sensors

MDPI

Article

Optimal Channel Training Design for Secure Short-Packet Communications

Dechuan Chen [1,2], Jin Li [1], Jianwei Hu [3], Xingang Zhang [4,*] and Shuai Zhang [1]

[1] College of Physics and Electronic Engineering, Nanyang Normal University, Nanyang 473061, China
[2] Key Lab of Broadband Wireless Communication and Sensor Network Technology (Nanjing University of Posts and Telecommunications), Ministry of Education, Nanjing 210003, China
[3] National Key Laboratory for Complex Systems Simulation, Beijing 100101, China
[4] College of Computer Science and Technology, Nanyang Normal University, Nanyang 473061, China
* Correspondence: xgzhang999@163.com

Abstract: Physical layer security is a promising technique to ensure the confidentiality of short-packet communications, since no additional channel uses are needed. Motivated by the fact of finite coding blocklength in short-packet communications, we attempt to investigate the problem of how many the channel uses utilized for channel training should be allocated to perform secure communications. Based on the finite blocklength information theory, we derive a closed-form expression to approximate the average achievable secrecy throughput. To gain more insights, we also present the asymptotic average secrecy throughput under two special cases, i.e., high signal-to-noise ratio (SNR) and infinite blocklength. Moreover, we determine the optimal channel training length to maximize the average secrecy throughput under the reliability constraint and given blocklength. Numerical results are provided to validate the analysis and demonstrate that the performance gain achieved by the optimal channel training length is remarkable, relative to other benchmark schemes.

Keywords: physical layer security; short-packet communications; channel training; average secrecy throughput

Citation: Chen, D.; Li, J.; Hu, J.; Zhang, X.; Zhang, S. Optimal Channel Training Design for Secure Short-Packet Communications. *Sensors* **2023**, *23*, 1068. https://doi.org/10.3390/s23031068

Academic Editors: Savio Sciancalepore, Giuseppe Piro and Nicola Zannone

Received: 19 December 2022
Revised: 9 January 2023
Accepted: 12 January 2023
Published: 17 January 2023

1. Introduction

Short-packet communications are recognized as a prominent technique for the fifth generation (5G) and next generation communication networks since they can fulfill two stringent quality-of-service (QoS) requirements, i.e., ultra-low latency and super-high reliability [1–3]. The typical size of packet in short-packet communications is only hundreds of bits (e.g., 80–160 bits of industrial manufacturing and control systems [4]). Due to the limited packet length, the decoding error probability in short-packet communications cannot be reduced to arbitrarily low. Motivated by this, block-error-rate as a proper performance metric was developed in [5] to measure the performance of short-packet communication systems, and the block-error-rate of the system increases with the decrease of the blocklength. Since then, short-packet communications have attracted considerable attention from both academia and the industry.

Due to the unchangeable open nature of the wireless transmission medium, security is also a challenging issue for short-packet communications [6,7]. Conventionally, the security is enhanced by encryption techniques, which are deployed at the network layer of communication systems. However, all cryptographic measures require more overhead for encryption and decryption and increase latency imposed, which may not be applicable for short-packet communications [8]. As an alternative to cryptography, physical layer security technique is more appealing for short-packet communications since no additional channel uses are needed [9].

Physical layer security has been well investigated in the existing literature, where the coding blocklength is sufficiently large for achieving the secrecy capacity [10,11]. For

short-packet communications, ref. [12] derived the maximal secret communication rate subject to reliability and security constraints. Subsequently, ref. [8] studied the secrecy throughput performance with an external multi-antenna eavesdropper, and found the optimal blocklength to maximize the secrecy throughput under reliability and latency constraints. Moreover, considering both reliability and security, ref. [13] established the outage probability and effective throughput to analyze the performance of secure short-packet communications. The authors in [9] considered a multiuser downlink network in the presence of an eavesdropper and developed efficient methods to solve the total transmit power minimization and weighted throughput maximization problems. Packet replication and interface diversity schemes were employed in [14] to improve the secure spectral efficiency, where eavesdroppers are randomly distributed according to Poisson point processes. In [15], the spectrum sensing blocklength and transmission blocklength were jointly optimized to maximize the secrecy throughput. In order to achieve both high spectral efficiency and low communication delay, incorporating short-packet communications with non-orthogonal multiple access (NOMA) networks was investigated in [16–18].

It is worth noting that the previous studies on physical layer security with finite blocklength assumed perfect channel state information (CSI) for communications. However, in most realistic scenarios, perfect CSI may not be easy to obtain due to the feedback delay, channel estimation errors, and limited feedback rate. Against this background, ref. [19] addressed the secrecy throughput of full-duplex multiuser multiple-input-multiple-output (MIMO) networks with short packets, where the impacts of imperfect CSI, co-channel interference and self interference are jointly considered. In [20], the optimal power control policy maximizing achievable secrecy rate under the queueing delay requirement was carried out with channel estimation error. It is noted that these studies in [19,20] have not considered explicit channel training schemes for channel estimation. In fact, the channel estimation error is closely related to channel training schemes, e.g., pilot length and pilot power. In particular, the pilot length significantly affects the overall performance of short-packet transmission systems [2]. In [21], the authors presented a pilot-assisted secure short-packet communications with randomly distributed eavesdroppers and characterized the reliability and security performance by transmission error probability and intercept probability, respectively. Furthermore, ref. [22] optimized the pilot length by an iterative algorithm to maximize the achievable effective secrecy rate of the system. It is further noted that the optimal pilot length that maximizes the secrecy rate has no closed-form solution in [22]. Although their results provide useful insights, the computational complexity of the iterative search algorithm is relatively high. On the other hand, the impact of the pilot length on the secrecy throughput of short-packet communications has not been examined thus far.

Motivated by the above considerations, we investigate the channel training design for secure short-packet communications, where a source transmits pilot symbols before its information transmission to enable channel estimation at a destination. In order to maximize the secrecy throughput of the considered system, the number of channel uses allocated to channel training and data transmission need to be carefully optimized. The main contributions of this paper are summarized as follows:

- Based on the finite blocklength information theory, we derive a closed-form expression to approximate the average achievable secrecy throughput, which provides an efficient means to comprehensively evaluate the impact of key system parameters, e.g., the channel training length and blocklength, on the latency-reliability tradeoff.
- To achieve additional insights on the application of the channel training scheme for secure short-packet communications into the practical design, we also present the asymptotic closed-form expressions for the average secrecy throughput under two special cases, i.e., high signal-to-noise ratio (SNR) and infinite blocklength.
- We determine the optimal channel training length to maximize the average secrecy throughput under the reliability constraint and given blocklength. Numerical results demonstrate the performance gain achieved by the optimal channel training length

is remarkable relative to the fixed-ratio channel training length and fixed channel training length schemes.

The remainder of this paper is organized as follows. In Section 2, we describe the secure short-packet communication system based on the channel training scheme. In Section 3, we present the closed-form expression to approximate the average achievable secrecy throughput, provide the high SNR and infinite blocklength analyses for the average secrecy throughput, and determine the optimal channel training length to maximize the average secrecy throughput. Finally, we respectively give numerical results and conclusions in Sections 4 and 5.

2. System Model

In this paper, we consider a secure short-packet communication system as shown in Figure 1, in which a source sends confidential short packets to a destination in the presence of a passive eavesdropper. Due to size limitation, each node is equipped with a single antenna. The channels from the source to the destination and the eavesdropper are subject to independent quasi-static Rayleigh fading, which means that the channel coefficients remain static during a coherence slot (n channel uses) and vary independently from one coherence slot to the next [22–24].

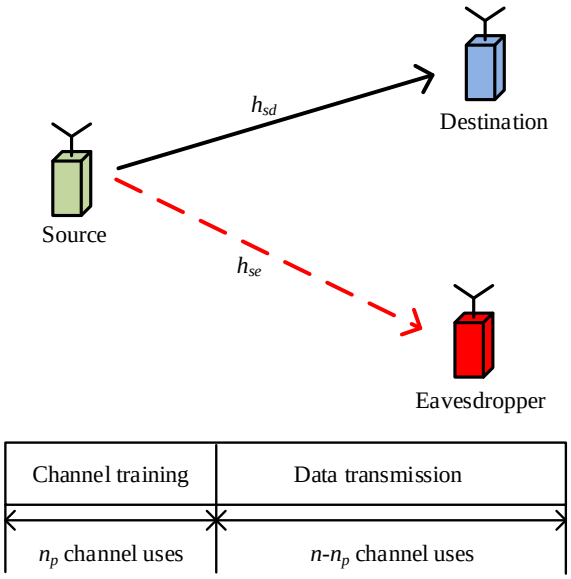

Figure 1. System model and packet structure for short-packet communications.

In each short-packet transmission, the source conveys L information bits over n channel uses to the destination. In order to support the high reliability requirement, we consider a two-phase training-based transmission scheme, which contains a channel training phase and a data transmission phase. In the channel training phase, the source transmits a predefined pilot sequence of n_p channel uses to enable channel estimation at the receiver. In the data transmission phase, the source utilizes the remaining $n - n_p$ channel uses for information transmission. Thus, the received signal vectors at the destination and the eavesdropper are, respectively, given by

$$\mathbf{y}_d = h_{sd}\mathbf{x} + \mathbf{n}_d, \tag{1}$$

$$\mathbf{y}_e = h_{se}\mathbf{x} + \mathbf{n}_e, \tag{2}$$

where $h_{sd} \sim \mathcal{CN}(0, \bar{\gamma}_{sd})$ is the channel coefficient between the source and the destination, $h_{se} \sim \mathcal{CN}(0, \bar{\gamma}_{se})$ is the channel coefficient between the source and the eavesdropper, $\mathbf{x}$ is the transmitted signal vector from the source, $\mathbf{n}_d$ and $\mathbf{n}_e$ are the additive white Gaussian noise (AWGN) with zero-mean and variance N_0 at the destination and the eavesdropper,

respectively. After receiving the signals, both the destination and the eavesdropper estimate their channels by the minimum mean-square error (MMSE) estimator and then decode the data. As such, the actual channel coefficient can be denoted as the sum of the estimated channel and the estimation error. According to [25], we have

$$h_{sd} = \hat{h}_{sd} + \tilde{h}_{sd}, \tag{3}$$

$$h_{se} = \hat{h}_{se} + \tilde{h}_{se}, \tag{4}$$

where $\hat{h}_{sd} \sim \mathcal{CN}\left(0, \frac{\rho_p n_p \bar{\gamma}_{sd}^2}{\rho_p n_p \bar{\gamma}_{sd} + N_0}\right)$ is the estimated value of h_{sd}, $\tilde{h}_{sd} \sim \mathcal{CN}\left(0, \frac{\bar{\gamma}_{sd} N_0}{\rho_p n_p \bar{\gamma}_{sd} + N_0}\right)$ is the estimation error of h_{sd}, $\hat{h}_{se} \sim \mathcal{CN}\left(0, \frac{\rho_p n_p \bar{\gamma}_{se}^2}{\rho_p n_p \bar{\gamma}_{se} + N_0}\right)$ is the estimated value of h_{se}, $\tilde{h}_{se} \sim \mathcal{CN}\left(0, \frac{\bar{\gamma}_{se} N_0}{\rho_p n_p \bar{\gamma}_{se} + N_0}\right)$ is the estimation error of h_{se}, and ρ_p is the average power of the pilot symbols.

The destination and the eavesdropper use the estimated channel for information reception. Thus, in the data transmission phase, the received signal vectors at the destination and the eavesdropper are, respectively, rewritten as

$$\mathbf{y}_d = \sqrt{\rho_d}\hat{h}_{sd}\mathbf{x}_d + \sqrt{\rho_d}\tilde{h}_{sd}\mathbf{x}_d + \mathbf{n}_d, \tag{5}$$

$$\mathbf{y}_e = \sqrt{\rho_d}\hat{h}_{se}\mathbf{x}_d + \sqrt{\rho_d}\tilde{h}_{se}\mathbf{x}_d + \mathbf{n}_e, \tag{6}$$

where ρ_d is the average power of the data symbols, and $\mathbf{x}_d$ is the data symbols. The actual instantaneous SNRs for information reception at the destination and the eavesdropper can be, respectively, given by

$$\gamma_{sd} = \frac{\rho_d \left|\hat{h}_{sd}\right|^2}{\rho_d \left|\tilde{h}_{sd}\right|^2 + N_0}, \tag{7}$$

$$\gamma_{se} = \frac{\rho_d \left|\hat{h}_{se}\right|^2}{\rho_d \left|\tilde{h}_{se}\right|^2 + N_0}. \tag{8}$$

We assume that the source uses a fraction α of the total power for data transmission and the remaining $1-\alpha$ portion for channel training, where α is the power allocation factor. Thus, we have

$$\rho_d(n - n_p) = \alpha\rho n, \rho_p n_p = (1-\alpha)\rho n, \tag{9}$$

where ρ is the average power of all the transmitted symbols at the source. Then, the instantaneous SNRs at the destination and the eavesdropper can be, respectively, rewritten as

$$\gamma_{sd} = \frac{\alpha\rho n \left|\hat{h}_{sd}\right|^2}{\alpha\rho n \left|\tilde{h}_{sd}\right|^2 + N_0(n - n_p)}, \tag{10}$$

$$\gamma_{se} = \frac{\alpha\rho n \left|\hat{h}_{se}\right|^2}{\alpha\rho n \left|\tilde{h}_{se}\right|^2 + N_0(n - n_p)}. \tag{11}$$

Since the eavesdropper's estimation error is typically unknown to the source, it is necessary to design a robust approach for the worst-case scenario. That is, there is no estimation error at the eavesdropper. Then, the actual instantaneous SNR at the eavesdropper can be rewritten as

$$\gamma_{se} = \frac{\alpha\rho n |h_{se}|^2}{N_0(n - n_p)}. \tag{12}$$

Based on [8], the achievable secrecy rate of the considered system with the blocklength n and channel training length n_p for a given constraint on the decoding error probability ϵ and a secrecy constraint on the information leakage δ can be approximated as

$$R_s(n, n_p, \epsilon, \delta) = \begin{cases} C_s - \sqrt{\frac{V_{sd}}{n-n_p}} \frac{Q^{-1}(\epsilon)}{\ln 2} - \sqrt{\frac{V_{se}}{n-n_p}} \frac{Q^{-1}(\delta)}{\ln 2}, & \gamma_{sd} > \gamma_{se}, \\ 0, & \gamma_{sd} \leq \gamma_{se}, \end{cases} \tag{13}$$

where $C_s = \log_2(1+\gamma_{sd}) - \log_2(1+\gamma_{se})$ is the secrecy capacity with infinite blocklength, $V_x = 1 - (1+\gamma_x)^{-2}$, $x \in \{sd, se\}$, is the channel dispersion, and $Q^{-1}(\cdot)$ is the inverse Q-function $Q(x) = \int_x^\infty \frac{1}{\sqrt{2\pi}} e^{-\frac{t^2}{2}} dt$.

3. Secrecy Performance Analysis

In this section, we investigate the average secrecy throughput performance of the short-packet communication system with the channel training scheme. Then, we focus on the asymptotic analysis for the average secrecy throughput. Finally, we determine the optimal channel training length to maximize the average secrecy throughput under the reliability constraint and given blocklength.

3.1. Secrecy Throughput Approximation

The secrecy throughput in short-packet communications is defined as the average secrecy rate where the data packet is reliably transmitted subject to a certain secrecy constraint. Mathematically, the average secrecy throughput of the considered system is formulated as

$$T = \mathbb{E}_{\gamma_{sd}, \gamma_{se}} \left(\frac{L}{n-n_p} (1-\epsilon) \right) = \frac{L}{n-n_p} (1-\bar{\epsilon}) \tag{14}$$

where $\bar{\epsilon} = \mathbb{E}_{\gamma_{sd}, \gamma_{se}}(\epsilon)$ is the average decoding error probability. When $\gamma_{sd} > \gamma_{se}$, the decoding error probability at the destination can be characterized by $\epsilon = Q\left(\sqrt{\frac{n-n_p}{V_{sd}}} \left(\ln \frac{1+\gamma_{sd}}{1+\gamma_{se}} - \sqrt{\frac{V_{se}}{n-n_p}} Q^{-1}(\delta) - \frac{L}{n-n_p} \ln 2 \right) \right)$. When $\gamma_{sd} \leq \gamma_{se}$, the achievable secrecy rate is zero and we set $\epsilon = 1$. The average secrecy throughput in (14) can be further derived as

$$T = \frac{L}{n-n_p} \int_0^\infty \Psi(y) f_{\gamma_{se}}(y) dy, \tag{15}$$

where $\Psi(y) = \int_y^\infty \left(1 - \epsilon_{\gamma_{sd}|\gamma_{se}=y}(x)\right) f_{\gamma_{sd}}(x) dx$, $\epsilon_{\gamma_{sd}|\gamma_{se}=y}(\cdot)$ is the conditional decoding error probability conditioned on $\gamma_{se} = y$, and $f_{\gamma_{se}}(y)$ is the probability density function (PDF) of γ_{se}. In order to calculate the double integral in (15), we propose to use the first-order approximation of $\epsilon_{\gamma_{sd}|\gamma_{se}=y}(x)$ as follows

$$\epsilon_{\gamma_{sd}|\gamma_{se}=y}(x) \approx P_{\gamma_{sd}|\gamma_{se}}(x) = \begin{cases} 1, & x < \frac{1}{2k} + x_0, \\ \frac{1}{2} + k(x - x_0), & x \in \left[\frac{1}{2k} + x_0, -\frac{1}{2k} + x_0 \right], \\ 0, & x > -\frac{1}{2k} + x_0, \end{cases} \tag{16}$$

where $x_0 = e^{\sqrt{\frac{V_{se}}{n-n_p}} Q^{-1}(\delta) + \frac{L}{n-n_p} \ln 2} (1+\gamma_{se}) - 1$ and $k = \left. \frac{d\epsilon_{\gamma_{sd}|\gamma_{se}=y}(x)}{dx} \right|_{x=x_0} = -\sqrt{\frac{n-n_p}{2\pi x_0 (x_0+2)}}$.

Based on the fact that $\epsilon_{\gamma_{sd}|\gamma_{se}=y}(x) > 1/2$ when $x < y$, the integral $\Psi(y)$ can be further simplified by changing the lower limit from y to 0. Therefore, we have

$$\begin{aligned}\Psi(y) &\approx \int_0^{\infty} \left(1 - \epsilon_{\gamma_{sd}|\gamma_{se}=y}(x)\right) f_{\gamma_{sd}}(x)dx \\ &\approx 1 - \int_0^{\infty} P_{\gamma_{sd}|\gamma_{se}}(x) f_{\gamma_{sd}}(x)dx \\ &= 1 + k \int_{\frac{1}{2k}+x_0}^{-\frac{1}{2k}+x_0} F_{\gamma_{sd}}(x)dx, \end{aligned} \tag{17}$$

where $F_{\gamma_{sd}}(x)$ and $f_{\gamma_{sd}}(x)$ are respectively the cumulative distribution function (CDF) and PDF of γ_{sd}. It is important to point out that $|k|$ is an increasing function of n. When n is in the moderate blocklength region, i.e., $10^2 \leq n \leq 10^3$, which is really important to short-packet communications, the integral interval $\left[\frac{1}{2k} + x_0, -\frac{1}{2k} + x_0\right]$ is generically small. Therefore, with the help of the first order Riemann integral approximation, we further approximate (17) as

$$\Psi(y) \approx 1 - F_{\gamma_{sd}}(x_0). \tag{18}$$

According to (10) and (12), the CDF of γ_{sd} and the PDF of γ_{se} can be, respectively, formulated as

$$F_{\gamma_{sd}}(x) = 1 - \frac{(1-\alpha)\rho n \bar{\gamma}_{sd}^2 e^{-\frac{xN_0(n-np)\left((1-\alpha)\rho n \bar{\gamma}_{sd} + N_0\right)}{\alpha(1-\alpha)\rho^2 n^2 \bar{\gamma}_{sd}^2}}}{x\bar{\gamma}_{sd}N_0 + (1-\alpha)\rho n \bar{\gamma}_{sd}^2}, \tag{19}$$

and

$$f_{\gamma_{se}}(y) = \frac{N_0(n-n_p)}{\alpha\rho n \bar{\gamma}_{se}} e^{-\frac{yN_0(n-np)}{\alpha\rho n \bar{\gamma}_{se}}}. \tag{20}$$

By applying (18)–(20) into (15), we have

$$\begin{aligned} T &\approx \frac{(1-\alpha)LN_0\bar{\gamma}_{sd}^2}{\alpha\bar{\gamma}_{se}} \int_0^{\infty} \frac{e^{-\left(\frac{x_0(y)N_0(n-np)}{\alpha\rho n\hat{\gamma}_{sd}} + \frac{yN_0(n-np)}{\alpha\rho n\bar{\gamma}_{se}}\right)}}{x_0(y)\bar{\gamma}_{sd}N_0 + (1-\alpha)\rho n\bar{\gamma}_{sd}^2} dy \\ &\approx \frac{(1-\alpha)LN_0\bar{\gamma}_{sd}^2}{\alpha\bar{\gamma}_{se}} \left(\underbrace{\int_0^{M_1} \frac{e^{-\left(\frac{x_0(y)N_0(n-np)}{\alpha\rho n\hat{\gamma}_{sd}} + \frac{yN_0(n-np)}{\alpha\rho n\bar{\gamma}_{se}}\right)}}{x_0(y)\bar{\gamma}_{sd}N_0 + (1-\alpha)\rho n\bar{\gamma}_{sd}^2} dy}_{\Xi_1} \right. \\ &\quad \left. + \underbrace{\int_{M_1}^{\infty} \frac{e^{-\left(\frac{(\varpi_1 y + \varpi_1 - 1)N_0(n-np)}{\alpha\rho n\hat{\gamma}_{sd}} + \frac{yN_0(n-np)}{\alpha\rho n\bar{\gamma}_{se}}\right)}}{(\varpi_1 y + \varpi_1 - 1)\bar{\gamma}_{sd}N_0 + (1-\alpha)\rho n\bar{\gamma}_{sd}^2} dy}_{\Xi_2} \right), \end{aligned} \tag{21}$$

where $\hat{\gamma}_{sd} = \frac{(1-\alpha)\rho n\bar{\gamma}_{sd}^2}{(1-\alpha)\rho n\bar{\gamma}_{sd} + N_0}$, $\varpi_1 = e^{\frac{Q^{-1}(\delta)}{\sqrt{n-np}} + \frac{L}{n-np}\ln 2}$ and M_1 is a sufficiently large parameter to ensure $V_{se} \approx 1$ when $\gamma_{se} > M_1$.

By leveraging Gaussian-Chebyshev quadrature, the integral Ξ_1 can be approximated as

$$\Xi_1 \approx \frac{M_1}{2} \sum_{m=1}^{M_2} \left(\frac{\pi}{M_2} f\left(\frac{M_1}{2}(t_m + 1)\right) \sqrt{1 - t_m^2} \right), \tag{22}$$

where M_2 is a parameter for the complexity accuracy tradeoff, $f(z) = \frac{e^{-\left(\frac{x_0(z)N_0(n-np)}{\alpha\rho n\hat{\gamma}_{sd}} + \frac{zN_0(n-np)}{\alpha\rho n\bar{\gamma}_{se}}\right)}}{x_0(z)\bar{\gamma}_{sd}N_0 + (1-\alpha)\rho n\bar{\gamma}_{sd}^2}$ with $x_0(z) = x_0|_{\gamma_{se}=z}$, and $t_m = \cos\left(\frac{2m-1}{2M_2}\pi\right)$.

According to [26] (3.352.2), the integral Ξ_2 can be derived as

$$\Xi_2 = -\frac{e^{\varpi_2\varpi_3 - \frac{(\varpi_1-1)N_0(n-n_p)}{\alpha\rho n\bar{\gamma}_{sd}}}}{\varpi_1\bar{\gamma}_{sd}N_0} Ei(-M_1\varpi_2 - \varpi_2\varpi_3), \tag{23}$$

where $Ei(\cdot)$ is the exponential integral function, $\varpi_2 = \frac{\varpi_1 N_0(n-n_p)}{\alpha\rho n\bar{\gamma}_{sd}} + \frac{N_0(n-n_p)}{\alpha\rho n\bar{\gamma}_{se}}$ and $\varpi_3 = \frac{(\varpi_1-1)N_0+(1-\alpha)\rho n\bar{\gamma}_{sd}}{\varpi_1 N_0}$.

The average secrecy throughput of the considered system with short-packet communications can be directly obtained by substituting (22) together with (23) into (21).

3.2. High SNR Regime

To further characterize the impact of key system parameters on the average secrecy throughput, we focus on the asymptotic average secrecy throughput in the high SNR regime, where the average transmit power ρ at the source approaches infinity. When $\rho \to \infty$, we know that the estimation error approaches zero and $\mathbb{E}(\gamma_{se})$ approaches infinity. According to (21), the average secrecy throughput in the high SNR regime of the considered system with finite blocklength can be simplified as

$$T^{\rho\to\infty} = \frac{L}{n-n_p}(1-\bar{\epsilon}^{\rho\to\infty}), \tag{24}$$

where $\bar{\epsilon}^{\rho\to\infty} = 1 - \frac{(\alpha-1)(n-n_p)\bar{\gamma}_{sd}}{\alpha\varpi_1\bar{\gamma}_{se}} e^{\frac{(1-\alpha)(n-n_p)}{\alpha}\left(1+\frac{\bar{\gamma}_{sd}}{\varpi_1\bar{\gamma}_{se}}\right)} Ei\left(\frac{(\alpha-1)(n-n_p)}{\alpha}\left(1+\frac{\bar{\gamma}_{sd}}{\varpi_1\bar{\gamma}_{se}}\right)\right)$. An important observation from (24) is that the average decoding error probability cannot reduce to zero even when the transmit power at the source approaches infinity. This is because not only the destination but also the eavesdropper will benefit from increasing the transmit power. Moreover, we know that the average secrecy throughput in the high SNR regime is dependent on the power allocation factor between channel training and data transmission.

3.3. The Class Case with Infinite Blocklength

To further understand the connection between finite blocklength and infinite blocklength, we turn our attention to the classical case with infinite blocklength. When $N \to \infty$, we know that $\epsilon \to 0$ as long as $\gamma_{sd} > \gamma_{se}$ (otherwise $\epsilon \to 1$). Thus, the average secrecy throughput of the considered system with infinite blocklength can be expressed as

$$\begin{aligned} T^{n\to\infty} &= \frac{L}{n-n_p}\Pr(\gamma_{sd} > \gamma_{se}), \\ &= \frac{L\bar{\gamma}_{sd}(\alpha-1)}{\alpha\bar{\gamma}_{se}} e^{\left(\frac{1}{\bar{\gamma}_{sd}} + \frac{1}{\bar{\gamma}_{se}} + \frac{N_0}{(1-\alpha)\rho n\bar{\gamma}_{sd}^2}\right)} \\ &\quad \times e^{\frac{(1-\alpha)(n-n_p)\bar{\gamma}_{sd}}{\alpha}} Ei\left(\frac{(\alpha-1)(n-n_p)\bar{\gamma}_{sd}}{\alpha}\right. \\ &\quad \left.\left(\frac{1}{\bar{\gamma}_{sd}} + \frac{1}{\bar{\gamma}_{se}} + \frac{N_0}{(1-\alpha)\rho n\bar{\gamma}_{sd}^2}\right)\right). \end{aligned} \tag{25}$$

From (25), it is worth noting that $T^{n\to\infty} \to 0$ due to the fact that $e^x Ei(-x) \to 0$ as $x \to \infty$. This is because the transmission rate $\frac{L}{n-n_p} \to 0$ as $n \to \infty$. However, when $\gamma_{sd} > \gamma_{se}$, the secrecy capacity of the considered system is not zero.

3.4. Optimal Transmission Design

To maximize the average secrecy throughput, the designers have to choose the suitable channel training length in a coherence slot. This is due to the fact that the channel estimation

becomes more accurate and the destination can decode more information bits reliably as the channel training length increases. However, this will reduce the duration for data transmission at the same time, which leads to the degradation of the average secrecy throughput. The optimization of n_p maximizing the average secrecy throughput under the reliability constraint and given blocklength can be formulated as

$$\max_{n_p} \quad T, \tag{26a}$$

$$s.t. \quad \bar{\epsilon} \leq \epsilon_{\max}, \tag{26b}$$

$$0 \leq n_p \leq n, \tag{26c}$$

$$n_p \in \mathbb{N}^+, \tag{26d}$$

where $\mathbb{N}^+$ denotes the non-negative integer set and (26b) denotes the system's reliability constraint.

In the following, we show that $\bar{\epsilon}$ is a convex increasing function of n_p and T is a quasi-concave function of n_p. Based on the Leibniz integral rule, the monotonicity of $\bar{\epsilon}$ with respect to n_p is consistent with that of ϵ with respect to n_p. Taking the first and second derivative of ϵ on n_p, we have

$$\frac{\partial \epsilon}{\partial n_p} = \frac{\partial \epsilon}{\partial \phi} \frac{\partial \phi}{\partial n_p}, \tag{27}$$

and

$$\frac{\partial^2 \epsilon}{\partial n_p^2} = \frac{\partial^2 \epsilon}{\partial \phi^2} \left(\frac{\partial \phi}{\partial n_p} \right)^2 + \frac{\partial \epsilon}{\partial \phi} \frac{\partial^2 \phi}{\partial n_p^2} \tag{28}$$

where $\phi = \sqrt{\frac{n-n_p}{V_{sd}}} \left(\ln \frac{1+\gamma_{sd}}{1+\gamma_{se}} - \sqrt{\frac{V_{se}}{n-n_p}} Q^{-1}(\delta) - \frac{L}{n-n_p} \ln 2 \right)$. For short-packet communications, ϵ is generally much smaller than 0.5. Hence, 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 need to check the sign of $\frac{\partial \phi}{\partial n_p}$ and $\frac{\partial^2 \phi}{\partial n_p^2}$. To facilitate analysis, we approximate $V_{sd} = V_{se} \approx 1$ and $\ln \frac{1+\gamma_{sd}}{1+\gamma_{se}} \approx \ln \frac{\gamma_{sd}}{\gamma_{se}} \approx \ln \frac{|h_{sd}|^2}{|h_{se}|^2}$, which is very accurate in the high SNR regime [8]. Then, we have $\frac{\partial \phi}{\partial n_p} = -\frac{(n-n_p) \ln \left(|h_{sd}|^2 / |h_{se}|^2 \right) + L \ln 2}{2(n-n_p)^{3/2}} < 0$ and $\frac{\partial^2 \phi}{\partial n_p^2} = -\frac{(n-n_p) \ln \left(|h_{sd}|^2 / |h_{se}|^2 \right) + 3L \ln 2}{4(n-n_p)^{5/2}} < 0$. Therefore, we state that $\bar{\epsilon}$ is a convex increasing function of n_p and T is a quasi-concave function of n_p.

When $\left. \frac{\partial T}{\partial n_p} \right|_{n_p=0} \leq 0$, the optimal channel training length for problem (26) is given by

$$n_p^* = 0. \tag{29}$$

When $\left. \frac{\partial T}{\partial n_p} \right|_{n_p=0} > 0$, the optimal channel training length for problem (26) is given by

$$n_p^* = \begin{cases} \arg \max_{n_p \in \{\lceil n_p^\# \rceil, \lfloor n_p^\# \rfloor\}} T, & n_p^\# < \min\left(\left\lceil n_p^o \right\rceil, n \right), \\ \min\left(\left\lceil n_p^o \right\rceil, n \right), & n_p^\# \geq \min\left(\left\lceil n_p^o \right\rceil, n \right). \end{cases} \tag{30}$$

where $n_p^\#$ is the solution of $\frac{\partial T}{\partial n_p} = 0$, n_p^o is the solution of $\bar{\epsilon} = \epsilon_{\max}$, and $\lceil \cdot \rceil$ and $\lfloor \cdot \rfloor$ are the ceiling and floor operations, respectively.

Proof. We first relax the integer constraint in problem (26). Then, the optimal channel training length can be derived directly from the fact that $\bar{\epsilon}$ is a convex increasing function of n_p and T is a quasi-concave function of n_p. □

4. Numerical Results

In this section, we provide simulation and numerical results to demonstrate how the key system parameters, i.e., channel training length and blocklength, impact the average secrecy throughput of the considered system. Unless otherwise stated, the system parameter settings are as follows: $L = 200$, $\delta = 10^{-2}$, $N_0 = 1$, $M_1 = 10$ and $M_2 = 20$.

Figure 2 shows the average secrecy throughput versus the average transmit power with different channel training length. We first observe that the approximation results in (21) coincide well with the Monte-Carlo simulation points, which corroborates the accuracy of the analytical expressions. Second, we observe that the average secrecy throughput increases as the average transmit power increases, and then converges to a constant when the average transmit power is sufficiently large. This is due to the fact that the average secrecy throughput is independent of the average transmit power in the high SNR regime according to (24). Moreover, we observe that the channel training length is not better when the blocklength is fixed.

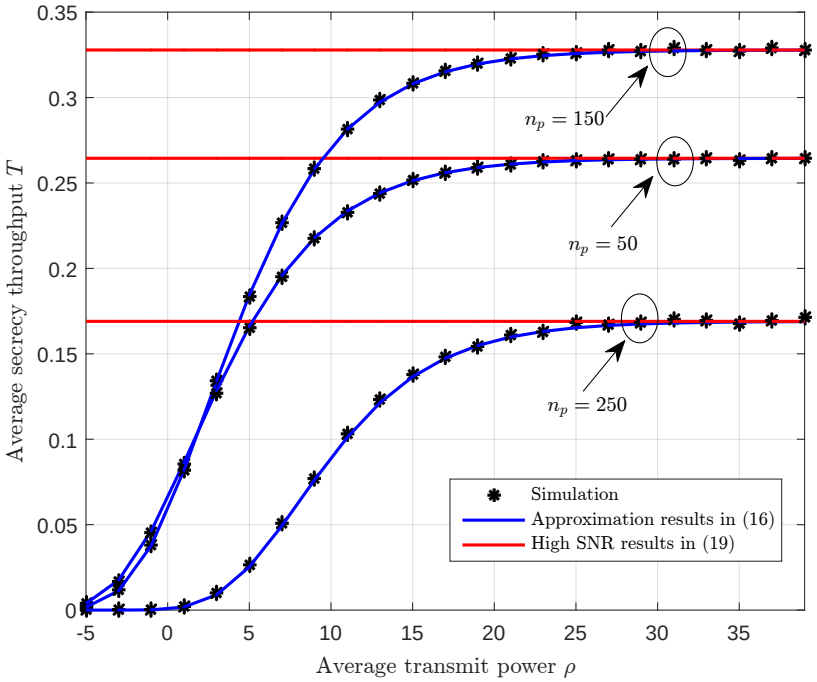

Figure 2. The average secrecy throughput T versus the average transmit power ρ with different channel training length n_p, where $\alpha = 0.5$, $n = 300$, $\bar{\gamma}_{sd} = 0$ dB, and $\bar{\gamma}_{se} = 0$ dB.

Figure 3 depicts the average secrecy throughput versus the power allocation factor with different channel training length. We observe that the average secrecy throughput increases as the power allocation factor increases from 0 to an optimal value but later, it starts decreasing as the power allocation factor increases from its optimal value. This can be explained as follows. When the power allocation factor is too small, there is less power available for data transmission, which, of course, will result in poor average secrecy throughput. When the power allocation factor is too large, there is less power available for channel training which, consequently, also leads to poor average secrecy throughput. Although an explicit solution for the optimal power allocation factor is intractable due to the complexity of the average secrecy throughput expression, the solution can be obtained offline by numerical search methods, for example, the gradient-based search method.

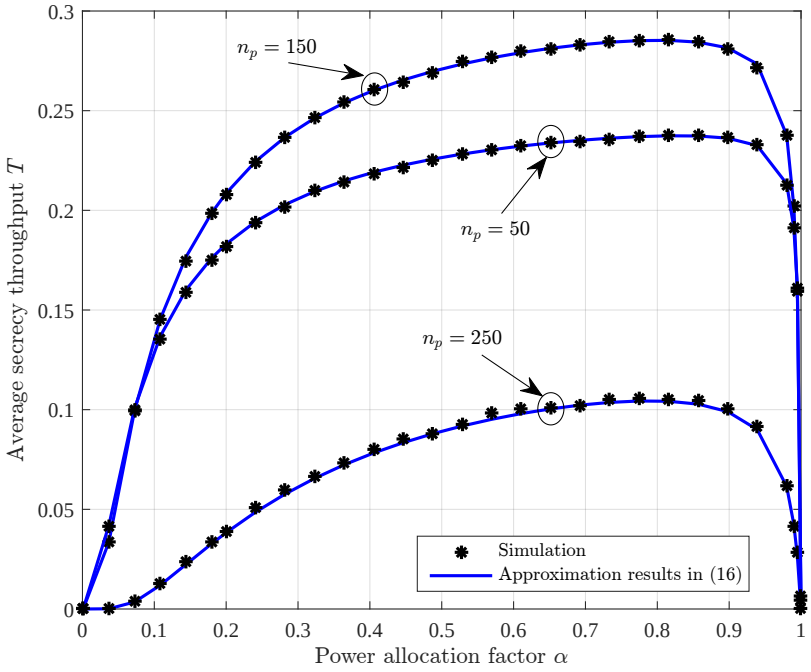

Figure 3. The average secrecy throughput T versus the power allocation factor α with different channel training length n_p, where $n = 300$, $\rho = 10$ dB, $\bar{\gamma}_{sd} = 0$ dB, and $\bar{\gamma}_{se} = 0$ dB.

Figure 4 demonstrates that the optimal channel training length can significantly improve the average secrecy throughput of the considered system. To obtain comparable results, we provide the following channel training transmission schemes: (1) Fixed-ratio channel training length, in which the channel training length $n_p = 0.5n$ is fixed; (2) Fixed channel training length, in which the channel training length $n_p = 20$ is fixed. It is clear that the average secrecy throughput with the optimal channel training is superior to the two benchmark schemes mentioned above, which implies that the average secrecy throughput of the considered system can be significantly improved via optimizing the channel training length.

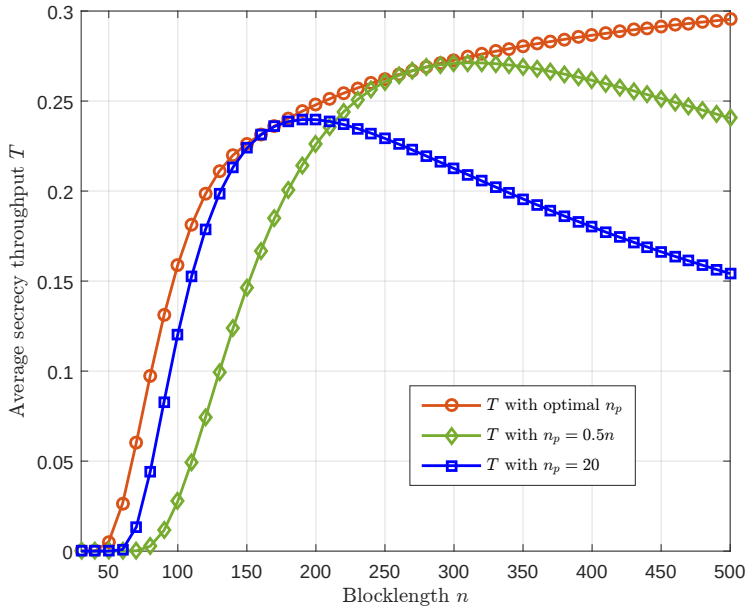

Figure 4. The average secrecy throughput T versus the blocklength n with $\alpha = 0.5$, $\rho = 10$ dB, $\bar{\gamma}_{sd} = 0$ dB, and $\bar{\gamma}_{se} = 0$ dB, where the optimal channel training length is obtained without reliability constraint.

Figure 5 depicts the optimal channel training length versus the blocklength with different values of δ. We observe that the optimal channel training length that maximizes the average secrecy throughput increases with the increase of the blocklength. Moreover, from Figure 4, one can observe that the average secrecy throughput with the optimal channel training length increases as the blocklength increases. Thus, we can conclude that when the transmission latency constraint is loose, it is favorable to allocate more channel uses for channel estimation to mitigate the decoding error.

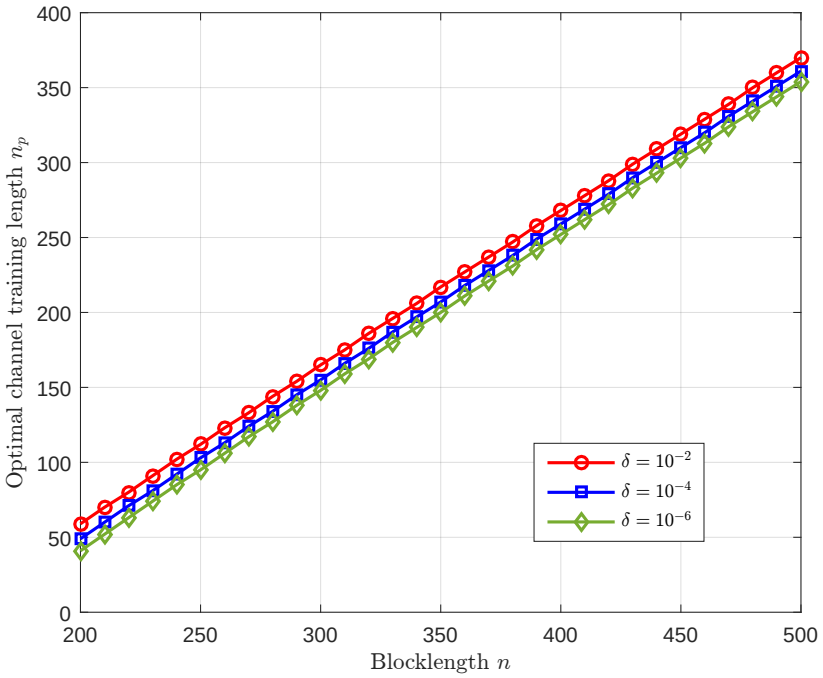

Figure 5. The optimal channel training length n_p versus the blocklength n with $\alpha = 0.5$, $\rho = 10$ dB, $\bar{\gamma}_{sd} = 0$ dB, and $\bar{\gamma}_{se} = 0$ dB, where the optimal channel training length is obtained without reliability constraint.

Figure 6 plots the optimal channel training length versus the average transmit power with different values of δ. We first observe that for a fixed δ, the optimal channel training length increases as the average transmit power increases. Moreover, we also observe that for a fixed average transmit power, the optimal channel training length increases as δ increases. This is because when either the average transmit power or the tolerance of the information leakage δ increases, the probability of decoding error decreases and the optimal channel training length becomes larger in order to support higher transmission rate.

Figure 7 plots the average secrecy throughput versus the channel training length with different values of $\epsilon_{\max}$. We first observe that strengthening the reliability constraint, i.e., reducing $\epsilon_{\max}$, decreases the average secrecy throughput. We further observe that the optimal channel training length maximizing the average secrecy throughput depends on the value of $\epsilon_{\max}$. In particular, when $\epsilon_{\max}$ is small, the average secrecy throughput monotonically increases as the channel training length increases, such that the optimal channel training length is at the right boundary. When $\epsilon_{\max}$ becomes larger, the average secrecy throughput first increases and then decreases as the channel training length increases, and the optimal channel training length is the one from $\left\{ \left\lceil \frac{\partial T}{\partial n_p} = 0 \right\rceil, \left\lfloor \frac{\partial T}{\partial n_p} = 0 \right\rfloor \right\}$ that yields the largest average secrecy throughput.

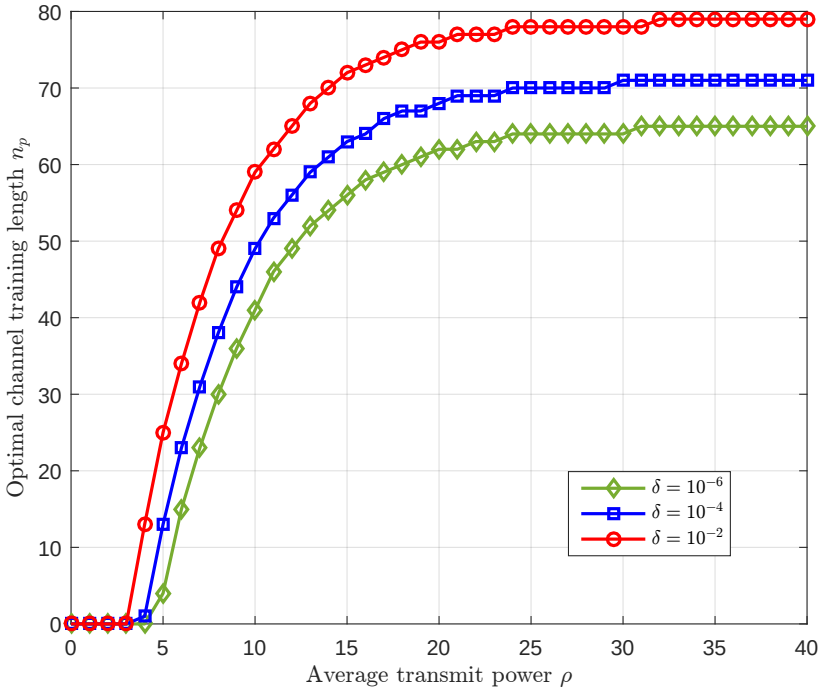

Figure 6. The optimal channel training length n_p versus the average transmit power ρ with $\alpha = 0.5$, $n = 200$, $\bar{\gamma}_{sd} = 0$ dB, and $\bar{\gamma}_{se} = 0$ dB, where the optimal channel training length is obtained without reliability constraint.

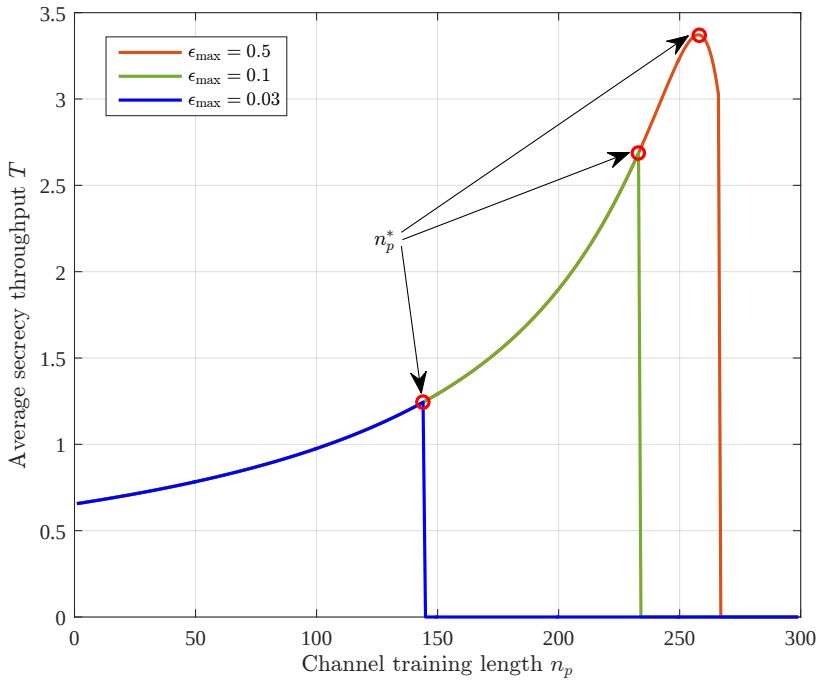

Figure 7. The average secrecy throughput T versus the channel training length n_p under the reliability constraint, where $\alpha = 0.5$, $n = 300$, $\rho = 10$ dB, $\bar{\gamma}_{sd} = 20$ dB, and $\bar{\gamma}_{se} = 0$ dB.

5. Conclusions

In this paper, we investigated the average secrecy throughput of a short-packet communication system with a two-phase training-based transmission scheme. Based on the finite blocklength information theory, the average secrecy throughput has been approximated in closed-form, which quantitatively reveals the impact of channel training length

on the the tradeoff between reliability and transmission latency under a secrecy constraint. In addition, we also derived simple asymptotic results for the average secrecy throughput to offer valuable insights into practical design. Finally, the optimal channel training length under the reliability constraint and given blocklength was obtained, and the simulation results demonstrated that the performance gain achieved by the optimal channel training length is remarkable, relative to the fixed-ratio channel training length and fixed channel training length schemes.

Author Contributions: D.C., J.L., J.H. and X.Z. conceived the main proposal of the secure transmission schemes. D.C. and J.L. wrote the original draft. J.H., X.Z. and S.Z. supervised the analysis and numerical simulation of the proposed schemes, reviewed and edited the manuscript. 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.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors extend their gratitude to the anonymous reviewers for their valuable and constructive comments, which have largely improved and clarified this paper.

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

References

1. Parvez, I.; Rahmati, A.; Guvenc, I.; Sarwat, A.I.; Dai, H. A Survey on Low Latency Towards 5G: RAN, Core Network and Caching Solutions. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3098–3130. [CrossRef]
2. Durisi, G.; Koch, T.; Popovski, P. Toward Massive, Ultrareliable, and Low-Latency Wireless Communication with Short Packets. *Proc. IEEE* **2016**, *104*, 1711–1726. [CrossRef]
3. Feng, D.; She, C.; Ying, K.; Lai, L.; Hou, Z.; Quek, T.Q.S.; Li, Y.; Vucetic, B. Toward Ultrareliable Low-Latency Communications: Typical Scenarios, Possible Solutions, and Open Issues. *IEEE Veh. Technol. Mag.* **2019**, *14*, 94–102. [CrossRef]
4. Ashraf, S.A.; Aktas, I.; Eriksson, E.; Helmersson, K.W.; Ansari, J. Ultra-Reliable and Low-Latency Communication for Wireless Factory Automation: From LTE to 5G. In Proceedings of the 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation, Berlin, Germany, 6–9 September 2016.
5. Polyanskiy, Y.; Poor, H.V.; Verdu, S. Channel Coding Rate in the Finite Blocklength Regime. *IEEE Trans. Inf. Theory* **2010**, *56*, 2307–2359. [CrossRef]
6. 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]
7. 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]
8. Wang, H.M.; Yang, Q.; Ding, Z.; Poor, H.V. Secure Short-Packet Communications for Mission-Critical IoT Applications. *IEEE Trans. Wireless Commun.* **2019**, *18*, 2565–2578. [CrossRef]
9. Ren, H.; Pan, C.; Deng, Y.; Elkashlan, M.; Nallanathan, A. Resource Allocation for Secure URLLC in Mission-Critical IoT Scenarios. *IEEE Trans. Wireless Commun.* **2020**, *68*, 5793–5807. [CrossRef]
10. 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]
11. Zou, Y.; Zhu, J.; Wang, X.; Hanzo, L. A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *Proc. IEEE* **2016**, *104*, 1727–1765. [CrossRef]
12. Yang, W.; Schaefer, R.F.; Poor, H.V. Wiretap channels: Nonasymptotic fundamental limits. *IEEE Trans. Inf. Theory* **2019**, *65*, 4069–4093. [CrossRef]
13. Feng, C.; Wang, H.M.; Poor, H.V. Reliable and Secure Short-Packet Communications. *IEEE Trans. Wirel. Commun.* **2022**, *21*, 1913–1926. [CrossRef]

14. 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]
15. 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]
16. 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]
17. 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]
18. 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]
19. 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]
20. 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]
21. Xie, Y.; Ren, P.; Xu, D.; Li, Q. Security and Reliability Performance Analysis for URLLC With Randomly Distributed Eavesdroppers. In Proceedings of the 2021 IEEE International Conference on Communications Workshops (ICC Workshops), Montreal, QC, Canada, 14–23 June 2021.
22. 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]
23. Li, C.; Yang, N.; Yan, S. Optimal Transmission of Short-Packet Communications in Multiple-Input Single-Output Systems. *IEEE Trans. Veh. Technol.* **2019**, *68*, 7199–7203. [CrossRef]
24. Lee, B.; Park, S.; Love, D.J.; Ji, H.; Shim, B. Packet Structure and Receiver Design for Low Latency Wireless Communications with Ultra-Short Packets. *IEEE Trans. Commun.* **2018**, *66*, 796–807. [CrossRef]
25. Gursoy, M.C. On the capacity and energy efficiency of training-based transmissions over fading channels. *IEEE Trans. Inf. Theory* **2009**, *55*, 4543–4567. [CrossRef]
26. Gradshteyn, I.S.; Ryzhik, I.M. *Tables of Integrals, Series, and Products*, 7th ed.; Academic Press, Inc.: Cambridge, MA, USA, 2007.