilde{\gamma}_{ae}}} Ei \left(-\frac{N_j}{\lambda_j \tilde{\gamma}_{jb}} - \frac{\tilde{\gamma}_{ab} N_j}{\lambda_j \tilde{\gamma}_{jb} \tilde{\gamma}_{ae}} \right). \quad (23)$$

According to (15), (18), and (21), the secrecy throughput of the three proposed transmission schemes approaches zero as $N \rightarrow \infty$. However, the secrecy capacity of the three proposed transmission schemes is not zero for this particular case. Moreover, the asymptotic secrecy throughput of the three proposed transmission schemes is independent of the parameter δ . This is because the secrecy rate $\frac{B}{N}$ can always be achieved without leaking any information to the eavesdropper in the infinite blocklength regime, when $\gamma_b^* > \gamma_e^*$.

3.3. Secrecy Throughput Maximization

We note that there exists a transmission latency–reliability tradeoff introduced by the blocklength. As such, in this subsection, we determine the optimal blocklength in terms of maximizing the secrecy throughput subject to the given latency and reliability constraints. Mathematically, the problem is formulated as:

$$\max_N T^*, \quad (24a)$$

$$s.t. \quad \bar{\epsilon} \leq \epsilon_{\max}, \quad (24b)$$

$$N \leq N_{\max}, \quad (24c)$$

$$N \in \mathbb{N}^+, \quad (24d)$$

where (24b) is the reliability constraint of the considered system, (24c) is the transmission latency constraint of the considered system, and \mathbb{N}^+ is the non-negative integer set.

Next, we will clarify that T^* is quasi-concave with respect to N . In the first step, by taking the first-order and second-order derivative of ϵ on N , we have:

$$\frac{\partial \epsilon}{\partial N} = \frac{\partial \epsilon}{\partial \phi} \frac{\partial \phi}{\partial N} \quad (25)$$

and

$$\frac{\partial^2 \epsilon}{\partial N^2} = \frac{\partial^2 \epsilon}{\partial \phi^2} \left(\frac{\partial \phi}{\partial N} \right)^2 + \frac{\partial \epsilon}{\partial \phi} \frac{\partial^2 \phi}{\partial N^2}, \quad (26)$$

where $\phi = \sqrt{\frac{N}{V_b^*}} \left(\ln \frac{1+\gamma_b^*}{1+\gamma_e^*} - \sqrt{\frac{V_b^*}{N}} Q^{-1}(\delta) - \frac{B}{N} \ln 2 \right)$. Note that ϵ is generally much smaller than 0.5 to ensure high reliability [34]; thus, we have $\phi = Q^{-1}(\epsilon) > 0$, $\frac{\partial \epsilon}{\partial \phi} = -\frac{1}{\sqrt{2\pi}} e^{-\frac{\phi^2}{2}} < 0$, and $\frac{\partial^2 \epsilon}{\partial \phi^2} = \frac{\phi}{\sqrt{2\pi}} e^{-\frac{\phi^2}{2}} > 0$. Then, we analyze the sign of $\frac{\partial \phi}{\partial N}$ and $\frac{\partial^2 \phi}{\partial N^2}$. By taking the first-order and second-order derivative of ϕ on N , we have:

$$\frac{\partial \phi}{\partial N} = \frac{\frac{N}{\sqrt{V_b^*}} \ln \frac{1+\gamma_b^*}{1+\gamma_e^*} + \frac{B \ln 2}{\sqrt{V_b^*}}}{2N^{3/2}} \quad (27)$$

and

$$\frac{\partial^2 \phi}{\partial N^2} = -\frac{\frac{N}{\sqrt{V_b^*}} \ln \frac{1+\gamma_b^*}{1+\gamma_e^*} + \frac{3B \ln 2}{\sqrt{V_b^*}}}{4N^{5/2}}. \quad (28)$$

From (27) and (28), it is straightforward to obtain that $\frac{\partial \phi}{\partial N} > 0$ and $\frac{\partial^2 \phi}{\partial N^2} < 0$. Thus, we know that ϵ is a convex decreasing function with respect to N . Based on the Leibniz integral rule, $\bar{\epsilon}$ is also a convex decreasing function with respect to N . Accordingly, T^* is a quasi-concave function with respect to N .

Based on the above discussions, problem (24) can be simplified as:

$$\max_N T^*, \quad (29a)$$

$$s.t. \quad N^0 \leq N \leq N_{\max}, \quad (29b)$$

$$N \in \mathbb{N}^+, \quad (29c)$$

where N^0 is the solution of $\bar{\epsilon} = \epsilon_{\max}$. We clarify that the optimal blocklength in terms of maximizing the secrecy throughput exists only when $\lceil N^0 \rceil \leq N_{\max}$, where $\lceil \cdot \rceil$ is the ceiling operation. Now, we present the optimal blocklength in terms of maximizing the secrecy throughput in the following corollary.

Corollary 4. When $\lceil N^0 \rceil \leq N_{\max}$, the optimal blocklength in terms of maximizing the secrecy throughput is:

$$N^* = \begin{cases} \lceil N^0 \rceil, & N^{\#} \leq N^0, \\ \arg \max_{N \in \{\lceil N^{\#} \rceil, \lfloor N^{\#} \rfloor\}} T^*, & N^0 < N^{\#} < N_{\max}, \\ N_{\max}, & N^{\#} \geq N_{\max}, \end{cases} \quad (30)$$

where $N^\#$ is the solution of $\frac{\partial T^*}{\partial N} = 0$ and $\lfloor \cdot \rfloor$ is the floor operation.

Proof. Firstly, the integer constraint in problem (29) is relaxed. Then, based on the fact that $\bar{\epsilon}$ is a convex decreasing function with respect to N and T^* is a quasi-concave function with respect to N , the optimal blocklength can be derived directly. \square

4. Simulation Results

In this section, computer simulations by Matlab are provided to verify the analytical results of the three proposed transmission schemes and evaluate the secrecy throughput performance of the three proposed transmission schemes. In simulations, unless specified otherwise, we assume that $N_j = 5$, $\delta = 10^{-2}$, $M_1 = 20$, $M_2 = 1500$, $\tilde{\gamma}_{ab} = \tilde{\gamma}_{ae} = \tilde{\gamma}_{jb} = \tilde{\gamma}_{je} = 1$, and $\sigma^2 = 0$ dBm. From the figures, we can see that the analytical results coincide well with the computer simulation points, which demonstrates the correctness of our analysis.

Figures 2–4 plot the secrecy throughput of the ZFB, NAN, and TAS schemes with different values of B , respectively. It is clear that the secrecy throughput first increases and then decreases as N increases, i.e., an optimal value for N exists to maximize the secrecy throughput. This phenomenon is explained as follows: when N is relatively small, increasing N is beneficial to improve the transmission reliability, which, of course, will lead to a higher secrecy throughput. However, when N is very large, the communication latency is large, which, consequently, will result in the degradation of the secrecy throughput. The second observation is that the optimal blocklength increases as B increases. This is because compared with communication latency, the decoding error at Bob becomes more obvious when the number of information bits gets larger.

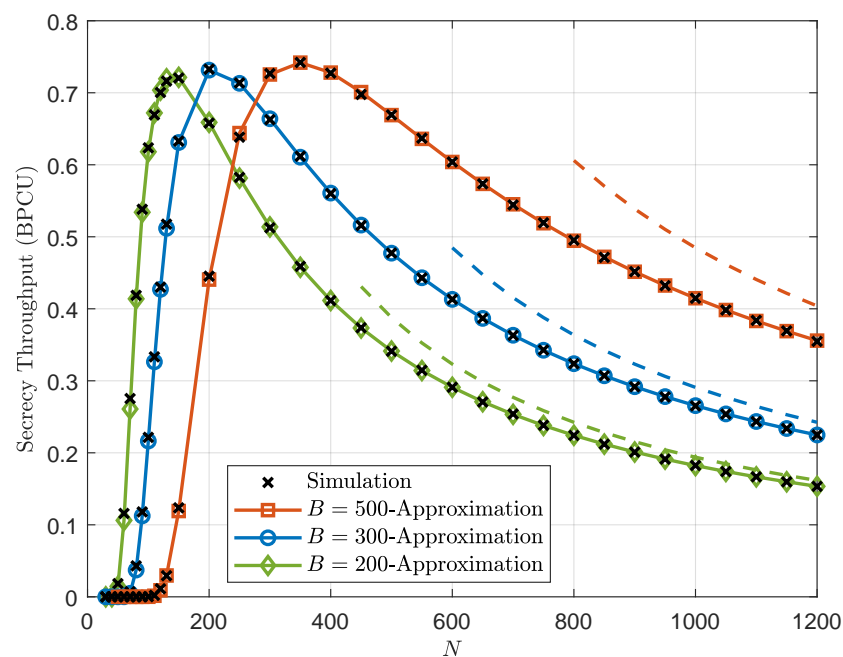


Figure 2. Secrecy throughput of the ZFB scheme versus the blocklength N with different values of B for $P_a = 5$ dBm and $P_j = 10$ dBm, where the dashed lines are (15) to represent the asymptotic secrecy throughput.

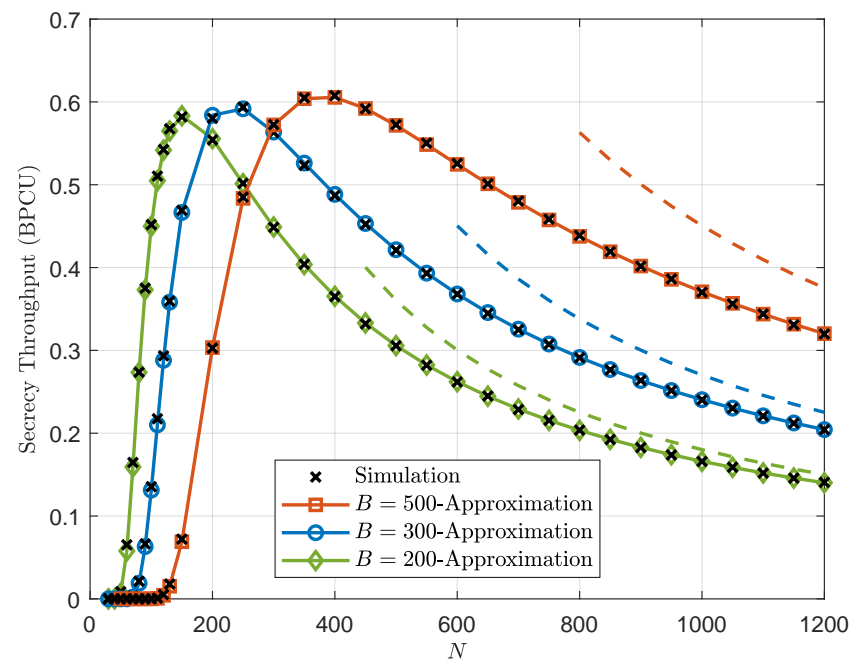


Figure 3. Secrecy throughput of the NAN scheme versus the blocklength N with different values of B for $P_a = 5$ dBm and $P_j = 10$ dBm, where the dashed lines are (18) to represent the asymptotic secrecy throughput.

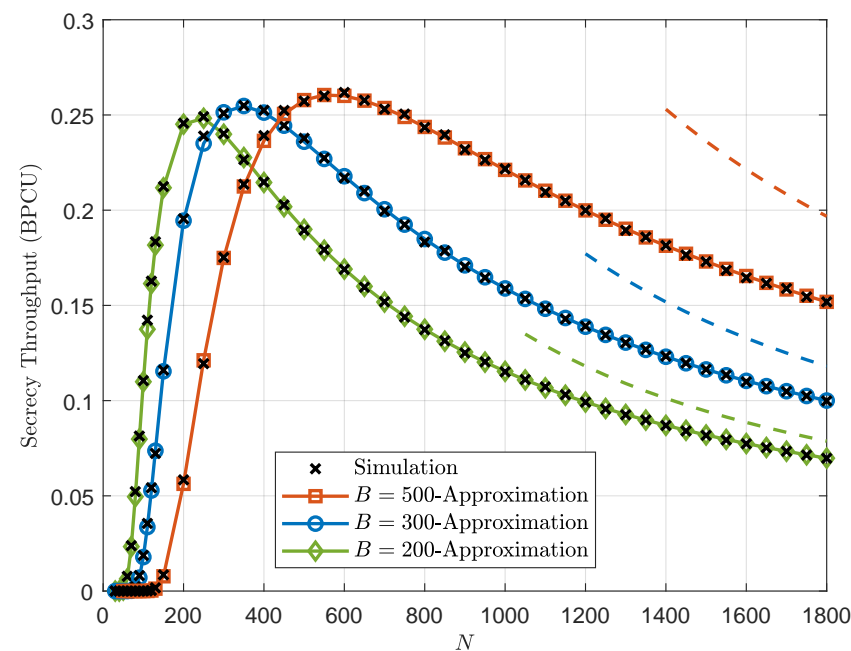


Figure 4. Secrecy throughput of the TAS scheme versus the blocklength N with different values of B for $P_a = 5$ dBm and $P_j = 10$ dBm, where the dashed lines are (21) to represent the asymptotic secrecy throughput.

Figure 5 investigates the impact of the transmit power P_a on the secrecy throughput with the three proposed schemes. Moreover, we present a benchmark scheme for comparison, i.e., without the jammer scheme, which consists of a source, a destination, and an eavesdropper, as in [20]. It is clear that the secrecy throughput of all the proposed schemes increases first and then stays constant as P_a increases. This is because the ratio of average channel gain on the legitimate link to the eavesdropping link becomes the bottleneck of the secrecy

throughput in the high-SNR regime. In addition, we observe that the ZFB and NAN schemes always attain better performance than the TAS and benchmark schemes. This is because the jamming signals of the ZFB scheme and the NAN scheme only selectively interfere with the eavesdropper and have no impact on the signal reception of the legitimate user. Thus, the multi-antenna jammer can be employed to improve the system performance.

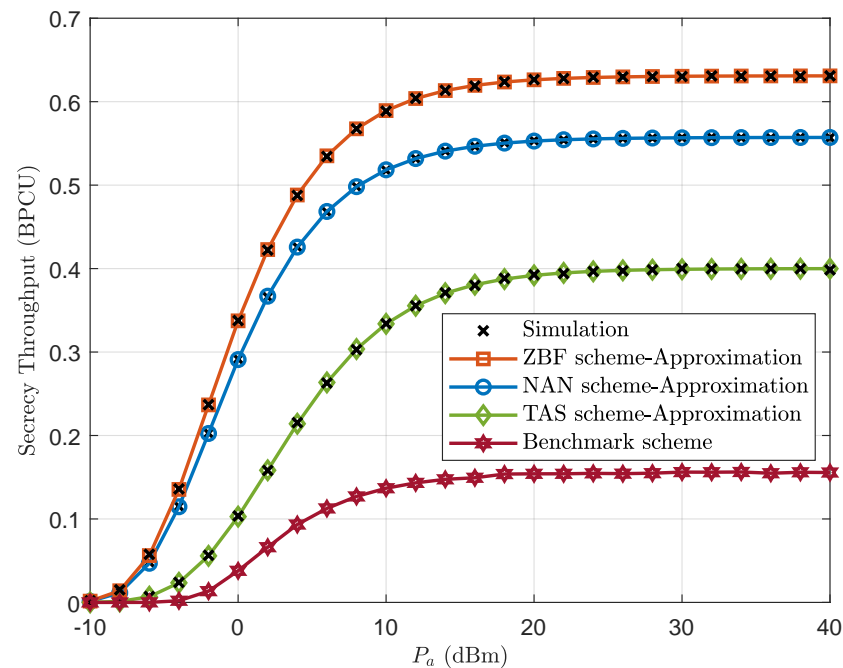


Figure 5. Secrecy throughput of the ZFB, NAN, TAS, and benchmark schemes versus P_a for $B = 200$, $N = 300$, and $P_j = 10$ dBm.

Figure 6 shows the impact of the jamming power P_j on the secrecy throughput with the three proposed schemes. We first observe that when P_j is sufficiently large, the secrecy throughput converges to a constant for the ZFB and NAN schemes, whereas it goes to zero for the TAS scheme. This can be explained by the fact that the use of the TAS scheme not only degrades the channel condition of the eavesdropper, which is beneficial to secure transmission, but also deteriorates the channel condition of the legitimate user, which is adverse to secure transmission. It is also worth noting that the TAS scheme outperforms the benchmark scheme in certain regimes, i.e., when the jamming power is small. Therefore, the designer has to carefully choose the jamming power of the TAS scheme.

Figure 7 examines the secrecy throughput of the three proposed schemes versus the number of antennas at the jammer. It is clear that the secrecy throughput of the three proposed schemes increases as the number of antennas at the jammer increases. Therefore, we conclude that increasing the number of antennas at the jammer can compensate for the performance loss from short packet transmissions. In particular, the TAS scheme can achieve more significant performance gains by adding more antennas at the jammer. This is attributed to the fact that increasing the number of antennas at the jammer will make it easier to select a better antenna, which reduces the jamming interference at the legitimate user.

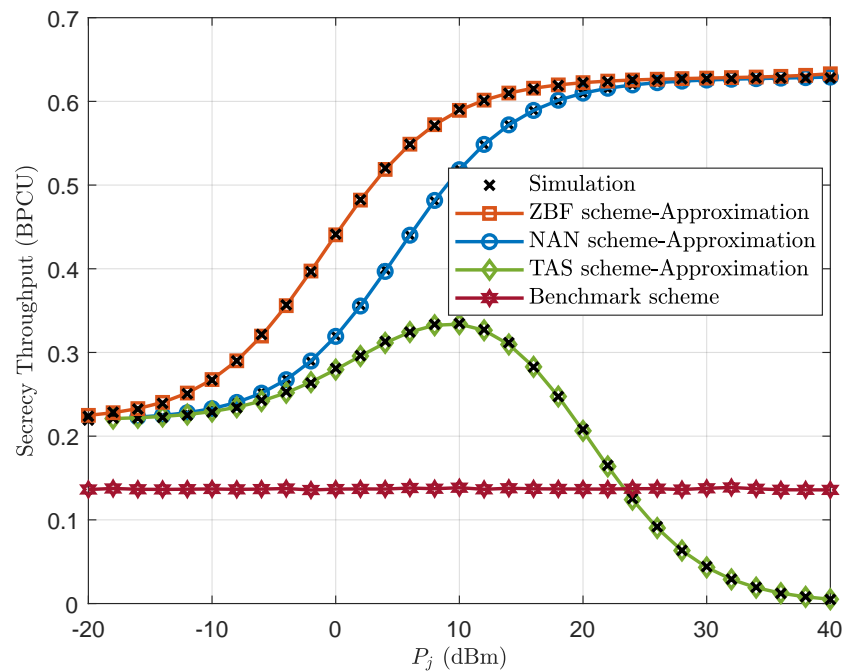


Figure 6. Secrecy throughput of the ZFB, NAN, TAS, and benchmark schemes versus P_j for $B = 200$, $N = 300$, and $P_a = 10$ dBm.

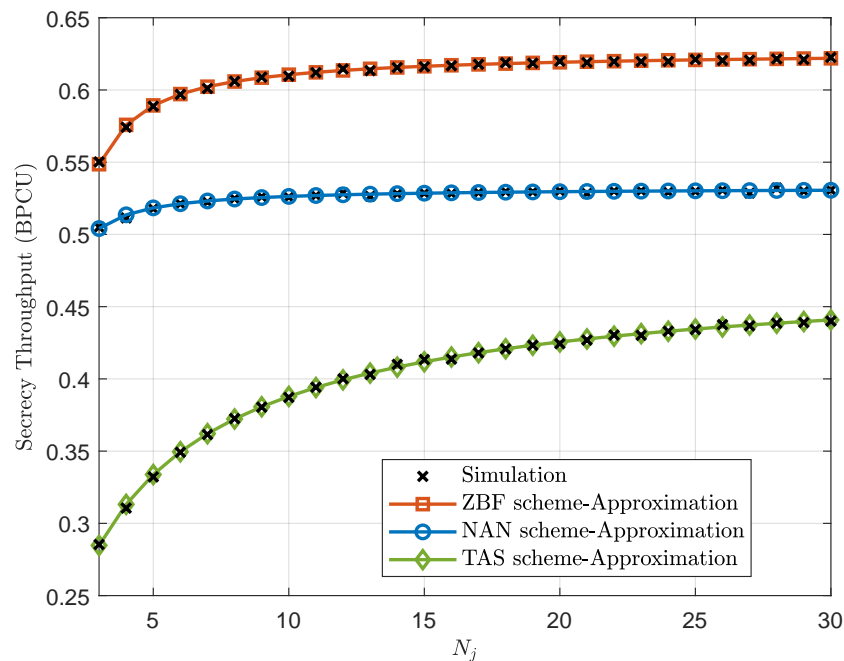


Figure 7. Secrecy throughput of the ZFB, NAN, and TAS schemes versus N_j for $B = 200$, $N = 300$, $P_a = 10$ dBm, and $P_j = 10$ dBm.

Figure 8 depicts the optimal blocklength and the corresponding maximum secrecy throughput versus the transmit power P_a subject to the latency and reliability constraints. When the optimization problem in terms of maximizing the secrecy throughput is infeasible, we set the optimal blocklength to zero and the maximum secrecy throughput is set to zero. We first observe that one critical point exists and when P_a does not exceed this point, the maximum secrecy throughput is zero. This is not surprising, since when P_a is small, it is unable to meet the reliability constraint. We further observe that both the optimal blocklength and the maximum secrecy throughput converge to nonzero constants

as $P_a \rightarrow \infty$. This is because the secrecy throughput of the considered system is independent of P_a in the high SNR regime.

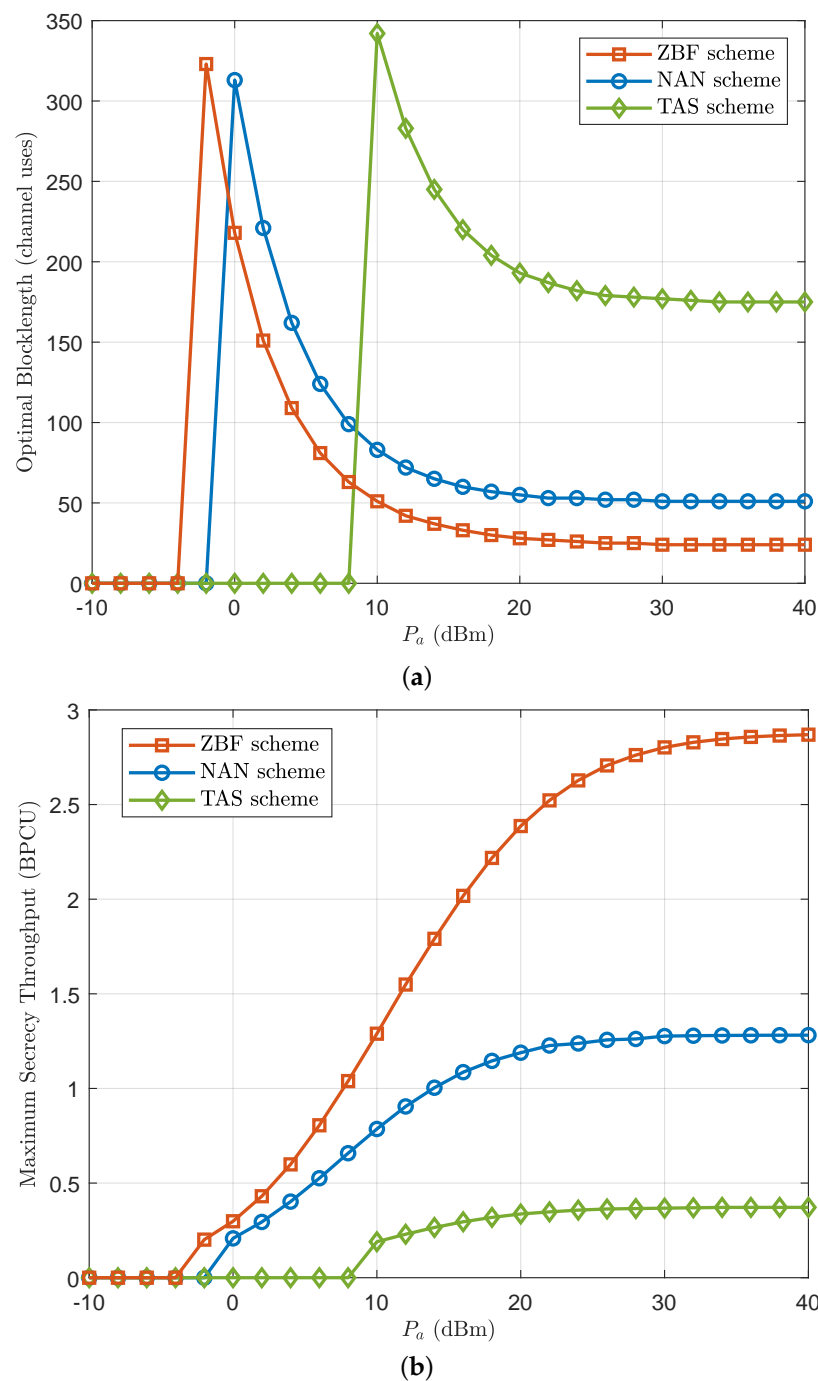


Figure 8. (a) The optimal blocklength and (b) the corresponding maximum secrecy throughput versus P_a for $B = 100$, $N_j = 8$, $P_j = 10$ dBm, $\epsilon_{\max} = 0.35$, and $N_{\max} = 400$.

Figure 9 illustrates the optimal blocklength and the corresponding maximum secrecy throughput versus the jamming power P_j subject to the latency and reliability constraints. We first observe that when P_j is either extremely small or large, the maximum secrecy throughput of the TAS scheme approaches zero. This is because the decoding error probability of the TAS scheme is large in the two extreme cases. Therefore, the TAS scheme can only achieve its best performance for in-between values of P_j . We further observe that the

optimal blocklength of the TAS scheme first decreases and then increases as P_j increases. This is because there exists a tradeoff between decoding error and transmission latency.

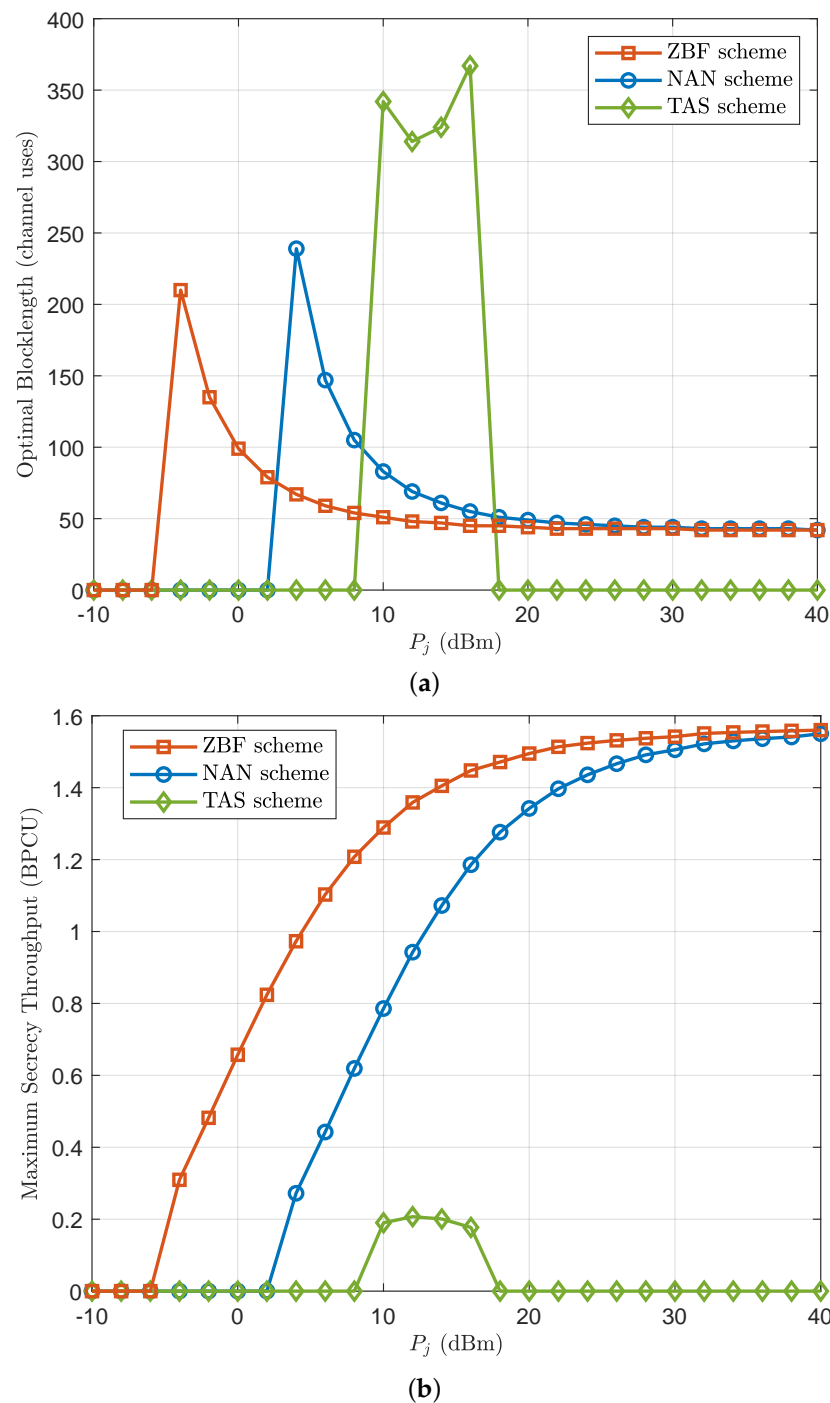


Figure 9. (a) The optimal blocklength and (b) the corresponding maximum secrecy throughput versus P_j for $B = 100$, $N_j = 8$, $P_a = 10$ dBm, $\epsilon_{\max} = 0.35$, and $N_{\max} = 400$.

5. Conclusions

In this paper, we investigated the secrecy performance of IoT networks with finite blocklength coding. To exploit the available multi-antenna jammer for secrecy enhancement, we proposed three different secure transmission schemes. Specifically, we derived approximate closed-form expressions for the secrecy throughput of all the proposed schemes. Moreover, we presented the asymptotic secrecy throughput in the case of infinite blocklength to gain further insights. In addition, we determined the optimal blocklength that

maximizes the secrecy throughput subject to the latency and reliability constraints. Numerical results demonstrated that both the ZFB scheme and the NAN scheme strictly outperform the TAS scheme in terms of the secrecy throughput, and the performance loss from short packet transmissions can be compensated for by increasing the number of antennas at the jammer.

Author Contributions: Methodology, D.C., J.L., J.H., and X.Z.; formal analysis, D.C., J.L., J.H., X.Z., and S.Z.; writing—original draft preparation, D.C. and J.L.; writing—review and editing, J.H., X.Z., and S.Z.; supervision, X.Z. and S.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the Doctoral Research Start-up Funding of Nanyang Normal University under Grant 2022ZX017; in part by the Cultivating Fund Project for the National Natural Science Foundation of China of Nanyang Normal University under Grant 2022PY024; in part by the open research fund of Key Lab of Broadband Wireless Communication and Sensor Network Technology (Nanjing University of Posts and Telecommunications), Ministry of Education, under Grant JZNY202107; in part by the Key Scientific Research Projects of Colleges and Universities in Henan Province of China under Grant 21A520033, 23A520038, and 23A510001; and in part by the Key Scientific and Technological Research Projects in Henan Province under Grant 222102320369, 232102210121, and 232102220101.

Data Availability Statement: Not applicable.

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

Appendix A

For the delivery of B information bits through N channel uses, the decoding error probability of the ZFB scheme can be characterized by:

$$\begin{aligned} & \epsilon^{ZFB}(\gamma_b^{ZFB}, \gamma_e^{ZFB}) \\ &= Q\left(\sqrt{\frac{N}{V_b^{ZFB}}} \left(\ln \frac{1 + \gamma_b^{ZFB}}{1 + \gamma_e^{ZFB}} - \sqrt{\frac{V_e^{ZFB}}{N}} Q^{-1}(\delta) - \frac{B}{N} \ln 2 \right)\right), \end{aligned} \quad (A1)$$

conditioned on $\gamma_b^{ZFB} > \gamma_e^{ZFB}$. Note that, $\epsilon^{ZFB} = 1$ if $\gamma_b^{ZFB} \leq \gamma_e^{ZFB}$. In order to obtain a closed-form expression of the secrecy throughput, we use a linear approximation of Q -function [35] and approximate the decoding error probability ϵ^{ZFB} as:

$$\epsilon^{ZFB}(\gamma_b^{ZFB}, \gamma_e^{ZFB}) \approx \begin{cases} 1, & \gamma_b^{ZFB} < \zeta^{ZFB}, \\ \frac{1}{2} + v^{ZFB}(\gamma_b^{ZFB} - \theta^{ZFB}), & \zeta^{ZFB} \leq \gamma_b^{ZFB} \leq \tilde{\zeta}^{ZFB}, \\ 0, & \gamma_b^{ZFB} > \tilde{\zeta}^{ZFB}, \end{cases} \quad (A2)$$

where $\theta^{ZFB} = e^{\sqrt{\frac{V_e^{ZFB}}{N}} Q^{-1}(\delta) + \frac{B}{N} \ln 2} (1 + \gamma_e^{ZFB}) - 1$, $v^{ZFB} = -\sqrt{\frac{N}{2\pi\theta^{ZFB}(\theta^{ZFB} + 2)}}$, $\zeta^{ZFB} = \theta^{ZFB} + \frac{1}{2v^{ZFB}}$, and $\tilde{\zeta}^{ZFB} = \theta^{ZFB} - \frac{1}{2v^{ZFB}}$.

Let $X = \gamma_b^{ZFB}$ and $Y = \gamma_e^{ZFB}$; the secrecy throughput of the ZFB scheme can be approximated as:

$$\begin{aligned} T^{ZFB} &= \frac{B}{N} \int_0^\infty \int_y^\infty (1 - \epsilon^{ZFB}(x, y)) f_{\gamma_b^{ZFB}}(x) f_{\gamma_e^{ZFB}}(y) dx dy \\ &\stackrel{(a)}{\approx} \frac{B}{N} \int_0^\infty \int_0^\infty (1 - \epsilon^{ZFB}(x, y)) f_{\gamma_b^{ZFB}}(x) f_{\gamma_e^{ZFB}}(y) dx dy \\ &\stackrel{(b)}{\approx} \frac{B}{N} \int_0^\infty \left(1 + v^{ZFB} \int_{\zeta^{ZFB}}^{\tilde{\zeta}^{ZFB}} F_{\gamma_b^{ZFB}}(x) dx \right) f_{\gamma_e^{ZFB}}(y) dy \\ &\stackrel{(c)}{\approx} \frac{B}{N} \int_0^\infty (1 - F_{\gamma_b^{ZFB}}(\theta^{ZFB}(y))) f_{\gamma_e^{ZFB}}(y) dy, \end{aligned} \quad (A3)$$

where (a) is based on the fact that $e^{ZFB} \rightarrow 1$ when $N \rightarrow \infty$ and $x < y$, while $e^{ZFB} \rightarrow 1$ as $N \rightarrow 0$, (b) is obtained by using (A2), (c) is obtained by leveraging the Riemann integral approximation [36], $f_{\gamma_b^{ZFB}}(x)$ is the PDF of γ_b^{ZFB} , $f_{\gamma_e^{ZFB}}(y)$ is the PDF of γ_e^{ZFB} , and $F_{\gamma_b^{ZFB}}(x)$ is the cumulative distribution function (CDF) of γ_b^{ZFB} .

Noticing that γ_b^{ZFB} is an exponentially distributed random variable, its CDF is given by:

$$F_{\gamma_b^{ZFB}}(x) = 1 - e^{-\frac{x}{\lambda_a \gamma_{ab}}}. \quad (\text{A4})$$

On the other hand, in order to derive the PDF of γ_e^{ZFB} , we first give the PDF of the random variable $Z = \left| \mathbf{h}_{je}^\dagger \mathbf{w}_{ZF} \right|^2$ as [37]:

$$f_Z(z) = \frac{z^{N_j-2}}{(N_j-2)! \tilde{\gamma}_{je}^{N_j-1}} e^{-\frac{z}{\tilde{\gamma}_{je}}}. \quad (\text{A5})$$

Then, the CDF of γ_e^{ZFB} is given by:

$$\begin{aligned} F_{\gamma_e^{ZFB}}(y) &= \int_0^\infty \left(1 - e^{-\frac{\lambda_j y z + y}{\lambda_a \tilde{\gamma}_{ae}}} \right) f_Z(z) dz \\ &= 1 - \frac{e^{-\frac{y}{\lambda_a \tilde{\gamma}_{ae}}}}{\tilde{\gamma}_{je}^{N_j-1}} \left(\frac{\lambda_j y}{\lambda_a \tilde{\gamma}_{ae}} + \frac{1}{\tilde{\gamma}_{je}} \right)^{1-N_j}. \end{aligned} \quad (\text{A6})$$

Taking the derivative of (A6) with respect to y , the PDF of γ_e^{ZFB} is given by:

$$\begin{aligned} f_{\gamma_e^{ZFB}}(y) &= \frac{e^{-\frac{y}{\lambda_a \tilde{\gamma}_{ae}}}}{\lambda_a \tilde{\gamma}_{ae} \tilde{\gamma}_{je}^{N_j-1}} \left(\frac{\lambda_j y}{\lambda_a \tilde{\gamma}_{ae}} + \frac{1}{\tilde{\gamma}_{je}} \right)^{1-N_j} \\ &\quad + \frac{\lambda_j (N_j - 1)}{\lambda_a \tilde{\gamma}_{ae} \tilde{\gamma}_{je}^{N_j-1}} e^{-\frac{y}{\lambda_a \tilde{\gamma}_{ae}}} \left(\frac{\lambda_j y}{\lambda_a \tilde{\gamma}_{ae}} + \frac{1}{\tilde{\gamma}_{je}} \right)^{-N_j}. \end{aligned} \quad (\text{A7})$$

Substituting (A4) and (A7) into (A3), we have:

$$T^{ZFB} = \frac{B}{N} \int_0^\infty e^{-\frac{\theta^{ZFB}(y)}{\lambda_a \tilde{\gamma}_{ab}}} f_{\gamma_e^{ZFB}}(y) dy. \quad (\text{A8})$$

To simplify the integral in (A8), we introduce a sufficiently large parameter M_1 to ensure $V_e^{ZFB} \approx 1$, when $\gamma_e^{ZFB} > M_1$, and then (A8) can be approximated as:

$$T^{ZFB} = \frac{B}{N} \left(\underbrace{\int_0^{M_1} e^{-\frac{\theta^{ZFB}(y)}{\lambda_a \tilde{\gamma}_{ab}}} f_{\gamma_e^{ZFB}}(y) dy}_{\Xi_1} + \underbrace{\int_{M_1}^\infty e^{-\frac{\omega_1 y + \omega_1 - 1}{\lambda_a \tilde{\gamma}_{ab}}} f_{\gamma_e^{ZFB}}(y) dy}_{\Xi_2} \right), \quad (\text{A9})$$

where $\omega_1 = e^{\frac{Q^{-1}(\delta)}{\sqrt{N}} + \frac{B}{N} \ln 2}$. By using Gaussian–Chebyshev quadrature [38], the integral Ξ_1 can be approximated as:

$$\begin{aligned} \Xi_1 &\approx \frac{M_1}{2} \sum_{m=1}^{M_2} \left(\frac{\pi}{M_2} \sqrt{1 - t_m^2} e^{-\frac{\omega_m}{\lambda_a \tilde{\gamma}_{ab}}} \left(\frac{e^{-\frac{M_1(t_m+1)}{2\lambda_a \tilde{\gamma}_{ae}}}}{\lambda_a \tilde{\gamma}_{ae} \tilde{\gamma}_{je}^{N_j-1}} \left(\frac{M_1 \lambda_j (t_m + 1)}{2\lambda_a \tilde{\gamma}_{ae}} + \frac{1}{\tilde{\gamma}_{je}} \right)^{1-N_j} \right. \right. \\ &\quad \left. \left. + \frac{\lambda_j (N_j - 1)}{\lambda_a \tilde{\gamma}_{ae} \tilde{\gamma}_{je}^{N_j-1}} e^{-\frac{M_1(t_m+1)}{2\lambda_a \tilde{\gamma}_{ae}}} \left(\frac{M_1 \lambda_j (t_m + 1)}{2\lambda_a \tilde{\gamma}_{ae}} + \frac{1}{\tilde{\gamma}_{je}} \right)^{-N_j} \right) \right), \end{aligned} \quad (\text{A10})$$

where M_2 is a parameter for the complexity accuracy tradeoff, $t_m = \cos\left(\frac{2m-1}{2M_2}\pi\right)$, and $\omega_m = e^{\sqrt{\frac{1-(1+M_1(t_m+1)/2)^{-2}}{N}}Q^{-1}(\delta)+\frac{B}{N}\ln 2\left(1+\frac{M_1}{2}(t_m+1)\right)-1}$. According to [3.353.1] [39], the integral Ξ_2 can be derived as:

$$\begin{aligned}\Xi_2 &= \frac{\lambda_a^{N_j-2}\tilde{\gamma}_{ae}^{N_j-2}e^{-\frac{\omega_1-1}{\lambda_a\tilde{\gamma}_{ab}}}}{\lambda_j^{N_j-1}\tilde{\gamma}_{je}^{N_j-1}}\left(\sum_{k=1}^{N_j-2}\frac{(k-1)!\lambda_j^k\tilde{\gamma}_{je}^k(-1)^{N_j-2-k}e^{-\frac{M_1\omega_1}{\lambda_a\tilde{\gamma}_{ab}}-\frac{M_1}{\lambda_a\tilde{\gamma}_{ae}}}}{(N_j-2)!(M_1\lambda_j\tilde{\gamma}_{je}+\lambda_a\tilde{\gamma}_{ae})^k}\right. \\ &\quad \times \left(\frac{\omega_1}{\lambda_a\tilde{\gamma}_{ab}}+\frac{1}{\lambda_a\tilde{\gamma}_{ae}}\right)^{N_j-2-k}-\frac{(-1)^{N_j-2}}{(N_j-2)!}\left(\frac{\omega_1}{\lambda_a\tilde{\gamma}_{ab}}+\frac{1}{\lambda_a\tilde{\gamma}_{ae}}\right)^{N_j-2} \\ &\quad \times e^{\frac{\omega_1\tilde{\gamma}_{ae}}{\lambda_j\tilde{\gamma}_{je}\tilde{\gamma}_{ab}}+\frac{1}{\lambda_j\tilde{\gamma}_{je}}}Ei\left(-\left(\frac{\omega_1}{\lambda_a\tilde{\gamma}_{ab}}+\frac{1}{\lambda_a\tilde{\gamma}_{ae}}\right)\left(M_1+\frac{\lambda_a\tilde{\gamma}_{ae}}{\lambda_j\tilde{\gamma}_{je}}\right)\right)\Bigg)+e^{-\frac{\omega_1-1}{\lambda_a\tilde{\gamma}_{ab}}} \\ &\quad \times \frac{\lambda_a^{N_j-1}\tilde{\gamma}_{ae}^{N_j-1}(N_j-1)e^{-\frac{\omega_1-1}{\lambda_a\tilde{\gamma}_{ab}}}}{\lambda_j^{N_j-1}\tilde{\gamma}_{je}^{N_j-1}(N_j-1)!}\left(\sum_{k=1}^{N_j-1}\frac{(k-1)!\lambda_j^k\tilde{\gamma}_{je}^ke^{-\frac{M_1\omega_1}{\lambda_a\tilde{\gamma}_{ab}}-\frac{M_1}{\lambda_a\tilde{\gamma}_{ae}}}}{(M_1\lambda_j\tilde{\gamma}_{je}+\lambda_a\tilde{\gamma}_{ae})^k}\right. \\ &\quad \times \left(-\frac{\omega_1}{\lambda_a\tilde{\gamma}_{ab}}-\frac{1}{\lambda_a\tilde{\gamma}_{ae}}\right)^{N_j-1-k}-\left(-\frac{\omega_1}{\lambda_a\tilde{\gamma}_{ab}}-\frac{1}{\lambda_a\tilde{\gamma}_{ae}}\right)^{N_j-1} \\ &\quad \times e^{\frac{\omega_1\tilde{\gamma}_{ae}}{\lambda_j\tilde{\gamma}_{je}\tilde{\gamma}_{ab}}+\frac{1}{\lambda_j\tilde{\gamma}_{je}}}Ei\left(-\left(\frac{\omega_1}{\lambda_a\tilde{\gamma}_{ab}}+\frac{1}{\lambda_a\tilde{\gamma}_{ae}}\right)\left(M_1+\frac{\lambda_a\tilde{\gamma}_{ae}}{\lambda_j\tilde{\gamma}_{je}}\right)\right)\Bigg).\end{aligned}\quad (A11)$$

Then, substituting (A10) together with (A11) into (A9), a closed-form approximation for the secrecy throughput of the ZFB scheme is presented in (11).

References

1. Brincat, A.A.; Pacifici, F.; Mazzola, F. IoT as a service for smart cities and nations. *IEEE Internet Things Mag.* **2019**, *2*, 28–31. [\[CrossRef\]](#)
2. Xiang, Z.; Yang, W.; Cai, Y.; Ding, Z.; Song, Y.; Zou, Y. NOMA-assisted secure short-packet communications in IoT. *IEEE Wirel. Commun.* **2020**, *27*, 8–15. [\[CrossRef\]](#)
3. Lianghai, J.; Han, B.; Liu, M.; Schotten, H.D. Applying device-to-device communication to enhance IoT services. *IEEE Commun. Stand. Mag.* **2017**, *1*, 85–91. [\[CrossRef\]](#)
4. Ji, B.; Liu, Y.; Xing, L.; Li, C.; Zhang, G.; Han, C.; Wen, H.; Mumtaz, S. Survey of Secure Communications of Internet of Things with Artificial Intelligence. *IEEE Internet Things Mag.* **2022**, *5*, 92–99. [\[CrossRef\]](#)
5. Feng, C.; Wang, H.M. Secure short-packet communications at the physical layer for 5G and beyond. *IEEE Commun. Stand. Mag.* **2021**, *5*, 96–102. [\[CrossRef\]](#)
6. Hu, J.; Cai, Y.; Yang, N. Secure transmission design with feedback compression for the Internet of Things. *IEEE Trans. Signal Process.* **2018**, *66*, 1580–1593. [\[CrossRef\]](#)
7. Farhat, J.; Brante, G.; Souza, R.D.; Vilela, J.P. On the secure spectral efficiency of URLLC with randomly located colluding eavesdroppers. *IEEE Internet Things J.* **2021**, *8*, 14672–14682. [\[CrossRef\]](#)
8. Feng, C.; Wang, H.M.; Poor, H.V. Reliable and secure short-packet communications. *IEEE Trans. Wirel. Commun.* **2022**, *21*, 1913–1926. [\[CrossRef\]](#)
9. Mukherjee, A. Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints. *Proc. IEEE* **2015**, *103*, 1747–1761. [\[CrossRef\]](#)
10. Li, C.; She, C.; Yang, N.; Quek, T.Q.S. Secure transmission rate of short packets with queueing delay requirement. *IEEE Trans. Wirel. Commun.* **2022**, *21*, 203–218. [\[CrossRef\]](#)
11. Xie, Y.; Ren, P. Optimizing training and transmission overheads for secure URLLC against randomly distributed eavesdroppers. *IEEE Trans. Veh. Technol.* **2022**, *71*, 11921–11935. [\[CrossRef\]](#)
12. Xu, D.; Zhao, H.; Zhu, H. Resource allocation for secure short packet communications in wireless powered IoT networks. *IEEE Trans. Veh. Technol.* **2023**, early access. [\[CrossRef\]](#)
13. 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. [\[CrossRef\]](#)
14. Hu, L.; Wen, H.; Wu, B.; Pan, F.; Liao, R.; Song, H.; Tang, J.; Wang, X. Cooperative Jamming for Physical Layer Security Enhancement in Internet of Things. *IEEE Internet Things J.* **2018**, *5*, 219–228. [\[CrossRef\]](#)
15. Xu, D.; Zhu, H. Secure transmission for SWIPT IoT systems with full-duplex IoT devices. *IEEE Internet Things J.* **2019**, *6*, 10915–10933. [\[CrossRef\]](#)

16. Abdullah, Z.; Chen, G.; Abdullah, M.A.M.; Chambers, J.A. Enhanced secrecy performance of multihop IoT networks with cooperative hybrid-duplex jamming. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 161–172. [\[CrossRef\]](#)
17. Schulz, P.; Matthe, M.; Klessig, H.; Simsek, M.; Fettweis, G.; Ansari, J.; Ashraf, S.A.; Almeroth, B.; Voigt, J.; Riedel, I.; et al. Latency Critical IoT Applications in 5G: Perspective on the Design of Radio Interface and Network Architecture. *IEEE Commun. Mag.* **2017**, *55*, 70–78. [\[CrossRef\]](#)
18. Ma, R.; Yang, W.; Shi, H.; Lu, X.; Liu, J. Covert communication with a spectrum sharing relay in the finite blocklength regime. *China Commun.* **2023**, *20*, 195–211. [\[CrossRef\]](#)
19. Yang, W.; Schaefer, R.F.; Poor, H.V. Wiretap channels: Nonasymptotic fundamental limits. *IEEE Trans. Inf. Theory* **2019**, *65*, 4069–4093. [\[CrossRef\]](#)
20. Wang, H.; Yang, Q.; Ding, Z.; Poor, H.V. Secure short-packet communications for mission-critical IoT applications. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 2565–2578. [\[CrossRef\]](#)
21. Ar, N.; Thomos, N.; Musavian, L. Performance analysis of short packet communications with multiple eavesdroppers. *IEEE Trans. Commun.* **2022**, *70*, 6778–6789. [\[CrossRef\]](#)
22. Wei, L.; Yang, Y.; Jiao, B. Secrecy throughput in full-duplex multiuser MIMO short-packet communications. *IEEE Wirel. Commun. Lett.* **2021**, *10*, 1339–1343. [\[CrossRef\]](#)
23. Chen, Y.; Zhang, Y.; Yu, B.; Zhang, T.; Cai, Y. Relay-assisted secure short-packet transmission in cognitive IoT with spectrum sensing. *China Commun.* **2021**, *18*, 37–50. [\[CrossRef\]](#)
24. Zheng, T.-X.; Wang, H.-M.; Ng, D.W.K.; Yuan, J. Physical layer security in the finite blocklength regime over fading channels. *IEEE Trans. Wirel. Commun.* **2020**, *19*, 3405–3420. [\[CrossRef\]](#)
25. Ren, H.; Pan, C.; Deng, Y.; El Kashlan, M.; Nallanathan, A. Resource allocation for secure URLLC in mission-critical IoT scenarios. *IEEE Trans. Commun.* **2020**, *68*, 5793–5807. [\[CrossRef\]](#)
26. Xiang, Z.; Yang, W.; Cai, Y.; Xiong, J.; Ding, Z.; Song, Y. Secure transmission in a NOMA-assisted IoT network with diversified communication requirements. *IEEE Internet Things J.* **2020**, *7*, 11157–11169. [\[CrossRef\]](#)
27. Lai, X.; Wu, T.; Zhang, Q.; Qin, J. Average secure BLER analysis of NOMA downlink short-packet communication systems in flat Rayleigh fading channels. *IEEE Trans. Wirel. Commun.* **2021**, *20*, 2948–2960. [\[CrossRef\]](#)
28. Lv, S.; Xu, X.; Han, S.; Tao, X.; Zhang, P. Energy-efficient secure short-packet transmission in NOMA-assisted mMTC networks with relaying. *IEEE Trans. Veh. Technol.* **2022**, *71*, 1699–1712. [\[CrossRef\]](#)
29. Tao, L.; Yang, W.; Lu, X.; Ma, R.; Yang, L.; Song, Y. Multi-antenna Jammer assisted covert communications in data collected IoT with NOMA. *China Commun.* **2023**, *20*, 217–231. [\[CrossRef\]](#)
30. Tao, L.; Yang, W.; Lu, X.; Wang, M.; Song, Y. Achieving covert communication in uplink NOMA systems via energy harvesting jammer. *IEEE Commun. Lett.* **2021**, *25*, 3785–3789. [\[CrossRef\]](#)
31. Basilevsky, A. *Applied Matrix Algebra in the Statistical Sciences*; North-Holland: New York, NY, USA, 1983.
32. Yang, M.; Zhang, B.; Huang, Y.; Yang, N.; da Costa, D.B.; Guo, D. Secrecy enhancement of multiuser MISO networks using OSTBC and artificial noise. *IEEE Trans. Veh. Technol.* **2017**, *66*, 11394–11398. [\[CrossRef\]](#)
33. Jiang, Y.; Wang, L.; Chen, H.-H. Covert communications in D2D underlaying cellular networks with antenna array assisted artificial noise transmission. *IEEE Trans. Veh. Technol.* **2020**, *69*, 2980–2992. [\[CrossRef\]](#)
34. Wang, K.; Pan, C.; Ren, H.; Xu, W.; Zhang, L.; Nallanathan, A. Packet Error Probability and Effective Throughput for Ultra-Reliable and Low-Latency UAV Communications. *IEEE Trans. Commun.* **2021**, *69*, 73–84. [\[CrossRef\]](#)
35. Makki, B.; Svensson, T.; Zorzi, M. Wireless energy and information transmission using feedback: Infinite and finite block-length analysis. *IEEE Trans. Commun.* **2016**, *64*, 5304–5318. [\[CrossRef\]](#)
36. Lai, X.; Zhang, Q.; Qin, J. Cooperative NOMA short-packet communications in flat Rayleigh fading channels. *IEEE Trans. Veh. Technol.* **2019**, *68*, 6182–6186. [\[CrossRef\]](#)
37. Zhang, T.; Huang, Y.; Cai, Y.; Zhong, C.; Yang, W.; Karagiannis, G.K. Secure multiantenna cognitive wiretap networks. *IEEE Trans. Veh. Technol.* **2017**, *66*, 4059–4072.
38. Abramowitz, M.; Stegun, I.A. *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, 9th ed.; US Govt. Print: Washington, DC, USA, 1972.
39. Gradshteyn, I.S.; Ryzhik, I.M.; Jeffrey, A.; Zwillinger, D.; Technica, S. *Table of Integrals, Series, and Products*, 7th ed.; Academic: New York, NY, USA, 2007.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.