He *et al. J Wireless Com Network* (2021) 2021:29
https://doi.org/10.1186/s13638-020-01862-7

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Secrecy analysis of short-packet transmissions in ultra-reliable and low-latency communications

Jianhua He[1,2,3*], Guangheng Zhao[3], Lu Wang[3], Xue Sun[1] and Lei Yang[3]

*Correspondence: hejianhua@csu.ac.cn
[3] Technology and Engineering Center for Space Utilization, Chinese Academy of Sciences, Beijing 100094, China
Full list of author information is available at the end of the article

Abstract

In this paper, we investigate the secrecy performance of short-packet transmissions in ultra-reliable and low-latency communications (URLLC). We consider the scenario where a multi-antenna source communicates with a single-antenna legitimate receiver requiring ultra-high reliability and low latency, in the presence of a single-antenna eavesdropper. In order to safeguard URLLC, the source transmits the artificial noise (AN) signal together with the confidential signal to confuse the eavesdropper. We adopt a lower bound on the maximal secrecy rate as the secrecy performance metric for short-packet transmissions in URLLC, which takes the target decoding error probabilities at the legitimate receiver and the eavesdropper into account. Using this metric, we first derive a compact expression of the generalized secrecy outage probability (SOP). Then, we formally prove that the generalized SOP is a convex function with respect to the power allocation factor between the confidential signal and the AN signal. We further determine the optimal power allocation factor that minimizes the generalized SOP. The results presented in this work can be useful for designing new secure transmission schemes for URLLC.

Keywords: Ultra-reliable and low-latency communications, Physical layer security, Short-packet transmissions

1 Introduction

Supporting ultra-reliable and low-latency communications (URLLC) is one of the major goals in the fifth generation (5G) and future wireless networks [1, 2], due to the requirements of various emerging applications, such as smart city, mission-critical internet-of-things, and vehicle-to-vehicle communications [3, 4]. However, the complicated propagation environment (e.g., path loss, shadowing, and fast fading) in wireless networks makes it very difficult to satisfy the strict quality-of-service (QoS) requirements on end-to-end (E2E) delay (e.g., 1 ms) and reliability (e.g., 10^{-7} packet loss probability) [5]. Against this background, significant research efforts have been devoted to fulfill the QoS requirements of URLLC in wireless networks [6–10].

On the other hand, security is another pivotal issue in URLLC, while so far has drawn little attention. Traditionally, security in wireless communications is achieved through

key-based cryptographic techniques applied on upper layers. However, with the development of wireless technology, the size of wireless networks has been expanding rapidly over the past decades, which makes the key generation, distribution, and management prohibitively expensive [11]. To tackle this problem, physical layer security has been proposed as an alternative for traditional key-based cryptography techniques, since it can ensure secure data transmissions by exploiting physical properties of wireless channels without using secret keys. Subsequently, enhancing physical layer security in wireless networks has been intensively examined [12].

However, it is very challenging to ensure the security of URLLC with the existing physical layer security techniques. This is mainly because how to evaluate the secrecy performance of URLLC remains an open problem. Specifically, the existing physical layer security schemes are commonly designed based on the classical information-theoretic secrecy,[1] the key assumption of which is that the transmissions can be error-free and the information leaked to the eavesdropper vanishes as the blocklength of channel codes goes to infinity. This assumption enables the use of secrecy performance metrics, such as the achievable secrecy rate and the secrecy outage probability (SOP), to characterize the secrecy performance of wireless communication systems. However, in URLLC, the blocklength of channel codes is short, which means the transmissions are no longer error-free and the information leaked to the eavesdropper cannot be vanished. It follows that the classical information-theoretic secrecy is not achievable, and thereby the secrecy performance metrics commonly adopted in the existing physical layer security schemes cannot be utilized to characterize the secrecy performance of URLLC.

Motivated by these observations, most recently, physical layer security of short-packet transmissions in URLLC has been receiving increasing research attention [13, 14]. In [13], a bound on the equivocation rate of relay wiretap channels with finite blocklength was derived, assuming that the eavesdropper can decode its received signal with an arbitrary small number of errors, which is less likely to be valid in practice. In [14], the secrecy throughput of URLLC was investigated, and the optimal block length that maximizes the secrecy throughput was examined. Different from [13, 14], in this work, we take both the decoding error probability at the legitimate receiver and the decoding error probability at the eavesdropper into consideration, and adopt a lower bound on the maximal secrecy rate of short-packet transmissions in URLLC derived in [15, 16] as the performance metric. Utilizing this metric, we derive the generalized SOP that the lower bound is less than a certain threshold. Moreover, we consider that the source transmits the artificial noise (AN) signal together with the confidential signal, and show how the secrecy performance of URLLC can be enhanced by judiciously selecting the power allocation factor between the confidential signal and the AN signal.

2 Methods

2.1 System model

We consider URLLC in a wiretap channel, where an N_s-antenna source transmits to a single-antenna legitimate receiver with ultra-high reliability and low latency, in the presence

[1] In this paper, we refer the term "classical information-theoretic secrecy" to as Shannon's weak secrecy only.

of a single-antenna eavesdropper. We denote $\mathbf{h}_{\mathrm{sr}}$ and $\mathbf{h}_{\mathrm{se}}$ as the $1 \times N_{\mathrm{s}}$ channel vectors from the source to the legitimate receiver and from the source to the eavesdropper, respectively. We assume that all the channels are subject to quasi-static independent and identical (i.i.d) Rayleigh fading with a finite blocklength L, i.e., the channels remain the same within a fading block. We further assume that the source can acquire the instantaneous channel state information (CSI) of the main channel from the source to the legitimate receiver through training-based channel estimation, while only statistical CSI from the eavesdropper is known to the source.

To safeguard URLLC, the source transmits the AN signal together with the confidential signal in order to confuse the eavesdropper. As such, the transmitted signal at the source can be expressed as

$$\mathbf{x}_{\mathrm{s}} = \mathbf{w}_{\mathrm{s}} t_{\mathrm{s}} + \mathbf{W}_{\mathrm{AN}} \mathbf{t}_{\mathrm{AN}}, \tag{1}$$

where $\mathbf{w}_{\mathrm{s}}$ denotes the $N_{\mathrm{s}} \times 1$ vector used for transmitting the confidential signal scalar t_{s}, and $\mathbf{W}_{\mathrm{AN}}$ denotes the $N_{\mathrm{s}} \times (N_{\mathrm{s}} - 1)$ matrix used for transmitting the AN signal vector $\mathbf{t}_{\mathrm{AN}}$. We define α, $0 < \alpha \leq 1$, as the fraction of power allocated for transmitting the confidential signal. Then, we have $\mathbb{E}\left[|t_{\mathrm{s}}|^2\right] = \alpha$ and $\mathbb{E}\left[t_{\mathrm{AN}} t_{\mathrm{AN}}^H\right] = \frac{1-\alpha}{N_{\mathrm{s}}-1} \mathbf{I}_{N_{\mathrm{s}}-1}$. In addition, we choose $\mathbf{w} = \frac{\mathbf{h}_{\mathrm{sr}}^H}{\|\mathbf{h}_{\mathrm{sr}}\|}$ and $\mathbf{W}_{\mathrm{AN}}$ as the projection matrix into the null space of $\mathbf{h}_{\mathrm{sr}}$. By doing so, the link quality of the eavesdropper can be degraded, while the link quality of the legitimate receiver is not affected.

Based on (1), we express the received signals at the legitimate receiver and the eavesdropper, respectively, as

$$y_b = \sqrt{P_{\mathrm{s}} d_{\mathrm{sr}}^{-\eta}} \mathbf{h}_{\mathrm{sr}} \mathbf{w}_{\mathrm{s}} t_{\mathrm{s}} + n_b, \tag{2}$$

$$y_e = \sqrt{P_{\mathrm{s}} d_{\mathrm{se}}^{-\eta}} \mathbf{h}_{\mathrm{se}} \mathbf{w}_{\mathrm{s}} t_{\mathrm{s}} + \sqrt{P_{\mathrm{s}} d_{\mathrm{se}}^{-\eta}} \mathbf{h}_{\mathrm{se}} \mathbf{W}_{\mathrm{AN}} \mathbf{t}_{\mathrm{AN}} + n_e, \tag{3}$$

where P_{s} denotes the transmit power of the source, d_{sr} and d_{se} denote the distance from the source to the legitimate receiver and the distance from the source to the eavesdropper, respectively, η denotes the path loss exponent, n_b and n_e denotes the thermal noise at the legitimate receiver and the eavesdropper, respectively, which are assumed to be complex Gaussian distributed random variables with zero mean and variances σ_b^2 and σ_e^2.

According to (2) and (3), we now characterize the achievable rates of the legitimate receiver and the eavesdropper. Note that, due to the short-packet transmissions in URLLC, it is difficult to obtain the closed-form expressions of the achievable rates of the legitimate receiver and the eavesdropper. However, they can be accurately approximated, respectively, as [17]

$$R_{\mathrm{sr}} \approx C(\gamma_{\mathrm{sr}}) - \sqrt{\frac{V(\gamma_{\mathrm{sr}})}{L}} f_{\mathrm{Q}}^{-1}(\varepsilon_{\mathrm{sr}}) \text{ bits/s/Hz}, \tag{4}$$

$$R_{\mathrm{se}} \approx C(\gamma_{\mathrm{se}}) - \sqrt{\frac{V(\gamma_{\mathrm{se}})}{L}} f_{\mathrm{Q}}^{-1}(\varepsilon_{\mathrm{se}}) \text{ bits/s/Hz}, \tag{5}$$

where $C(\gamma) = \log_2(1+\gamma)$ and $V(\gamma) = (\log_2(e))^2(1 - 1/(1+\gamma)^2)$, $\varepsilon_{\mathrm{sr}}$ and $\varepsilon_{\mathrm{se}}$ denotes the target decoding error probabilities of the legitimate receiver and the eavesdropper, respectively, and f_{Q}^{-1} denotes the inverse Q-function. In (4) and (5), $\gamma_{\mathrm{sr}} = \alpha\overline{\gamma}_{\mathrm{sr}}\|\mathbf{h}_{\mathrm{sr}}\|^2$ and $\gamma_{\mathrm{se}} = \frac{\alpha\overline{\gamma}_{\mathrm{se}}\|\mathbf{h}_{\mathrm{se}}\mathbf{w}_{\mathrm{s}}\|^2}{\frac{1-\alpha}{N_{\mathrm{s}}-1}\overline{\gamma}_{\mathrm{se}}\|\mathbf{h}_{\mathrm{sr}}\mathbf{W}_{\mathrm{AN}}\|^2+1}$, where $\overline{\gamma}_{\mathrm{sr}} = P_{\mathrm{s}}d_{\mathrm{sr}}^{-\eta}/\sigma_b^2$ and $\overline{\gamma}_{\mathrm{se}} = P_{\mathrm{s}}d_{\mathrm{se}}^{-\eta}/\sigma_e^2$.

The source needs to transmit a packet with b_r bits to the legitimate receiver with transmission delay τ, which equals to the transmission duration. In addition, the decoding error probability at the legitimate receiver should not exceed $\varepsilon_{\max}$ such that the legitimate receiver's requirement on the reliability can be satisfied. As such, we have

$$\tau W R_{\mathrm{sr}} \geq b_r, \tag{6}$$

where W denotes the bandwidth for data transmission. Substituting (4) into (6), we obtain that, in order to fulfill the requirements of URLLC on the decoding error probability and the latency at the legitimate receiver, the average SNR in the main channel should satisfy

$$\overline{\gamma}_{\mathrm{sr}} \geq \frac{1}{\|\mathbf{h}_{\mathrm{sr}}\|^2}\left(2^{\Psi(b_r,\varepsilon_{\mathrm{sr}},L)} - 1\right), \tag{7}$$

where $\Psi(b_r, \varepsilon_{\mathrm{sr}}, L) = \left(\frac{b_r}{L} + \frac{f_{\mathrm{Q}}^{-1}(\varepsilon_{\mathrm{sr}})}{\ln 2\sqrt{L}}\right)$. In (7), we apply the equality that $\tau W = L$ and the approximation that $V(\gamma_{\mathrm{sr}}) \approx \frac{1}{\ln 2}$ when γ_{sr} is relatively large (e.g., $\gamma_{\mathrm{sr}} = 10$ dB), which can be easily achieved in wireless networks for supporting URLLC. According to (7), the source needs to adaptively adjust its transmit power based on the small-scale fading in the main channel such that URLLC can be supported.

2.2 Secrecy performance analysis

In this section, we characterize the secrecy performance of URLLC in our system. Specifically, we first derive a lower bound on the maximal secrecy rate. Based on the derived lower bound, we then derive the generalized SOP of our system.

2.2.1 Secrecy performance metrics for URLLC

In this subsection, we first elaborate more on why classical information-theoretic secrecy cannot be used to evaluate the level of secrecy in URLLC. We assume that the confidential message $\mathcal{M}$ is encoded into $\mathcal{X}^L$ at the source. We denote $\mathcal{Y}^L$ and $\mathcal{Z}^L$ as the received messages at the legitimate receiver and the eavesdropper, respectively. According to [18, 19], in order to achieve secure transmission, a wiretap code with parameter pair (R_b, R_s) needs to be used, where R_b and R_s denote the transmission rate of $\mathcal{X}^L$ and the target secrecy rate. In addition, we note that $R_b - R_s$ denotes the redundancy rate of the wiretap code, representing the cost of preventing the confidential message $\mathcal{M}$ from being eavesdropped. By using the wiretap code, classical information-theoretic secrecy can be achieved when 1) the message $\mathcal{M}$ is correctly decoded at the legitimate receiver,

i.e., $R_b \leq I\left(\mathcal{M}; \mathcal{Y}^L\right)$, where $I(X; Y)$ denotes the mutual information between X and Y, and the information leakage to the eavesdropper vanishes for infinite blocklength, i.e.,

$$\lim_{L\to\infty} \frac{1}{L} I\left(\mathcal{M}; \mathcal{Z}^L\right) = 0. \tag{8}$$

However, in URLLC, the blocklength L is short. As a result, the confidential message $\mathcal{M}$ cannot be decoded at the legitimate receiver with an arbitrary small number of errors and the information leakage to the eavesdropper cannot be vanished. It follows that traditional secrecy performance metrics, such as the achievable secrecy rate and the SOP, cannot be directly applied to evaluate the level of secrecy in URLLC. To address this problem, we adopt a lower bound on the maximal secrecy rate (derived in [15, 16]) as the secrecy performance metric of URLLC, given by,

$$\rho(\alpha, L, \varepsilon_{\rm sr}, \varepsilon_{\rm se}) = \begin{cases} R_{\rm sr} - R_{\rm se} - 2\sqrt{\frac{V(\gamma_{\rm se})}{L}} f_{\rm Q}^{-1}(\varepsilon_{\rm se}), & \text{if } R_{\rm sr} > R_{\rm se}, \\ 0, & \text{if } R_{\rm sr} \leq R_{\rm se}. \end{cases} \tag{9}$$

We note that the lower bound on the maximal secrecy rate in (9) takes both the target decoding error probabilities at the legitimate receiver and the eavesdropper, i.e., $\varepsilon_{\rm sr}$ and $\varepsilon_{\rm se}$, into consideration. We also note that $f_{\rm Q}^{-1}(\varepsilon)$ increases as ε decreases. As such, $\rho(\alpha, L, \varepsilon_{\rm sr}, \varepsilon_{\rm se})$ increases as $\varepsilon_{\rm sr}$ and $\varepsilon_{\rm se}$ increase. Moreover, we note that $\rho(\alpha, L, \varepsilon_{\rm sr}, \varepsilon_{\rm se})$ can reduce to the classical achievable secrecy rate used in existing works on physical layer security when the blocklength $L \to \infty$, indicating that short-packet transmissions in URLLC will lead to the reduction in the achievable secrecy rate.

Based on (9), we can further define the generalized SOP for URLLC as the probability that the lower bound on the maximal secrecy rate is smaller than a certain threshold β. Mathematically, it is given by

$$P_{\rm so}(\alpha, \beta, L, \varepsilon_{\rm sr}, \varepsilon_{\rm se}) = \Pr\{\rho(\alpha, L, \varepsilon_{\rm sr}, \varepsilon_{\rm se}) < \beta\}. \tag{10}$$

2.2.2 Generalized secrecy outage probability

Since the instantaneous CSI of the main channel is available at the source (i.e., $\gamma_{\rm sr}$ is known to the source), we consider the adaptive transmission by setting the transmission rate of the wiretap code $R_b = R_{\rm sr}$ (as in [20]). The generalized SOP of URLLC in our considered system can be characterized in the following theorem.

Theorem 1 *The generalized SOP of URLLC in our system is given by*

$$P_{\rm so}(\alpha, \beta, L, \varepsilon_{\rm sr}, \varepsilon_{\rm se}) = \frac{\exp\left(-\frac{2^{\Phi(\alpha,\beta,R_{\rm sr})}-1}{\alpha\overline{\gamma}_{\rm se}}\right)}{\left(1 + \frac{1-\alpha}{\alpha(N_{\rm s}-1)}\left(2^{\Phi(\alpha,\beta,R_{\rm sr})} - 1\right)\right)^{N_{\rm s}-1}}, \tag{11}$$

where $\Phi(\alpha, \beta, R_{\rm sr}) = R_{\rm sr} - \beta - \frac{1}{\ln 2\sqrt{L}} f_{\rm Q}^{-1}(\varepsilon_{\rm se})$.

Proof With the aid of [20, 21], we express the cumulative probability function of $\gamma_{\rm se}$ as

$$F_{\gamma_{\rm se}}(\gamma) = 1 - \left(1 + \frac{(1-\alpha)\gamma}{\alpha(N_{\rm s}-1)}\right)^{1-N_{\rm s}} \exp\left(-\frac{\gamma}{\alpha\overline{\gamma}_{\rm se}}\right). \tag{12}$$

Based on (9) and (10), we re-express the generalized SOP as

$$\begin{aligned}
&P_{\rm so}(\alpha,\beta,L,\varepsilon_{\rm sr},\varepsilon_{\rm se}) \\
&\quad= \Pr\{R_{\rm se} > R_{\rm sr}\} \\
&\qquad+ \Pr\left\{R_{\rm sr} - 2\sqrt{\frac{V(\gamma_{\rm se})}{L}} f_{\rm Q}^{-1}(\varepsilon_{\rm se}) - \beta < R_{\rm se} \le R_{\rm sr}\right\} \\
&\quad= \Pr\left\{R_{\rm se} > R_{\rm sr} - 2\sqrt{\frac{V(\gamma_{\rm se})}{L}} f_{\rm Q}^{-1}(\varepsilon_{\rm se}) - \beta\right\} \\
&\quad\overset{(a)}{\approx} \Pr\left\{\log_2(1+\gamma_{\rm se}) \right. \\
&\quad\left. > R_{\rm sr} - \beta - \frac{\log_2 e}{\sqrt{L}} f_{\rm Q}^{-1}(\varepsilon_{\rm se})\right\} \\
&\quad= \Pr\left(\gamma_{\rm se} > 2^{\Phi(\alpha,\beta,R_{\rm sr})} - 1\right) \\
&\quad= 1 - F_{\gamma_{\rm se}}\left(2^{\Phi(\alpha,\beta,R_{\rm sr})} - 1\right),
\end{aligned} \tag{13}$$

where (a) holds by applying the approximation that $V(\gamma_{\rm se}) \approx (\log_2(e))^2$ when $\gamma_{\rm se}$ is relatively large.[2] Substituting (12) into (13), we obtain the desired result in (11), which completes the proof. □

We note that (11) is accurate for arbitrary values of R_s, $\varepsilon_{\rm se}$, and L. According to Theorem 1, several interesting observations can be made, as follows.

Remark 1 The generalized SOP decreases as $R_{\rm sr}$ increases. As such, For a fixed $\varepsilon_{\rm sr}$, efforts of enhancing the link quality in the main channel can also improve the secrecy performance of URLLC in our system.

Remark 2 The generalized SOP increases as $\varepsilon_{\rm sr}$ and $\varepsilon_{\rm se}$ decrease, implying that the secrecy performance of URLLC in our system degrades when the source and/or the eavesdropper requires a higher decoding accuracy.

Based on Theorem 1, we examine the convexity of the generalized SOP with respect to the power allocation factor α in the following lemma.

Lemma 1 *The generalized SOP is a convex function of the power allocation factor* α.

Proof In order to prove Lemma 1, we need to show that the second derivative of $P_{\rm so}(\alpha,\beta,L,\varepsilon_{\rm sr},\varepsilon_{\rm se})$ with respect to α is positive. To this end, according to (11), we first express $\frac{\partial^2 P_{\rm so}(\alpha,\beta,L,\varepsilon_{\rm sr},\varepsilon_{\rm se})}{\partial^2\alpha}$ as

[2] This assumption refers to a worst-case scenario where $\rho(\alpha, L, \varepsilon_{\rm sr}, \varepsilon_{\rm se})$ is minimized. As such, our derived expression of the generalized SOP can be regarded as an upper bound on the secrecy outage performance of short-packet transmissions in URLLC.

$$\frac{\partial^2 P_{\mathrm{so}}(\alpha,\beta,L,\varepsilon_{\mathrm{sr}},\varepsilon_{\mathrm{se}})}{\partial^2\alpha} = \frac{1}{g^2(\alpha)}\left[\frac{\partial^2 f(\alpha)}{\partial^2\alpha}g(\alpha) - f(\alpha)\frac{\partial^2 g(\alpha)}{\partial^2\alpha} - 2\frac{\partial f(\alpha)}{\partial\alpha}\frac{\partial g(\alpha)}{\partial\alpha} + \frac{2f(\alpha)\frac{\partial g(\alpha)}{\partial\alpha}}{g(\alpha)}\right], \tag{14}$$

where

$$f(\alpha) = \exp\left(-\frac{\zeta(\alpha)}{\alpha\overline{\gamma}_{\mathrm{se}}}\right), \tag{15}$$

with $\zeta(\alpha) = 2^{\Phi(\alpha,\beta,R_{\mathrm{sr}})} - 1$

$$\frac{\partial f(\alpha)}{\partial\alpha} = \frac{\xi-1}{\alpha^2\overline{\gamma}_{\mathrm{se}}}f(\alpha) \tag{16}$$

with $\xi = 2^{-\frac{1}{\ln 2\sqrt{L}}\left(f_{\mathrm{Q}}^{-1}(\varepsilon_{\mathrm{sr}})+f_{\mathrm{Q}}^{-1}(\varepsilon_{\mathrm{se}})\right)-\beta}$,

$$\frac{\partial^2 f(\alpha)}{\partial^2\alpha} = \frac{(\xi-1)}{\alpha^4\overline{\gamma}_{\mathrm{se}}}\left(\frac{\xi-1}{\overline{\gamma}_{\mathrm{se}}} - 2\alpha\right)f(\alpha), \tag{17}$$

$$g(\alpha) = \left(1 + \frac{1-\alpha}{\alpha(N_{\mathrm{s}}-1)}\zeta(\alpha)\right)^{N_{\mathrm{s}}-1}, \tag{18}$$

$$\frac{\partial g(\alpha)}{\partial\alpha} = \frac{-\alpha^2\xi\gamma_{\mathrm{sr}} - \xi + 1}{\alpha^2}\left(1 + \frac{1-\alpha}{\alpha(N_{\mathrm{s}}-1)}\zeta(\alpha)\right)^{N_{\mathrm{s}}-2}, \tag{19}$$

and

$$\frac{\partial^2 g(\alpha)}{\partial^2\alpha} = \left(1 + \frac{1-\alpha}{\alpha(N_{\mathrm{s}}-1)}\zeta(\alpha)\right)^{2N_{\mathrm{s}}-5} \times \frac{N_{\mathrm{s}}-2}{N_{\mathrm{s}}-1}\left(\frac{-\alpha^2\xi\gamma_{\mathrm{sr}} - \xi + 1}{\alpha^2}\right)^2\left(\frac{2(\xi-1)}{\alpha^3}\right). \tag{20}$$

Based on (15)–(20), we further derive $\frac{\partial^2 P_{\mathrm{so}}(\alpha,\beta,L,\varepsilon_{\mathrm{sr}},\varepsilon_{\mathrm{se}})}{\partial^2\alpha}$ as (21), shown at the top of the next page. In (21), $\Theta(\alpha)$ and $\Upsilon(\alpha)$ are respectively given by

$$\frac{\partial^2 P_{\mathrm{so}}(\alpha,\beta,L,\varepsilon_{\mathrm{sr}},\varepsilon_{\mathrm{se}})}{\partial^2\alpha} = \frac{f(\alpha)}{g^2(\alpha)}\Theta^{N_{\mathrm{s}}-3}(\alpha)\left[\frac{\xi-1}{\overline{\gamma}_{\mathrm{se}}\alpha^4}\left(\frac{\xi-1}{\overline{\gamma}_{\mathrm{se}}} - 2\alpha\right)\Theta^2(\alpha) - \left(\frac{(N_{\mathrm{s}}-2)\Upsilon^2(\alpha)}{\alpha^4(N_{\mathrm{s}}-1)} + \frac{2(\xi-1)\Theta(\alpha)}{\alpha^3}\right) - \frac{2(\xi-1)\Upsilon(\alpha)\Theta(\alpha)}{\alpha^4\overline{\gamma}_{\mathrm{se}}} + \frac{2}{\alpha^4}\Upsilon^2(\alpha)\right] \tag{21}$$

$$\Theta(\alpha) = 1 + \frac{1-\alpha}{\alpha(N_{\mathrm{s}}-1)}\zeta(\alpha), \tag{22}$$

$$\Upsilon(\alpha) = \alpha^2\xi\gamma_{\mathrm{sr}} - \xi + 1. \tag{23}$$

Then, with some mathematical manipulations, we obtain the following inequality

$$\begin{aligned}\frac{\partial^2 P_{\rm so}(\alpha,\beta,L,\varepsilon_{\rm sr},\varepsilon_{\rm se})}{\partial^2\alpha} &> \frac{f(\alpha)}{\alpha^4 g^2(\alpha)}\Theta^{N_{\rm s}-3}(\alpha)\\ &\times\left[\left(\left(\frac{\xi-1}{\overline{\gamma}_{\rm se}}\right)^2+\frac{2\alpha(1-\xi)}{\overline{\gamma}_{\rm se}}\right)\Theta^2(\alpha)\right.\\ &\left.+2\alpha(1-\xi)\Theta(\alpha)-\frac{2(\xi-1)}{\overline{\gamma}_{\rm se}}\Theta(\alpha)\Upsilon(\alpha)+\Upsilon^2(\alpha)\right]\\ &=\frac{f(\alpha)}{\alpha^4 g^2(\alpha)}\Theta^{N_{\rm s}-3}(\alpha)\left[\left(\frac{1-\xi}{\overline{\gamma}_{\rm se}}\Theta(\alpha)+\Upsilon(\alpha)\right)^2+\frac{2\alpha(1-\xi)}{\overline{\gamma}_{\rm se}}\Theta^2(\alpha)+2\alpha(1-\xi)\Theta(\alpha)\right].\end{aligned} \tag{24}$$

Note that $\xi < 1$ and $\Theta(\alpha) > 0$, we confirm that $\frac{\partial^2 P_{\rm so}(\alpha,\beta,L,\varepsilon_{\rm sr},\varepsilon_{\rm se})}{\partial^2\alpha} > 0$. The proof is completed. □

Lemma 1 indicates that there exists a unique optimal α^* that minimizes the generalized SOP. Mathematically, α^* can be expressed as

$$\alpha^* = \underset{0<\alpha\le 1}{\operatorname{argmin}} P_{\rm so}(\alpha,\beta,L,\varepsilon_{\rm sr},\varepsilon_{\rm se}). \tag{25}$$

We note that it is difficult to obtain the closed-form expression of α^*. However, α^* can be effectively determined by using the bisection method. Then, we define the minimum generalized SOP achieved by α^* as $P^*_{\rm so}(\alpha,\beta,L,\varepsilon_{\rm sr},\varepsilon_{\rm se})$.

3 Experiment

In this section, we provide numerical results to validate our analysis of the generalized SOP and examine the impacts of system parameters (e.g., $\overline{\gamma}_{\rm sr}$, $\overline{\gamma}_{\rm se}$, α, $N_{\rm s}$, and $\varepsilon_{\rm se}$) on the generalized SOP. Throughout this section, the requirement on the decoding error probability at the legitimate receiver is 10^{-7}, the packet size is 32 bytes, the transmission duration is 0.5 ms, and the bandwidth is 1 MHz [1].

We first verify the accuracy of our expression of the generalized SOP $P_{\rm so}(\alpha,\beta,L,\varepsilon_{\rm sr},\varepsilon_{\rm se})$ in Fig. 1. In this figure, we plot $P_{\rm so}(\alpha,\beta,L,\varepsilon_{\rm sr},\varepsilon_{\rm se})$ versus $\overline{\gamma}_{\rm sr}$ for different ratios between $\overline{\gamma}_{\rm sr}$ and $\overline{\gamma}_{\rm se}$ with $N_{\rm s}=2$, $\varepsilon_{\rm sr}=10^{-7}$, $\varepsilon_{\rm se}=10^{-6}$, $\beta=0.5$, and $R_s=1$ bits/s/Hz. We can see that the analytical curves, obtained from Theorem 1, accurately match the simulation points generated from Monte Carlo simulations, demonstrating the accuracy of our analysis for $P_{\rm so}(\alpha,\beta,L,\varepsilon_{\rm sr},\varepsilon_{\rm se})$ in Theorem 1. We also see that $P_{\rm so}(\alpha,\beta,L,\varepsilon_{\rm sr},\varepsilon_{\rm se})$ decreases as $\overline{\gamma}_{\rm sr}$ increases, indicating that the level of secrecy in URLLC can be enhanced through increasing the transmit power at the source. Moreover, we see that $P_{\rm so}(\alpha,\beta,L,\varepsilon_{\rm sr},\varepsilon_{\rm se})$ decreases as $\overline{\gamma}_{\rm sr}/\overline{\gamma}_{\rm se}$ increases.

In Fig. 2, we examine the impact of the power allocation factor between the confidential signal and the AN signal, α, on the secrecy performance of URLLC. In Fig. 2a, we plot $P_{\rm so}(\alpha,\beta,L,\varepsilon_{\rm sr},\varepsilon_{\rm se})$ versus α for different values of $\overline{\gamma}_{\rm sr}/\overline{\gamma}_{\rm se}$. We see that, for each value of $\overline{\gamma}_{\rm sr}/\overline{\gamma}_{\rm se}$, $P_{\rm so}(\alpha,\beta,L,\varepsilon_{\rm sr},\varepsilon_{\rm se})$ first decreases then increases as α varies from 0 to 1, and there is a unique α^* that minimizes $P_{\rm so}(\alpha,\beta,L,\varepsilon_{\rm sr},\varepsilon_{\rm se})$. We also see that the optimal α^* that achieves the minimum generalized SOP, i.e., $P^*_{\rm so}(\alpha,\beta,L,\varepsilon_{\rm sr},\varepsilon_{\rm se})$, increases the value of $\overline{\gamma}_{\rm sr}/\overline{\gamma}_{\rm se}$ increases. This indicates that, when the eavesdropper is relatively far away from the source, transmitting the AN signal becomes less effective. In order to achieve the optimal secrecy performance, the source needs to allocate more power to the

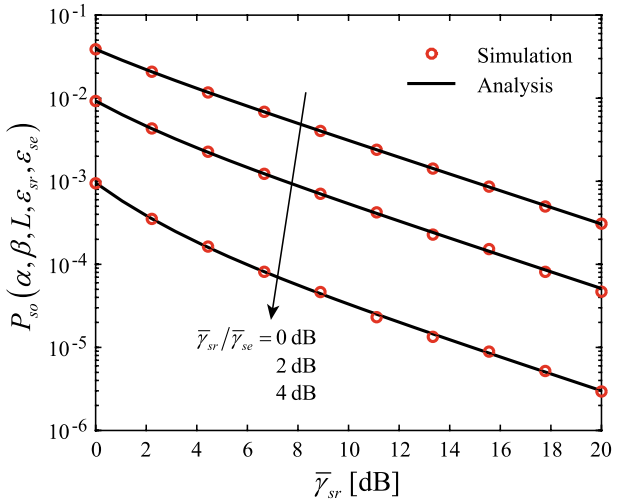

Fig. 1 $P_{so}(\alpha,\beta,L,\varepsilon_{sr},\varepsilon_{se})$ versus $\overline{\gamma}_{sr}$ for different values of $\overline{\gamma}_{sr}/\overline{\gamma}_{se}$ with $N_s = 2, \varepsilon_{sr} = 10^{-7}, \varepsilon_{se} = 10^{-6}$, $\beta = 0.5$ bits/s/Hz

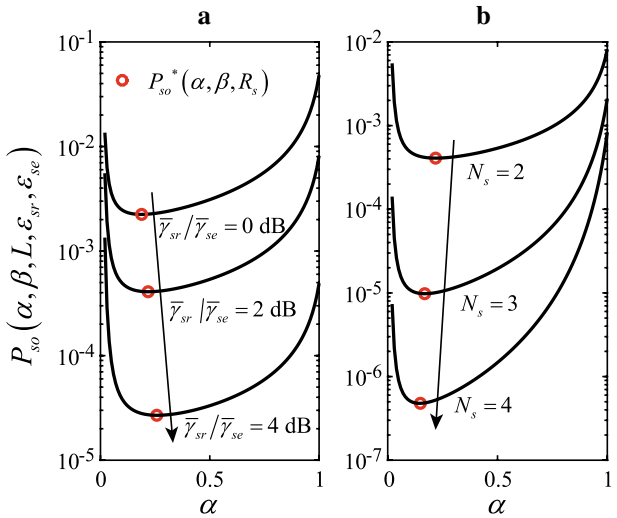

Fig. 2 $P_{so}(\alpha,\beta,L,\varepsilon_{sr},\varepsilon_{se})$ versus α for different values of **a** $\overline{\gamma}_{sr}/\overline{\gamma}_{se}$ and **b** N_s with $\varepsilon_{sr} = 10^{-7}, \varepsilon_{se} = 10^{-6}$, $\beta = 0.5$ bits/s/Hz

confidential signal. In Fig. 1b, we plot $P_{so}(\alpha,\beta,L,\varepsilon_{sr},\varepsilon_{se})$ versus α for different values of $\overline{\gamma}_{sr}/\overline{\gamma}_{se}$ with $\overline{\gamma}_{sr}/\overline{\gamma}_{se} = 2$ dB. We see that the minimum generalized SOP decreases as N_s increases, showing that the secrecy performance of URLLC can be enhanced by deploying more antennas at the source. Moreover, we see that the optimal α^* that minimizes $P_{so}(\alpha,\beta,L,\varepsilon_{sr},\varepsilon_{se})$ decreases as N_s increases, demonstrating that, with more antennas deploys at the source, the source can allocate less transmit power to the confidential signal and still achieve the minimum generalized SOP.

Finally, we examine the impact of the target decoding error probability at the eavesdropper, ε_{se}, on the optimal power allocation factor in Fig. 3. In this figure, we plot α^* versus ε_{se} for different values of $\overline{\gamma}_{sr}/\overline{\gamma}_{se}$. We can see that the optimal α^* that achieves

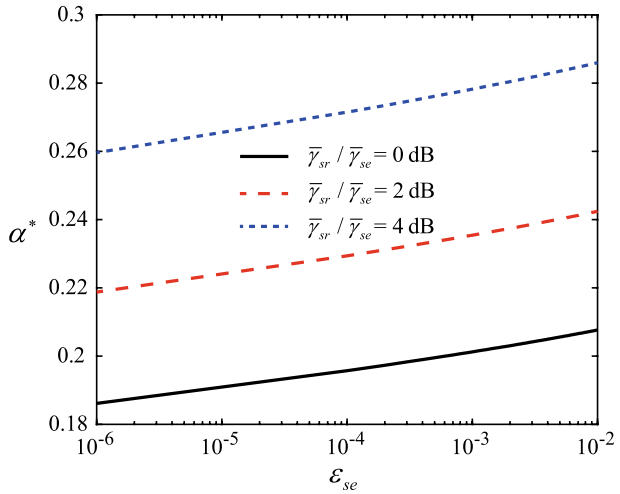

Fig. 3 α^* versus ε_{se} for different values of $\overline{\gamma}_{sr}/\overline{\gamma}_{se}$ with $N_s = 2, \varepsilon_{sr} = 10^{-7}, \beta = 0.5$ bits/s/Hz

$P^*_{so}(\alpha, \beta, L, \varepsilon_{sr}, \varepsilon_{se})$ decreases as ε_{se} decreases, indicating that the source needs to use more power to confuse the eavesdropper when the eavesdropper requires a higher decoding accuracy. Although not shown here, we note that the target decoding error probability at the legitimate receiver ε_{sb} also has a significant impact on the optimal power allocation factor. Specifically, α^* increases when ε_{sb} decreases. This is because, when the legitimate receiver has a more strict requirement on the decoding error probability, the source needs to allocate more power to the confidential signal in order to achieve the optimal secrecy performance.

4 Results and discussion

Due to short-packet transmissions in URLLC, the confidential information is inevitably leaked to the eavesdropper and perfect secrecy cannot be achieved. It follows that secrecy performance metrics commonly used in existing physical layer security techniques, such as the achievable secrecy rate and the SOP, are not directly applicable for evaluating the secrecy performance of URLLC. To address this problem, we adopt a lower bound on the maximal secrecy rate for short-packet transmissions in URLLC, characterizing the relationships among the target decoding error probabilities at the legitimate receiver and the eavesdropper, and derived the generalized SOP that the lower bound is smaller than a certain threshold. In addition, we considered that the source transmits the AN signal, in addition to the confidential signal, and showed how the secrecy performance of URLLC can be significantly improved by adjusting the power allocated to the confidential signal.

Abbreviations

URLLC: Ultra-reliable and low-latency communications; AN: Artificial noise; SOP: Secrecy outage probability; 5G: The fifth generation; QoS: Quality-of-service; E2E: End-to-end; CSI: Channel state information.

Acknowledgements

Not applicable.

Authors' contributions
JH carried out the statistical analysis and drafted the manuscript. GZcarried out the system modeling and the design of the artificial noise. LW performed the simulations and helped to draft the manuscript. XS helped with the statistical analysis and participated in the simulations. LY participated in the simulations and helped to draft the manuscript. All the authors read and approved the submitted manuscript.

Funding
This work was supported in part by the National Natural Science Foundation of China under Grant No. 61971403 and in part by the Special Presidential Foundation of Technology and Engineering Center for Space Utilization of the Chinese Academy of Sciences under Project CSU-QZKT-2018-16.

Availability of data and materials
Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Competing interests
The authors declare that they have no competing interests.

Author details
[1] University of Chinese Academy of Sciences, Beijing 100094, China. [2] Key Laboratory of Space Utilization, Chinese Academy of Sciences, Beijing 100094, China. [3] Technology and Engineering Center for Space Utilization, Chinese Academy of Sciences, Beijing 100094, China.

Received: 2 September 2020 Accepted: 6 November 2020
Published online: 15 February 2021

References

1. 3GPP TR 38.913: study on scenarios and requirements for next generation access technologies. Technical report. Release 14. 3GPP (2016)
2. C. Yang, C. Sun, Z. Gu, Y. Li, C. Yang, H.V. Poor, B. Vucetic, A tutorial of ultra-reliable and low-latency communications in 6G: integrating theoretical knowledge into deep learning. arXiv:2009.06010
3. A. Aijaz, M. Dohler, A.H. Aghvami, V. Friderikos, M. Frodigh, Realizing the tactile internet: haptic communications over next generation 5G cellular networks. IEEE Wirel. Commun. **24**(2), 82–89 (2017)
4. P. Schulz, M. Matthé, H. Klessig et al., Latency critical IoT applications in 5G: perspective on the design of radio interface and network architecture. IEEE Commun. Mag. **55**(2), 70–78 (2017)
5. H.V.K. Mendis, F.Y. Li, Achieving ultra reliable communication in 5G networks: a dependability perspective availability analysis in the space domain. IEEE Commun. Lett. **21**(9), 2057–2060 (2017)
6. C. She, C. Yang, T.Q.S. Quek, Radio resource management for ultra-reliable and low-latency communications. IEEE Commun. Mag. **55**(6), 72–78 (2017)
7. C. She, C. Yang, T.Q.S. Quek, Cross-layer optimization for ultra-reliable and low-latency radio access networks. IEEE Trans. Wirel. Commun. **17**(1), 127–141 (2018)
8. C. She, C. Liu, T.Q.S. Quek, C. Yang, Y. Li, Ultra-reliable and low-latency communications in unmanned aerial vehicle communication systems. IEEE Trans. Commun. **67**(5), 3768–3781 (2019)
9. P. Popovski, et al. Deliverable d6.3 intermediate system evaluation results. ICT-317669-METIS/D6.3 (2014)
10. C. She et al., Deep learning for ultra-reliable and low-latency communications in 6G networks. IEEE Netw. (2020). https://doi.org/10.1109/MNET.011.1900630
11. N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, M.D. Renzo, Safeguarding 5G wireless communication networks using physical layer security. IEEE Commun. Mag. **53**(4), 20–27 (2015)
12. A. Mukherjee, S.A.A. Fakoorian, J. Huang, A.L. Swindlehurst, Principles of physical layer security in multiuser wireless networks: a survey. IEEE Commun. Surv. Tutor. **16**(3), 1550–1573 (2014)
13. L. Senigagliesi, M. Baldi, S. Tomasin, Resource allocation for secure Gaussian parallel relay channels with finite-length coding and discrete constellations. arxiv:1807.06448
14. H.-M. Wang, Q. Yang, Z. Ding, H.V. Poor, Secure short-packet communications for mission-critical IoT applications. IEEE Trans. Wirel. Commun. **18**(5), 2565–2578 (2019)
15. W. Yang, R.F. Schaefer, H.V. Poor, Finite-blocklength bounds for wiretap channels, in *Proceedings of IEEE International Symposium on Information Theory (ISIT)*. Barcelona, Spain, pp. 3087–3091 (2016)
16. W. Yang, R.F. Schaefer, H.V. Poor, Wiretap channels: nonasymptotic fundamental limits. arxiv.org/pdf/1706.03866v1
17. W. Yang, G. Durisi, T. Koch, Y. Polyanskiy, Quasi-static multiple-antenna fading channels at finite blocklength. IEEE Trans. Inf. Theory **60**(7), 4232–4264 (2014)
18. A.D. Wyner, The wire-tap channel. Bell Syst. Tech. J. **54**(8), 1355–1387 (1975)
19. M. Bloch, J. Barros, *Physical-Layer Security. From Information Theory to Security Engineering* (Cambridge University Press, Cambridge, 2011)
20. C. Liu, N. Yang, J. Yuan, R. Malaney, Location-based secure transmission for wiretap channels. IEEE J. Sel. Areas Commun. **33**(7), 1458–1470 (2015)
21. C. Liu, J. Lee, T.Q.S. Quek, Safeguarding UAV communications against full-duplex active eavesdropper. IEEE Trans. Wirel. Commun. **18**(6), 2919–2931 (2019)

Publisher's Note