Secrecy Analysis of Context-Aware Short Packet Transmission

Nihan Arı, Leila Musavian and Nikolaos Thomos
School of Computer Science and Electronic Engineering
University of Essex
Colchester, United Kingdom
Email: {nkaraca, leila.musavian, nthomos}@essex.ac.uk

***Abstract*—Sixth-generation (6G) systems are expected to require enhanced security measures and face new challenges while incorporating communication context. Physical layer security (PLS) techniques emerge as promising solutions for securing contextual communications thanks to its flexibility a nd adaptability. Applications using short packet transmissions can benefit f rom c ontext-aware P LS. T his p aper a nalyzes t he security performance of a wiretap channel during the contextual short packet data transmission. We quantify the channel rate for both contextual and non-contextual information and determine the average context-aware rate. Furthermore, the average block error probabilities for both types of information are defined. Monte-Carlo simulations are employed to validate the derived theoretical formulas.**

***Index Terms*—context-awareness, short packet communication, physical layer security**

I. Introduction

In the context of physical layer security (PLS), a wiretap channel is a communication channel where a legitimate sender (Alice) wants to send messages to a legitimate receiver (Bob) while ensuring that an eavesdropper (Eve) gains as little information as possible. The objective is to maximize the secure transmission rate while minimizing information leakage to Eve. This becomes increasingly challenging with short packet transmission, as its inherent constraints make it hard to attain the desired level of information leakage. Short packet communication is a key technology to support systems such as ultra reliable low latency communications (URLLC), which aims to guarantee very high reliability and very low latency [1]. 6G is expected to support more complex applications and scenarios, including future network advancements where the sensing and learning capabilities of 6G devices interpret the context of communication and improve awareness. Context involves information about the environment, devices, and users, including network node resource limitations, computational capabilities, or environmental data such as channel quality. Packets carrying contextual information may contain essential or highly sensitive information and require a high level of security, while other packets may contain less sensitive data, and their security is less crucial. PLS solutions stand out as strong candidates for 6G by achieving low-complexity, low-delay, adaptive, flexible, and context-aware security [2], [3]. These solutions leverage the physical layer to introduce robust security measures. Context-awareness is especially valuable for future wireless networks, such as ultra-low latency scenarios, when combined with PLS [2]. Therefore, this paper explores the secrecy analysis of short packet transmission, integrating the concept of context-awareness with PLS.

This work was funded by the Engineering and Physical Science Research Council, UK, [Grant Numbers: EP/X04047X/1 and EP/Y037243/1].

A. Related Works and Motivation

Shannon introduced the perfect secrecy concept [4] and the problem of secure communication from an information theoretic perspective. Then, Wyner's pioneering work followed, forming the basis of secrecy capacity in [5]. The secrecy capacity was defined as the maximal secret communication rate at which information can be transmitted securely and reliably over a wiretap channel with the assumption of an infinitely large blocklength [6]. However, the work in [7] evaluated how channel capacity is affected when transmission must maintain reliability and security within a fixed finite blocklength. Furthermore, the impact of the decoding error probability and information leakage probability on secrecy capacity is not negligible for finite blocklength cases especially if, the blocklength is short. The works in [8]–[10] determined the achievable secrecy rate bounds for finite blocklength regime. There are studies that have conducted performance analysis of PLS in the context of short packet communication [11]–[16]. These works explored different factors and parameters to assess PLS in systems that transmit short data packets. The study in [11] examined the average secrecy throughput for secure internet of things (IoT) applications in the presence of an external multi-antenna eavesdropper. Similarly, [12] optimized secrecy throughput for scenarios involving both single and multiple antenna transmitters with an eavesdropper, proposing adaptive and non-adaptive parameter design schemes. In another work, [13] evaluated the performance of full-duplex (FD) multi-user multiple-input-multiple-output (MIMO) systems, deriving the secrecy throughput when a multi-antenna eavesdropper is present. Differently, [14] addressed scenarios with multiple eavesdroppers, investigating the average secrecy throughput for single and multiple antenna transmitters, as well as determining the optimal blocklength that maximized average secrecy throughput for both single and multiple eavesdropper cases. Furthermore, [15] introduced a best node selection scheme for dual-hop cooperative

IoT networks with multiple IoT devices and eavesdroppers, considering both non-colluding and colluding eavesdropping scenarios.

Recently, the idea of incorporating PLS with context awareness has been discussed in a survey paper in [2]. This paper comprehensively explored directions how the next generation of wireless networks can achieve enhanced security by integrating context-aware mechanisms and PLS. It highlighted open security issues in 5G, the roadmap to security challenges in 6G, and explored context-aware security solutions for future wireless networks. The work in [3] examined the role of PLS in enhancing 6G network security by highlighting its advantages and also discussed security challenges in the transition from 5G to 6G. It suggested that integrating context-aware mechanisms into 6G systems could allow PLS schemes to serve as lightweight, adaptable security solutions based on available contextual information. In addition, the work in [17] shared the vision for a context-aware PLS and the authors pointed out that a single PLS scheme cannot be applied universally across all scenarios. Although existing studies emphasize its importance for future networks, a context-aware PLS still remains an open challenge. This paper aims to explore a context-aware PLS approach to short packet communication from a novel and distinct perspective that has not been addressed in previous research.

B. Contributions

To the best of our knowledge, this is the first attempt to examine PLS performance analysis of context-aware communication from the perspective of short packet transmission. This paper aims to introduce a wiretap channel rate that reflects whether contextual information is being transmitted or not. The security implications of each type of transmission can be better assessed by distinguishing contextual from non-contextual information. More specifically, average block error probabilities of contextual and non-contextual information are derived in closed forms. Next, the instantaneous and average rates of both contextual and non-contextual information are determined to form the total average rate of the wiretap channel. All the theoretical works are validated through Monte-Carlo simulation under different conditions. Finally, we discuss the security performance of context-aware communication in detail. Our approach involves several key steps and examines how various factors, such as the distance of the eavesdropper and the nature of the transmitted information, impact the overall security of the system.

II. System Model and Problem Definition

This paper examines the security performance of a short packet transmission system over a wiretap channel. The objective is to formulate and analyze the context-aware security of a legitimate communication pair (Alice and Bob) in the presence of an eavesdropper (Eve). All the channels are assumed to experience block fading, meaning that the fading characteristics remain stable for the duration of each packet's transmission and only vary between packets. In other words, the channel coefficients stay constant during each packet transmission and change only afterwards. All nodes are equipped with a single antenna. The transmitted signal is denoted by x. The transmission power of the transmitter is P. The channel gain from Alice to Bob is denoted by h_{AB}, and the one from Alice to Eve is denoted by h_{AE}. These gains are determined based on node distances as $h_{\mathrm{AB}} = \sqrt{d_{\mathrm{AB}}^{-v}} g_{\mathrm{AB}}$, $h_{\mathrm{AE}} = \sqrt{d_{\mathrm{AE}}^{-v}} g_{\mathrm{AE}}$, where d_{AB} is Alice-Bob distance, d_{AE} is Alice-Eve distance, v represents the path-loss exponent, g_{AB} and g_{AE} denote small-scale fading coefficients of the respective communication links. The noise at the legitimate receiver and the eavesdropper is represented by n_B and n_E, respectively. The received signal at Bob and Eve can be written as

$$\begin{aligned} y_{\mathrm{B}} &= \sqrt{P} h_{\mathrm{AB}} x + n_{\mathrm{B}}, \\ y_{\mathrm{E}} &= \sqrt{P} h_{\mathrm{AE}} x + n_{\mathrm{E}}. \end{aligned} \tag{1}$$

Notably, Alice has knowledge of the instantaneous channel state information (CSI) of the main channel between herself and Bob, but only has access to the statistical CSI of Eve's channel. The received instantaneous signal-to-noise ratio (SNR) at Bob, γ_{B}, and at Eve, γ_{E}, are as follows

$$\begin{aligned} \gamma_{\mathrm{B}} &= \frac{P|h_{\mathrm{AB}}|^2}{\sigma_{\mathrm{B}}^2} = \rho_{\mathrm{AB}} |g_{\mathrm{AB}}|^2, \\ \gamma_{\mathrm{E}} &= \frac{P|h_{\mathrm{AE}}|^2}{\sigma_{\mathrm{E}}^2} = \rho_{\mathrm{AE}} |g_{\mathrm{AE}}|^2. \end{aligned} \tag{2}$$

Noise variance at Bob is denoted by σ_{B}^2 and σ_{E}^2 at Eve and they are assumed $\sigma_{\mathrm{B}}^2 = \sigma_{\mathrm{E}}^2 = 1$, which result in P is also being the transmit SNR.

In traditional information theory, the channel coding rate is analyzed in the asymptotic regime where blocklengths tend to approach infinity, leading to Shannon capacity. However, blocklengths are in reality finite or even short, which leads to an investigation of the channel rates in the finite blocklength regime. Indeed, the following approximation indicates that there is a penalty on the rate to sustain the desired error probability at a finite blocklength. The maximum rate of a channel for a given blocklength, n, and the decoding error probability, ϵ is approximated by [7], [18], [19]

$$R^*(n, \epsilon) \approx C - \sqrt{\frac{V}{n}} Q^{-1}(\epsilon), \tag{3}$$

where C is the channel capacity with being $C > 0$ and V is the dispersion of the channel. Q function is defined as $Q(\epsilon) = \int_{\epsilon}^{\infty} \frac{1}{\sqrt{2\pi}} e^{-\frac{t^2}{2}} dt$ and $Q^{-1}(\epsilon)$ is its inverse. The error probability ϵ can be extracted from the previous approximation in (3) as

$$\epsilon = Q\left(\sqrt{\frac{n}{V}} \Big(C - R(n, \epsilon) \Big) \right). \tag{4}$$

When it comes to the maximum achievable secrecy rate for a finite blocklength, not only a decoding error at Bob but also an

information leakage to Eve may occur. This leads to a further reduction of the communication rate. Hence, the secrecy rate $R^*(n,\epsilon,\delta)$ with information leakage probability, δ, is defined as [8], [9], [10]

$$R^*(n,\epsilon,\delta) \approx C_{\rm s} - \sqrt{\frac{V_{\gamma_{\rm B}}}{n}}\frac{Q^{-1}(\epsilon)}{\log(2)} - \sqrt{\frac{V_{\gamma_{\rm E}}}{n}}\frac{Q^{-1}(\delta)}{\log(2)}, \quad (5)$$

The channel dispersions of the main and adversary channels are $V_{\gamma_{\rm B}} = 1-(1+\gamma_{\rm B})^{-2}$ and $V_{\gamma_{\rm E}} = 1-(1+\gamma_{\rm E})^{-2}$, respectively [7]. The secrecy capacity of the wiretap channel $C_{\rm s}$ is given by

$$\begin{aligned} C_{\rm s} &= [\log_2(1+\gamma_{\rm B}) - \log_2(1+\gamma_{\rm E})]^+, \\ &= \Big[\log_2\Big(\frac{1+\gamma_{\rm B}}{1+\gamma_{\rm E}}\Big)\Big]^+. \end{aligned} \quad (6)$$

where $[.]^+ = \max[.\ ,0]$. The error probability ϵ in the finite blocklength regime is obtained from (5) as follows

$$\epsilon = Q\Bigg(\sqrt{\frac{n}{V_{\gamma_{\rm B}}}}\Big(C_s - \sqrt{\frac{V_{\gamma_{\rm E}}}{n}}Q^{-1}(\delta) - R^*(n,\epsilon,\delta)\Big)\Bigg). \quad (7)$$

Here, the secret contextual information transmission rate will be formulated under the assumption that the eavesdropper remains passive. Some packets are considered to carry contextual information, whereas others are irrelevant to the eavesdropper. The primary aim of the eavesdropper is to capture the contextual information. It is assumed that there are far fewer contextual packets than non-contextual ones. The rate for context-aware transmission is hence given by

$$R = \bar{\rm I}R_{\rm NC} + {\rm I}R_{\rm C}, \quad (8)$$

where $R_{\rm NC}$ is the rate for non-context information transmission and $R_{\rm C}$ is the rate for contextual information transmission. The overall transmission rate for each packet in a block fading channel will be either $R_{\rm NC}$ or $R_{\rm C}$, both measured in bits per channel use (BPCU). More specifically, the indicator I shows whether the transmitted data is contextual or non-contextual data. Accordingly, the maximum achievable transmission rate for a given packet is the wiretap channel rate or the secrecy rate, depending on the packet's context. ${\rm I} = 1$ indicates that a data packet transmission that should be kept secure. Conversely, the complement of I, denoted as $\bar{\rm I}$, is employed when the packet's context is not significant enough to be protected from the eavesdropper. The cases are explained in detail below

1) Alice transmits contextual information to Bob while Eve attempts to eavesdrop. Because the packet carries sensitive contextual information, the highest achievable rate to transmit it is a measure of the secrecy rate of short packet communication. The secrecy rate ensures that this data is securely transmitted from Alice to Bob without being compromised by Eve. In this scenario, the information indicator is ${\rm I} = 1$, while the complementary indicator is $\bar{\rm I} = 0$, so this leads to the determination of the contextual information rate, denoted as $R_{\rm C}$.

$$R_{\rm C}(n,\epsilon_{\rm C},\delta) = C_{\rm s} - \sqrt{\frac{V_{\gamma_{\rm B}}}{n}}\frac{Q^{-1}(\epsilon_{\rm C})}{\log(2)} - \sqrt{\frac{V_{\gamma_{\rm E}}}{n}}\frac{Q^{-1}(\delta)}{\log(2)}, \quad (9)$$

where $\epsilon_{\rm C}$ is the probability of decoding block error of the contextual data packet.

2) If non-context information is being transmitted, the channel capacity between Alice and Bob will be the appropriate performance metric.It is assumed that the non-context information is not useful unless the context is detected correctly. In other words, the non-context data becomes relevant or meaningful only, when the correct context is identified, as the context provides essential insight to properly interpret and utilize the non-context information. Without accurate detection of the context, the non-context data cannot be fully understood. In this situation, the information indicator for contextual rate is ${\rm I} = 0$, while the information indicator for non-relevant information is $\bar{\rm I} = 1$. Therefore, the rate of non-contextual information is calculated based on the channel capacity between Alice and Bob and denoted as $R_{\rm NC}$.

$$R_{\rm NC}(n,\epsilon_{\rm NC}) = (1-\epsilon_{\rm C})\log_2(1+\gamma_{\rm B}) - \sqrt{\frac{V_{\gamma_{\rm B}}}{n}}\frac{Q^{-1}(\epsilon_{\rm NC})}{\log(2)}, \quad (10)$$

where $\epsilon_{\rm NC}$ is the probability of decoding block error of the non-contextual data packet.

Here, the average decoding block error probability of contextual and non-contextual information are investigated and analyzed. Firstly, the derivation of the expression for $\bar{\epsilon}_{\rm C}$ is the average block error probability of contextual data when Eve is passive is presented below

$$\bar{\epsilon}_{\rm C} \approx \int_0^\infty \int_0^\infty \epsilon_{\gamma_{\rm B}|\gamma_{\rm E}}(x) f(\gamma_{\rm B}) d\gamma_{\rm B} f(\gamma_{\rm E}) d\gamma_{\rm E}. \quad (11)$$

The error probability is conditioned on the channel realizations of both main and wiretapper. The probability density function (pdf) for the main and eavesdropper's channels are given by

$$\begin{aligned} f(\gamma_{\rm B}) &= \frac{1}{\rho_{\rm AB}} e^{-\frac{\gamma_{\rm B}}{\rho_{\rm AB}}}, \\ f(\gamma_{\rm E}) &= \frac{1}{\rho_{\rm AE}} e^{-\frac{\gamma_{\rm E}}{\rho_{\rm AE}}}. \end{aligned} \quad (12)$$

The block error probability of contextual information transmission is represented by the expression in (7) and can be written by substituting the secrecy rate $R^*(n,\epsilon,\delta)$ with b/n, where b represents the number of information bits transmitted in a blocklength n. For $\gamma_{\rm B} > \gamma_{\rm E}$, i.e., when the secrecy capacity is greater than zero, the decoding block error probability of a wiretap channel can be computed according to

$$\epsilon_{\rm C} = Q\Bigg(\sqrt{\frac{n}{V_{\gamma_{\rm B}}}}\Big(\log\Big(\frac{1+\gamma_{\rm B}}{1+\gamma_{\rm E}}\Big) - \sqrt{\frac{V_{\gamma_{\rm E}}}{n}}Q^{-1}(\delta) - \frac{b}{n}\log(2)\Big)\Bigg) \quad (13)$$

In the case that $\gamma_{\rm B} \leq \gamma_{\rm E}$, $\epsilon_{\rm C}$ is set to 1. There is no exact closed-form expression for the average block error probability of contextual data. However, $\epsilon_{\gamma_{\rm B}|\gamma_{\rm E}}$ can be approximated using the linearization method described in [20] and can be found as follows

$$\epsilon_{\gamma_{\rm B}|\gamma_{\rm E}}(z) \approx \begin{cases} 1, & z < \alpha + \frac{1}{2\beta}, \\ \frac{1}{2} + \beta(z-\alpha), & \alpha + \frac{1}{2\beta} \leq z \leq \alpha - \frac{1}{2\beta}, \\ 0, & z > \alpha - \frac{1}{2\beta}, \end{cases} \quad (14)$$

1) $\bar{\epsilon}_C$ calculation: To continue evaluating $\epsilon_{\rm C}$ in (13), α and β in (14) are renamed as $\alpha_{\rm C}$ and $\beta_{\rm C}$, respectively to avoid confusion on the linearization technique. Here, $\alpha_{\rm C}$ enables $Q(0) = 1/2$ in (13) at $z = \alpha_{\rm C}$. Therefore, α_C is derived by solving $\left(\log\left(\frac{1+\alpha_C}{1+\gamma_{\rm E}}\right) - \sqrt{\frac{V_{\gamma_{\rm E}}}{n}}Q^{-1}(\delta) - \frac{b}{n}\log(2)\right) = 0$. As a result, $\alpha_{\rm C}$ is found according to

$$\alpha_{\rm C} = e^{\left(\sqrt{\frac{V_{\gamma_{\rm E}}}{n}}Q^{-1}(\delta) + \frac{b}{n}\log(2)\right)}(1+\gamma_{\rm E}) - 1, \quad (15)$$

For the sake of simplicity, we can approximate $V_{\gamma_{\rm E}} \approx 1$, and then (15) is rewritten as

$$\alpha_{\rm C} = e^{\left(\frac{Q^{-1}(\delta)}{\sqrt{n}} + \frac{b}{n}\log(2)\right)}(1+\gamma_{\rm E}) - 1, \quad (16)$$

which can be further rewritten by using the substitution of $r = e^{\left(\frac{Q^{-1}(\delta)}{\sqrt{n}} + \frac{b}{n}\log(2)\right)}$ in (16),

$$\alpha_{\rm C} = r(1+\gamma_{\rm E}) - 1. \quad (17)$$

The slope β_C of $\epsilon_{\gamma_{\rm B}|\gamma_{\rm E}}(z)$ at $z = \alpha_C$ is defined as

$$\begin{aligned} \beta_{\rm C} &= \frac{d\epsilon_{\gamma_{\rm B}|\gamma_{\rm E}}(z)}{dz}\Big|_{z=\alpha_{\rm C}} \\ &= -\sqrt{\frac{n}{2\pi\alpha_{\rm C}(\alpha_{\rm C}+2)}}, \end{aligned} \quad (18)$$

and it satisfies $\frac{1}{2} + \beta_{\rm C}(\alpha_{\rm C} + \frac{1}{2\beta_{\rm C}} - \alpha_{\rm C}) = 1$ and $\frac{1}{2} + \beta_{\rm C}(\alpha_{\rm C} - \frac{1}{2\beta_{\rm C}} - \alpha_{\rm C}) = 0$.
The evaluation of $\bar{\epsilon}_{\rm C}$ in (11) can be written as

$$\bar{\epsilon}_{\rm C} \approx \int_0^\infty \Omega f(\gamma_{\rm E}) d\gamma_{\rm E}. \quad (19)$$

Here, Ω represents the following

$$\Omega \approx \int_0^\infty \epsilon_{\gamma_{\rm B}|\gamma_{\rm E}}(z)\Big|_{\gamma_{\rm B}=z} \frac{1}{\rho_{\rm AB}} e^{-\frac{\gamma_{\rm B}}{\rho_{\rm AB}}} d\gamma_{\rm B}, \quad (20)$$

and it is expanded as

$$\begin{aligned} \Omega \approx &\int_0^{\alpha_{\rm C}+\frac{1}{2\beta_{\rm C}}} \frac{1}{\rho_{\rm AB}} e^{-\frac{\gamma_{\rm B}}{\rho_{\rm AB}}} d\gamma_{\rm B} \\ &+ \int_{\alpha_{\rm C}+\frac{1}{2\beta_{\rm C}}}^{\alpha_{\rm C}-\frac{1}{2\beta_{\rm C}}} (\beta_{\rm C}(z-\alpha_{\rm C}) + 1/2)\frac{1}{\rho_{\rm AB}} e^{-\frac{\gamma_{\rm B}}{\rho_{\rm AB}}} \gamma_{\rm B}, \end{aligned} \quad (21)$$

Then, we get

$$\Omega \approx 1 - \beta_{\rm C}\rho_{\rm AB} e^{-\frac{\alpha_{\rm C}}{\rho_{\rm AB}}}\left(e^{\frac{1/2\beta_{\rm C}}{\rho_{\rm AB}}} - e^{-\frac{1/2\beta_{\rm C}}{\rho_{\rm AB}}}\right). \quad (22)$$

For large values of $\rho_{\rm AB}$, (22) can be further simplified as

$$\Omega \approx 1 - e^{-\frac{\alpha_{\rm C}}{\rho_{\rm AB}}}, \quad (23)$$

Exploiting the above approximation, (19) can be further approximated by inserting Ω as given in (23)

$$\bar{\epsilon}_{\rm C} \approx \int_0^\infty \left(1 - e^{-\frac{(r(1+\gamma_{\rm E})-1)}{\rho_{\rm AB}}}\right)\frac{1}{\rho_{\rm AE}} e^{-\frac{\gamma_{\rm E}}{\rho_{\rm AE}}} d\gamma_{\rm E}, \quad (24)$$

and we can obtain the final expression of $\bar{\epsilon}_{\rm C}$ as

$$\bar{\epsilon}_{\rm C} \approx 1 - \frac{\rho_{\rm AB}}{\rho_{\rm AE} r + \rho_{\rm AB}} e^{\frac{1-r}{\rho_{\rm AB}}}. \quad (25)$$

2) $\bar{\epsilon}_{NC}$ calculation: On the other hand, the block error probability of the non-contextual information is defined as

$$\epsilon_{\rm NC} \approx \epsilon_{\rm C} + (1-\epsilon_{\rm C})\epsilon. \quad (26)$$

This implies that the block error probability of non-contextual information can be expressed as the sum of the block error probability of contextual information and the conditional probability that, given the context is not in error, but the non-contextual information is in error. Then, the expected average block error probability of non-contextual data is expressed as

$$\mathbb{E}[\epsilon_{\rm NC}] = \mathbb{E}[\epsilon_{\rm C}] + (1 - \mathbb{E}[\epsilon_{\rm C}])\mathbb{E}[\epsilon] \quad (27)$$

where $\mathbb{E}[.]$ is the expectation operator. To find the average decoding block error probability of a channel with a given transmission rate as shown in (4), the following calculation is determined

$$\bar{\epsilon} = \int_0^\infty \epsilon f(\gamma_{\rm B}) d\gamma_{\rm B}. \quad (28)$$

A similar calculation in the block error probability of contextual information was performed here to apply the approximation in (14). The parameters are found by setting $Q\left(\sqrt{\frac{n}{V_{\gamma_{\rm B}}}}\left(\log(1+\gamma_{\rm B}) - \frac{b}{n}\log(2)\right)\right) = 1/2$ and solving $\left(\log(1+\alpha) - \frac{b}{n}\log(2)\right) = 0$, and the following solutions are found

$$\begin{aligned} \alpha &= e^{\frac{b}{n}\log(2)} - 1, \\ \beta &= -\sqrt{\frac{n}{2\pi(e^{2\frac{b}{n}\log(2)} - 1)}}. \end{aligned} \quad (29)$$

Then, the approximation is obtained as follows

$$\bar{\epsilon} \approx 1 - e^{-\frac{\alpha}{\rho_{\rm AB}}}. \quad (30)$$

By substituting this result in (27), it becomes

$$\bar{\epsilon}_{\rm NC} \approx \bar{\epsilon}_{\rm C} + (1-\bar{\epsilon}_{\rm C})(1 - e^{-\frac{\alpha}{\rho_{\rm AB}}}), \quad (31)$$

Finally, the average block error probability of the non-contextual data transmission is found in the following extended form

$$\bar{\epsilon}_{\rm NC} \approx \left(1 - \frac{\rho_{\rm AB}}{\rho_{\rm AE} r + \rho_{\rm AB}} e^{\frac{1-r}{\rho_{\rm AB}}}\right) + \left(\frac{\rho_{\rm AB}}{\rho_{\rm AE} r + \rho_{\rm AB}} e^{\frac{1-r}{\rho_{\rm AB}}}\right)(1 - e^{-\frac{\alpha}{\rho_{\rm AB}}}), \quad (32)$$

The expression in (32) is further simplified as

$$\bar{\epsilon}_{\rm NC} \approx 1 - {\rm K} e^{-\frac{\alpha}{\rho_{\rm AB}}}. \quad (33)$$

where ${\rm K} = \frac{\rho_{\rm AB}}{\rho_{\rm AE} r + \rho_{\rm AB}} e^{\frac{1-r}{\rho_{\rm AB}}}$.

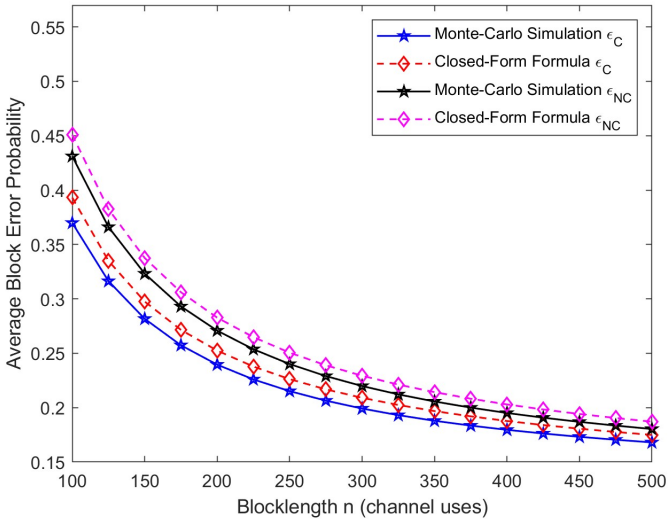

Fig. 1. Average block error probability for contextual data and average error probability for non-contextual data vs blocklength.

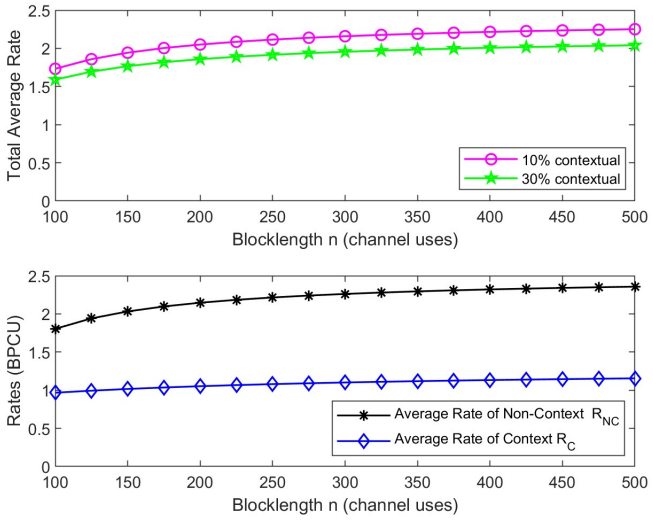

Fig. 2. Average transmission rates vs blocklength.

III. Numerical Results

In this section, the simulation results validating the accuracy of the analytical expression are presented. Unless otherwise stated, the system parameters are as follows for all the numerical evaluations: Information message length is $b = 100$ bits, the blocklength n ranges from 100 to 500, distances are $d_{\text{AB}} = 1, d_{\text{AE}} = 2$m, the transmit power of Alice is 10 dB, the information leakage probability is $\delta = 10^{-4}$, and the path-loss exponent is $v = 3$. It is assumed that 90% of the transmitted packets contain non-contextual information. All the simulation results are obtained by averaging over $100,000$ trials.

Fig. 1 shows the average block error probability of contextual and non-contextual data by assuming Bob is positioned closer to Alice than Eve. The closed-form formulas for both types of packets are plotted alongside Monte-Carlo simulations, which validate the proposed formulas. As illustrated in the figure, ϵ_{NC} is slightly larger than ϵ_{C} given the system parameters. For a fixed b, when the ratio of b/n is large, the block error probabilities for both types of data are higher.

Fig. 2 illustrates the relationship between the individual rates of context and non-context data. The average rate of context data is lower than that of non-context data, because context is constrained by the secrecy rate of a wiretap channel, whereas non-context data corresponds to the Shannon rate and the expectation is that the non-context communication rate is higher than of the context. The context rate remains consistent across all block lengths, while the non-context rate rises slightly. In addition, the non-contextual information is not useful unless the contextual information is correctly detected, the total rate is only dependent on the proportion of the contextual packets to the non-contextual packets, which can be demonstrated by the average of the indicator I. To this end, when the ratio of the contextual packets increases, total average rate tends to decrease.

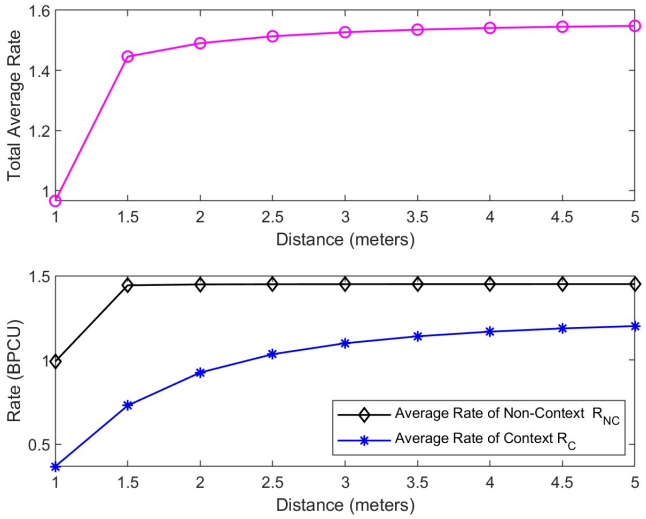

Fig. 3. Average transmission rates vs distance.

Mobility should be considered carefully to assess the secure communication strategies. In Fig. 3, the system's performance is evaluated by varying the distance between the eavesdropper and the transmitter to assess its impact on the total average rate. In this analysis, information bits are transmitted over a blocklength of $n = 200$. The distance between the transmitter and the legitimate receiver is fixed at 1 meter. Then, the eavesdropper is positioned at the same distance, which starts at 1 meter, and gradually moves further away from the transmitter. The average non-context rate stabilizes after reaching a peak, whereas the average context rate, which represents the secrecy rate, increases as the eavesdropper moves away. The total average rate also shows a peak followed by a slight rise.

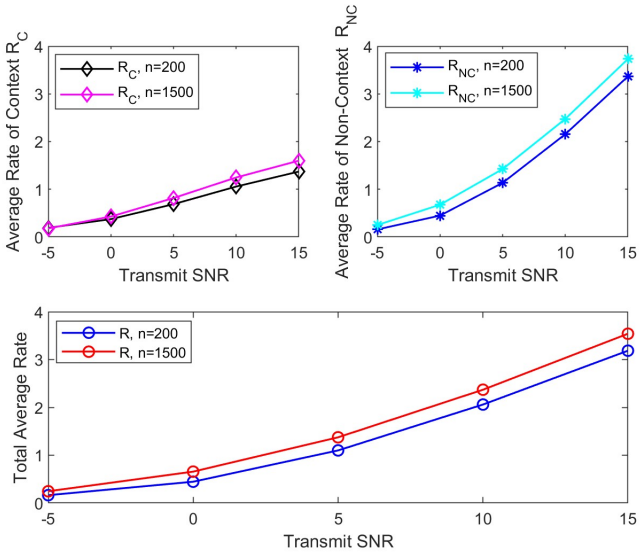

Fig. 4. Average transmission rates vs transmit power of Alice.

Lastly, the impact of transmit power is depicted in Fig. 4, where the analysis compares short and large blocklengths for transmitting an equal amount of information bits ($b = 100$). While both the average context rate and the average non-context rate increase with transmit power, the average context rate consistently remains lower. Moreover, the performance of short packets are comparable to that of larger ones. For transmitting 100 bits, a shorter packet length is sufficient to maintain a similar average rate.

IV. Conclusion

In this paper, the security performance of PLS of context-aware communication is studied with the help of short packet transmission. The framework has been proposed to approximate a wiretap channel rate, ensuring the packets containing contextual information remain secure. This approach demonstrated how to evaluate the security of a system within the scope of physical layer security. Specifically, average block error probabilities of contextual and non-contextual data are derived. Then, a total rate is introduced by distinguishing contextual and non-contextual data rates. Numerical results verify the accuracy of the proposed approximation method. Subsequently, the impacts of blocklength, distance, and transmit power are observed. The rate for contextual information remains low to secure packet transmission in contrast to the non-contextual rate. Additionally, the increase in the contextual packet ratio further lowers the overall average rate. Furthermore, the analysis reveals that short packet communication can achieve good performance compared to larger packet lengths, making it an efficient and secure method for transmitting information. Context-aware approaches in physical layer security with short packet communication demonstrate significant potential in enhancing data transmission security. These findings highlights the importance of integrating context-awareness into physical layer security to optimize both performance and security in future communication systems.

References

[1] C. Feng and H.-M. Wang, "Secure short-packet communications at the physical layer for 5G and beyond," *IEEE Commun. Stand. Mag.*, vol. 5, no. 3, pp. 96–102, Sep. 2021.

[2] A. Chorti, A. Noll-Barreto, S. Köpsell, M. Zoli, M. Chafii, P. Sehier, G. Fettweis, and H. V. Poor, "Context-aware security for 6G wireless: The role of physical layer security," *IEEE Commun. Stand. Mag.*, vol. 6, no. 1, pp. 102–108, Mar. 2022.

[3] M. Mitev, A. Chorti, H. Poor, and G. Fettweis, "What physical layer security can do for 6G security," *IEEE Open Journal of Vehic. Tech.*, vol. 4, pp. 375–388, Feb. 2023.

[4] C. E. Shannon, "Communication theory of secrecy systems," *The Bell system technical journal*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[5] A. D. Wyner, "The wire-tap channel," *Bell system technical journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[6] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proceedings of the National Academy of Sciences*, vol. 114, no. 1, pp. 19–26, Jan. 2017.

[7] Y. Polyanskiy, H. V. Poor, and S. Verdú, "Channel coding rate in the finite blocklength regime," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2359, May 2010.

[8] W. Yang, R. F. Schaefer, and H. V. Poor, "Finite-blocklength bounds for wiretap channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Barcelona, Spain, Jul. 2016, pp. 3087–3091.

[9] ——, "Secrecy-reliability tradeoff for semi-deterministic wiretap channels at finite blocklength," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Aachen, Germany, Jun. 2017, pp. 2133–2137.

[10] ——, "Wiretap channels: Nonasymptotic fundamental limits," *IEEE Trans. Inf. Theory*, vol. 65, no. 7, pp. 4069–4093, Jul. 2019.

[11] H. Wang, Q. Yang, Z. Ding, and H. V. Poor, "Secure short-packet communications for mission-critical IoT applications," *IEEE Trans. Wireless Commun.*, vol. 18, no. 5, pp. 2565–2578, May 2019.

[12] T. Zheng, H. Wang, D. W. K. Ng, and J. Yuan, "Physical-layer security in the finite blocklength regime over fading channels," *IEEE Trans. Wireless Commun.*, vol. 19, no. 5, pp. 3405–3420, May 2020.

[13] L. Wei, Y. Yang, and B. Jiao, "Secrecy throughput in full-duplex multiuser MIMO short-packet communications," *IEEE Wireless Commun. Lett.*, vol. 10, no. 6, pp. 1339–1343, Jun. 2021.

[14] N. Arı, N. Thomos, and L. Musavian, "Performance analysis of short packet communications with multiple eavesdroppers," *IEEE Trans. Commun.*, vol. 70, no. 10, pp. 6778 –6789, Oct. 2022.

[15] T. Nguyen and V. Quoc Bao, "Secure short-packet communications in dual-hop cooperative IoT networks with multiple eavesdroppers," in *RIVF International Conference on Computing and Communication Technologies (RIVF)*, Hanoi, Vietnam, Dec. 2023, pp. 189–193.

[16] T. Yu, X. Sun, and Y. Cai, "Secure short-packet transmission in uplink massive MU-MIMO IoT Networks," in *Proc. Int. Conf. Wirel. Commun. Signal Process. (WCSP)*, Nanjing, China, Oct. 2020, pp. 50–55.

[17] M. Mitev, T. Pham, A. Chorti, A. Noll-Barreto, and G.Fettweis, "Physical layer security - from theory to practice," *IEEE BITS Mag.*, vol. 3, no. 2, pp. 67 – 79, Jun. 2023.

[18] W. Yang, G. Durisi, T. Koch, and Y. Polyanskiy, "Quasi-static simo fading channels at finite blocklength," in *Proc. IEEE Int. Symp. Inf. Theory*, Istanbul, Turkey, Jul. 2013, pp. 1531–1535.

[19] P. Mary, J.-M. Gorce, A. Unsal, and H. V. Poor, "Finite blocklength information theory: What is the practical impact on wireless communications?" in *IEEE Glob. Commun. Conf. (GC Wkshps)*, Washington, DC, USA, Dec. 2016, pp. 1–6.

[20] B. Makki, T. Svensson, and M. Zorzi, "Finite block-length analysis of the incremental redundancy HARQ," *IEEE Wireless Commun. Lett.*, vol. 3, no. 5, pp. 529–532, Oct. 2014.