Performance Analysis of Short Packet Communications with Multiple Eavesdroppers

Nihan Arı, *Member, IEEE,* Nikolaos Thomos, *Senior Member, IEEE,*
and Leila Musavian, *Member, IEEE*

***Abstract*—This paper studies the performance of short packet communications in the presence of multiple eavesdroppers. We start our investigation by examining the fading wiretap channel, where the communication is overheard by multiple non-colluding single antenna eavesdroppers. A closed-form expression for the average secrecy throughput is derived, when the transmitter has a single antenna. The Monte-Carlo simulations show a close match of the analytical expression with the numerical results. Moreover, the optimal blocklength value that maximizes the secrecy throughput is determined, when the communication is observed by single and multiple eavesdroppers. We then extend our analysis for the case of a multiple-antenna transmitter and consider artificial noise (AN) to confuse the eavesdroppers. A closed-form expression for the average secrecy throughput is obtained for the scenario of a two-antenna transmitter and two eavesdroppers with a single antenna. The results demonstrate the validity of the approximation when compared with Monte-Carlo simulations. The results further reveal that an increased number of antennas at the transmitter is associated with higher average secrecy throughput and applying AN helps to eliminate the harm of the eavesdroppers.**

***Index Terms*—Finite blocklength, physical layer security, secrecy throughput, multiple eavesdroppers, multiple antennas**

I. Introduction

PHYSICAL layer security (PLS) has received a lot of interest in recent years. It exploits the randomness of the wireless medium for securing communication, eliminating the need to use cryptographic solutions which are computationally expensive [1]. This renders PLS a potential candidate for securing future communication systems. These systems need to support different traffic types, including those consisting of shorter packets like industrial Internet of Things (IoT) messages, and haptic communications packets, among others, that demand low latency and increased reliability. In practical wireless communication systems, the communication is subject to overhearing by external eavesdroppers due to the broadcast nature of wireless communications. Particularly, the use of short packets introduces a penalty on the secrecy capacity because it is well-known that PLS is based on the assumption that transmission happens with a maximum rate reliably and securely when the blocklengths are sufficiently large. Therefore, the communication links that transmit short packets may become more prone to security attacks. Apart from that, in applications like IoT, there are typically a massive number of connected devices and users. Due to the large-scale nature of the 5G systems, they may be less robust to adversaries. On the other hand, short packet communications result in new challenges in terms of security. Although existing works on PLS have extensively investigated several communication scenarios for wiretap channels, there are only a few studies that focus on PLS for short packet communications. Further, the existing works are limited as they mainly assume a single eavesdropper. Motivated by the above, in this paper, we conduct a short packet analysis of PLS for multiple eavesdroppers and multiple-antenna transmitter settings.

N. Arı, N. Thomos, L. Musavian are with the School of Computer Science and Electronic Engineering, University of Essex, Colchester CO4 3SQ, U.K. (e-mails: nkaraca@essex.ac.uk; nthomos@essex.ac.uk; leila.musavian@essex.ac.uk).

Manuscript received December 06, 2021; revised May 12, 2022 and July 23, 2022; accepted July 31, 2022. The associate editor coordinating the review of this article and approving it for publication was Dr. Kyeong Jin Kim. (*Corresponding author: Nihan Arı.*)

Part of this paper is published in 2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC).

A. Related Works and Motivations

This section summarizes works studying single and multiple-antenna transmitters in the wiretap channels under the presence of multiple eavesdroppers when medium to large size packets are employed. A framework to find the maximum secrecy level for a multiple-input multiple-output (MIMO) channel when there are multiple multiple-antenna eavesdroppers in unknown locations was presented in [2]. AN-aided transmission strategy that results in maximizing the secrecy rate was considered in [3] for a multiple-input single-output (MISO) channel in the presence of multiple eavesdroppers. On the other hand, the secrecy outage probability (SOP) for a wiretap channel scenario, which involves MISO wiretap channel in the presence of Poisson distributed passive eavesdroppers, was obtained in [4]. The proposed approach employed AN and used stochastic geometry theory to provide a solution to the defined problem. A comprehensive study on performance analysis for the scenario of randomly located eavesdroppers with a multiple-antenna transmitter, which injects AN, was presented in [5]. A closed-form expression was derived for the optimal power allocation that minimizes secrecy outage probability. Similarly, AN-aided secure transmission in MISO channels was investigated in [6]. A semi-adaptive transmission scheme was proposed in [7] where the focus was on maximization of the secrecy throughput. In another study [8], a MISO multiple eavesdropper system with the existence of two receivers, where one of them receives the confidential data and the other one helps to confuse the eavesdroppers, are considered. Transmission schemes that maximize the effective secrecy throughput (EST) are investigated as well as the joint

optimization of power allocations and wiretap code rates. In [9], a traditional cellular and a millimeter wave base station are compared by obtaining the secrecy throughput and millimeter wave systems are found to improve the secrecy performance. Unlike the mentioned studies, which focused on passive and non-colluding eavesdroppers, cooperation between the adversaries are also explored in the literature. Both non-colluding and colluding eavesdroppers cases are analysed in [10] and [11] to obtain the probability of secrecy outage. The study in [12] takes into account a different scenario, where the model is finite-sized in-band selective relaying system with multiple transmitters and multiple collaborative eavesdroppers. Closed-form expressions of the secrecy outage probability, probability of non-zero achievable secrecy rate and ergodic secrecy rate are derived. Relaying scenario is again considered in [13] and the expressions for the secrecy outage probability, the non-zero secrecy rate and the ergodic secrecy rate are obtained, while a group of eavesdroppers monitors the relays.

Recent works in [14]–[16] extended their analysis in wiretap channel scenarios by focusing on short packet communications. The authors in [14] investigated the performance of secure short packet communications in a mission-critical IoT system in the presence of a multiple-antenna eavesdropper. In this work, the AN impact on the system performance was analyzed and also the optimal blocklength that maximizes the secrecy throughput was found. The impact of finite blocklength secrecy coding on the design of secure transmission in a wiretap channel was explored in [15]. Specifically, an optimization problem was defined, which aimed at maximizing the secrecy throughput considering various blocklengths, code rates, and transmission policies. Moreover, the power allocation of AN was optimized for a multiple-antenna setting. In [16], a full-duplex multiple-user MIMO wiretap scenario was introduced. The system performance was again quantified by secrecy throughput, and the transmission strategy was explored by considering self-interference, co-channel interference, and imperfect channel state information.

The aforementioned studies either consider multiple independent/collaborative adversaries with no limitation on the blocklength size or take into account a single eavesdropper in the context of short packet communications. Specifically, the presence of a single eavesdropper may not be representative of practical settings, where typically multiple eavesdroppers exist. In addition, to the best of our knowledge, the security of wiretap channels against multiple adversaries in the context of secrecy throughput for short packet communications has not been studied previously. In this work, we focus on secure short packet communications against multiple independent passive eavesdroppers, when the transmitter is equipped with either a single or multiple antennas. The multiple-antenna transmitter case scenario allows us to show the impact of AN on the system performance.

B. Contributions

This paper examines the average secrecy throughput of secure short packet communications between legitimate parties when multiple, passive, and single-antenna eavesdroppers exist. This research aims to address the design of short packet communications for large-scale networks under the presence of multiple adversaries. Specifically, the novelty of our work lies on the fact that we assume each eavesdropper is independent, a.k.a. non-colluding. Further, any of the eavesdroppers has the ability to individually overhear the transmitted message that is intended for the legitimate receiver, but each eavesdropper channels are affected by different fading parameters. If multiple eavesdroppers can collaborate and perform joint processing and try to decode the message with the gathered information, namely colluding eavesdroppers, then they can be seen as a single eavesdropper with multiple antennas, which is not the case in our system model. Our work is based upon our preliminary study presented in [17], where we analyzed the performance of the system for a transmitter with a single antenna scenario. In this paper, we extend those findings to the case of a multiple-antenna transmitter and carry out an optimal blocklength evaluation.

The main contributions of this paper are listed as follows:

- We derive a closed-form approximation of average secrecy throughput for the single antenna transmitter scenario when multiple eavesdroppers exist. The proposed approximation is validated through Monte-Carlo simulations, which show the validity of our approximation;
- We provide a framework to derive the optimal blocklength that maximizes the average secrecy throughput for both single and multiple eavesdroppers cases;
- We formulate the average secrecy throughput for the multiple-antenna transmitter case, where AN is introduced to the system model to confuse the eavesdroppers. We obtained a closed-form expression for the special case, where the transmitter has two antennas, and there are two eavesdroppers. Monte-Carlo simulations show the closeness of the closed-form formula with the simulations;
- Finally, we study extensively the impact of the AN, the number of transmitter antennas, and the number of eavesdroppers on system security performance.

The rest of the paper is organized as follows. Section II describes the system model and performance metric formulation. The average secrecy throughput is also characterized in this section. Section III presents an analysis for both single and multiple-antenna transmitter settings. Section IV presents the corresponding numerical results and discussion. Finally, Section V concludes the paper and summarizes the numerical findings.

Notation: Small letters depict scalars. Matrices are denoted by capital bold letters, while vectors are represented by bold lower case letters. $\mathbb{E}\{.\}$ denotes expectation operator. $f(.)$ and $F(.)$ stand for the probability density function (PDF) and the cumulative distribution function (CDF). $\Pr(.)$ represents probability. $[.]^T$, $[.]^\dagger$ denote the transpose and Hermitian transpose, respectively. $\mathcal{N}(\mu, \sigma^2)$ means μ-mean complex Gaussian distribution with variance σ^2. $|.|$ and $||.||$ correspond to absolute value and norm. $\mathbb{C}$ shows the set of complex numbers.

II. SYSTEM MODEL AND PERFORMANCE METRIC FORMULATION

A. Average Secrecy Throughput

In this work, the average secrecy throughput is used as the performance metric. Therefore, in this section, we will first introduce what steps are followed to obtain the average secrecy throughput, then this approach is implemented for single and multiple-antenna transmitter cases, respectively.

Secrecy capacity is the theoretical upper bound of the secret information rate of a wiretap channel. The maximum secret information rate over a wiretap channel is achieved only when the message is mapped to sufficiently long codewords that renders both the decoding error probability ϵ and information leakage δ very small [18], [19]. For the finite blocklength case, the impact of the decoding error probability and information leakage probability on both receiver and eavesdropper are not negligible. In other words, the transmission rate stays close to the channel capacity when the decoding error probability tends to zero at infinite blocklength. For this reason, the channel capacities of the main and wiretapper cannot be achieved with low error probabilities when the blocklength n is finite. In addition, in short packet communications, classical information-theoretic performance metrics, such as secrecy outage probability, do not apply [20]. Therefore, it is fundamental to investigate the achievable secrecy rate for finite blocklengths. For short codewords with blocklength n, given a target decoding error probability ϵ and information leakage probability δ, the maximal achievable secrecy rate $R^*(n,\epsilon,\delta)$ can be approximated (as in [14], [21]–[23]) as follows

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

where $V_{\gamma_{\rm B}} = 1-(1+\gamma_{\rm B})^{-2}$ and $V_{\gamma_{\rm E}} = 1-(1+\max\limits_{k}\gamma_{{\rm E}_k})^{-2}$ are the dispersion of the main and eavesdropper channels, respectively. $Q(x)$ is the Q-function, which is defined as $Q(x)=\int_x^\infty \frac{1}{\sqrt{2\pi}}e^{-\frac{t^2}{2}}dt$, while $Q^{-1}(x)$ represent its inverse. Under the considered setting, the secrecy capacity can be, hence, computed as

$$C_{\rm s} = \begin{cases} C_{\rm B} - C_{\rm E}, & \text{when} \quad \gamma_{\rm B} > \gamma_{\rm E}, \\ 0, & \text{when} \quad \gamma_{\rm B} \le \gamma_{\rm E}, \end{cases} \quad (2)$$

where the capacity of the main channel is

$$C_{\rm B} = \log_2(1+\gamma_{\rm B}), \quad (3)$$

and the capacity of the strongest eavesdropper's channel equals to

$$\begin{aligned} C_{\rm E} &= \log_2(1+\max_k \gamma_{{\rm E}_k}) \\ &= \log_2(1+\gamma_{\rm E}). \end{aligned} \quad (4)$$

Each independent eavesdropper channels are affected by different fading parameters and any of the eavesdroppers can individually retrieve the message that is intended for Bob. In this case, secure communication has limitation and can only be guaranteed when the instantaneous SNR of the legitimate receiver is larger than the strongest eavesdropper. In addition, the secrecy capacity will be almost zero, if eavesdroppers are located closer to Alice than Bob. Therefore, to achieve a non-zero secrecy capacity, all eavesdroppers should be prevented to be close to the transmitter than the legitimate receiver and the worst-case scenario is when all eavesdroppers are located on the same distance ring as the legitimate user.

To characterize the decoding error probability, the transmission rate is given by $R^* = b/n$, which corresponds to b bits of information message that is transmitted by the blocklength n. (Throughout this paper, the arguments of (n,ϵ,δ) are dropped in R^*). For $\gamma_{\rm B} > \gamma_{\rm E}$, i.e., when the secrecy capacity is greater than zero, the decoding error probability can be computed according to [14] as

$$\epsilon = Q\left(\sqrt{\frac{n}{V_{\gamma_{\rm B}}}}\left(\log\left(\frac{1+\gamma_{\rm B}}{1+\gamma_{\rm E}}\right) - \sqrt{\frac{V_{\gamma_{\rm E}}}{n}}Q^{-1}(\delta) - \frac{b}{n}\log(2)\right)\right). \quad (5)$$

For $\gamma_{\rm B} \le \gamma_{\rm E}$, the decoding error probability ϵ is set simply to 1. The decoding error probability ϵ in (5) is defined by the instantaneous SNR of the main channel, $\gamma_{\rm B}$, conditioned on the eavesdropper's instantaneous maximum SNR, $\gamma_{\rm E}$, and is represented as $\epsilon_{\gamma_{\rm B}|\gamma_{\rm E}}$.

The average achievable secrecy throughput, $T_{\rm s}$, (measured in bits per channel use (BPCU)), can be computed as [14]

$$\begin{aligned} T_{\rm s} &= \mathbb{E}_{\gamma_{\rm B},\gamma_{\rm E}}\left\{\frac{b}{n}(1-\epsilon)\right\} \\ &= \frac{b}{n}(1-\bar{\epsilon}), \end{aligned} \quad (6)$$

The parameter $\bar{\epsilon} = \mathbb{E}_{\gamma_{\rm B}\gamma_{\rm E}}[\epsilon]$ stands for the average error probability. Therefore, the average successful decoding probability is given by

$$1-\bar{\epsilon} = 1 - \mathbb{E}_{\gamma_{\rm B},\gamma_{\rm E}}[\epsilon]. \quad (7)$$

Now, we can obtain the closed-form approximation for the average secrecy throughput when all the channels are affected by Rayleigh fading, as

$$T_{\rm s} = \int_0^\infty \int_0^\infty (1-\epsilon)\frac{b}{n} f(\gamma_{\rm B}) f(\gamma_{\rm E}) d\gamma_{\rm B} d\gamma_{\rm E}. \quad (8)$$

We can analyze the integral in (8) into two integrals:

$$T_{\rm s} = \frac{b}{n}\int_0^\infty S(\gamma_{\rm E}) f(\gamma_{\rm E}) d\gamma_{\rm E}, \quad (9)$$

and

$$S(\gamma_{\rm E}) = \int_0^\infty (1-\epsilon_{\gamma_{\rm B}|\gamma_{\rm E}}) f(\gamma_{\rm B}) d\gamma_{\rm B}. \quad (10)$$

When $\gamma_{\rm B} \le \gamma_{\rm E}$, which means secrecy capacity is zero, $\epsilon_{\gamma_{\rm B}|\gamma_{\rm E}}$ is set to 1. In the more interesting case $\gamma_{\rm B} > \gamma_{\rm E}$, $\epsilon_{\gamma_{\rm B}|\gamma_{\rm E}}$ has an intractable form, and thus we approximate it using the linearization technique presented in [14], [24], [25]. According to this approximation, it is:

$$\epsilon_{\gamma_{\rm B}|\gamma_{\rm E}}(x) \approx \begin{cases} 1, & x < \alpha + u, \\ \frac{1}{2} + \beta(x-\alpha), & \alpha - u \le x \le \alpha + u, \\ 0, & x > \alpha - u, \end{cases} \quad (11)$$

where $u = \frac{1}{2\beta}$. The parameter α is found by

$$\alpha = e^{\left(\sqrt{\frac{V_{\gamma_{\rm E}}}{n}}Q^{-1}(\delta) + \frac{b}{n}\log(2)\right)}(1+\gamma_{\rm E}) - 1, \quad (12)$$

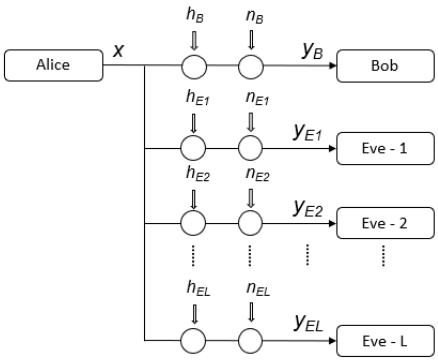

Fig. 1. Wiretap channel model

and β, the slope of the $\epsilon_{\gamma_{\rm B}|\gamma_{\rm E}}(x)$, is computed by

$$\beta = \frac{d\epsilon_{\gamma_{\rm B}|\gamma_{\rm E}}(x)}{dx}\Big|_{x=\alpha} = -\sqrt{\frac{n}{2\pi\alpha(\alpha+2)}}. \tag{13}$$

If we set $V\gamma_{\rm E} \approx 1$, then α can be simplified as:

$$\alpha = e^{\left(\frac{Q^{-1}(\delta)}{\sqrt{n}} + \frac{b}{n}\log(2)\right)}(1+\gamma_{\rm E}) - 1. \tag{14}$$

To derive the final expression, we set $r = e^{\frac{Q^{-1}(\delta)}{\sqrt{n}} + \frac{b}{n}\log(2)}$, and then (14) can be compactly written as

$$\alpha = r(1+\gamma_{\rm E}) - 1. \tag{15}$$

III. SYSTEM ANALYSIS

A. Single Antenna Alice

The considered setting is shown in Fig. 1, where we assume only a single antenna at the transmitter. The transmitter, Alice, wants to send a message to a legitimate receiver, Bob, while the communication is overheard by multiple eavesdroppers, Eves. The message at Alice is encoded into a set of $\mathbf{x}^l = [x(1), x(2), .., x(i), .., x(l)]$ codewords and Bob receives these codewords as

$$y_{\rm B}(i) = h_{\rm B}(i)x(i) + n_{\rm B}(i), \tag{16}$$

where $h_{\rm B}(i)$ is Bob's channel fading coefficient at time i and $n_{\rm B}(i)$ is the Additive White Gaussian Noise (AWGN) experienced during transmission with $n_{\rm B} \sim \mathcal{N}(0, \sigma_{\rm B}^2)$, which has zero mean and variance $\sigma_{\rm B}^2$. As we mentioned, besides Bob, there exist L eavesdroppers and the links connecting them with Alice are represented as E_k, where $k = \{1, \ldots, L\}$. Each eavesdropper observes the main channel transmission and is affected by a fading channel. Assume that the kth eavesdropper overhears the transmission in its attempt to acquire the transmitted information by Alice. Then, the kth eavesdropper observes a message

$$y_{{\rm E}_k}(i) = h_{{\rm E}_k}(i)x(i) + n_{{\rm E}_k}(i), \quad k = 1, 2, .., L, \tag{17}$$

where $h_{{\rm E}_k}(i)$ denotes the fading coefficient at time i of the kth eavesdropper. The transmission is corrupted by AWGN noise of $n_{{\rm E}_k}(i) \sim \mathcal{N}(0, \sigma_{{\rm E}_k}^2)$ with zero mean and variance $\sigma_{{\rm E}_k}^2$. We assume the channel coefficients remain constant over a block period and vary across the blocks independently. Therefore, we omit the time index of the channels coefficients hereafter. The channel state information (CSI) of the legitimate receiver, Bob is known to the transmitter, Alice, while only the statistics of the channel distribution of eavesdroppers are available to the transmitter. This is very common assumption in physical layer security literature, even if the eavesdropper is passive [5], [7], [25]. The instantaneously received signal-to-noise ratio (SNR) at Bob and kth Eve can be formulated as

$$\gamma_{\rm B} = \frac{|h_{\rm B}|^2 P}{\sigma_{\rm B}^2}, \tag{18}$$

and

$$\gamma_{{\rm E}_k} = \frac{|h_{{\rm E}_k}|^2 P}{\sigma_{{\rm E}_k}^2}, \tag{19}$$

respectively, where P is the transmit power. Therefore, Bob's channel average SNR is given by

$$\overline{\gamma}_{\rm B} = \frac{\mathbb{E}\{|h_{\rm B}|^2\}P}{\sigma_{\rm B}^2}, \tag{20}$$

Let us denote the maximum average SNR of all the eavesdroppers now as $\overline{\gamma}_{\rm E}$ and the instantaneous SNR of the strongest eavesdropper as $\gamma_{\rm E} = \max_k \gamma_{{\rm E}_k}$. It holds that

$$\overline{\gamma}_{\rm E} = \frac{\mathbb{E}\{|h_{\rm E}|^2\}P}{\sigma_{{\rm E}_k}^2}. \tag{21}$$

Recall that the channels from transmitter to the legitimate receiver and eavesdroppers are Rayleigh fading. Hence, the probability density function of the main channel, according to [26], is given by

$$f(\gamma_{\rm B}) = \frac{1}{\overline{\gamma}_{\rm B}} e^{-\frac{\gamma_{\rm B}}{\overline{\gamma}_{\rm B}}}. \tag{22}$$

Differently from the setting in [14], which considers an external multi-antenna eavesdropper, our system has multiple independent eavesdropper channels, which their channel gains follow the same distribution. Therefore, according to [26], the probability distribution function of the adversarial channels becomes

$$f(\gamma_{\rm E}) = L\Big(1 - e^{-\frac{\gamma_{\rm E}}{\overline{\gamma}_{\rm E}}}\Big)^{L-1} \frac{1}{\overline{\gamma}_{\rm E}} e^{-\frac{\gamma_{\rm E}}{\overline{\gamma}_{\rm E}}}. \tag{23}$$

The average secrecy throughput evaluation for single antenna Alice is done as follows. First, we compute

$$S(\gamma_{\rm E}) = \int_0^\infty (1 - \epsilon_{\gamma_{\rm B}|\gamma_{\rm E}}(x)) \frac{1}{\overline{\gamma}_{\rm B}} e^{-\frac{\gamma_{\rm B}}{\overline{\gamma}_{\rm B}}} d\gamma_{\rm B}, \tag{24}$$

where $f(\gamma_{\rm B})$ is defined as in (22). Then, the integral can be written for given values of $\gamma_{\rm B} = x$ and $\gamma_{\rm E} = y$ as

$$S(y) = \int_0^\infty (1 - \epsilon_{\gamma_{\rm B}|\gamma_{\rm E}}(x)) \frac{1}{\overline{\gamma}_{\rm B}} e^{-\frac{x}{\overline{\gamma}_{\rm B}}} dx, \tag{25}$$

which can be rewritten as

$$S(y) = 1 - \int_0^\infty \epsilon(x) \frac{1}{\overline{\gamma}_{\rm B}} e^{-\frac{x}{\overline{\gamma}_{\rm B}}} dx. \tag{26}$$

Replacing (11) into (26) yields

$$S(\gamma_{\rm E}) = 1 - \Big(\underbrace{\int_0^{\alpha+u} \frac{1}{\overline{\gamma}_{\rm B}} e^{-\frac{x}{\overline{\gamma}_{\rm B}}} dx}_{\rm D} + \underbrace{\int_{\alpha+u}^{\alpha-u} (\beta(x-\alpha)+1/2) \frac{1}{\overline{\gamma}_{\rm B}} e^{-\frac{x}{\overline{\gamma}_{\rm B}}} dx}_{\rm G} \Big). \tag{27}$$

With some manipulation, we find that the first integral is equal to

$$D = 1 - e^{-\frac{\alpha+u}{\overline{\gamma}_{\rm B}}}, \tag{28}$$

and the second integral is given by

$$G = \beta(\alpha+u+\overline{\gamma}_{\rm B}) e^{-\frac{\alpha+u}{\overline{\gamma}_{\rm B}}} - \beta(\alpha-u+\overline{\gamma}_{\rm B}) e^{-\frac{\alpha-u}{\overline{\gamma}_{\rm B}}} + \Big(\frac{1}{2} - \beta\alpha\Big)\Big(e^{-\frac{\alpha+u}{\overline{\gamma}_{\rm B}}} - e^{-\frac{\alpha-u}{\overline{\gamma}_{\rm B}}}\Big). \tag{29}$$

Thus, by inserting (28) and (29) into (27), the following is obtained

$$S(\gamma_{\rm E}) = \overline{\gamma}_{\rm B}\beta\Big(e^{-\frac{\alpha-u}{\overline{\gamma}_{\rm B}}} - e^{-\frac{\alpha+u}{\overline{\gamma}_{\rm B}}}\Big), \tag{30}$$

and, hence, it is rearranged as

$$S(\gamma_{\rm E}) = \overline{\gamma}_{\rm B}\beta e^{-\frac{\alpha}{\overline{\gamma}_{\rm B}}}\Big(e^{\frac{u}{\overline{\gamma}_{\rm B}}} - e^{-\frac{u}{\overline{\gamma}_{\rm B}}}\Big). \tag{31}$$

Also, by following [14], for large values of $\overline{\gamma}_{\rm B}$, (31) can be further simplified as

$$S(\gamma_{\rm E}) \approx e^{-\frac{\alpha}{\overline{\gamma}_{\rm B}}}. \tag{32}$$

Now, by replacing (32) into (9), we get

$$T_{\rm s} \approx \frac{b}{n}\int_0^{\infty} e^{-\frac{\alpha}{\overline{\gamma}_{\rm B}}} L(1-e^{-\frac{\gamma_{\rm E}}{\overline{\gamma}_{\rm E}}})^{L-1} \frac{1}{\overline{\gamma}_{\rm E}} e^{-\frac{\gamma_{\rm E}}{\overline{\gamma}_{\rm E}}} d\gamma_E \Longrightarrow$$
$$T_{\rm s} \approx \frac{bL}{n\overline{\gamma}_{\rm E}}\int_0^{\infty} e^{-\frac{\alpha}{\overline{\gamma}_{\rm B}}} e^{-\frac{\gamma_{\rm E}}{\overline{\gamma}_{\rm E}}} (1-e^{-\frac{\gamma_{\rm E}}{\overline{\gamma}_{\rm E}}})^{L-1} d\gamma_{\rm E}. \tag{33}$$

Thus, we find

$$T_{\rm s} \approx \frac{bL}{n\overline{\gamma}_{\rm E}}\int_0^{\infty} e^{-\frac{r(1+\gamma_{\rm E})-1}{\overline{\gamma}_{\rm B}}} e^{-\frac{\gamma_{\rm E}}{\overline{\gamma}_{\rm E}}} (1-e^{-\frac{\gamma_{\rm E}}{\overline{\gamma}_{\rm E}}})^{L-1} d\gamma_{\rm E} \Longrightarrow$$
$$T_{\rm s} \approx \frac{bL}{n\overline{\gamma}_{\rm E}} e^{\frac{1-r}{\overline{\gamma}_{\rm B}}} \int_0^{\infty} e^{-(\frac{\overline{\gamma}_{\rm E} r - \overline{\gamma}_{\rm B}}{\overline{\gamma}_{\rm B}\overline{\gamma}_{\rm E}})\gamma_{\rm E}} (1-e^{-\frac{\gamma_{\rm E}}{\overline{\gamma}_{\rm E}}})^{L-1} d\gamma_{\rm E}. \tag{34}$$

by using the following based on [27, Eq. 3.312.1]

$$\int_0^{\infty} \big(1-e^{-\frac{x}{\beta}}\big)^{v-1} e^{-\mu x} dx = \beta {\rm B}(\beta\mu, v), \quad [{\rm Re} \quad \beta, v, \mu > 0], \tag{35}$$

where Re depicts the real part of the imaginary numbers and the beta function ${\rm B}(.,.)$ can be represented as follows [27, Eq. 8.384.1]:

$${\rm B}(x,y) = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)} \tag{36}$$

where $\Gamma(z) = \int_0^{\infty} t^{z-1} e^{-t} dt$ is the gamma function [27, Eq. 8.310.1]. Therefore, our simplified expression for the average secrecy throughput is given by:

$$T_{\rm s} \approx \frac{bL}{n} e^{\frac{1-r}{\overline{\gamma}_{\rm B}}} {\rm B}(z, L), \tag{37}$$

with $z = \frac{\overline{\gamma}_{\rm E} r + \overline{\gamma}_{\rm B}}{\overline{\gamma}_{\rm B}}$.

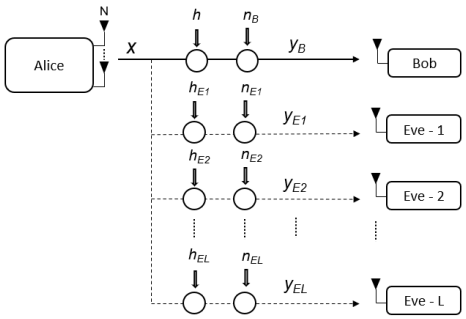

Fig. 2. Multi-antenna transmitter system model

For the case of single antenna Alice and single antenna single Eve, we set $L = 1$ to (37) and we can further simplify the average secrecy throughput as follows

$$T_{\rm s1} \approx \frac{b\overline{\gamma}_{\rm B} e^{\frac{1-r}{\overline{\gamma}_{\rm B}}}}{n(\overline{\gamma}_{\rm E} r + \overline{\gamma}_{\rm B})}. \tag{38}$$

When there is flexibility in choosing the blocklength n, we can determine the value of n that optimizes the secrecy throughput. To do so, we evaluate the optimal blocklength n considering that the message size b is fixed. We find that the optimal blocklength that maximizes the secrecy throughput for single-antenna Alice and a single Eve is characterized by Lemma 1.

Lemma 1: For the case of a single eavesdropper, the optimal blocklength that gives the highest secrecy throughput for (38) can be determined by solving

$$\Delta(n) = \Big(\frac{Q^{-1}(\delta)}{2\sqrt{n}} + \frac{b}{n}\log(2)\Big)\Big(r + \frac{\overline{\gamma}_{\rm E}\overline{\gamma}_{\rm B} r}{\overline{\gamma}_{\rm E} r + \overline{\gamma}_{\rm B}}\Big) - \overline{\gamma}_{\rm B} = 0, \tag{39}$$

taking into consideration that blocklength should be a positive value. The optimal blocklength can be determined by applying bisection method. The proof can be found in Appendix A.
Now, we focus on finding the optimal blocklength for the wiretap channel, which consists of single-antenna Alice and multiple Eves in the following.

Lemma 2: For the case of multiple eavesdroppers, the optimal blocklength for (37) is obtained by finding a positive root of the following expression by setting it to zero.

$$\Omega(n) = \frac{1}{n\overline{\gamma}_{\rm B}}\Big(Mr\Big(1 + \overline{\gamma}_{\rm E}\big(\psi_0(z+L) - \psi_0(z)\big)\Big) - \overline{\gamma}_{\rm B}\Big) = 0, \tag{40}$$

where $\psi_0(.)$ is the digamma function [28, Eq. 6.3.1], which is the logarithmic derivative of the gamma function. Similar to the single antenna case, the bisection search method is applied to solve the expression numerically. The proof is given in Appendix B.

B. Multiple-Antenna Alice

In this section, we consider the more general case, where multiple-antenna Alice communicates with Bob under the presence of L non-colluding passive eavesdroppers. In particular, the transmitter, Alice, is equipped with N antennas,

while the receiver and the eavesdroppers are equipped with a single antenna. The system model is presented in Fig. 2. All channels are Rayleigh fading and are independent of each other. In this setting, secure communication is achieved only when no eavesdropper can retrieve the information of the transmitted message. $\mathbf{h}_{\mathrm{B}}$ is $1\times N$ vector denoting the main channel between Alice and Bob. The elements of $\mathbf{h}_{\mathrm{B}}$ are independent and identically distributed zero-mean complex Gaussian random variables with unit variance. The transmitted signal $\mathbf{x}$ in Alice consists of two parts, x_t, which is the information to be sent to the receiver Bob and $\mathbf{x}_a$, which is the $(N-1)\times$ 1 vector of artificial noise signal added to confuse the eavesdroppers [8], [29], [30]. The AN is transmitted to degrade the quality of channels in all directions except towards Bob. Transmission happens with the help of $N \times N$ matrix of $\mathbf{W} = [\mathbf{w}_t, \mathbf{W}_a]$, which is an orthonormal basis of $\mathbb{C}^N$ and a unitary matrix. The reason to transmit $\mathbf{W}$ as AN is to reduce the quality of the received signal by Eves. While $\mathbf{w}_t$ is used to transmit x_t, $\mathbf{W}_a$ is used for transmission of $\mathbf{x}_a$. $\mathbf{w}_t$ is chosen as the largest eigenvalue vector of $\mathbf{h}_{\mathrm{B}}^{\dagger}||\mathbf{h}_{\mathrm{B}}||$, where $\mathbf{h}_{\mathrm{B}}^{\dagger}$ corresponds to the Hermitian transpose of $\mathbf{h}_{\mathrm{B}}$ and the rest of the $(N-1)$ eigenvectors are used for transmitting $\mathbf{W}_a$. Also, $\mathbf{w}_t$ is normalized as $||\mathbf{w}_t||^2 = 1$. Overall, $N\times$ 1 transmitted vector at Alice is given by

$$\mathbf{x} = [\mathbf{w}_t \quad \mathbf{W}_a][x_t \quad \mathbf{x}_a]^T = \mathbf{w}_t x_t + \mathbf{W}_a \mathbf{x}_a. \tag{41}$$

The received signal at Bob

$$\begin{aligned} y_{\mathrm{B}} &= \mathbf{h}_{\mathrm{B}}\mathbf{x} + n_{\mathrm{B}} \\ y_{\mathrm{B}} &= \mathbf{h}_{\mathrm{B}}\mathbf{w}_t x_t + \mathbf{h}_{\mathrm{B}}\mathbf{W}_a\mathbf{x}_a + n_{\mathrm{B}} \\ y_{\mathrm{B}} &= \mathbf{h}_{\mathrm{B}}\mathbf{w}_t x_t + n_{\mathrm{B}}. \end{aligned} \tag{42}$$

and n_{B} like in the single antenna case is AWGN with $n_{\mathrm{B}} \sim (0, {\sigma_{\mathrm{B}}}^2)$. The reason of the transition in the equation (42) is the columns of $\mathbf{W}_a$ create $\mathbf{h}_{\mathrm{B}}\mathbf{W}_a = \mathbf{0}$. This happens as $\mathbf{W}_a$ is chosen such that it lies on the null space of $\mathbf{h}_{\mathrm{B}}$ so that Bob is not affected by AN. The elements of each $\mathbf{h}_{\mathrm{E}_k}$ are independent and identically distributed zero mean complex Gaussian random variables with unit variance. The received signal at kth Eve

$$\begin{aligned} y_{\mathrm{E}_k} &= \mathbf{h}_{\mathrm{E}_k}\mathbf{x} + n_{\mathrm{E}_k} \\ y_{\mathrm{E}_k} &= \mathbf{h}_{\mathrm{E}_k}\mathbf{w}_t x_t + \mathbf{h}_{\mathrm{E}_k}\mathbf{W}_a\mathbf{x}_a + n_{\mathrm{E}_k}, \quad k = 1, 2, .., L. \end{aligned} \tag{43}$$

and n_{E_k} is AWGN with $n_{\mathrm{E}_k} \sim (0, {\sigma_{\mathrm{E}_k}}^2)$. Similar to the single antenna case, P denotes the total transmit power. We define a parameter, ϕ, which represents the power allocation ratio ($0 < \phi \leq 1$) between the information signal power and AN. In other words, it represents the fraction of the power allocated to x_t. Alice equally allocates the transmit power of AN to each entry of $\mathbf{x}_a$. Hence, the total power is $P = {\sigma_t}^2 + {\sigma_a}^2(N-1)$, where the variance of the transmitted information signal equals to ${\sigma_t}^2 = \phi P$ and the variance of artificial noise equals to ${\sigma_a}^2 = \frac{(1-\phi)P}{(N-1)}$. Additionally, the scope of this work does not cover the power allocation optimization issues, which we plan to investigate in the future. The average SNR at Bob is given by

$$\overline{\gamma}_{\mathrm{B}} = \frac{P}{{\sigma_{\mathrm{B}}}^2}, \tag{44}$$

and the instantaneous received SNR at Bob

$$\gamma_{\mathrm{B}} = \phi\overline{\gamma}_{\mathrm{B}}||\mathbf{h}_{\mathrm{B}}||^2. \tag{45}$$

Next, we define the statistics of γ_{B} according to $||\mathbf{h}_{\mathrm{B}}||^2 \sim \Gamma(N, 1)$ due to multiple antennas at the transmitter under Rayleigh fading environment

$$f_{\gamma_{\mathrm{B}}}(\gamma) = \frac{\gamma^{N-1}e^{-\frac{\gamma}{\phi\overline{\gamma}_{\mathrm{B}}}}}{(\phi\overline{\gamma}_{\mathrm{B}})^N\Gamma(N)}. \tag{46}$$

Further, the cumulative distribution function of γ_{B} is given as

$$\begin{aligned} F_{\gamma_{\mathrm{B}}}(\gamma) &= 1 - \frac{\Gamma(N, \frac{\gamma}{\phi\overline{\gamma}_{\mathrm{B}}})}{\Gamma(N)}, \quad \text{or} \\ F_{\gamma_{\mathrm{B}}}(\gamma) &= 1 - e^{-\frac{\gamma}{\phi\overline{\gamma}_{\mathrm{B}}}}\sum_{k=0}^{N-1}\frac{1}{k!}\Big(\frac{\gamma}{\phi\overline{\gamma}_{\mathrm{B}}}\Big)^k. \end{aligned} \tag{47}$$

As in this work, we consider the presence of multiple eavesdroppers, secure message transmission is only possible when the channel gain between the transmitter and the legitimate receiver is greater than the maximum gain between the transmitter and any of the eavesdroppers. Therefore, the secrecy capacity, when there are multiple eavesdroppers, depends on the strongest eavesdropper's (best channel condition), i.e., the channel, which is less degraded by fading and noise. The average signal-to-interference-plus-noise-ratio (SINR) at kth Eve is equal to

$$\overline{\gamma}_{\mathrm{E}_k} = \frac{P}{\sigma_{\mathrm{E}_k}^2}, \tag{48}$$

and the instantaneous received SINR at the kth Eve is

$$\begin{aligned} \gamma_{\mathrm{E}_k} &= \frac{\phi P||\mathbf{h}_{\mathrm{E}_k}\mathbf{w}_t||^2}{\frac{1-\phi}{N-1}P||\mathbf{h}_{\mathrm{E}_k}\mathbf{W}_a||^2 + \sigma_{\mathrm{E}_k}^2}, \quad \text{or} \\ \gamma_{\mathrm{E}_k} &= \frac{\phi\overline{\gamma}_{\mathrm{E}_k}||\mathbf{h}_{\mathrm{E}_k}\mathbf{w}_t||^2}{\frac{1-\phi}{N-1}\overline{\gamma}_{\mathrm{E}_k}||\mathbf{h}_{\mathrm{E}_k}\mathbf{W}_a||^2 + 1}. \end{aligned} \tag{49}$$

The PDF of $f(\gamma_{\mathrm{E}})$ is as following

$$f_{\gamma_{\mathrm{E}}}(\gamma) = L\Big(1 - \tau^{1-N}e^{-\frac{\gamma}{\phi\overline{\gamma}_{\mathrm{E}}}}\Big)^{L-1}e^{-\frac{\gamma}{\phi\overline{\gamma}_{\mathrm{E}}}}\left(\frac{\tau^{1-N}}{\phi\overline{\gamma}_{\mathrm{E}}} + \frac{(1-\phi)}{\phi\tau^N}\right), \tag{50}$$

where $\tau = 1 + \frac{(1-\phi)\gamma}{\phi(N-1)}$. The derivations can be found in Appendix C.

With all the above information, we can obtain the average secrecy throughput by calculating the expression in (8). For simplicity, first, $S(\gamma_{\mathrm{E}})$ as in (10) is approximated, and then this result is used in (9). The following shows the steps of the approximation process for $S(\gamma_{\mathrm{E}})$

$$\begin{aligned} S(\gamma_{\mathrm{E}}) &= \int_0^{\infty}(1 - \epsilon_{\gamma_{\mathrm{B}}|\gamma_{\mathrm{E}}}(x))\frac{x^{N-1}e^{-\frac{x}{\phi\overline{\gamma}_{\mathrm{B}}}}}{(\phi\overline{\gamma}_{\mathrm{B}})^N\Gamma(N)}dx \\ &= 1 - \int_0^{\infty}\epsilon(x)\frac{x^{N-1}e^{-\frac{x}{\phi\overline{\gamma}_{\mathrm{B}}}}}{(\phi\overline{\gamma}_{\mathrm{B}})^N\Gamma(N)}dx. \end{aligned} \tag{51}$$

Now, $S(\gamma_{\rm E})$ is rewritten in the form of $1-(S1+S2)$ in the following

$$S(y)=1-\Big(\underbrace{\int_0^{\alpha+u}\frac{x^{N-1}e^{-\frac{x}{\phi\overline{\gamma}_{\rm B}}}}{(\phi\overline{\gamma}_{\rm B})^N\Gamma(N)}dx}_{\rm S1} + \underbrace{\int_{\alpha+u}^{\alpha-u}(\beta(x-\alpha)+1/2)\frac{x^{N-1}e^{-\frac{x}{\phi\overline{\gamma}_{\rm B}}}}{(\phi\overline{\gamma}_{\rm B})^N\Gamma(N)}dx}_{\rm S2}\Big). \tag{52}$$

where β, α have been defined in (13), (14), respectively. The calculation of $S1$ is based on the following

$$S1=\frac{1}{(\phi\overline{\gamma}_{\rm B})^N\Gamma(N)}\int_0^{\alpha+u}x^{N-1}e^{-\frac{x}{\phi\overline{\gamma}_{\rm B}}}dx, \tag{53}$$

and $S2$ is obtained as calculating the following expression

$$S2=\frac{1}{(\phi\overline{\gamma}_{\rm B})^N\Gamma(N)}\int_{\alpha+u}^{\alpha-u}(\beta(x-\alpha)+1/2)x^{N-1}e^{-\frac{x}{\phi\overline{\gamma}_{\rm B}}}dx. \tag{54}$$

Then, $S(\gamma_{\rm E})$ is approximated by

$$S(\gamma_{\rm E})\approx(1-F_{\gamma_{\rm B}}(\alpha)), \tag{55}$$

while $F_{\gamma_{\rm B}}(\alpha)$ is given as

$$F_{\gamma_{\rm B}}(\alpha)=1-e^{-\frac{\alpha}{\phi\overline{\gamma}_{\rm B}}}\sum_{k=0}^{N-1}\frac{1}{k!}\Big(\frac{\alpha}{\phi\overline{\gamma}_{\rm B}}\Big)^k. \tag{56}$$

Further, $S(\gamma_{\rm E})$ is also can be rewritten either of the following forms

$$\begin{aligned} S(\gamma_{\rm E})\approx&1-\Big[1-\frac{\Gamma(N,\frac{\alpha}{\phi\overline{\gamma}_{\rm B}})}{\Gamma(N)}\Big], \quad \text{or}\\ S(\gamma_{\rm E})\approx&e^{-\frac{\alpha}{\phi\overline{\gamma}_{\rm B}}}\sum_{k=0}^{N-1}\frac{1}{k!}\Big(\frac{\alpha}{\phi\overline{\gamma}_{\rm B}}\Big)^k. \end{aligned} \tag{57}$$

The approximation in (55) also overlaps with the approximation given in [14]

$$S(\gamma_{\rm E})\approx 1+\beta\int_{\alpha+u}^{\alpha-u}F_{\gamma_{\rm B}}(x)dx, \tag{58}$$

Then T_s becomes

$$T_{\rm s}\approx\frac{b}{n}\int_0^{\infty}(1-F_{\gamma_{\rm B}}(\alpha))f(\gamma_{\rm E})d(\gamma_{\rm E}). \tag{59}$$

It is hard to obtain a closed-form formula for (59) due to the complexity of the integral. However, we obtained a closed form approximation by transforming (50) into the following by setting L = 2

$$f_{\gamma_{\rm E}}(\gamma)=\Big(2e^{-\frac{\gamma}{\phi\overline{\gamma}_{\rm E}}}-2e^{-\frac{2\gamma}{\phi\overline{\gamma}_{\rm E}}}\tau^{1-N}\Big)\Big(\frac{\tau^{1-N}}{\phi\overline{\gamma}_{\rm E}}+\frac{(1-\phi)}{\phi\tau^N}\Big), \tag{60}$$

Then, (59) is simplified with the help of (56) and (60)

$$\begin{aligned} T_{\rm s}\approx&\frac{2b}{n}\sum_{k=0}^{N-1}\frac{e^{\frac{1-r}{\phi\overline{\gamma}_{\rm B}}}}{k!}\sum_{j=0}^{k}\binom{k}{j}\Big(\frac{r-1}{\phi\overline{\gamma}_{\rm B}}\Big)^{k-j}\Big(\frac{r}{\phi\overline{\gamma}_{\rm B}}\Big)^k G^{-\lambda}\Gamma(\lambda)\times\\ &\Big[\frac{1}{\phi\overline{\gamma}_{{\rm E}_k}}(\psi(\lambda,\lambda+2-N,\Theta_1)-\psi(\lambda,\lambda+3-2N,\Theta_2))+\\ &G(1-N)(\psi(\lambda,\lambda+2-2N,\Theta_2)-\psi(\lambda,\lambda+1-N,\Theta_1))\Big], \end{aligned} \tag{61}$$

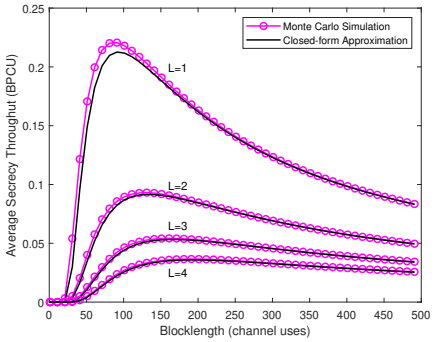

Fig. 3. Achieved Average Achievable Secrecy Throughput with respect to different Blocklength values for various number of eavesdroppers.

for $\lambda=(k+1)$, $\Theta_1=\frac{\frac{r}{\phi\overline{\gamma}_{\rm B}}+\frac{1}{\phi\overline{\gamma}_{{\rm E}_k}}}{G}$ and $\Theta_2=\frac{\frac{r}{\phi\overline{\gamma}_{\rm B}}+\frac{2}{\phi\overline{\gamma}_{{\rm E}_k}}}{G}$ and $G=\frac{1-\phi}{\phi(N-1)}$.

We obtained simulation results of the formula in (61) for the special case of 2 antenna transmitter and 2 eavesdroppers. In the next section, both the general formula for $T_{\rm s}$ in (59) and closed-form approximation (61) are numerically evaluated and presented with the other numerical results.

IV. SIMULATION RESULTS

In this section, we examine the impact of the number of transmitter antennas, the number of eavesdroppers, blocklength and power allocation ratio on the system performance. Unless otherwise stated, we assume the parameters presented in Table I for the simulations. The rest of the parameters are reported when the setting for each figure is discussed. We also stated in each figure captions when the initial parameter values are changed. For all the evaluations, the number of Monte-Carlo trials is 10^4.

TABLE I
SYSTEM PARAMETERS

Notation	Description	Value
b	Information Message (bits)	100
δ	Information Leakage Probability	10^{-4}
$\overline{\gamma}_{\rm B}$	Average SNR of the main channel	10 dB
$\overline{\gamma}_{\rm E}$	Average SNR of the eavesdropper channel	10 dB
ϕ	Power Allocation Coefficient	0.8

A. Single Antenna Transmitter and Multiple Eavesdroppers

First, we investigate the accuracy of the approximation derived in (37) by comparing it with Monte-Carlo simulation results.

In Fig. 3, we evaluate the average achieved secrecy throughput by Monte-Carlo simulation and compare it with our closed-form approximation in (37) for various blocklength values n. In this comparison, we consider various numbers of eavesdroppers. By observing Fig. 3, we can see that the Monte-Carlo simulation results and our derived approximation formula closely match, which confirms the accuracy of our approximation. This figure further shows that the average secrecy

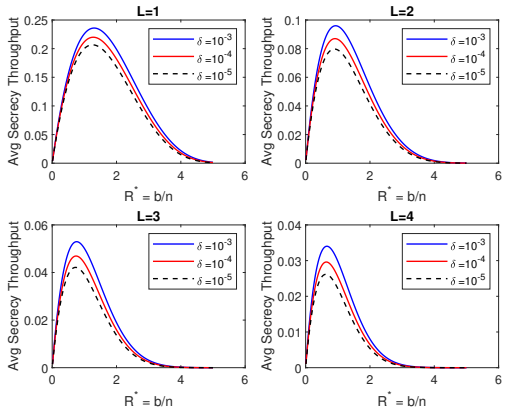

Fig. 4. Achieved Average Achievable Secrecy Throughput with respect to R^* = b/n for various numbers of eavesdroppers, L, and information leakage probabilities δ.

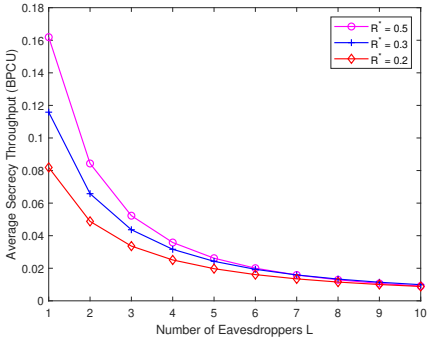

Fig. 5. Average Achievable Secrecy Throughput with respect Number of Eavesdroppers for various transmission rates R^*.

throughput decreases with the number of eavesdroppers. This is according to our expectations as the more eavesdroppers exist, the more likely is one of them to receive the message with fewer errors.

In Fig. 4, we explore the evolution of the average secrecy throughput versus $R^* = b/n$ for various information leakage probability values δ and for various numbers of eavesdroppers L. For this simulation, we fix the blocklength n to 100 channel uses, whereas the number of information bits b takes values up to 500 bits. This evaluation confirms the trend we reported in Fig. 3, i.e., when the number of eavesdroppers increases, the secrecy throughput falls. Information leakage probability also affects the average secrecy throughput, which drops when the information leakage to the eavesdropper decreases. For a greater number of eavesdroppers, the transmission should be at the lower transmission rates in order to maintain an achievable secrecy throughput, but values of the information leakage probability still behave similarly in each case with respect to average secrecy throughput.

In Fig. 5, we study the impact of having an increased number of eavesdroppers on the average secrecy throughput for various transmission rates. From this simulation, for the same number of eavesdroppers in the channel, lower transmission rates result in low average secrecy throughput. In addition,

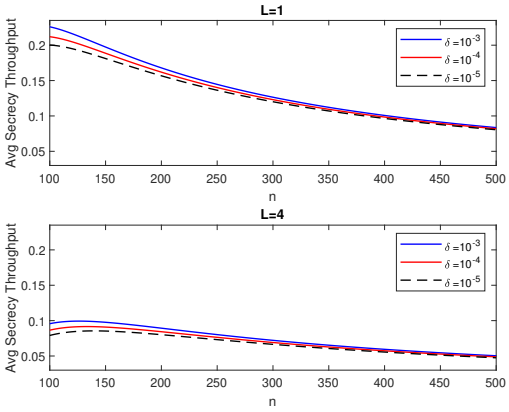

Fig. 6. Average Achievable Secrecy Throughput with respect to various Blocklength values for various number of eavesdroppers L and information leakage probabilities values δ.

we observe that as the number of eavesdroppers increases, it causes a considerable loss in average secrecy throughput. Further, we note that although the rate values differ, they all converge to the same point when there are more than eight eavesdroppers and result in very low average secrecy throughput. This also shows that secure communication can be guaranteed, but the secure transmission rate is very low.

In Fig. 6, we show the average achievable secrecy throughput with respect to different numbers of eavesdroppers for information leakage probabilities that vary from 10^{-3} to 10^{-5}. For this simulation, the considered blocklength n is between 100 to 500 channel uses. We can observe from this simulation that as the number of eavesdroppers increases, shorter blocklengths result in higher average secrecy throughput. Another conclusion derived from Fig. 6 is that the average secrecy throughput for the examined information leakage probabilities (δ) has closer outputs for different blocklength values when the number of eavesdroppers is small. When the eavesdroppers' number increases, the gap between the average secrecy throughput for various information leakage probabilities widens. For example, for a single eavesdropper, the average secrecy throughput for all the examined information leakage probability values decreases for larger blocklengths. However, when the number of eavesdroppers increases, a larger blocklength results in a slightly lesser average secrecy throughput.

The impact of the blocklength on the average secrecy throughput is presented in Fig. 7. The optimal blocklength is calculated according to Theorem 1 for various values of transmitted information bits. The optimal value is illustrated by a purple marker in Fig. 7. By observing this figure, we can see that the optimal average secrecy throughput is lower when the transmitted messages are shorter.

Finally, Fig. 8 shows the secrecy throughput and the numerical results that are obtained as described in Theorem 2 when there are multiple eavesdroppers. We examine different settings, i.e., the number of eavesdroppers and different combinations of received SNR values at the legitimate receiver (Bob) and the eavesdroppers (Eves). The evaluation shows

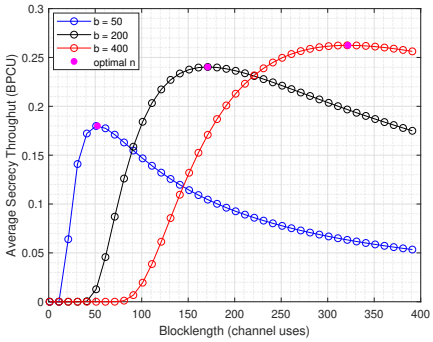

Fig. 7. Average Achievable Secrecy Throughput with respect to different Blocklength values and a single eavesdropper. Different number of information bits b are considered. The optimal value is calculated as described in Theorem 1.

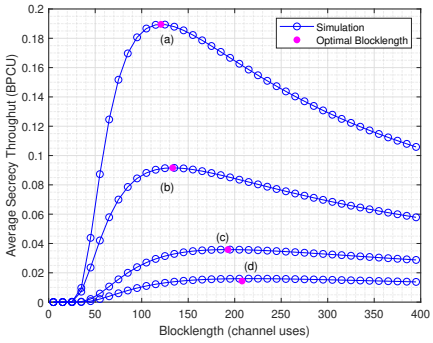

Fig. 8. Average Achievable Secrecy Throughput with respect to different Blocklength values for multiple eavesdroppers. The optimal value is calculated as described in Theorem 2. Settings: (a) $L = 4$, $\overline{\gamma}_{\mathrm{B}} = 10$ dB, $\overline{\gamma}_{\mathrm{E}} = 5$ dB, (b) $L = 2$, $\overline{\gamma}_{\mathrm{B}} = \overline{\gamma}_{\mathrm{E}} = 10$ dB, (c) $L = 4$, $\overline{\gamma}_{\mathrm{B}} = \overline{\gamma}_{\mathrm{E}} = 10$ dB, (d) $L = 2$, $\overline{\gamma}_{\mathrm{B}} = 5$ dB, $\overline{\gamma}_{\mathrm{E}} = 10$ dB.

that the analytical calculations for optimal blocklength meet the highest average secrecy throughput for each case. Apart from that, when the average received SNRs are the same, the presence of more eavesdroppers leads to lower average secrecy throughput. If the eavesdroppers are weaker than the legitimate receiver, higher average secrecy throughput is achievable, even if the number of eavesdroppers is high. For the case of weaker Bob than the strongest eavesdropper, when several eavesdroppers exist, the average secrecy throughput is in the lowest level.

B. Multiple-Antenna Transmitter and Multiple Eavesdroppers

In this section, we examine the impact of having multiple antennas at the transmitter on system performance. Specifically, we explore the validity of the approximations given in (59) and (61), which quantify the average secrecy throughput when the transmitter has multiple antennas.

In Fig. 9, the transmitter has 3 antennas. This evaluation shows the impact of blocklength on the average secrecy throughput for various combinations of information leakage probabilities and number of eavesdroppers. The proposed approximation is compared with the Monte-Carlo simulations. The first general conclusion is that an increase in the number

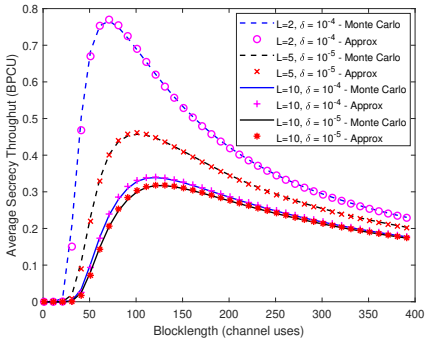

Fig. 9. Average Achievable Secrecy Throughput with respect to different Blocklength values for various number of eavesdroppers and the information leakage probability values.

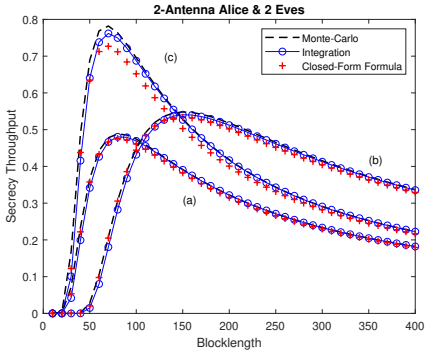

Fig. 10. Average Achievable Secrecy Throughput with respect to Blocklength. Settings: (a) b = 100 bits, (b) b = 200 bits, (c) $\overline{\gamma}_{\mathrm{E}} = 5$ dB.

of eavesdroppers leads to a lower throughput. This is expected as the higher the number of eavesdroppers is, the larger is the probability that one of the eavesdroppers is less affected by the noise than Bob. Another conclusion is that the higher the dispersion probability is, the higher is the achieved average secrecy throughput, but the difference is not significant. Finally, from this figure, we can observe that Monte-Carlo simulations match the approximation given in (59).

We now examine the accuracy of the derived closed-form formula of the average secrecy throughput for a 2-antenna Alice and 2 eavesdroppers (given in 61). The results are depicted in Fig. 10 where the evaluation of (61) is compared with the general expression presented in (59) and Monte-Carlo simulations. The figure shows the combined impact of the number of antennas and eavesdroppers on the system performance. It is clear that the Monte-Carlo simulation, the closed-form formula and the general expression perform very close to each other, which validates the accuracy of our closed-form formula. We can see that for the same received SNR values for Bob and Eves, the achieved average secrecy throughput is higher for a smaller number of information bits (see scenarios (a) and (b)). Moreover, when the channel conditions at the eavesdroppers are worse (scenario (c)), the secrecy throughput tends to be higher compared to having the same average received SNR with the legitimate receiver (scenario (a)).

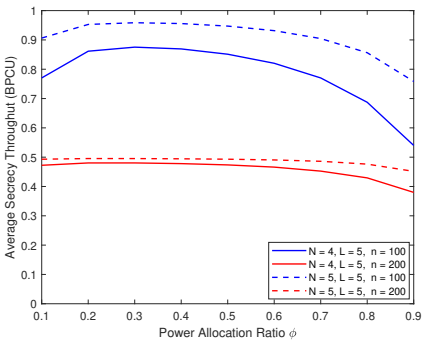

Fig. 11. Average Achievable Secrecy Throughput with respect to Power Allocation Ratio.

Fig. 11 captures the relation between power allocation rate and secrecy throughput. From the evaluation, we observe that higher throughput is achieved when 100 information bits are transmitted with 100 channel uses compared to when this happens with 200 channel uses. This is the case regardless of the number of antennas at the transmitter. Further, when the number of antennas increases, the throughput gets higher for the same number of eavesdroppers. From this figure, we can also observe that the throughput almost halves if the transmission rate decreases to half ($R^* = b/n = 0.5$). Further, we can see the impact of the number of antennas on the throughput becomes lesser when the transmission rate decreases. Moreover, the power allocation ratio affects the system more when the number of channel uses is small. However, when the power allocation ratio of the AN becomes larger, the average secrecy throughput drops. In other words, if the transmitter allocates more of its power to inject AN, the average secrecy throughput drops.

V. Conclusion

In this paper, we provide a novel approximation of the average secrecy throughput for a wiretap channel under Rayleigh fading with multiple eavesdroppers for short packet communications. We observed that the average secrecy throughput depends on the transmission rate, the average SNR of the legitimate receiver, and the received average SNR of the strongest eavesdropper, as well as the number of the eavesdroppers. We compare the theoretical and analytical results and find that the obtained approximations are very close to the simulated performance. The evaluation shows that when the number of eavesdroppers increases, the average secrecy throughput decreases, and the strict information leakage probability decreases, resulting in lower average secrecy throughput. In addition, the optimal blocklength value that maximizes the average secrecy throughput is obtained for the single antenna transmitter scenario. Moreover, we extend the scenario when the transmitter has multiple antennas and examine the impact of the AN allocation ratio at the transmitter on the overall system performance. We also carry out Monte-Carlo simulations to confirm the derived results. A closed-form formula is found for the case the transmitter has two antennas and there are two adversaries. The further evaluation shows that our proposed approximation for a multiple-antenna transmitter also matches the numerical results. Although an increased number of antennas leads to higher average secrecy throughput, higher transmission rates are more effective in obtaining high average secrecy throughput. Finally, although AN is helpful to have even higher secrecy throughput, we can conclude that the transmitter should not use all of its power to inject AN. A promising future direction is to investigate the scenario with users having non-identical distribution channel statistics due to different distances from the transmitter.

Acknowledgments

This work was supported by the European Union Horizon 2020, RISE 2018 Scheme (H2020-MSCA-RISE-2018) under the Marie Sklodowska-Curie Grant Agreement 823903 (RECENT).

Appendix A
Proof of Lemma 1

We first compute the partial derivative of T_{s1} w.r.t. n to obtain the optimal blocklength for the secrecy throughput in (38) :

$$\frac{\partial T_{s1}}{\partial n} = \frac{b\overline{\gamma}_{\mathrm{B}} e^{\frac{1-r}{\overline{\gamma}_{\mathrm{B}}}}}{n^2(\overline{\gamma}_{\mathrm{E}} r + \overline{\gamma}_{\mathrm{B}})}\Big(Mr + \frac{\overline{\gamma}_{\mathrm{E}}\overline{\gamma}_{\mathrm{B}} r M}{\overline{\gamma}_{\mathrm{E}} r + \overline{\gamma}_{\mathrm{B}}} - \overline{\gamma}_{\mathrm{B}}\Big). \tag{62}$$

where $M = \frac{Q^{-1}(\delta)}{2\sqrt{n}} + \frac{b}{n}\log(2)$. Since $\frac{b\overline{\gamma}_{\mathrm{B}} e^{\frac{1-r}{\overline{\gamma}_{\mathrm{B}}}}}{n^2(\overline{\gamma}_{\mathrm{E}} r + \overline{\gamma}_{\mathrm{B}})} > 0$, the sign of the partial derivative of T_{s1} depends on the sign of the following expression:

$$\Delta(n) = \Big(\frac{Q^{-1}(\delta)}{2\sqrt{n}} + \frac{b}{n}\log(2)\Big)\Big(r + \frac{\overline{\gamma}_{\mathrm{E}}\overline{\gamma}_{\mathrm{B}} r}{\overline{\gamma}_{\mathrm{E}} r + \overline{\gamma}_{\mathrm{B}}}\Big) - \overline{\gamma}_{\mathrm{B}}. \tag{63}$$

$\Delta(n)$ is a decreasing function with respect to n for $n > 0$ and $\Delta(n)$ is concave. r is also a decreasing function of n and always positive. We know that $\overline{\gamma}_{\mathrm{B}} \geq 0$ and $Q^{-1}(\delta) \geq 0$. We also have $\lim_{n\to 0}\Delta > 0$ and $\lim_{n\to\infty}\Delta < 0$, which means the average secrecy throughput first increases and then falls. We take the second derivative of (63) in order to find out whether the function concave or convex :

$$\frac{\partial \Delta(n)}{\partial n} = \frac{1}{n(\overline{\gamma}_{\mathrm{E}} r + \overline{\gamma}_{\mathrm{B}})}\underbrace{\Big(\frac{M^2\overline{\gamma}_{\mathrm{E}}^2\overline{\gamma}_{\mathrm{B}} D}{(\overline{\gamma}_{\mathrm{E}} r + \overline{\gamma}_{\mathrm{B}})} - r(\overline{\gamma}_{\mathrm{E}}\overline{\gamma}_{\mathrm{B}} + \overline{\gamma}_{\mathrm{E}} r + \overline{\gamma}_{\mathrm{B}})(M^2 + H)\Big)}_{\Delta_1} \tag{64}$$

where $D = e^{2\frac{Q^{-1}(\delta)}{\sqrt{n}} + \frac{2b}{n}\log(2)}$ and $H = \frac{Q^{-1}(\delta)}{4\sqrt{n}} + \frac{b}{n}\log(2)$. In (64) $\frac{1}{n(\overline{\gamma}_{\mathrm{E}} r + \overline{\gamma}_{\mathrm{B}})} > 0$, therefore the sign of the equation depends on the expression inside the brackets.

$$\Delta_1 = \underbrace{\frac{M^2\overline{\gamma}_{\mathrm{E}}^2\overline{\gamma}_{\mathrm{B}} D}{(\overline{\gamma}_{\mathrm{E}} r + \overline{\gamma}_{\mathrm{B}})}}_{\mathrm{J1}} - \underbrace{r(\overline{\gamma}_{\mathrm{E}}\overline{\gamma}_{\mathrm{B}} + \overline{\gamma}_{\mathrm{E}} r + \overline{\gamma}_{\mathrm{B}})(M^2 + H)}_{\mathrm{J2}}. \tag{65}$$

Since $\log(\mathrm{J1}) < \log(\mathrm{J2})$, the second derivative in (64) is negative and hence T_{s1} is concave.

APPENDIX B
PROOF OF LEMMA 2

To find the optimal blocklength value that maximizes the secrecy throughput in (37), we take the partial derivative of the logarithm of T_s with respect to n :

$$\frac{\partial \log T_s}{\partial n} = \frac{\partial \Omega(n)}{\partial n} = \frac{\partial \log\left(\frac{bL}{n} e^{\frac{1-e^{\frac{Q^{-1}(\delta)}{\sqrt{n}}+\frac{b}{n}\log(2)}}{\overline{\gamma}_{\mathrm{B}}}} \mathrm{B}\left(\frac{\overline{\gamma}_{\mathrm{E}} e^{\frac{Q^{-1}(\delta)}{\sqrt{n}}+\frac{b}{n}\log(2)}}{\overline{\gamma}_{\mathrm{B}}}+1, L\right)\right)}{\partial n} \tag{66}$$

We apply the following equality to take the logarithm of gamma function: $\log \mathrm{B}(z, L) = \log \Gamma(z) + \log \Gamma(L) - \log \Gamma(z+L)$.

$$\Omega(n) = \frac{1}{\overline{\gamma}_{\mathrm{B}} n}\left[Mr\Big(1+\overline{\gamma}_{\mathrm{E}}\big(\psi_0(z,L)-\psi_0(z)\big)\Big) - \overline{\gamma}_{\mathrm{B}}\right]. \tag{67}$$

Here ψ_0 is the digamma function. We know that $\frac{1}{n\overline{\gamma}_{\mathrm{B}}} > 0$, since $n > 0$ and $\overline{\gamma}_{\mathrm{B}} \geq 0$. We then take the second derivative of T_s :

$$\frac{\partial \Omega(n)}{\partial n} = \frac{1}{\overline{\gamma}_{\mathrm{B}} n^2}\Big(\frac{\overline{\gamma}_{\mathrm{E}}^2 D M^2}{\overline{\gamma}_{\mathrm{B}}} g_1 + \quad r(M^2+H+M)\big(\overline{\gamma}_{\mathrm{E}} g_2 - 1\big)\Big) + \frac{1}{n^2}. \tag{68}$$

where the trigamma function is denoted by $\psi_1(.)$ [28, Eq. 6.4.1] and the substitutions of $_1 = \big(\psi_1(z) - \psi_1(z+L)\big)$, $g_2 = \big(\psi_0(z) - \psi_0(z+L)\big)$ are applied. This expression is always negative and the proof is complete.

APPENDIX C

For several eavesdroppers, the CDF of γ_{E} is calculated by:

$$\begin{aligned} F_{\gamma_{\mathrm{E}}}(\gamma) &= \Pr(\gamma_{\mathrm{E}} < \gamma) = \Pr(\max_k \gamma_{\mathrm{E}_k} < \gamma) \\ &= \Pr\{\gamma_{\mathrm{E}_1} < \gamma, \gamma_{\mathrm{E}_2} < \gamma, ..., \gamma_{\mathrm{E}_k} < \gamma\} \\ &= \Big[\int_0^{\gamma} f_{\gamma_{\mathrm{E}}}(x)dx\Big]^L. \end{aligned} \tag{69}$$

According to [29], [30], the CDF of the instantaneous SINR at an Eve under AN is given by

$$F_{\gamma_{\mathrm{E}}}(\gamma) = 1 - \Big(1+\frac{(1-\phi)\gamma}{\phi(N-1)}\Big)^{1-N} e^{-\frac{\gamma}{\phi\overline{\gamma}_{\mathrm{E}}}}. \tag{70}$$

For L non-colluding eavesdroppers, $F_{\gamma_{\mathrm{E}}}(\gamma)$ becomes:

$$F_{\gamma_{\mathrm{E}}}(\gamma) = \left(1 - \Big(1+\frac{(1-\phi)\gamma}{\phi(N-1)}\Big)^{1-N} e^{-\frac{\gamma}{\phi\overline{\gamma}_{\mathrm{E}}}}\right)^L. \tag{71}$$

Then, the PDF of the instantaneous SINR at Eve is described by

$$f_{\gamma_{\mathrm{E}}}(\gamma) = \frac{dF_{\gamma_{\mathrm{E}}}(\gamma)}{d\gamma} = L f_{\gamma_{\mathrm{E}}}(\gamma)\Big[\int_0^{\gamma} f_{\gamma_{\mathrm{E}}}(x)dx\Big]^{L-1} \tag{72}$$

and

$$f_{\gamma_{\mathrm{E}}}(\gamma) = L\left(1 - \Big(1+\frac{(1-\phi)\gamma}{\phi(N-1)}\Big)^{1-N} e^{-\frac{\gamma}{\phi\overline{\gamma}_{\mathrm{E}}}}\right)^{L-1} \times \left(\frac{\Big(1+\frac{(1-\phi)\gamma}{\phi(N-1)}\Big)^{1-N} e^{-\frac{\gamma}{\phi\overline{\gamma}_{\mathrm{E}}}}}{\phi\overline{\gamma}_{\mathrm{E}}} - \frac{(1-\phi)(1-N)e^{-\frac{\gamma}{\phi\overline{\gamma}_{\mathrm{E}}}}}{\phi(N-1)\Big(\frac{(1-\phi)\gamma}{\phi(N-1)}+1\Big)^N}\right). \tag{73}$$

If we set $\tau = 1 + \frac{(1-\phi)\gamma}{\phi(N-1)}$ in (73), the PDF of $f(\gamma_{\mathrm{E}})$ simplifies to:

$$f_{\gamma_{\mathrm{E}}}(\gamma) = L\Big(1 - \tau^{1-N} e^{-\frac{\gamma}{\phi\overline{\gamma}_{\mathrm{E}}}}\Big)^{L-1} e^{-\frac{\gamma}{\phi\overline{\gamma}_{\mathrm{E}}}}\left(\frac{\tau^{1-N}}{\phi\overline{\gamma}_{\mathrm{E}}} + \frac{(1-\phi)}{\phi\tau^N}\right). \tag{74}$$

REFERENCES

[1] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 20–27, Apr. 2015.

[2] M. Ghogho and A. Swami, "Physical-layer secrecy of MIMO communications in the presence of a Poisson random field of eavesdroppers," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Kyoto, Japan, Jun. 2011, pp. 1–5.

[3] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization," *IEEE Trans. Signal Process.*, vol. 61, no. 10, pp. 2704–2717, May 2013.

[4] L. Zhang, H. Zhang, D. Wu, and D. Yuan, "Improving physical layer security for MISO systems via using artificial noise," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2015, pp. 1–6.

[5] T.-X. Zheng, H.-M. Wang, J. Yuan, D. Towsley, and M. H. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. on Commun.*, vol. 63, no. 11, pp. 4347–4362, Nov. 2015.

[6] Z. Li, P. Mu, B. Wang, and X. Hu, "Optimal semiadaptive transmission with artificial-noise-aided beamforming in MISO wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 65, no. 9, pp. 7021–7035, Sep. 2016.

[7] Z. Chu, H. Xing, M. Johnston, and S. Le Goff, "Secrecy rate optimizations for a MISO secrecy channel with multiple multiantenna eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 283–297, Jan. 2016.

[8] W. Wang, K. C. Teh, and K. H. Li, "Secrecy throughput maximization for MISO multi-eavesdropper wiretap channels," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 3, pp. 505–515, Mar. 2017.

[9] L. Wang, M. Elkashlan, T. Q. Duong, and R. W. Heath, "Secure communication in cellular networks: The benefits of millimeter wave mobile broadband," in *IEEE Int. Workshop on Signal Processing Advances in Wireless Comm. (SPAWC)*, Toronto, ON, Canada, Jun. 2014, pp. 115–119.

[10] G. Geraci, S. Singh, J. G. Andrews, J. Yuan, and I. B. Collings, "Secrecy rates in broadcast channels with confidential messages and external eavesdroppers," *IEEE Trans. Wirel. Commun.*, vol. 13, no. 5, pp. 2931–2943, May 2014.

[11] Y. Chen, W. Li, and H. Shu, "Wireless physical-layer security with multiple receivers and eavesdroppers: Outage probability and average secrecy capacity," in *IEEE Int. Symp. Pers. Indoor Mob. Radio Commun. (PIMRC)*, Hong Kong, China, Aug. 2015, pp. 662–667.

[12] H. Liu, P. L. Yeoh, K. J. Kim, P. V. Orlik, and H. V. Poor, "Secrecy performance of finite-sized in-band selective relaying systems with unreliable backhaul and cooperative eavesdroppers," *IEEE J. on Sel. Areas in Commun.*, vol. 36, no. 7, pp. 1499–1516, Apr. 2018.

[13] L. Wang, K. J. Kim, T. Q. Duong, M. Elkashlan, and H. V. Poor, "Security enhancement of cooperative single carrier systems," *IEEE Trans. on Inf. Forensics and Secur.*, vol. 10, no. 1, pp. 90–103, Sep. 2014.

[14] 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.

[15] 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.

[16] 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.
[17] N. Arı, N. Thomos, and L. Musavian, "Average secrecy throughput analysis with multiple eavesdroppers in the finite blocklength," in *IEEE Int. Symp. Pers. Indoor Mob. Radio Commun. (PIMRC)*, London, UK, Aug. 2020, pp. 1–5.
[18] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.
[19] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978.
[20] R. Chen, C. Li, S. Yan, R. Malaney, and J. Yuan, "Physical layer security for ultra-reliable and low-latency communications," *IEEE Trans. Wireless Commun.*, vol. 26, no. 5, pp. 6–11, Oct. 2019.
[21] 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.
[22] ——, "Wiretap channels: Nonasymptotic fundamental limits," *IEEE Trans. Inf. Theory*, vol. 65, no. 7, pp. 4069–4093, Jul. 2019.
[23] ——, "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.
[24] 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.
[25] L. Zhang and Y. Liang, "Average throughput analysis and optimization in cooperative IoT networks with short packet communication," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 11 549–11 562, Dec. 2018.
[26] P. Wang, G. Yu, and Z. Zhang, "On the Secrecy Capacity of Fading Wireless Channel with Multiple Eavesdroppers," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Nice, France, Jun. 2007, pp. 1301–1305.
[27] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series, and Products*, 7th ed. New York, NY, USA: Academic press, 2007.
[28] M. Abramowitz and I. A. Stegun, *Handbook of mathematical functions with formulas, graphs, and mathematical tables*. Washington D.C., USA: US Government printing office, 1964.
[29] N. Yang, S. Yan, J. Yuan, R. Malaney, R. Subramanian, and I. Land, "Artificial Noise: Transmission optimization in multi-input single-output wiretap channels," *IEEE Trans. on Commun.*, vol. 63, no. 5, pp. 1771–1783, May 2015.
[30] S. Yan, N. Yang, I. Land, R. Malaney, and J. Yuan, "Three artificial-noise-aided secure transmission schemes in wiretap channels," *IEEE Trans. Veh. Technol.*, vol. 67, no. 4, pp. 3669–3673, Apr. 2017.

Nihan Arı is currently a Ph.D. candidate in Electronic Systems Engineering at the University of Essex, UK. She received her M.Sc. in Advanced Communication Systems (with distinction) in 2017 from the University of Essex, UK, and B.Sc. in Industrial Engineering in 2009 from Gazi University, Turkey. Her research interests include wireless communication, physical layer security, short packet communications, and security of the Internet of Things. She is a member of IEEE since 2019.

Nikolaos Thomos (S'02,M'06,SM'16) received the Diploma and PhD degrees from the Aristotle University of Thessaloniki, Greece, in 2000 and 2005, respectively. He was a Senior Researcher with the Ecole Polytechnique Federale de Lausanne (EPFL) and the University of Bern, Switzerland. He is currently a Chair Professor in the School of Computer Science and Electronic Engineering at the University of Essex, U.K. His research interests include machine learning for communications, multimedia communications, network coding, semantic communications, information-centric networking, source and channel coding, and signal processing. He is an elected member of the IEEE MMSP Technical Committee (MMSP-TC) for the period 2019-2024. He received the highly esteemed Ambizione Career Award from the Swiss National Science Foundation (SNSF).

Leila Musavian received her PhD degree in Telecommunications at Centre for Telecommunications Research (CTR), Kings College London, UK. She is currently working as Professor of Wireless Communications at University of Essex. She was Deputy Pro-Vice-Chancellor for Research at University of Essex between September 2018 and December 2020 and Reader in Telecommunications at the School of Computer Science and Electronic Engineering from 2016-2020. Prior to that, she was Lecturer at InfoLab21, Lancaster University (Dec 2012-Aug 2016), Senior Lecturer at InfoLab21, Lancaster University (Aug 2016-Nov 2016), Research Associate at McGill University, Canada (2011-2012), research associate at Loughborough University, UK (2009-2010) and post-doctoral fellow at INRS-EMT, Canada (2006-2008).

Her research interests lie in Radio Resource Management for 6G/B5G communications, low latency communications, Machine learning for Communications, Massive MIMO, Energy Harvesting and Semantic Communications. She has been editor of IEEE TRANSACTIONS OF WIRELESS COMMUNICATIONS between 2015-2020, Executive Editor of Transactions on Emerging Telecommunications Technologies between 2016-2019 and Associate Editor of Wiley's Internet Technology Letters. She has been lead chair for UHS5G WP in IEEE Globecom 2018, UHSLLS WP in IEEE WCNC 2019, lead chair for URLLC Special Session in IEEE PIMRC 2018, TPC Co-Chair of CorNer 2016 (in conjunction with ISWCS 2016) and Co-Chair of mmWave 5G (STEMCOM 2016) and also TPC member of several conferences including IEEE ICC, IEEE GLOBECOM, IEEE WCNC, IEEE ICCCN, IEEE PIMRC, ChinaCom, etc. She was the workshop co-chair of VTC-Spring-2020, the Wireless Communications Symposium Lead Co-Chair for IEEE ICC 2021, Montreal, Canada, and the TPC chair of IEEE CANMAD 2021, Portugal. She is the founding member and co-chair of the IEEE UK and Ireland Section Future Networks Local Group.