Physical Layer Security of Short Packet Communications

Nihan Arı

School of Computer Science and Electronic Engineering
University of Essex

A thesis submitted for the degree of
Doctor of Philosophy

May 2023

To Barış

Acknowledgements

I would like to express my sincere gratitude to my supervisors, Professor Leila Musavian and Professor Nikolaos Thomos, for their invaluable guidance, support, and encouragement throughout my Ph.D. journey. I am especially grateful for all the opportunities that they provided in shaping my research and helping me with my academic and intellectual development.

I would like to thank my supervisory panel members, Dr Faiyaz Doctor and Dr Haider Raza, for their suggestions and comments on each step of my research.

I am also grateful to my friends and family, who have been a constant source of motivation and emotional support. I would like to thank my friends, Rukiye Savran Kızıltepe and Eleni Nisioti. They have been by my side during the ups and downs of my research. I also would like to thank the Arı and Başaran families, for their encouragement and support.

I would not have been able to make it this far without the unconditional love and support of my mother Nurten Karaca, my father Nurhan Karaca, and my sister Gülnihal Karaca. I am also grateful to Daisy, our furry family member, who brought joy and happiness to my life.

Finally, I dedicate this thesis to my partner, Barış Arı. I am grateful for his patience and kindness, which helped me through the most challenging times. He certainly encouraged me to stay focused all the time, especially during the pandemic days.

Once again, thank you to everyone who has contributed to my journey and supported me in countless ways.

Abstract

This dissertation aims to conduct research on security issues of 5G wireless networks, which are vulnerable to external security threats while supporting services for a massive number of users and devices. In practical wireless communication systems, the communication is subject to overhearing by external eavesdroppers due to the broadcast nature of the wireless medium. Physical layer security (PLS) shows promise as a viable option for securing future communication systems because it utilizes channel characteristics to hide transmitted messages from possible adversaries without depending on traditional cryptographic solutions. However, 5G systems are expected to support various traffic types, including short packet transmission, which results in new challenges in terms of security. Particularly, short packet transmission introduces a penalty on the secrecy capacity, which is the rate of secure communication between authorized parties in the presence of an adversary. 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. In the literature, limited studies focus on PLS for short packet communications (SPC) and the performance analysis of secure SPC remains an open problem.

Our goal is to study large-scale networks, but first, as a simple case, secure communication of a wiretap channel under the attack of an active eavesdropper, with two capabilities, namely half-duplex and full-duplex, is investigated. It appears that an active eavesdropper is more harmful to the secrecy throughput than a passive one, and the full-duplex eavesdropper (Eve) is more dangerous than a half-duplex Eve. Indeed, the performance is measured in terms of average secrecy throughput and theoretical approximations are validated through Monte Carlo simulations throughout all the contributions of the dissertation. Second, the wiretap channel model with multiple passive eavesdroppers is explored to shed light on a more realistic scenario in large-scale wireless networks. Although an increased number of antennas can lead to higher average secrecy throughput, achieving higher secrecy throughput is more effectively accomplished by increasing the transmission rates. As a final contribution, the previous wiretap channel setting is extended by adding multiple receivers. The security performance against colluding and non-colluding attackers is thoroughly examined. According to our results, it is more advantageous for eavesdroppers to collude and they are more powerful when their number increases.

And we conclude the dissertation with a discussion of future work.

Table of contents

List of figures

List of tables

Nomenclature

Abbreviations

5G Fifth Generation Mobile Network

AN Artificial Noise

AWGN Additive White Gaussian Noise

CSI Channel State Information

FD Full Duplex

HD Half Duplex

IoT Internet of Things

MIMO Multiple-Input Multiple-Output

MISO Multiple-Input Single-Output

PHY Physical Layer

PLS Physical Layer Security

SINR Signal-to-Interference-Plus-Noise Ratio

SNR Signal-to-Noise Ratio

SPC Short Packet Communications

URLLC Ultra-reliable Low-latency Communication

Notations

δ Information Leakage Probability

ε	Decoding Error Probability
γ_X	Received Instantaneous SNR at X
ϕ	Power Allocation Ratio
$\mathbf{X}$	Matrix
$\mathbf{x}$	Vector
b	Message size
C_s	Secrecy Capacity
d_{XY}	Distance Between X and Y Nodes
g_{XY}	Fading Coefficients Between X and Y Nodes
h_{XY}	Channel Gains Between X and Y Nodes
L	Number of Eavesdroppers
M	Number of Receivers
N	Number of Antenna at the Transmitter
n	Blocklength
P	Transmit Power
P_A	Transmit Power of Alice
P_E	Jamming Power of Eve
q	Probability of Listening (Being Passive Eavesdropper)
$R^*(n,\varepsilon,\delta)$	Maximum Achievable Secrecy Rate
T_s	Average Secrecy Throughput
V	Channel Dispersion
v	Path Loss Exponent

Chapter 1

Introduction

Security is becoming more critical in wireless communications with the evolution of 5G and beyond networks, which brings many new challenges. The transmission of confidential data has always been an important subject over wireless channels. In practical wireless communication systems, communication is subject to increased vulnerability to malicious attacks due to the broadcast nature of wireless communications and severe security issues arise in such large-scale wireless networks with the expansion of many connected smart devices, applications, and services.

In recent years, there has been a lot of interest in PLS, which exploits the randomness of the wireless medium to secure communication without relying on complex and computationally expensive secret key-based cryptographic methods [1], [2], [3]. This renders PLS a potential candidate for securing future communication systems. The widely used information-theoretic secrecy metrics such as secrecy capacity and secrecy outage probability cannot accurately evaluate the performance of PLS in short packet communications (SPC) [4], [5]. However, 5G systems need to support different traffic types, including shorter packets. 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 the information can be transmitted through a channel with a maximum rate reliably and securely when the blocklengths are sufficiently large. To be more specific, the decoding errors at both the legitimate receiver (Bob) and the eavesdropper (Eve) cannot be ignored by transmitting small blocklengths, which may compromise communication links to Eve. In other words, the communication links that transmit short packets may become more prone to security attacks and they may be less robust to adversaries. In this regard, secure SPC is an essential topic to be addressed and PLS requires thorough examination when it comes to supporting short packet transmission. Alternative performance metrics, such as the probability of error, can provide a more accurate

representation of the security performance of the system, and help make SPC more robust to adversaries in large-scale 5G systems.

1.1 Motivation

Despite a significant amount of work that has been conducted in PLS [2, 3, 6–27], SPC from the perspective of PLS is still far from well investigated. The reason is that most of the existing work on PLS assumes an infinite blocklength and these assumptions may not hold in scenarios that require short packet transmission, which presents unique challenges that cannot be adequately addressed by traditional PLS methods. For example, in the context of systems such as the Internet of Things (IoT) and 5G networks, the presence of numerous interconnected heterogeneous devices creates considerable vulnerabilities that can be exploited by malicious parties. The vast number of devices in IoT networks makes it challenging to implement traditional PLS methods effectively. Similarly, high-speed data transmission and the numerous connected devices in 5G networks require optimized PLS methods that can adapt to changing conditions quickly. As a result, it is crucial to employ innovative PLS methods to ensure the robust and secure transmission of short data in large-scale networks. Therefore, we address the secrecy performance of SPC over fading wiretap channels for different communication scenarios or with different eavesdropper strategies.

Since large-scale systems are our main concern, it is possible to face more capable eavesdroppers, who can operate in passive or active modes. At first, we simply focus on a simple wiretap scenario, where we can analyze the performance of an active eavesdropper in the context of secure SPC. An active eavesdropper has the capability to monitor a transmission between the parties in silent mode or jam the transmission so that the receiver can not recover its intended message. The active eavesdropper model is a concern that is more likely to disrupt the overall system transmission more efficiently if short packets are conveyed. Thus, secure SPC from a legitimate transmitter to a receiver is examined in the presence of an active eavesdropper over fading channels. We assume that the eavesdropper has the capability to operate half-duplex (HD), which allows the eavesdropper to select when it will perform either eavesdropping or jamming or full-duplex (FD), which enables performing eavesdropping and jamming simultaneously. In HD mode, passive eavesdropper impact can also be observed, and how it has an impact on overall security performance.

We then change the wiretap channel scenario and assume multiple, independent, and passive eavesdroppers. We start our investigation by examining the fading wiretap channel, where the communication between a single antenna transmitter and receiver pair is overheard by multiple non-colluding single antenna eavesdroppers. The novelty of this work lies in

the fact that we assume each eavesdropper is independent, a.k.a. non-colluding. 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. We then extend our analysis for the case of a multiple antenna transmitter and consider artificial noise (AN) to confuse the eavesdroppers. Therefore, we obtain results regarding how transmitter antenna and eavesdropper numbers change the system security performance.

We further investigate a different setting, where multiple receivers are added to the wiretap channel. Differently from the previous analysis, not only the system model considered an increased number of receivers, but also eavesdropper cooperation is analyzed. The security performance of a wiretap channel is evaluated both for colluding and non-colluding eavesdropper cases. Colluding means multiple eavesdroppers can collaborate, perform joint processing, and try to decode the message with the gathered information, so they can be seen as a single eavesdropper with multiple antennas.

Overall, three different wiretap channel models are considered in this thesis to study the secrecy performance of SPC.

1.2 Contributions

The contributions of this thesis are summarised as follows.

Chapter 3

Analysis of the security performance of a SPC over a fading wiretap channel is conducted under the existence of an active eavesdropper. A closed-form approximation is found for the average secrecy throughput when the eavesdropper acts in half-duplex mode, which allows the eavesdropper to either listen to Alice's short packet transmission or jam Bob's communication. In addition, an approximation of the average secrecy throughput is found for a full-duplex eavesdropper is present, i.e., eavesdropping and jamming happen simultaneously. Both derived expressions are validated through Monte Carlo (MC) simulations and the findings show that the evaluation of the analytical framework closely matches with the performance of the simulations. Apart from the HD and FD modes, we further explore the impact of the distance between the nodes on the average secrecy throughput for two different topologies, namely line and triangular, to capture how the eavesdropper location changes the system performance.

The initial results of Chapter 3 have been published in the following conference proceedings:

N. Arı, N. Thomos and L. Musavian (2021). Active eavesdropping in short packet communication: Average secrecy throughput analysis. In Proc. IEEE Int. Conf. on Commun. Workshops (ICC Workshops), pages 1–6, Montreal, QC, Canada.

In addition, a journal paper related to this chapter titled '*Secrecy Analysis of Active Eavesdropping in Short Packet Communications*' is under review in IEEE Transactions on Wireless Communications.

Chapter 4

In the previous chapter, only one eavesdropper presence is considered in the system model. However, it may not be representative of large-scale networks, which may contain several malicious eavesdroppers. Therefore, in this chapter, we explore the security performance of SPC in a fading wiretap channel, which is under the threat of multiple adversaries. In a simpler setting, multiple eavesdroppers are assumed to be independent and passive. Specifically, we assume each eavesdropper is independent, a.k.a. non-colluding. Both receiver and eavesdroppers each have single antennas, whereas the transmitter is equipped with either single or multiple antennas. First, a closed-form approximation of the average secrecy throughput for secure SPC is derived for the single antenna transmitter scenario. We provide a framework to derive the optimal blocklength that maximizes the average secrecy throughput for both single and multiple eavesdroppers cases. Then, the average secrecy throughput is formulated for the multiple antenna transmitter case, where AN is introduced to the system model to eliminate the negative impact of 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 are performed to show the validity of the closed-form formulas with the simulations.

The initial results of Chapter 4 have been published in the following conference proceedings:

N. Arı, N. Thomos and L. Musavian (2020). Average secrecy throughput analysis with multiple eavesdroppers in the finite blocklength. In Proc. IEEE Int. Symp. Pers. Indoor Mob. Radio Commun. (PIMRC), pages 1–5, London, UK.

Furthermore, the journal paper related to this chapter has been accepted for publication in IEEE Transactions on Communications.

N. Arı, N. Thomos and L. Musavian, "Performance Analysis of Short Packet Communications with Multiple Eavesdroppers," in IEEE Transactions on Communications, 2022, doi: 10.1109/TCOMM.2022.3198111.

Chapter 5

Finally, we extended the analysis in Chapter 4 to multiple receivers case. The security performance of SPC is examined in large-scale networks, which contain multiple users against several malicious eavesdroppers. Specifically, we consider external eavesdroppers in two scenarios, i.e., non-colluding and colluding, and obtain closed-form formulas of average secrecy throughput for each mode when all transmitter, receivers and eavesdroppers have single antennas. We then perform Monte Carlo simulations to evaluate the performance of the system. We compare the simulated results by evaluating the derived closed-form formulas.

The results of Chapter 5 have been published in the following conference proceedings:

N. Arı, N. Thomos and L. Musavian (2022). Secrecy performance of short packet communications: Wiretap channel with multiple receivers and eavesdroppers. In Int. Wirel. Commun. Mob. Comput. Conf. (IWCMC), pages 395–400, Dubrovnik, Croatia.

1.3 Outline of the Dissertation

This dissertation is organized as follows. Chapter 2 summarizes the state of the art on PLS and SPC. Our main discussion and numerical results on PLS for SPC are presented in Chapters 3, 4 and 5. Particularly, Chapter 3 contains the performance analysis of the secure SPC of a wiretap channel, while an active eavesdropper operates in half or full-duplex modes. Chapter 4 introduces multiple passive eavesdroppers to a wiretap channel scenario and secrecy analysis are conducted in terms of evaluating average secrecy throughput by considering single and multiple antenna transmitter. Chapter 5 focuses on the security performance investigation of a larger network, which contains multiple receivers as well as multiple eavesdroppers, who either collaborate or act individually. Finally, Chapter 6 summarizes our conclusions and mentions future research.

Chapter 2

Background Information

This chapter summarizes the general background of physical layer security and short packet communications. It also provides an overview of the recent studies of PLS under the SPC perspective.

2.1 Physical Layer Security

PLS has emerged as a promising alternative to conventional secret key-based cryptographic approaches to defend wireless security [2],[3]. Traditionally, communication security is provided by using techniques at the upper layers that include secret key exchange. In this regard, PLS appears to be advantageous because of being less complex than cryptographic methods, simply because it relies on employing the characteristics of the communication medium only, such as fading, noise, etc., to safeguard the communication channel. Fig. 2.1 illustrates a communication scenario between a sender and a legitimate receiver against an unauthorized eavesdropper. The transmitter, receiver, and eavesdropper are called Alice, Bob, and Eve, respectively.

The foundations of the PLS date back to the pioneering work of Shannon [6], which the theoretical limit of secure transmission was characterized over noiseless wireless channels. Particularly, the groundbreaking work included secret key encrypted security from an information-theoretic perspective. Later, Wyner introduced the wiretap channel that generalizes a scenario in a noisy communication channel [7]. This model considered a more realistic and practical system, where no secret key distribution or exchange is available to legitimate users. The work in [7] revealed that secure communication is possible if the eavesdropper channel is noisier than the main channel. Csiszár and Körner extended Wyner's work for broadcast channels [8].

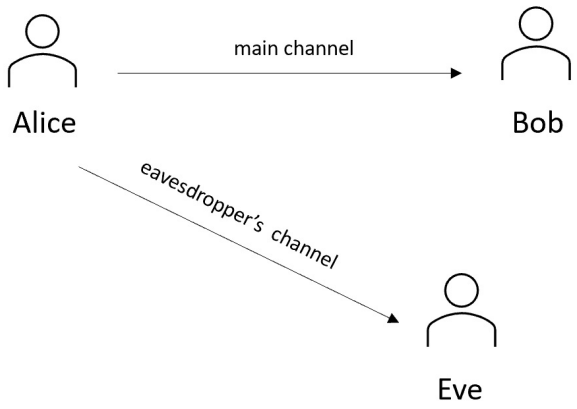

Fig. 2.1 A wireless network with an eavesdropper. A sender, Alice, communicates with a receiver, Bob, over a wireless medium (main channel), while an eavesdropper, Eve, listens to the transmission through another wireless link.

In general, eavesdroppers are divided into two types: active and passive. Wiretap channels under the existence of an active eavesdropper have been previously studied in the literature. The works in [9–12] examined the secure transmission over wiretap channels following a game-theoretic approach. Specifically, physical layer security games are employed to explore the dynamics between a legitimate user and a full-duplex eavesdropper. These works mainly proposed PLS games to examine the power strategies of the transmitter who tries to increase the secrecy rate when at the same time a full-duplex eavesdropper aims to reduce the achievable rate. Likewise, a game-theoretical approach is proposed to solve an optimal power allocation problem in [13] to ensure security in a multiple-input single-output (MISO) system in the presence of multiple eavesdroppers, who have the capability of either being half-duplex (HD) or full-duplex (FD). The work in [14] proposed using artificial noise (AN) to defend the security of a system and characterized an on-off transmission scheme for a Rayleigh fading wiretap channel. Closed-form expressions for generalized secrecy outage probability and average fractional equivocation are obtained. Using AN signals from a multiple antenna transmitter to confuse the full-duplex eavesdropper is investigated in [15] where an expression for the hybrid outage probability is derived. Moreover, the impact of two eavesdroppers, i.e., active and passive is examined and active eavesdropping is found to bring harm more to the system's security. Similary, in [16], a multiple antenna transmitter setting in the presence of an active full-duplex eavesdropper was investigated by considering channel estimation error both at the receiver and adversary. Closed-form expressions for the probability of positive secrecy capacity and secrecy outage probability are derived and theoretical analysis is validated through Monte Carlo simulations.

The case of multiple and passive eavesdroppers in a wiretap channel is investigated in detail in many studies in the literature. For example, for the wiretap channels that involve the unknown location of the eavesdroppers, stochastic geometry theory has widely been used. A stochastic geometry framework to find the maximum secrecy level for a multiple-input multiple-output (MIMO) channel when there are multiple passive eavesdroppers in random locations with unknown channels state information was presented in [17]. The probability of secrecy was investigated by employing beamforming and artificial noise. It has been found that MIMO is beneficial in achieving secrecy only when the eavesdroppers are with single antennas. In addition, the authors stated that AN may not have a significant impact if the path-loss exponent is large. Similarly, a MISO system in the presence of randomly distributed single antenna passive eavesdroppers was investigated in [18] based on the stochastic geometry theory to obtain secrecy outage probability (SOP). According to the observations, AN helped significantly improve the secrecy performance and it improved by diminishing the intensity of the eavesdroppers. A performance analysis if AN-aided multi-antenna transmission for the scenario of randomly located eavesdroppers with a multiple-antenna transmitter was presented in [19] again under a stochastic geometry theory. A closed-form expression of the optimal power allocation that minimizes the secrecy outage probability was derived. AN-aided transmission strategy that results in maximizing the secrecy rate was considered in [20] for a multiple-input single-output (MISO) channel in the presence of multiple eavesdroppers with multiple antennas, while both perfect and imperfect CSI cases are taken into account. Their results show that AN is useful to efficiently enhance the transmission security especially when the number of Eves is large. Another study proposed an AN-aided semi-adaptive secure transmission scheme for MISO wiretap channels where secrecy rate is adjusted according to the legitimate channel's CSI. Multiple eavesdroppers are assumed to be passive and equipped with single antennas, where only the statistics of them are available to the transmitter. A closed-form expression of secrecy throughput was derived and secrecy outage probability was used to evaluate the performance [21]. It has been found that semi-adaptive transmission is effective under strict secrecy constraints. Secrecy rate optimization in MISO wiretap channel with multiple multi-antenna eavesdroppers is studied in [22]. Optimization problem based on perfect and imperfect CSI, in which the transmit power is minimized subject to the secrecy rate constraint. Sometimes, eavesdroppers may share their observations with each other to create more impact (known as colluding), while in other cases they may act as individuals (known as non-colluding). The authors in [23] proposed a secure transmission strategy for a multiple non-colluding (independent) eavesdroppers system. A MISO multiple eavesdroppers system with the existence of two receivers, where one of them receives the confidential data and the other

one helps to confuse the eavesdroppers, is 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. Unlike the mentioned studies, which focused on passive and non-colluding eavesdroppers in their system models, cooperation between the multiple adversaries is also explored. In [24], stochastic geometry and random matrix theory are applied to obtain the probability of secrecy outage for both non-colluding and colluding eavesdroppers cases, where a multi-antenna transmitter communicates to multiple malicious users. Similarly, non-colluding and colluding eavesdroppers are again analyzed in [25] in terms of secrecy outage probability as well as the average secrecy capacity.

There are also research efforts have been dedicated to studying the performance of the wiretap channels in large-scale systems with multiple receivers and eavesdroppers. In particular, in [26], for a secure wireless multi-casting scheme consisting of a single antenna transmitter with multiple receivers and several eavesdroppers, the closed-form expressions for computing the probabilities of existence of non-zero secrecy capacity and secrecy outage are obtained. For a similar system model, in [27], the connection outage probability is derived.

2.2 Short Packet Communications

Recently, there has been much interest in the analysis of finite blocklength information theory in order to identify the performance of wireless systems [28–36]. As it is mentioned before, in classic information theory, capacity is the maximum coding rate. It is well-known that traditional PLS schemes are based on the assumption that the information can be transmitted through a channel with the maximum rate when the blocklengths are sufficiently large [7], [37]. However, communication with shorter packets results in a penalty on the secrecy capacity of the channel and affects the reliability and security of the communication. SPC becomes critical as an ever-increasing number of applications, including industrial IoT, intelligent transportation systems, among others, employ short packets. In this regard, PLS requires thorough examination when it comes to supporting short packet transmission.

Therefore, one of the earliest work in the field of finite blocklength information theory by Polyanskiy et al. [28] analyzed the channel coding performance. According to this work, the maximum coding rate $R^*(n,\varepsilon)$ in SPC for blocklength n given the packet error probability ε is obtained by

$$R^*(n,\varepsilon) = C - \sqrt{\frac{V}{n}} Q^{-1}(\varepsilon) \tag{2.1}$$

where C is the channel capacity, V is the channel dispersion and $Q(x)$ 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. If n approaches infinity, penalty term that occurs due to short blocklength vanishes and $R^*(n,\varepsilon)$ converges to C.

There are many works that focus on developing the bounds on the achievable rate in finite blocklength regime. Specifically, the channel dispersion of a single-user, scalar, coherent fading channel with additive Gaussian noise was derived [29], when channel state information (CSI) is available at the receiver. Previous result was extended to block-memoryless fading channels in [30], where both the transmitter and the receiver are assumed to have no knowledge of the fading realizations and provided upper and lower bounds on maximal achievable rate in the finite blocklength. Achievable rates for MIMO systems with imperfect CSI under both ergodic and non-ergodic scenarios were developed in [31].

The maximal achievable rate over quasi-static single input multiple-output (SIMO) fading channels are studied in [32] under two scenarios, which rely on the assumptions that perfect CSI and no CSI are available at both the transmitter and the receiver. The authors further broaden their research in [33] for quasi-static MIMO fading channels. The authors reached to conclusion that the dispersion of quasi-static fading channels are zero regardless of the availability of CSI, which is shown in both studies as the following

$$R^*(n,\varepsilon) = C_\varepsilon + \mathscr{O}\left(\frac{\log n}{n}\right) \tag{2.2}$$

The maximal channel coding rate of two channel models, i.e., AWGN and the quasi-static fading channels with the assumption that both the transmitter and the receiver have perfect channel state information (CSI), are derived, when long-term power constraint was considered [35]. [36] explored the relationship between reliability, throughput and latency for short packet transmission over MIMO Rayleigh block-fading channels, where the priori availability of perfect CSI does not exist. Upper and lower bounds on maximum coding rate over such channels was obtained for finite-blocklength for a given packet error probability. The findings suggest wireless systems need thorough analysis on the balance between packet-error probability, communication rate, and packet size, because performance metrics that is are valid for traditional infinite blocklength do not capture the trade-off between reliability, throughput and latency in finite blocklength regime. [34] investigates the goodput analysis, which is the average probability of successful transmission rate for a given number of message bits sent in a blocklength, in additive white Gaussian noise (AWGN) with the assumption of the fading channel with no channel state information at transmitter (CSIT) and finds the

impact of the finite blocklength on some parameters such as the energy-efficiency (EE) or packet error rate (PER).

2.3 Security of Short Packet Communications

Some preliminary works on improving the bounds of the maximal secure achievable rate of finite blocklength regime have been put forward. The authors in [38] provided achievable bounds for the maximal secrecy rate to capture the impact of finite blocklength, error probability, and information leakage (in terms of the variational distance) for both degraded discrete-memoryless and Gaussian wiretap channels. The work in [39] evaluated the trade-off between secrecy and reliability and derived an upper bound on secrecy rate. The bounds on the second-order coding rate (also known as dispersion) are analysed for degraded discrete-memoryless wiretap channels (DM-WTC) and Gaussian wiretap channels in [40] and obtained the following

$$C_{\mathrm{S}} - \sqrt{\frac{V_1}{n}}Q^{-1}(\varepsilon) - \sqrt{\frac{V_2}{n}}Q^{-1}(\delta) \lessapprox R^*(n,\varepsilon,\delta) \lessapprox C_{\mathrm{S}} - \sqrt{\frac{V_3}{n}}Q^{-1}(\varepsilon+\delta) \tag{2.3}$$

where C_{S} is the secrecy capacity and δ denotes the information leakage probability, while the symbol $\lessapprox$ is used to indicate less-than or approximately. The work in [41] was a conference paper, which contained initial results of [42], addresses the trade-off between reliability and secrecy at a given blocklength. The achievability and converse bounds that were found in [40] were tightened for a semi-deterministic wiretap channel. The defining feature of this channel is a deterministic channel between the transmitter and legitimate receiver, while the communication link between the transmitter and the eavesdropper is a discrete memoryless channel. The mathematical expression is provided below.

$$R^*(n,\varepsilon,\delta) = C_{\mathrm{S}} - \sqrt{\frac{V_{\mathrm{S}}}{n}}Q^{-1}\Big(\frac{\delta}{1-\varepsilon}\Big) \tag{2.4}$$

for every ε and δ satisfy $\varepsilon+\delta<1$.

Although the existing works on PLS have extensively investigated several communication scenarios for wiretap channels, there are only a few studies that focus on PLS for SPC. Further, the existing works are limited as they mainly assume a single passive eavesdropper. In addition, the majority of the wiretap channel investigations are focused on measuring the performance of a system with the average secrecy throughput. In [43], cooperative relaying is introduced in an IoT network and approximated the average throughput for it in closed-form expression. The authors in [44] investigated the performance of secure SPC

in a mission-critical IoT system with the presence of a multiple antenna eavesdropper and calculated average secrecy throughput for single and multi-antenna transmitter settings, when there is a multi-antenna passive eavesdropper. At this work, not only AN impact on the system performance was analysed, but also the optimal blocklength that maximize the secrecy throughput was found. Similarly, the study in [45] explored a fading wiretap channel with single or multi-antenna transmitters with the existence of a single antenna passive eavesdropper. Basically, the throughput is maximized by considering the optimal transmission policy, blocklength, code rates, and power allocation of the AN scheme, with further examination of multiple antenna eavesdropper. It has been found that enhancement on the reliability and security depends on increasing the blocklength with the on-off policy. Multi-user MIMO systems are also investigated in [46] and [47]. In [46], uplink massive multi-user multiple-input-multiple-output (MU-MIMO) IoT networks are explored and an analytical expression for secrecy throughput is derived, when a multi-antenna eavesdropper is present. The results show that average secrecy throughput can be improved by increasing the number of antennas at the base station as well as increasing the transmission SNR. Differently, the authors in [47] investigate the full-duplex (FD) mode of base station for MU-MIMO and obtain a closed-form formula of the average secrecy throughput by taking into account the self-interference (SI) and the co-channel interference (CCI) from uplink to downlink. It has been shown that the FD multi-user MIMO systems outperform the half-duplex ones when SI and CCI are properly managed. In [48], the average secure block error rate was analyzed in a non-orthogonal multiple access (NOMA) downlink SPC system. In a recent study in [49] the outage probability and effective throughput are used to evaluate the performance of SPC systems in order to guarantee reliability and security simultaneously.

So far, the aforementioned studies only consider the presence of a single eavesdropper. Multiple eavesdroppers are more representative of real scenario settings when it comes to large-scale wireless network systems. From the above, it is clear that only a few works investigate multiple-user networks and there is a lack of studies for multiple eavesdroppers perspective. For example, a closed-form approximations of the average secrecy throughput for single and multiple antenna transmitter are presented in [50] for Rayleigh fading wiretap channels, where multiple passive eavesdroppers exist. The impacts of the number of antennas, eavesdroppers and the transmission rate on the average secrecy throughput are discussed. The previous work has been extended to investigate the impact of multiple antenna transmitter in [51]. Moreover, multiple eavesdroppers context is employed in a wiretap channel where there are also multiple receivers [52]. Average secrecy throughput analysis are conducted for colluding and non-colluding adversary cases to obtain insights on how eavesdropper cooperation affects the system performance in the case of short packet transmission.

Although most of the studies consider passive eavesdropper models in which the eavesdropper only overhears the transmission, the work in [53] brings attention to the direction of an active eavesdropper, which is more likely to disrupt the overall system transmission more efficiently if short packets are conveyed. Novel approximations of the average secrecy throughput for a Rayleigh fading wiretap channel, where an active eavesdropper either operates in half duplex or full duplex mode.

Chapter 3

Secrecy Analysis of an Active Eavesdropper

This chapter studies secure short packet communications in a wiretap channel when an active eavesdropper exists. Although both passive and active eavesdropper scenarios are already well studied in physical layer scenarios, it is still not addressed how secure communication can be established in these scenarios with SPC. Therefore, this investigation is motivated by the fact that whether eavesdropping or jamming activities are beneficial for the adversary to degrade the secrecy throughput in a wiretap scenario. We begin exploring the impact of half-duplex eavesdropper on secure communication, then we further consider full-duplex mode and compare their performance.

3.1 Background Information

With the evolution to 5G and beyond communication systems, the security of wireless communication becomes more important, and new challenges arise. The broadcast nature of the wireless communication link makes the communication vulnerable to malicious attacks. Security threats may not only be by passive adversaries, but also by active ones. A passive eavesdropper can monitor the transmission silently so that it is hard to be detected because of its ability to hide itself. Besides, an active eavesdropper may remain silent and overhear the transmission of legitimate parties, or may jam the transmission to degrade the quality and security of the communication. Therefore, active eavesdropping may be potentially more harmful than passive one when it comes to the security of wireless communication links.

To this end, secure SPC is an essential topic to be addressed. Active eavesdropper model is a concern that is more likely to disrupt the overall system transmission more efficiently if short packets are conveyed.

3.1.1 Motivation and Contributions

Given the increasing number of connected devices and users in networks, it is possible to face more advanced eavesdroppers capable of operating in both passive and active modes. Therefore, it is crucial to examine the performance of active eavesdropping. Previous studies have not investigated such analysis for finite blocklengths. Our research aims to address this gap in the literature by analyzing the impact of active eavesdropping on the performance of secure SPC.

In this chapter, we explore the security performance of a short packet transmission system over a wiretap channel under the existence of an active eavesdropper. The performance metric for evaluating the effectiveness of our approach is the average secrecy throughput. It is defined as the average secrecy rate at which data packets can be reliably transmitted while satisfying a specific secrecy constraint. Approximated expressions for the average secrecy throughput for both the half and full-duplex eavesdropper modes are found and the results are compared with those derived by Monte Carlo (MC) simulations. In addition, we explore the impact of the distance between legitimate nodes and the eavesdropper on the average secrecy throughput for two topologies and various settings. Our preliminary analysis regarding to full-duplex eavesdropper is presented in [53].
In particular, the contributions of this work are summarized as follows

- A closed-form approximation is found for the average secrecy throughput when eavesdropper acts in HD mode, which allows the eavesdropper to either listen to Alice's short packet transmission or to jam Bob's communication. A simpler approximation of the average secrecy throughput is found when a FD eavesdropper is present, i.e., eavesdropping and jamming happen simultaneously.

- Both derived expressions are validated through MC simulations and the findings show that evaluation of the analytical framework closely matches with performance of the simulations.

- We further investigated the impact of the distance between the nodes for two different topologies, namely line and triangular, to capture how eavesdropper's location affects the system performance.

3.2 Performance Metric Formulation

3.2.1 Average Secrecy Throughput

In this section, we will introduce what steps are followed to obtain the average secrecy throughput, which is the chosen performance metric for this work.

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 [7], [8]. 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 SPC, classical information-theoretic performance metrics, such as secrecy outage probability, do not apply [4]. 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 $R^*(n,\varepsilon,\delta)$ can be approximated (as in [40, 42, 41, 44]) as follows

$$R^*(n,\varepsilon,\delta) = C_{\mathrm{s}} - \sqrt{\frac{V_{\gamma_{\mathrm{B}}}}{n}}\frac{Q^{-1}(\varepsilon)}{\log(2)} - \sqrt{\frac{V_{\gamma_{\mathrm{E}}}}{n}}\frac{Q^{-1}(\delta)}{\log(2)}, \tag{3.1}$$

where γ_{B} is the signal-to-noise ratio (SNR) at the legitimate receiver, whereas γ_{E} is the SNR at the eavesdropper. Hence, $V_{\gamma_{\mathrm{B}}} = 1-(1+\gamma_{\mathrm{B}})^{-2}$ and $V_{\gamma_{\mathrm{E}}} = 1-(1+\gamma_{\mathrm{E}})^{-2}$ are the dispersion of the main and eavesdropper channels [28], respectively. $Q^{-1}(.)$ is the inverse of the Q-function. The secrecy capacity of the wiretap channel C_{s} is computed as

$$\begin{aligned} C_{\mathrm{s}} &= [\log_2(1+\gamma_{\mathrm{B}}) - \log_2(1+\gamma_{\mathrm{E}})]^+ \\ &= \left[\log_2\left(\frac{1+\gamma_{\mathrm{B}}}{1+\gamma_{\mathrm{E}}}\right)\right]^+. \end{aligned} \tag{3.2}$$

In particular,

$$C_{\mathrm{s}} = \begin{cases} C_{\mathrm{B}} - C_{\mathrm{E}}, & \text{when} \quad \gamma_{\mathrm{B}} > \gamma_{\mathrm{E}}, \\ 0, & \text{when} \quad \gamma_{\mathrm{B}} \leq \gamma_{\mathrm{E}}, \end{cases} \tag{3.3}$$

where the capacity of the main channel is

$$C_{\mathrm{B}} = \log_2(1+\gamma_{\mathrm{B}}), \tag{3.4}$$

and the capacity of the eavesdropper's channel equals to

$$C_{\mathrm{E}} = \log_2(1+\gamma_{\mathrm{E}}). \tag{3.5}$$

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 study, the arguments of (n,ε,δ) may be dropped in R^*). For $\gamma_{\mathrm{B}} > \gamma_{\mathrm{E}}$, i.e., when the secrecy capacity is greater than zero, the decoding error probability, by substituting b/n into (3.1), is expressed according to [44] as follows

$$\varepsilon = Q\left(\sqrt{\frac{n}{V_{\gamma_{\mathrm{B}}}}}\left(\log\left(\frac{1+\gamma_{\mathrm{B}}}{1+\gamma_{\mathrm{E}}}\right) - \sqrt{\frac{V_{\gamma_{\mathrm{E}}}}{n}}Q^{-1}(\delta) - \frac{b}{n}\log(2)\right)\right). \tag{3.6}$$

The decoding error probability ε in (3.6) is defined by the instantaneous SNR of the main channel, γ_{B}, conditioned on the eavesdropper's instantaneous SNR, γ_{E}, and is represented as $\varepsilon_{\gamma_{\mathrm{B}}|\gamma_{\mathrm{E}}}$. The average achievable secrecy throughput, T_{s}, (measured in bits per channel use (BPCU)), can be computed as [44]

$$\begin{aligned} T_{\mathrm{s}} &= \mathbb{E}_{\gamma_{\mathrm{B}},\gamma_{\mathrm{E}}}\left\{\frac{b}{n}(1-\varepsilon)\right\} \\ &= \frac{b}{n}(1-\overline{\varepsilon}), \end{aligned} \tag{3.7}$$

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

$$1-\overline{\varepsilon} = 1-\mathbb{E}_{\gamma_{\mathrm{B}},\gamma_{\mathrm{E}}}[\varepsilon]. \tag{3.8}$$

Now, we can obtain the closed-form approximation for the average secrecy throughput as

$$T_{\mathrm{s}} = \int_0^\infty \int_0^\infty (1-\varepsilon)\frac{b}{n} f(\gamma_{\mathrm{B}}) f(\gamma_{\mathrm{E}}) d\gamma_{\mathrm{B}} d\gamma_{\mathrm{E}}. \tag{3.9}$$

We can analyze the integral in (3.9) into two integrals

$$T_{\mathrm{s}} = \frac{b}{n}\int_0^\infty S(\gamma_{\mathrm{E}}) f(\gamma_{\mathrm{E}}) d\gamma_{\mathrm{E}}, \tag{3.10}$$

and

$$S(\gamma_E) = \int_0^\infty (1 - \varepsilon_{\gamma_B|\gamma_E}) f(\gamma_B) d\gamma_B. \tag{3.11}$$

When $\gamma_B \leq \gamma_E$, which means secrecy capacity is zero, $\varepsilon_{\gamma_B|\gamma_E}$ is set to 1. In the more interesting case $\gamma_B > \gamma_E$, $\varepsilon_{\gamma_B|\gamma_E}$ has an intractable form, and thus we approximate it by using the linearization technique presented in [54]. Furthermore, this method was implemented in [43], [44] as well. According to this approximation, it is

$$\varepsilon_{\gamma_B|\gamma_E}(x) \approx \begin{cases} 1, & x < \alpha + u, \\ \frac{1}{2} + \beta(x - \alpha), & \alpha + u \leq x \leq \alpha - u, \\ 0, & x > \alpha - u, \end{cases} \tag{3.12}$$

The parameter α is found by

$$\alpha = e^{\left(\sqrt{\frac{V_{\gamma_E}}{n}} Q^{-1}(\delta) + \frac{b}{n}\log(2)\right)} (1 + \gamma_E) - 1, \tag{3.13}$$

α in (3.13) is obtained by setting $Q\left(\sqrt{\frac{n}{V_\alpha}}\left(\log\left(\frac{1+\alpha}{1+\gamma_E}\right) - \sqrt{\frac{V_{\gamma_E}}{n}} Q^{-1}(\delta) - \frac{b}{n}\log(2)\right)\right) = 1/2.$
Since $Q(0) = 1/2$, α is derived by solving $\left(\log\left(\frac{1+\alpha}{1+\gamma_E}\right) - \sqrt{\frac{V_{\gamma_E}}{n}} Q^{-1}(\delta) - \frac{b}{n}\log(2)\right) = 0.$
For the sake of simplicity, we can approximate $V_{\gamma_E} \approx 1$ in (3.13), and then we obtain

$$\alpha = e^{\left(\frac{Q^{-1}(\delta)}{\sqrt{n}} + \frac{b}{n}\log(2)\right)} (1 + \gamma_E) - 1, \tag{3.14}$$

which can be further rewritten as

$$\alpha = r(1 + \gamma_E) - 1. \tag{3.15}$$

where $r = e^{\left(\frac{Q^{-1}(\delta)}{\sqrt{n}} + \frac{b}{n}\log(2)\right)}$. The slope β of $\varepsilon_{\gamma_B|\gamma_E}(x)$ at $x = \alpha$ in (3.12) is defined as

$$\beta = \frac{d\varepsilon_{\gamma_B|\gamma_E}(x)}{dx}\Big|_{x=\alpha} = -\sqrt{\frac{n}{2\pi\alpha(\alpha+2)}}, \tag{3.16}$$

and it satisfies $\frac{1}{2} + \beta(\alpha + u - \alpha) = 1$ and $\frac{1}{2} + \beta(\alpha - u - \alpha) = 0$ then we get $u = \frac{1}{2\beta}$.

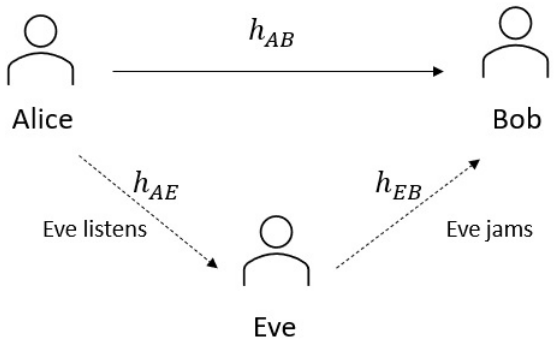

Fig. 3.1 Wiretap Channel Model in the Presence of Half-Duplex Eavesdropper. The channel gain from Alice to Bob: h_{AB}; the channel gain from Alice to Eve's receiving antenna: h_{AE}; the channel gain from Eve's transmitting antenna to Bob: h_{EB}.

3.3 System Model and Problem Description

3.3.1 Half-Duplex Eve

In the half-duplex scenario, Alice and Bob are equipped with a single antenna, whereas Eve has two antennas, one used for receiving signals and another one for jamming [10], [11]. All the channels are Rayleigh fading. It is worth noting that the instantaneous channel state information (CSI) of the main channel between Bob and Alice is known to Alice, whereas only the statistical CSI of Eve's channel is known to Alice as in [43]. Let us denote the channel gain of the main channel, i.e., from Alice to Bob as h_{AB}, the channel gain from Alice to Eve's receiving antenna as h_{AE}, and the channel gain from Eve's transmitting antenna to Bob as h_{EB}. Channel gains are formulated with respect to the distances between the nodes as follows; $h_{\mathrm{AB}} = \sqrt{d_{\mathrm{AB}}^{-v}} g_{\mathrm{AB}}$, $h_{\mathrm{AE}} = \sqrt{d_{\mathrm{AE}}^{-v}} g_{\mathrm{AE}}$ and $h_{\mathrm{EB}} = \sqrt{d_{\mathrm{EB}}^{-v}} g_{\mathrm{EB}}$, where d_{AB} stands for the distance between Alice and Bob, d_{AE} is the distance between Alice and Eve and d_{EB} represents the distance between Eve and Bob. The parameter v is the path-loss exponent. In addition, g_{AB}, g_{AE} and g_{EB} are the fading coefficients of the aforementioned communication links, respectively. Finally, let σ_{B}^2, σ_{E}^2 denote the noise variance at Bob and Eve, respectively. A half-duplex eavesdropper is considered in a wireless communication system as shown in Fig. 3.1. Eve can either jam the communication or eavesdrops it, but she cannot do both at the same time. Eavesdropper's preference on jamming or eavesdropping affects the channel coefficients. Let the transmitted signal be denoted by x. Alice transmits the message with the power of P_A, while Eve can disrupt the communication with jamming power P_E. The noise at Bob and Eve are represented by n_{B} and n_{E}, respectively. We assume $\sigma_{\mathrm{B}}^2 = \sigma_{\mathrm{E}}^2 = 1$, for the

sake of simplicity. Thus, P_A and P_E are also the signal-to-noise ratios.
When Eve is passive, the received signal at Bob and Eve can be written as

$$\begin{aligned} y_{\mathrm{B}} &= \sqrt{P_{\mathrm{A}}} h_{\mathrm{AB}} x + n_{\mathrm{B}}, \\ y_{\mathrm{E}} &= \sqrt{P_{\mathrm{A}}} h_{\mathrm{AE}} x + n_{\mathrm{E}}. \end{aligned} \tag{3.17}$$

Differently, when Eve is active, only Bob receives the signal, and Eve jams Bob's received signal. Therefore, $y_{\mathrm{E}} = 0$ and the received signal at Bob is

$$y_{\mathrm{B}} = \sqrt{P_{\mathrm{A}}} h_{\mathrm{AB}} x + \sqrt{P_{\mathrm{E}}} h_{\mathrm{EB}} x + n_{\mathrm{B}}. \tag{3.18}$$

When Eve is in eavesdrop mode, the received instantaneous SNR at Bob, γ_{B}, and at Eve, γ_{E}, are as follows

$$\begin{aligned} \gamma_{\mathrm{B}} &= \frac{P_{\mathrm{A}} |h_{\mathrm{AB}}|^2}{\sigma_{\mathrm{B}}^2} = \rho_{\mathrm{AB}} |g_{\mathrm{AB}}|^2, \\ \gamma_{\mathrm{E}} &= \frac{P_{\mathrm{A}} |h_{\mathrm{AE}}|^2}{\sigma_{\mathrm{E}}^2} = \rho_{\mathrm{AE}} |g_{\mathrm{AE}}|^2, \end{aligned} \tag{3.19}$$

with the substitution of $\rho_{\mathrm{XY}} = \frac{P_{\mathrm{X}} d_{\mathrm{XY}}^{-\nu}}{\sigma_{\mathrm{Y}}^2}$.
When Eve operates in jamming mode, the received instantaneous SNR at Bob, γ_{J} and at Eve are given below

$$\begin{aligned} \gamma_{\mathrm{J}} &= \frac{|h_{\mathrm{AB}}|^2 P_{\mathrm{A}}}{|h_{\mathrm{EB}}|^2 P_{\mathrm{E}} + \sigma_{\mathrm{N}}^2} = \frac{\rho_{\mathrm{AB}} |g_{\mathrm{AB}}|^2}{\rho_{\mathrm{EB}} |g_{\mathrm{EB}}|^2 + 1}, \\ \gamma_{\mathrm{E}} &= 0. \end{aligned} \tag{3.20}$$

Then, secret transmission rate, R_{s}, during jamming is

$$R_{\mathrm{s}} = \log_2 \left(1 + \frac{\rho_{\mathrm{AB}} |g_{\mathrm{AB}}|^2}{\rho_{\mathrm{EB}} |g_{\mathrm{EB}}|^2 + 1} \right) \tag{3.21}$$

When Eve is in passive mode the error probability, ε_{P}, is defined in the following as in (3.6)

$$\varepsilon_{\mathrm{P}} = Q\left(\sqrt{\frac{n}{V_{\gamma_{\mathrm{B}}}}} \left(\log \left(\frac{1+\gamma_{\mathrm{B}}}{1+\gamma_{\mathrm{E}}} \right) - \sqrt{\frac{V_{\gamma_{\mathrm{E}}}}{n}} Q^{-1}(\delta) - \frac{b}{n} \log(2) \right) \right), \tag{3.22}$$

However, when Eve is in active mode the error probability, ε_{J}, becomes

$$\varepsilon_{\mathrm{J}} = Q\left(\sqrt{\frac{n}{V_{\gamma_{\mathrm{J}}}}} \left(\log(1+\gamma_{\mathrm{J}}) - \frac{b}{n} \log(2) \right) \right). \tag{3.23}$$

The secrecy throughput for for HD Eve can be formulated as

$$T_{\mathrm{s}} = \mathbb{E}\gamma_{\mathrm{B}},\gamma_{\mathrm{E}},\gamma_{\mathrm{J}}\Big[\frac{b}{n}(1-\overline{\varepsilon})\Big]. \tag{3.24}$$

If we assume that Eve eavesdrops with a probability of q and jams with a probability of $1-q$, we can formulate overall average error probability by $\overline{\varepsilon} = q\overline{\varepsilon}_{\mathrm{P}} + (1-q)\overline{\varepsilon}_{\mathrm{J}}$. Then, the average secrecy throughput becomes

$$T_{\mathrm{s}} = \frac{b}{n}\Big(1 - \big(q\overline{\varepsilon}_{\mathrm{P}} + (1-q)\overline{\varepsilon}_{\mathrm{J}}\big)\Big). \tag{3.25}$$

Calculation of $\overline{\varepsilon}_{\mathrm{P}}$

In this subsection, we show how to derive the expression for $\overline{\varepsilon}_{\mathrm{P}}$, which is the average error probability of passive Eve.

$$\overline{\varepsilon}_{\mathrm{P}} = \int_0^{\infty}\int_0^{\infty} \varepsilon_{\gamma_{\mathrm{B}}|\gamma_{\mathrm{E}}}(x) f(\gamma_{\mathrm{B}}) f(\gamma_{\mathrm{E}}) d\gamma_{\mathrm{B}} d\gamma_{\mathrm{E}}. \tag{3.26}$$

where the channel statistics for main and eavesdropper's channels are given

$$f(\gamma_{\mathrm{B}}) = \frac{1}{\rho_{\mathrm{AB}}} e^{-\frac{\gamma_{\mathrm{B}}}{\rho_{\mathrm{AB}}}}, \quad f(\gamma_{\mathrm{E}}) = \frac{1}{\rho_{\mathrm{AE}}} e^{-\frac{\gamma_{\mathrm{E}}}{\rho_{\mathrm{AE}}}} \tag{3.27}$$

$\overline{\varepsilon}_{\mathrm{P}}$ can be rewritten as

$$\overline{\varepsilon}_{\mathrm{P}} = \int_0^{\infty} \Omega f(\gamma_{\mathrm{E}}) d\gamma_{\mathrm{E}}, \tag{3.28}$$

where

$$\Omega = \int_0^{\infty} \varepsilon_{\gamma_{\mathrm{B}}|\gamma_{\mathrm{E}}}(x) \frac{1}{\rho_{\mathrm{AB}}} e^{-\frac{\gamma_{\mathrm{B}}}{\rho_{\mathrm{AB}}}} d\gamma_{\mathrm{B}}, \tag{3.29}$$

and it is expanded by employing (3.12)

$$\Omega = \int_0^{\alpha+u} \frac{1}{\rho_{\mathrm{AB}}} e^{-\frac{\gamma_{\mathrm{B}}}{\rho_{\mathrm{AB}}}} dx + \int_{\alpha+u}^{\alpha-u} (\beta(x-\alpha)+1/2) \frac{1}{\rho_{\mathrm{AB}}} e^{-\frac{x}{\rho_{\mathrm{AB}}}} dx. \tag{3.30}$$

By solving (3.30), we get

$$\Omega = 1 - \beta\rho_{\mathrm{AB}} e^{-\frac{\alpha}{\rho_{\mathrm{AB}}}} (e^{\frac{u}{\rho_{\mathrm{AB}}}} - e^{-\frac{u}{\rho_{\mathrm{AB}}}}). \tag{3.31}$$

for the large values of ρ_{AB}, (3.31) can be further simplified as

$$\Omega \approx 1 - e^{-\frac{\alpha}{\rho_{\mathrm{AB}}}}. \tag{3.32}$$

Exploiting the above approximation, (3.28) can be approximated as

$$\overline{\varepsilon}_{\mathrm{P}} \approx \int_0^{\infty} (1 - e^{-\frac{\alpha}{\rho_{\mathrm{AB}}}}) \frac{1}{\rho_{\mathrm{AE}}} e^{-\frac{\gamma_{\mathrm{E}}}{\rho_{\mathrm{AE}}}} d\gamma_{\mathrm{E}} \tag{3.33}$$

and we can obtain the expression for $\overline{\varepsilon}_{\mathrm{P}}$

$$\overline{\varepsilon}_{\mathrm{P}} \approx 1 - \frac{\rho_{\mathrm{AB}}}{\rho_{\mathrm{AE}} r + \rho_{\mathrm{AB}}} e^{\frac{1-r}{\rho_{\mathrm{AB}}}}. \tag{3.34}$$

Calculation of $\overline{\varepsilon}_{\mathrm{J}}$

Similar to $\overline{\varepsilon}_{\mathrm{P}}$ case, we use the linearization method in (3.12), which is reorganized to approximate the average error probability when Eve is in active mode. Parameters of α_{J}, β_{J}, u_{J} are defined for the jamming case as

$$\begin{aligned} \alpha_{\mathrm{J}} &= e^{\frac{b}{n}\log(2)} - 1, \\ \beta_{\mathrm{J}} &= -\sqrt{\frac{n}{2\pi(e^{2\frac{b}{n}\log(2)} - 1)}}, \\ u_{\mathrm{J}} &= -\frac{1}{2\beta_{\mathrm{J}}}. \end{aligned} \tag{3.35}$$

where α_{J} is obtained by setting $\log(1+\alpha_{\mathrm{J}}) - \frac{b}{n}\log(2) = 0$, which makes $Q\left(\sqrt{\frac{n}{V_{\alpha_{\mathrm{J}}}}}\left(\log(1+\alpha_{\mathrm{J}}) - \frac{b}{n}\log(2)\right)\right) = 1/2$.

The jamming average error probability $\overline{\varepsilon}_{\mathrm{J}}$ is equal to

$$\overline{\varepsilon}_{\mathrm{J}} = \int_0^{\infty} \varepsilon(j) f(\gamma_{\mathrm{J}}) d\gamma_{\mathrm{J}}. \tag{3.36}$$

In order to find the channel statistics, we use the definition of the received SNR on the main channel

$$\gamma_{\mathrm{J}} = \frac{|h_{\mathrm{AB}}|^2 P_{\mathrm{A}}}{|h_{\mathrm{EB}}|^2 P_{\mathrm{E}} + \sigma_{\mathrm{N}}^2} = \frac{\rho_{\mathrm{AB}} |g_{\mathrm{AB}}|^2}{\rho_{\mathrm{EB}} |g_{\mathrm{EB}}|^2 + 1} = \frac{\mu_{\mathrm{AB}}}{\mu_{\mathrm{EB}} + 1} \tag{3.37}$$

where $\mu_{\mathrm{XY}} = \rho_{\mathrm{XY}} |g_{\mathrm{XY}}|^2$. μ_{AB} and μ_{EB} are random variables that follow exponential distribution, because $|g_{\mathrm{XY}}|^2$ follows exponential distribution. Thus, the CDF of γ_{J} is evaluated by

considering $F(\gamma_{\text{J}}) = \Pr\Big(\frac{\mu_{\text{AB}}}{\mu_{\text{EB}}+1} \leq \gamma_{\text{J}}\Big)$, therefore

$$F(\gamma_{\text{J}}) = \int_0^{\infty} \int_0^{\gamma_{\text{J}}(\mu_{\text{EB}}+1)} f(\mu_{\text{AB}}) f(\mu_{\text{EB}}) d\mu_{\text{AB}} d\mu_{\text{EB}}. \tag{3.38}$$

wherein

$$\begin{aligned} f(\mu_{\text{AB}}) &= \frac{1}{\rho_{\text{AB}}} e^{-\frac{\mu_{\text{AB}}}{\rho_{\text{AB}}}}, \\ f(\mu_{EB}) &= \frac{1}{\rho_{\text{EB}}} e^{-\frac{\mu_{\text{EB}}}{\rho_{\text{EB}}}} \end{aligned} \tag{3.39}$$

Finally, by calculating (3.38) we obtain

$$F(\gamma_{\text{J}}) = 1 - \frac{\rho_{\text{AB}}}{\rho_{\text{EB}}\gamma_{\text{J}} + \rho_{\text{AB}}} e^{-\frac{\gamma_{\text{J}}}{\rho_{\text{AB}}}}, \tag{3.40}$$

Hence, the PDF of γ_{J} is computed as

$$f(\gamma_{\text{J}}) = \frac{\rho_{\text{EB}}\gamma_{\text{J}} + \rho_{\text{AB}} + \rho_{\text{AB}}\rho_{\text{EB}}}{(\rho_{\text{EB}}\gamma_{\text{J}} + \rho_{\text{AB}})^2} e^{-\frac{\gamma_{\text{J}}}{\rho_{\text{AB}}}}. \tag{3.41}$$

Using the linearization method in (3.12), (3.36) and (3.41), we can compute the average error probability for the jamming case as

$$\begin{aligned} \overline{\varepsilon}_{\text{J}} = &\int_0^{\alpha_{\text{J}}+\frac{1}{2\beta_J}} \frac{\rho_{\text{EB}}\gamma_{\text{J}} + \rho_{\text{AB}} + \rho_{\text{AB}}\rho_{\text{EB}}}{(\rho_{\text{EB}}\gamma_{\text{J}} + \rho_{\text{AB}})^2} e^{-\frac{\gamma_{\text{J}}}{\rho_{\text{AB}}}} d\gamma_{\text{J}} \\ &+ \int_{\alpha_{\text{J}}+\frac{1}{2\beta_J}}^{\alpha_{\text{J}}-\frac{1}{2\beta_J}} (\beta_{\text{J}}(\gamma_{\text{J}} - \alpha_{\text{J}}) + 1/2) \frac{\rho_{\text{EB}}\gamma_{\text{J}} + \rho_{\text{AB}} + \rho_{\text{AB}}\rho_{\text{EB}}}{(\rho_{\text{EB}}\gamma_{\text{J}} + \rho_{\text{AB}})^2} e^{-\frac{\gamma_{\text{J}}}{\rho_{\text{AB}}}} d\gamma_{\text{J}}. \end{aligned} \tag{3.42}$$

and we obtain an approximation for (3.36) according to

$$\overline{\varepsilon}_{\text{J}} \approx 1 + \frac{\beta_{\text{J}}\rho_{\text{AB}} e^{\frac{1}{\rho_{\text{EB}}}}}{\rho_{\text{EB}}} \Big[\text{E}_1\Big(\frac{\alpha_{\text{J}} + \frac{1}{2\beta_J}}{\rho_{\text{AB}}} + \frac{1}{\rho_{\text{EB}}}\Big) - \text{E}_1\Big(\frac{\alpha_{\text{J}} - \frac{1}{2\beta_J}}{\rho_{\text{AB}}} + \frac{1}{\rho_{\text{EB}}}\Big)\Big]. \tag{3.43}$$

The overall average error probability is calculated using (3.34) and (3.43)

$$\overline{\varepsilon} \approx q\Big(1 - \frac{\rho_{\text{AB}}}{\rho_{\text{AE}} r + \rho_{\text{AB}}} e^{\frac{1-r}{\rho_{\text{AB}}}}\Big) + (1-q)\Big(1 + \frac{\beta_{\text{J}}\rho_{\text{AB}} e^{\frac{1}{\rho_{\text{EB}}}}}{\rho_{\text{EB}}} \Big[\text{E}_1(H) - \text{E}_1(G)\Big]\Big). \tag{3.44}$$

where $H = \frac{\alpha_J + \frac{1}{2\beta_J}}{\rho_{AB}} + \frac{1}{\rho_{EB}}$ and $G = \frac{\alpha_J - \frac{1}{2\beta_J}}{\rho_{AB}} + \frac{1}{\rho_{EB}}$.
Then, we can easily derive T_s in (3.25) as follows

$$T_s \approx \frac{b}{n}\Big[1 - \Big(q\Big(1 - \frac{\rho_{AB}}{\rho_{AE}r + \rho_{AB}} e^{\frac{1-r}{\rho_{AB}}}\Big) + (1-q)\Big(1 + \frac{\beta_J \rho_{AB} e^{\frac{1}{\rho_{EB}}}}{\rho_{EB}}\Big[E_1(H) - E_1(G)\Big]\Big)\Big)\Big]. \tag{3.45}$$

Impact of eavesdropping probability q

In order to investigate the impact of the eavesdropping probability q to the system, we take the derivative of T_s with respect to q.

$$\frac{\partial T_s}{\partial q} = \frac{\partial\left[\frac{b}{n}\Big(1 - \big(q\overline{\varepsilon}_P + (1-q)\overline{\varepsilon}_J\big)\Big)\right]}{\partial q} = \frac{b}{n}(\overline{\varepsilon}_J - \overline{\varepsilon}_P) \tag{3.46}$$

We know that $\frac{b}{n} > 0$ is always positive. Therefore, the sign of the $\frac{\partial T_s}{\partial q}$ depends on the rest of the expression $(\overline{\varepsilon}_J - \overline{\varepsilon}_P)$, which leads us to following

$$\begin{aligned}\overline{\varepsilon}_J - \overline{\varepsilon}_P &= \Big(1 + \frac{\beta_J \rho_{AB} e^{\frac{1}{\rho_{EB}}}}{\rho_{EB}}\Big[E_1(H) - E_1(G)\Big]\Big) - \Big(1 - \frac{\rho_{AB}}{\rho_{AE}r + \rho_{AB}} e^{\frac{1-r}{\rho_{AB}}}\Big) \\ &= \underbrace{\Big(\frac{\beta_J \rho_{AB} e^{\frac{1}{\rho_{EB}}}}{\rho_{EB}}\Big[E_1(H) - E_1(G)\Big]\Big)}_{\text{I}} + \underbrace{\Big(\frac{\rho_{AB}}{\rho_{AE}r + \rho_{AB}} e^{\frac{1-r}{\rho_{AB}}}\Big)}_{\text{II}}\end{aligned} \tag{3.47}$$

Summand I is monotonically decreasing w.r.t. n and runs in negative region, while summand II monotonically increasing for short blocklength range. Overall result of $\overline{\varepsilon}_J - \overline{\varepsilon}_P$ is negative, because summand I is dominant over summand II. Naturally, the partial derivative of T_s with respect to q is always negative. It can be concluded that T_s is monotonically decreasing function of q. This finding suggests that the eavesdropping probability q has a detrimental impact on the secrecy throughput T_s, which indicates that an eavesdropper in passive mode can effectively reduce the secrecy throughput.

3.3.2 Full-Duplex Eve

In the full duplex scenario, we consider a wireless communication system as shown in Fig. 3.2, where a legitimate transmitter, Alice, tries to communicate secretly with a legitimate receiver, Bob, while the eavesdropper, Eve, is actively operating in full-duplex mode. In this scenario, the eavesdropper tries to receive information from the legitimate transmitter and

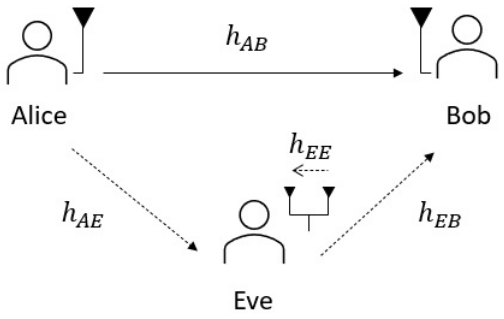

Fig. 3.2 Wiretap Channel Model in the Presence of Full-Duplex Eavesdropper. The channel gain from Alice to Bob: h_{AB}; the channel gain from Alice to Eve's receiving antenna: h_{AE}; the channel gain from Eve's transmitting antenna to Bob: h_{EB}; the channel gain from Eve's transmitting antenna to its receiving antenna: h_{EE}.

at the same time sends disruptive signals to the legitimate receiver. We know that jamming results in interference at the eavesdropper's own receiver antenna. Therefore, in addition to the specified channel gains in HD Eve case, a further definition for the link gain from Eve's transmitting antenna to its receiving antenna is given by $h_{\mathrm{EE}} = \sqrt{d_{\mathrm{EE}}^{-v} g_{\mathrm{EE}}}$, while d_{EE} denotes the distance between Eve's own antennas, v is the path-loss exponent and g_{EE} corresponds to the fading coefficient. Let us denote by ϕ the self-interference coefficient ($0 \leq \phi \leq 1$). When $\phi = 0$, the self-interference is cancelled perfectly, whereas if $\phi = 1$, it cannot be eliminated [9–11]. We assume that Alice carries out the transmission with transmit power of P_{A} and Eve jams the signal with transmit power of P_{E}. Let us denote the transmitted signal by x_{A} and the jamming signal by x_{E}. Both signals are normalized, i.e., $\mathbb{E}[|x_{\mathrm{A}}|^2] = 1$ and $\mathbb{E}[|x_{\mathrm{E}}|^2] = 1$. Considering the above, the received signal at Bob can be written as

$$y_{\mathrm{B}} = \sqrt{P_{\mathrm{A}}} h_{\mathrm{AB}} x_{\mathrm{A}} + \sqrt{P_{\mathrm{E}}} h_{\mathrm{EB}} x_{\mathrm{E}} + n_{\mathrm{B}}, \tag{3.48}$$

and the received signal at Eve can be written as

$$y_{\mathrm{E}} = \sqrt{P_{\mathrm{A}}} h_{\mathrm{AE}} x_{\mathrm{A}} + \sqrt{\phi P_{\mathrm{E}}} h_{\mathrm{EE}} x_{\mathrm{E}} + n_{\mathrm{E}}. \tag{3.49}$$

The instantaneous signal-to-interference-plus-noise ratio (SINR) for Bob and Eve can hence be computed as

$$\gamma_{\mathrm{B}} = \frac{P_{\mathrm{A}} |h_{\mathrm{AB}}|^2}{P_{\mathrm{E}} |h_{\mathrm{EB}}|^2 + \sigma_{\mathrm{B}}^2} = \frac{\rho_{\mathrm{AB}} |g_{\mathrm{AB}}|^2}{\rho_{\mathrm{EB}} |g_{\mathrm{EB}}|^2 + 1}, \tag{3.50}$$

$$\gamma_{\mathrm{E}} = \frac{P_{\mathrm{A}}|h_{\mathrm{AE}}|^2}{\phi P_{\mathrm{E}}|h_{\mathrm{EE}}|^2 + \sigma_{\mathrm{E}}^2} = \frac{\rho_{\mathrm{AE}}|g_{\mathrm{AE}}|^2}{\phi \rho_{\mathrm{EE}}|g_{\mathrm{EE}}|^2 + 1}. \tag{3.51}$$

The secrecy throughput depends on the statistics of the main and the eavesdropper's channels. Following [10], the derivation of the cumulative distribution function (CDF) of the received SINR at Bob is expressed as follows

$$F(\gamma_{\mathrm{B}}) = 1 - \frac{\rho_{\mathrm{AB}}}{\rho_{\mathrm{EB}}\gamma_{\mathrm{B}} + \rho_{\mathrm{AB}}} e^{-\frac{\gamma_{\mathrm{B}}}{\rho_{\mathrm{AB}}}}, \tag{3.52}$$

while the CDF of the received SINR at Eve is given as

$$F(\gamma_{\mathrm{E}}) = 1 - \frac{\rho_{\mathrm{AE}}}{\phi\rho_{\mathrm{EE}}\gamma_{\mathrm{E}} + \rho_{\mathrm{AE}}} e^{-\frac{\gamma_{\mathrm{E}}}{\rho_{\mathrm{AE}}}}. \tag{3.53}$$

Thus, the corresponding probability density function of the received SINR at Bob is

$$f(\gamma_{\mathrm{B}}) = \frac{\rho_{\mathrm{EB}}\gamma_{\mathrm{B}} + \rho_{\mathrm{AB}}\rho_{\mathrm{EB}} + \rho_{\mathrm{AB}}}{(\rho_{\mathrm{EB}}\gamma_{\mathrm{B}} + \rho_{\mathrm{AB}})^2} e^{-\frac{\gamma_{\mathrm{B}}}{\rho_{\mathrm{AB}}}}, \tag{3.54}$$

and that of the received SINR at Eve is

$$f(\gamma_{\mathrm{E}}) = \frac{\phi\rho_{\mathrm{EE}}\gamma_{\mathrm{E}} + \phi\rho_{\mathrm{EE}}\rho_{\mathrm{AE}} + \rho_{\mathrm{AE}}}{(\phi\rho_{\mathrm{EE}}\gamma_{\mathrm{E}} + \rho_{\mathrm{AE}})^2} e^{-\frac{\gamma_{\mathrm{E}}}{\rho_{\mathrm{AE}}}}. \tag{3.55}$$

By simplifying the secrecy throughput (T_{s}) expression by dividing into parts, we get

$$T_{\mathrm{s}} = \frac{b}{n}\int_0^{\infty} \Psi(\gamma_{\mathrm{E}}) f(\gamma_{\mathrm{E}}) d\gamma_{\mathrm{E}}, \tag{3.56}$$

where

$$\Psi(\gamma_{\mathrm{E}}) = \int_0^{\infty} (1 - \varepsilon_{\gamma_{\mathrm{B}}|\gamma_{\mathrm{E}}}) f(\gamma_{\mathrm{B}}) d\gamma_{\mathrm{B}}. \tag{3.57}$$

Thus, the computation of $\Psi(\gamma_{\mathrm{E}})$ in (3.57) is as follows

$$\Psi = 1 - \int_0^{\infty} \varepsilon_{\gamma_{\mathrm{B}}|\gamma_{\mathrm{E}}} \frac{\rho_{\mathrm{EB}}\gamma_{\mathrm{B}} + \rho_{\mathrm{AB}}\rho_{\mathrm{EB}} + \rho_{\mathrm{AB}}}{(\rho_{\mathrm{EB}}\gamma_{\mathrm{B}} + \rho_{\mathrm{AB}})^2} e^{-\frac{\gamma_{\mathrm{B}}}{\rho_{\mathrm{AB}}}} d\gamma_{\mathrm{B}}. \tag{3.58}$$

which can be written as

$$\Psi = 1 - \int_0^{\infty} \varepsilon_{\gamma_{\mathrm{B}}|\gamma_{\mathrm{E}}}(x) \frac{\rho_{\mathrm{EB}}x + \rho_{\mathrm{AB}}\rho_{\mathrm{EB}} + \rho_{\mathrm{AB}}}{(\rho_{\mathrm{EB}}x + \rho_{\mathrm{AB}})^2} e^{-\frac{x}{\rho_{\mathrm{AB}}}} dx. \tag{3.59}$$

By exploiting the linearization method in (3.12), (3.59) can be rewritten as

$$\Psi = 1 - \int_0^{\alpha+u} \frac{\rho_{\mathrm{EB}} x + \rho_{\mathrm{AB}}\rho_{\mathrm{EB}} + \rho_{\mathrm{AB}}}{(\rho_{\mathrm{EB}} x + \rho_{\mathrm{AB}})^2} e^{-\frac{x}{\rho_{\mathrm{AB}}}} dx \quad + \int_{\alpha+u}^{\alpha-u} D \frac{\rho_{\mathrm{EB}} x + \rho_{\mathrm{AB}}\rho_{\mathrm{EB}} + \rho_{\mathrm{AB}}}{(\rho_{\mathrm{EB}} x + \rho_{\mathrm{AB}})^2} e^{-\frac{x}{\rho_{\mathrm{AB}}}} dx. \tag{3.60}$$

where $D = (\beta(x-\alpha)+1/2)$. Then, the final result of the approximation for $\Psi(y)$ is

$$\Psi(y) \approx \frac{\beta\rho_{\mathrm{AB}} e^{\frac{1}{\rho_{\mathrm{EB}}}}}{\rho_{\mathrm{EB}}} \Big[\mathrm{Ei}\Big(-\frac{(\alpha+u)}{\rho_{\mathrm{AB}}} - \frac{1}{\rho_{\mathrm{EB}}} \Big) - \mathrm{Ei}\Big(-\frac{(\alpha-u)}{\rho_{\mathrm{AB}}} - \frac{1}{\rho_{\mathrm{EB}}} \Big) \Big]. \tag{3.61}$$

By setting $K = -\frac{(\alpha+u)}{\rho_{\mathrm{AB}}} - \frac{1}{\rho_{\mathrm{EB}}}$ and $W = -\frac{(\alpha-u)}{\rho_{\mathrm{AB}}} - \frac{1}{\rho_{\mathrm{EB}}}$ replacement, (3.61) can be simply rewritten as

$$\Psi(y) \approx \frac{\beta\rho_{\mathrm{AB}} e^{\frac{1}{\rho_{\mathrm{EB}}}}}{\rho_{\mathrm{EB}}} \Big[\mathrm{Ei}(K) - \mathrm{Ei}(W) \Big]. \tag{3.62}$$

With the approximation in (3.61), T_s is simplified to the following expression;

$$T_s \approx \frac{b}{n} \int_0^{\infty} \Psi(y) \frac{\phi\rho_{\mathrm{EE}} y + \phi\rho_{\mathrm{EE}}\rho_{\mathrm{AE}} + \rho_{\mathrm{AE}}}{(\phi\rho_{\mathrm{EE}} y + \rho_{\mathrm{AE}})^2} e^{-\frac{y}{\rho_{\mathrm{AE}}}} dy. \tag{3.63}$$

Although T_s has been significantly simplified, it is still a rather complicated expression. Next, we proceed with the numerical evaluations of the derived approximated formulas in the following section.

3.4 Numerical Results

Table 3.1 System Parameters

Notation	Description	Value
b	Information Message (bits)	100
v	Path Loss Coefficient	3
δ	Information Leakage Probability	10^{-4}

This section presents the numerical results to validate the theoretical analysis of average secrecy throughput for both half-duplex and full-duplex active eavesdropper settings. Firstly, we examine the findings that involve the comparison of HD and FD, and then HD and FD cases are separately investigated. Proposed approximations are evaluated in two different topologies, i.e., Scenario 1, shown in Fig. 3.1 and Fig. 3.2, where Alice, Bob and Eve are located in a triangular topology, and Scenario 2 shown in Fig. 3.3, where all the nodes are located on a straight line and Bob is between Alice and Eve. All the distances are expressed

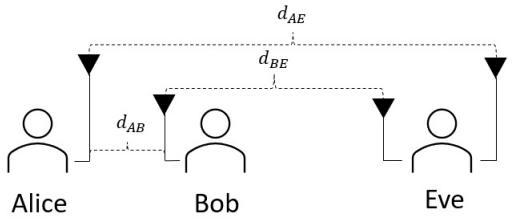

Fig. 3.3 Eavesdropper Location - Scenario 2

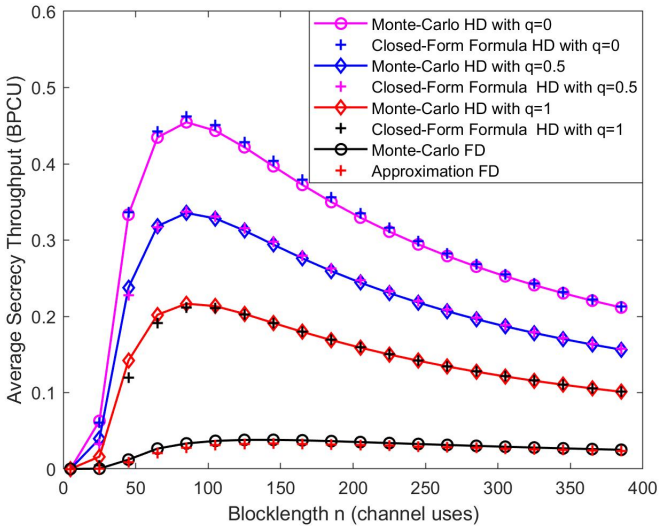

Fig. 3.4 Average Secrecy Throughput versus Blocklength with $P_{\mathrm{A}}, P_{\mathrm{E}} = 10$ dB

in meters. The numerical results were obtained by Monte Carlo simulations, involving 10^4 trials, and subsequently compared against the proposed theoretical formulas. Unless otherwise stated, we assume the parameters presented in Table 3.1 for the simulations. All the other parameters are introduced and reported for each specific simulation settings.

Fig. 3.4 presents the evaluation of average secrecy throughput approximations of (3.45) and (3.63) validated by MC simulations. It demonstrates the impact of HD and FD eavesdropper behaviours on the average secrecy throughput by plotting against different blocklengths for different eavesdropping probabilities of q. For this comparison, we assume that all nodes are in equal distance, which is 1 meter, except d_{EE}, which is 10 cm. To demonstrate how listening, jamming and FD affect the system performance, we first set the eavesdropping probability q to 1 in HD case, which means eavesdropper only listens to Alice's transmission to Bob. Conversely, when q is 0, Eve only jams the communication link while operating in HD mode. Naturally, $q = 0.5$ corresponds to half of the time listening and half of the time jamming. First of all, we can see that our proposed analytical approximations accurately

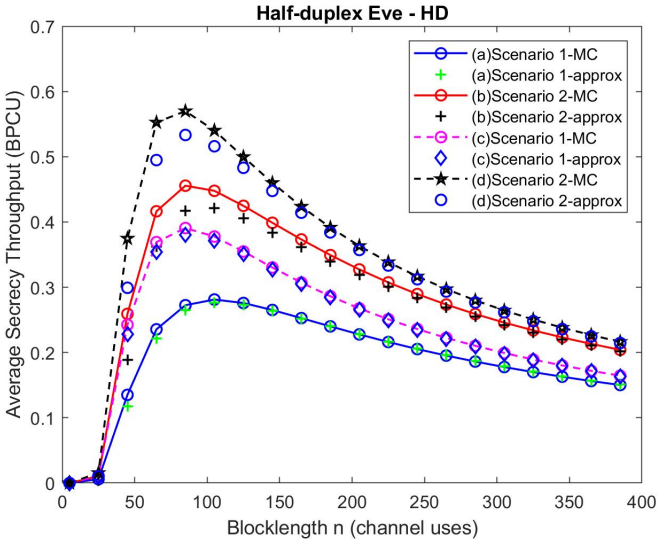

Fig. 3.5 Average Secrecy Throughput versus Blocklength for HD Eve. System parameters: $q = 0.5$, (a) $d_{\mathrm{AB}} = d_{\mathrm{AE}} = d_{\mathrm{EB}} = 2$ m, $P_{\mathrm{A}} = P_{\mathrm{E}} = 15$ dB (b) $d_{\mathrm{AB}} = d_{\mathrm{EB}} = 2$ m, $d_{\mathrm{AE}} = 4$ m, $P_{\mathrm{A}} = P_{\mathrm{E}} = 15$ dB (c) $d_{\mathrm{AB}} = d_{\mathrm{AE}} = d_{\mathrm{EB}} = 2$ m, $P_{\mathrm{A}} = 15$ dB, $P_{\mathrm{E}} = 10$ dB (d) $d_{\mathrm{AB}} = d_{\mathrm{EB}} = 2$ m, $d_{\mathrm{AE}} = 4$ m, $P_{\mathrm{A}} = 15$ dB, $P_{\mathrm{E}} = 10$ dB.

match the performance obtained by MC simulations for both HD and FD cases. Further from this evaluation, it appears that a FD Eve causes greater secrecy throughput degradation than a HD Eve. This happens as FD mode allows Eve to do simultaneously both actions. In other words, performing jamming and listening simultaneously is more beneficial for Eve in her attempt to degrade the average secrecy throughput. Moreover, we can observe that if Eve chooses to monitor the main channel rather than jam it during HD mode, reduction in the average secrecy throughput is greater.

3.4.1 Half-duplex

Fig. 3.5 illustrates the impact of distance between Alice, Bob and Eve for the two examined scenarios for selected power levels of Alice and Eve on average secrecy throughput, when Eve operates in HD mode with $q = 0.5$. For Scenario 1, all nodes are assumed to be in equal distance, whereas in Scenario 2, Bob is assumed to be located in the middle of the distance between Alice and Eve. The evaluation of the approximated secrecy throughput formulas are validated again through MC simulations. Based on the results, we state that our proposed approximation matches closely to the MC evaluation for the triangular topology, a.k.a Scenario 1 given the system parameters. The reason is that the impact of the distance between the parties is a more powerful parameter in Scenario 2, which affects the good

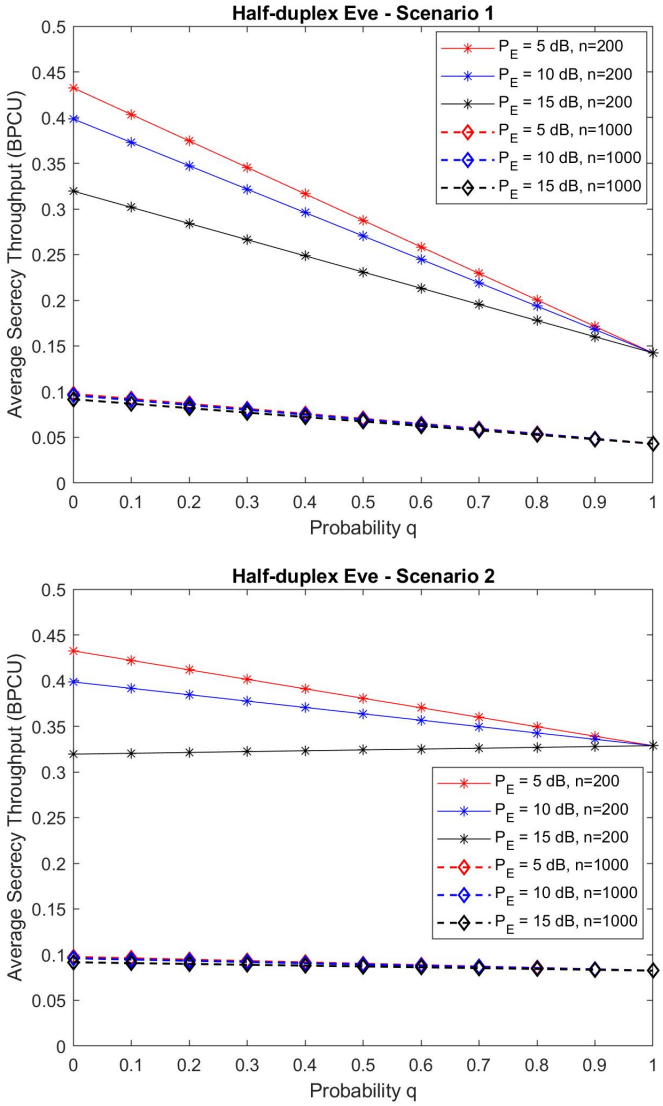

Fig. 3.6 Average Secrecy Throughput versus Probability q. System parameters: $d_{\mathrm{AB}} = d_{\mathrm{AE}} = d_{\mathrm{EB}} = 2$ m in Scenario 1, $d_{\mathrm{AB}} = d_{\mathrm{EB}} = 2, d_{\mathrm{AE}} = 4$ m in Scenario 2, $P_{\mathrm{A}} = 10$ dB

fit of our approximation especially on the top values. It appears that Scenario 2 is more advantageous for Alice, which results in higher throughput, whereas Eve operates better to minimize the overall throughput in Scenario 1. Moreover, it is clear that regardless of the topologies, the total average throughput is high on the condition that Eve is weaker than Alice.

Fig. 3.6 explores the impact of the eavesdropping probability q for HD Eve on the average secrecy throughput under the consideration of two topology scenarios. We assume that all the parties are 2 meters away from each other in Scenario 1. From Fig. 3.6, we observe that transmitting a message of $b = 100$ bits with a blocklength $n = 200$ and transmit power of 15 dB works better rather than using a larger blocklength. From this evaluation, it can be concluded that short message size transmission requires an optimal amount of blocklength to obtain the highest level of secrecy throughput given the parameters. This also explains the bell shape in the previous figures, while plotting secrecy throughput versus blocklength. Irrespective of the scenario, having a larger jamming power than the transmit power is favourable to Eve for short packet lengths. However, jamming the main channel all the time, i.e. $q = 0$, does not help Eve to degrade the average secrecy throughput. According to Fig. 3.6, passive mode is more advantageous for the adversary. We also analyzed Scenario 2, in which Bob is equally spaced between Alice and Eve. Due to the change of the location, Eve cannot perform better than Scenario 1, if she only listens. Interestingly, according to Scenario 2 results, Eve has a chance to degrade the average secrecy throughput very slightly while fully jamming on condition that she is stronger ($P_{\mathrm{E}} = 10$ dB) than Alice and the blocklength is short ($n = 200$). In addition, in both scenarios, if blocklength gets larger, e.g. $n = 1000$, not only average secrecy throughput decreases, changes on the jamming power is negligible to achieve a higher secrecy throughput. We can state that the approximations of average secrecy throughput in short packet transmission do not capture the impact for larger blocklengths, which is not a case of interest in this chapter as we focus on SPC.

3.4.2 Full-duplex

Fig. 3.7 shows the average secrecy throughput results with respect to different transmit and jamming power levels for different blocklengths. We first consider the setting in Scenario 1. It is assumed that all nodes are very close to each other and the distance between them is 1 meter. The distance between the antennas of the eavesdropper is assumed to be 5 cm. By observing the figure, we can see that, the proposed mathematical evaluation matches with the performance derived by MC simulations. For example, (b) in Fig. 3.7 shows the results for equal transmit and jamming powers of both Alice and Eve. If we assume Alice's transmit power is higher than Eve's jamming power, average secrecy throughput

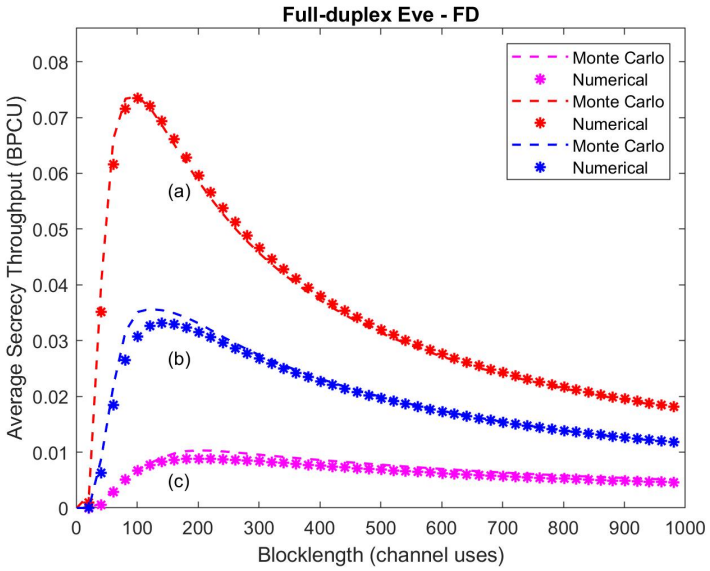

Fig. 3.7 Average Achievable Secrecy Throughput versus Blocklength in Scenario 1. System parameters are: (a) $P_{\mathrm{A}} = 15$ dB, $P_{\mathrm{E}} = 7$ dB, (b) $P_{\mathrm{A}} = P_{\mathrm{E}} = 10$ dB (c) $P_{\mathrm{A}} = 7$ dB, $P_{\mathrm{E}} = 15$ dB. $d_{\mathrm{AB}} = d_{\mathrm{AE}} = d_{\mathrm{EB}} = 1$ meter.

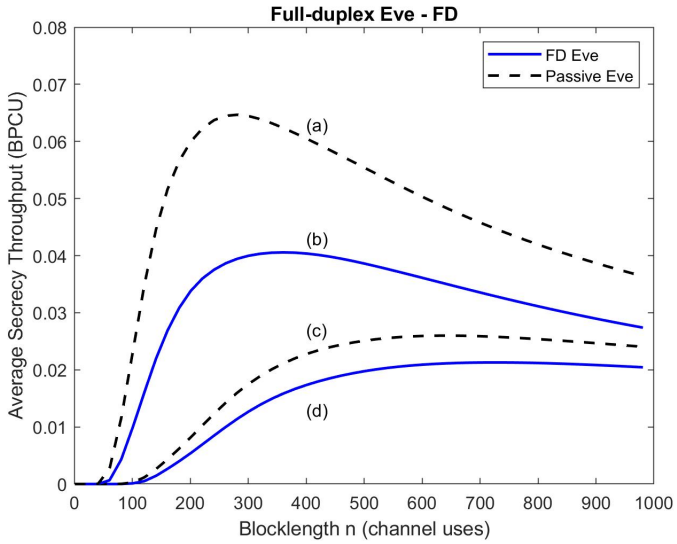

Fig. 3.8 Average Achievable Secrecy Throughput versus Blocklength in Scenario 1. System parameters are: (a) $P_{\mathrm{A}} = 15$ dB, (b) $P_{\mathrm{A}} = P_{\mathrm{E}} = 15$ dB, (c) $P_{\mathrm{A}} = 10$ dB, (d) $P_{\mathrm{A}} = P_{\mathrm{E}} = 10$ dB. $d_{\mathrm{AB}} = d_{\mathrm{AE}} = d_{\mathrm{EB}} = 4$ meters.

significantly increases. Conversely, for a weaker Alice, secrecy throughput tends to be lower. In addition, for the given information bits, when the blocklength value gets larger, average secrecy throughput begins to decrease.

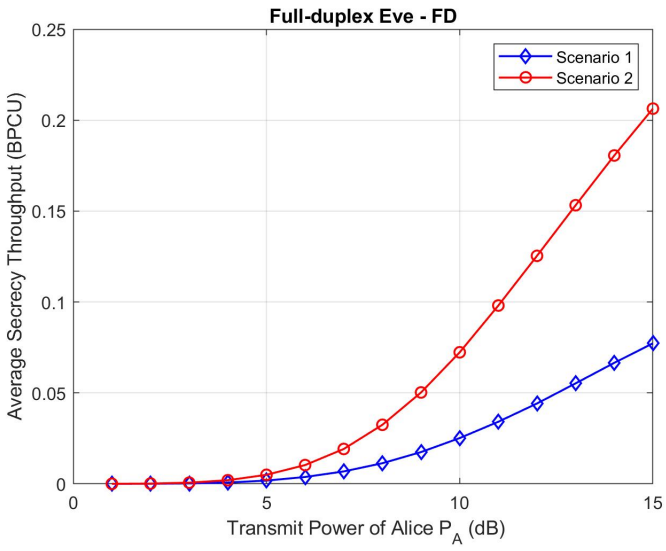

Fig. 3.9 Average Achievable Secrecy Throughput versus Transmit Power of Alice. System parameters are: $P_{\mathrm{E}} = 10$ dB, $b = 100$, $n = 200$, Scenario 1: $d_{\mathrm{AB}} = d_{\mathrm{AE}} = d_{\mathrm{EB}} = 3$m. Scenario 2: $d_{\mathrm{AB}} = d_{\mathrm{EB}} = 3$ m, $d_{\mathrm{AE}} = 6$ m.

Fig. 3.8 compares the achievable secrecy throughput of FD active and passive eavesdropping in the finite blocklength regime. The aim of this comparison is to explore whether a FD Eve affects the secrecy throughput more than a passive eavesdropper. In this evaluation, the distances between the nodes are assumed to be equal and 4 meters each, while the antennas of the eavesdroppers are 5 cm apart. Two Alice's transmit power levels are examined, 10 dB and 15 dB, and plotted against the modes of Eve. Eve is actively jamming the system, and her jamming power is assumed to be the same as Alice's transmit power. From the evaluation, it is clear that despite the power level differences of Eve, active eavesdropping causes a decrease in the average secrecy throughput of the system compared to that achieved when a passive eavesdropper is present. By comparing Fig. 3.7 and Fig. 3.8 we can get further insights in terms of the impact of distance on the secrecy throughput. While the setting (b) in Fig. 3.7 assumes distances of 1 meter, the setting (d) in Fig. 3.8 considers the same systems parameters apart from the longer distances (4 meters). From this, we conclude that when nodes are further away from each other, the average secrecy throughput decreases. In addition, longer distances require larger blocklength in order to have a non-negative average secrecy throughput.

Fig. 3.9 shows the numerical evaluations that shed light on how the transmitter power impacts on average secrecy throughput for both Scenario 1 and Scenario 2, while Eve operates in FD. For this evaluation, we assume $b = 100$ information bits are transmitted with $n = 200$ channel uses. When Alice's transmitter power is almost half of the Eve's jamming power,

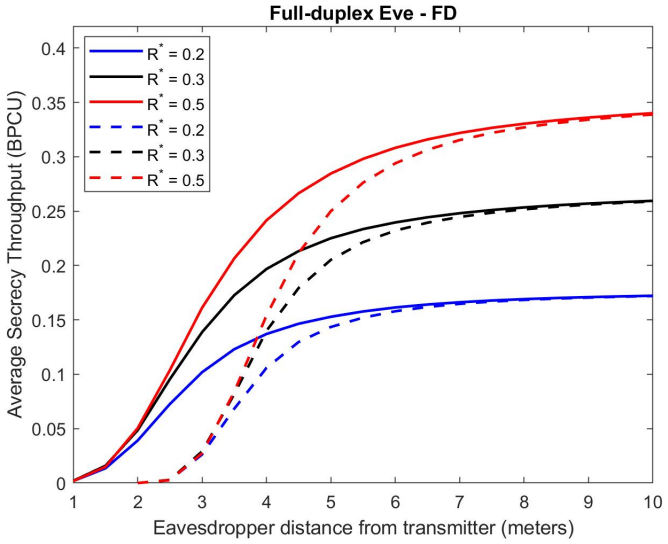

Fig. 3.10 Average Achievable Secrecy Throughput versus Eavesdropper Distance. Straight lines for Scenario 1, whereas dashed lines for Scenario 2. $d_{AB} = 2$ m.

average secrecy throughput becomes larger than zero and monotonically increases in both of the scenarios. When Alice's power is greater than Eve's, Alice has an opportunity to almost double throughput. Therefore, the best topology for Eve is the triangular one, when Alice is much stronger than Eve.

In Fig. 3.10, we investigate the average secrecy throughput with respect to eavesdropper distance from the transmitter for various values of rate ($R^* = b/n$). For this comparison, we fixed the distance between Alice and Bob at 2 meters while the distance of Eve's antennas is 10 cm. We allow only Eve to move. We set the transmit and jamming powers to 10 dB each for Alice and Eve. By observing the figure, we conclude that the higher rate results in higher average secrecy throughput. Further, we note that for Scenario 1 (straight lines), when Eve is closer to Alice and Bob, the average secrecy throughput is very low, close to zero for small distances. When Eve moves equally further away from both of Alice and Bob, average secrecy throughput increases. Similarly, for Scenario 2 (dashed lines), when Eve is located next to Bob, the average secrecy throughput is zero. It gradually increases, when Eve moves away from Bob and eventually, Eve's impact becomes negligible.

Finally, the impact of self-interference on the average secrecy rate is investigated in Fig. 3.11. For Scenario 1, all nodes are located at equal distances (3 m). Similar to the previous comparisons, it is assumed that d_{AB} and d_{EB} distances are equal (3 m) and Bob is located in the middle between Alice and Eve. In this setting, Eve is placed further away from Alice (6 m). Eve's antennas are located in 10 cm apart. For the case of perfectly cancelled self-interference ($\phi = 0$), the average secrecy throughput is at its lowest for both scenarios.

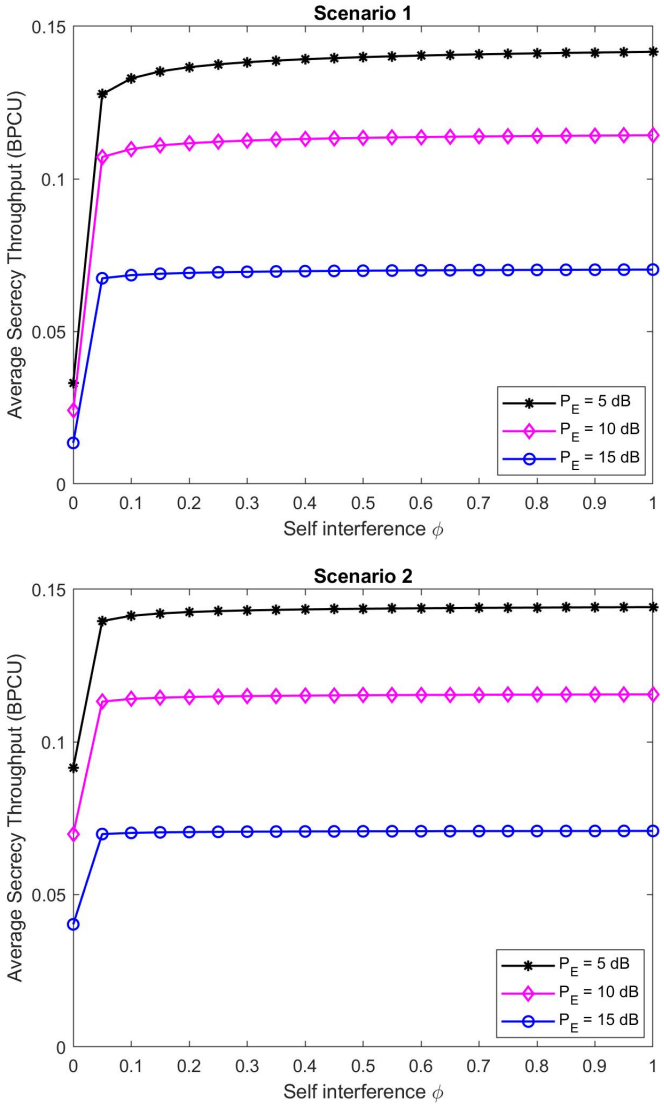

Fig. 3.11 Average Achievable Secrecy Throughput versus Self Interference Ratio. Systems parameters are: $n = 200$, for Scenario 1 - $d_{AB} = d_{AE} = d_{EB} = 3$, for Scenario 2 - $d_{AB} = 3, d_{AE} = 6, d_{EB} = 3$.

This happens as eavesdropper can operate at its best to disrupt the communication of the legitimate parties. Up to a certain level of self-interference ($\phi < 0.1$), value of the average secrecy throughput changes. On the other hand, when the self-interference parameter is higher than 0.1, jamming becomes more disadvantageous for eavesdropper itself. Therefore, average secrecy throughput seems to have a stable value. Even though jamming power rises, the throughput gets lower and the value of the throughput does not change significantly after exceeding the self-interference threshold. With the given system parameters, the throughput only reaches to a maximum point, where the self-interference of an adversary cannot be cancelled ($\phi = 1$). Another interesting conclusion from this comparison is that when the self-interference can be fairly cancelled, Scenario 2 seems to give higher average secrecy throughput, although Eve is further away from Alice. This also means that Eve loses its control over monitoring Alice's transmission to Bob. Overall, we can conclude that Scenario 2 works better when the self-interference coefficient is very low.

3.5 Summary

This chapter analyzes the performance of an active eavesdropper scenario in the context of SPC. We propose a novel approximation for the average secrecy throughput for a Rayleigh fading wiretap channel with an active eavesdropper either in half duplex or full duplex mode, while transmitting short packets. The average secrecy throughput is investigated by observing different parameters, such as eavesdropper distance from the legitimate nodes, the transmission rate, jamming power level, and the eavesdropper's passive and half-duplex and full-duplex active modes. The proposed approximations are also tested over two network topologies. The Monte Carlo simulations verify that the proposed theoretical approximation findings are very close to the simulated performance in both half-duplex and full-duplex cases. Overall, a full-duplex Eve is more capable to deteriorate average secrecy throughput than a half-duplex Eve. Naturally, it appears that an active eavesdropper affects more the secrecy throughput compared to passive adversary case. Although the secrecy throughput improves with higher transmission rates, our findings show that there is certain blocklength to transmit a short message whether an eavesdropper attack happens in a half or a full-duplex nature. Further, when the blocklength n gets very large, it results to a decrease in the throughput. Moreover, the comparison reveals that the distance and location of the eavesdropper on the topology play an important role on the achieved secrecy throughput as well as the jamming power level of the eavesdropper. We finally investigate whether to actively jamming or passive affects the overall system performance. For the evaluation, it appears that choosing jamming mode all the time is not always useful to Eve.

In the following chapter, we tackle a different problem that allows us to grasp the performance analysis of large-scale networks. More specifically, wiretap channel scenario with the multiple and passive eavesdroppers is investigated in detail.

Chapter 4

Secrecy Analysis of Multiple Eavesdroppers

Differently from the previous analysis, this chapter only focuses on the passive eavesdropper perspective. This section presents the work studying single and multiple antenna transmitters in the wiretap channels under the presence of multiple passive eavesdroppers and the performance of SPC is investigated. This chapter builds upon the numerical evaluation of average secrecy throughput obtained in Chapter 3. We start our investigation by examining the fading wiretap channel, where the communication is overheard by multiple non-colluding single-antenna eavesdroppers. We then extend our analysis for the case of a multiple-antenna transmitter and consider artificial noise to confuse the eavesdroppers.

4.1 Background Information

4.1.1 Motivation and Contributions

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 SPC. In real-world wiretap scenarios, it is common to encounter multiple unintended users attempting to extract information from a communication channel. These eavesdroppers may choose to remain passive and hidden, making it challenging to detect their presence. As a result, it is essential to consider the possibility of multiple adversaries in wiretap channels to minimize information loss and maintain the security of the communication. In addition, to the best of our knowledge, the security of wiretap channels against multiple adversaries in the context of secrecy throughput for SPC has not been studied previously. In this work, we focus on secure SPC 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. This chapter examines the average secrecy throughput of secure SPC between legitimate parties when multiple, passive, and single-antenna eavesdroppers exist. This research aims to address the design of SPC 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 [50], where we analyzed the performance of the system for a transmitter with a single antenna scenario. In this study, we extend those findings to the case of a multiple-antenna transmitter and carry out an optimal blocklength evaluation.

The main contributions of this research 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.

4.2 System Model and Problem Description

In this section, we will implement the average secrecy throughput derivation steps, which are already explained thoroughly in the previous section, for single and multiple-antenna transmitter scenarios, respectively. 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. Under the considered wiretap channel scenario setting, the secrecy capacity definition is different due to the existence of multiple adversaries, hence, computed as

$$C_{\mathrm{s}} = \begin{cases} C_{\mathrm{B}} - C_{\mathrm{E}}, & \text{when} \quad \gamma_{\mathrm{B}} > \gamma_{\mathrm{E}}, \\ 0, & \text{when} \quad \gamma_{\mathrm{B}} \leq \gamma_{\mathrm{E}}, \end{cases} \tag{4.1}$$

where the capacity of the main channel is

$$C_{\mathrm{B}} = \log_2(1+\gamma_{\mathrm{B}}), \tag{4.2}$$

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

$$\begin{aligned} C_{\mathrm{E}} &= \log_2(1+\max_k \gamma_{\mathrm{E}_k}) \\ &= \log_2(1+\gamma_{\mathrm{E}}). \end{aligned} \tag{4.3}$$

The received SNR of the eavesdropper equals to the highest amongst all the eavesdroppers and is defined as $\gamma_{\mathrm{E}} = \max_k \gamma_{\mathrm{E}_k}$. In addition, the dispersion of the main and eavesdropper channels becomes as $V_{\gamma_{\mathrm{B}}} = 1-(1+\gamma_{\mathrm{B}})^{-2}$ and $V_{\gamma_{\mathrm{E}}} = 1-(1+\max_k \gamma_{\mathrm{E}_k})^{-2}$, respectively.

4.2.1 System Analysis

4.2.2 Single Antenna Alice

The considered setting is shown in Fig. 4.1, 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

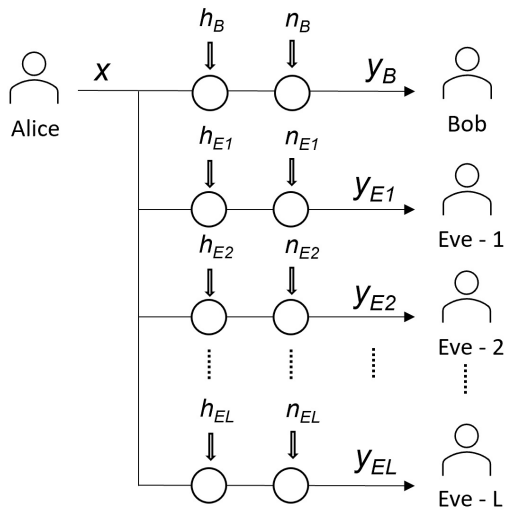

Fig. 4.1 Wiretap channel model

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

$$y_{\mathrm{B}}(i) = h_{\mathrm{B}}(i)x(i) + n_{\mathrm{B}}(i), \tag{4.4}$$

where $h_{\mathrm{B}}(i)$ is Bob's channel fading coefficient at time i and $n_{\mathrm{B}}(i)$ is the Additive White Gaussian Noise (AWGN) experienced during transmission with $n_{\mathrm{B}} \sim \mathcal{N}(0, \sigma_{\mathrm{B}}^2)$, which has zero mean and variance σ_{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

$$y_{\mathrm{E}_k}(i) = h_{\mathrm{E}_k}(i)x(i) + n_{\mathrm{E}_k}(i), \quad k = 1, 2, .., L, \tag{4.5}$$

where $h_{\mathrm{E}_k}(i)$ denotes the fading coefficient at time i of the kth eavesdropper. The transmission is corrupted by AWGN noise of $n_{\mathrm{E}_k}(i) \sim \mathcal{N}(0, \sigma_{\mathrm{E}_k}^2)$ with zero mean and variance $\sigma_{\mathrm{E}_k}^2$. 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 PLS literature, even if the eavesdropper is passive [19], [22], [43]. The instantaneously received signal-to-noise ratio (SNR) at Bob

and kth Eve can be formulated as

$$\gamma_{\mathrm{B}} = \frac{|h_{\mathrm{B}}|^2 P}{\sigma_{\mathrm{B}}^2}, \tag{4.6}$$

and

$$\gamma_{\mathrm{E}_k} = \frac{|h_{\mathrm{E}_k}|^2 P}{\sigma_{\mathrm{E}_k}^2}, \tag{4.7}$$

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

$$\overline{\gamma}_{\mathrm{B}} = \frac{\mathbb{E}\{|h_{\mathrm{B}}|^2\} P}{\sigma_{\mathrm{B}}^2}, \tag{4.8}$$

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

$$\overline{\gamma}_{\mathrm{E}} = \frac{\mathbb{E}\{|h_{\mathrm{E}}|^2\} P}{\sigma_{\mathrm{E}_k}^2}. \tag{4.9}$$

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 [55], is given by

$$f(\gamma_{\mathrm{B}}) = \frac{1}{\overline{\gamma}_{\mathrm{B}}} e^{-\frac{\gamma_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}}}. \tag{4.10}$$

Differently from the setting in [44], 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 [55], the probability distribution function of the adversarial channels becomes

$$f(\gamma_{\mathrm{E}}) = L\Big(1 - e^{-\frac{\gamma_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}}\Big)^{L-1} \frac{1}{\overline{\gamma}_{\mathrm{E}}} e^{-\frac{\gamma_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}}. \tag{4.11}$$

The average secrecy throughput evaluation for single antenna Alice is done as follows. In order to calculate the closed-form approximation for the average secrecy throughput in (3.9), (3.10) and (3.11) are formulated separately. First, we compute the expression below according to (3.11)

$$S(\gamma_{\mathrm{E}}) = \int_0^{\infty} (1 - \varepsilon_{\gamma_{\mathrm{B}}|\gamma_{\mathrm{E}}}(x)) \frac{1}{\overline{\gamma}_{\mathrm{B}}} e^{-\frac{\gamma_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}}} d\gamma_{\mathrm{B}}, \tag{4.12}$$

where $f(\gamma_{\mathrm{B}})$ is defined as in (4.10). Then, the integral can be written for given values of $\gamma_{\mathrm{B}} = x$ and $\gamma_{\mathrm{E}} = y$ as

$$S(y) = \int_0^{\infty} (1 - \varepsilon_{\gamma_{\mathrm{B}}|\gamma_{\mathrm{E}}}(x)) \frac{1}{\overline{\gamma}_{\mathrm{B}}} e^{-\frac{x}{\overline{\gamma}_{\mathrm{B}}}} dx, \tag{4.13}$$

which can be rewritten as

$$S(y) = 1 - \int_0^{\infty} \varepsilon(x) \frac{1}{\overline{\gamma}_{\mathrm{B}}} e^{-\frac{x}{\overline{\gamma}_{\mathrm{B}}}} dx. \tag{4.14}$$

Replacing (3.12) into (4.14) yields

$$S(\gamma_{\mathrm{E}}) = 1 - \Big(\underbrace{\int_0^{\alpha+u} \frac{1}{\overline{\gamma}_{\mathrm{B}}} e^{-\frac{x}{\overline{\gamma}_{\mathrm{B}}}} dx}_{\mathrm{D}} + \underbrace{\int_{\alpha+u}^{\alpha-u} (\beta(x-\alpha)+1/2) \frac{1}{\overline{\gamma}_{\mathrm{B}}} e^{-\frac{x}{\overline{\gamma}_{\mathrm{B}}}} dx}_{\mathrm{G}} \Big). \tag{4.15}$$

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

$$D = 1 - e^{-\frac{\alpha+u}{\overline{\gamma}_{\mathrm{B}}}}, \tag{4.16}$$

and the second integral is given by

$$G = \beta(\alpha+u+\overline{\gamma}_{\mathrm{B}}) e^{-\frac{\alpha+u}{\overline{\gamma}_{\mathrm{B}}}} - \beta(\alpha-u+\overline{\gamma}_{\mathrm{B}}) e^{-\frac{\alpha-u}{\overline{\gamma}_{\mathrm{B}}}} + \Big(\frac{1}{2} - \beta\alpha\Big)\Big(e^{-\frac{\alpha+u}{\overline{\gamma}_{\mathrm{B}}}} - e^{-\frac{\alpha-u}{\overline{\gamma}_{\mathrm{B}}}}\Big). \tag{4.17}$$

Thus, by inserting (4.16) and (4.17) into (4.15), the following is obtained

$$S(\gamma_{\mathrm{E}}) = \overline{\gamma}_{\mathrm{B}} \beta \Big(e^{-\frac{\alpha-u}{\overline{\gamma}_{\mathrm{B}}}} - e^{-\frac{\alpha+u}{\overline{\gamma}_{\mathrm{B}}}}\Big), \tag{4.18}$$

and, hence, it is rearranged as

$$S(\gamma_{\mathrm{E}}) = \overline{\gamma}_{\mathrm{B}} \beta e^{-\frac{\alpha}{\overline{\gamma}_{\mathrm{B}}}} \Big(e^{\frac{u}{\overline{\gamma}_{\mathrm{B}}}} - e^{-\frac{u}{\overline{\gamma}_{\mathrm{B}}}}\Big). \tag{4.19}$$

Also, by following [44], for large values of $\overline{\gamma}_{\mathrm{B}}$, (4.19) can be further simplified as

$$S(\gamma_{\mathrm{E}}) \approx e^{-\frac{\alpha}{\overline{\gamma}_{\mathrm{B}}}}. \tag{4.20}$$

Now, by replacing (4.20) into (3.10), we get

$$\begin{aligned} T_{\mathrm{s}} &\approx \frac{b}{n} \int_0^{\infty} e^{-\frac{\alpha}{\overline{\gamma}_{\mathrm{B}}}} L(1 - e^{-\frac{\gamma_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}})^{L-1} \frac{1}{\overline{\gamma}_{\mathrm{E}}} e^{-\frac{\gamma_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}} d\gamma_E \Longrightarrow \\ T_{\mathrm{s}} &\approx \frac{bL}{n\overline{\gamma}_{\mathrm{E}}} \int_0^{\infty} e^{-\frac{\alpha}{\overline{\gamma}_{\mathrm{B}}}} e^{-\frac{\gamma_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}} (1 - e^{-\frac{\gamma_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}})^{L-1} d\gamma_{\mathrm{E}}. \end{aligned} \tag{4.21}$$

Thus, we find

$$\begin{aligned} T_{\mathrm{s}} &\approx \frac{bL}{n\overline{\gamma}_{\mathrm{E}}} \int_0^{\infty} e^{-\frac{r(1+\gamma_{\mathrm{E}})-1}{\overline{\gamma}_{\mathrm{B}}}} e^{-\frac{\gamma_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}} (1-e^{-\frac{\gamma_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}})^{L-1} d\gamma_{\mathrm{E}} \Longrightarrow \\ T_{\mathrm{s}} &\approx \frac{bL}{n\overline{\gamma}_{\mathrm{E}}} e^{\frac{1-r}{\overline{\gamma}_{\mathrm{B}}}} \int_0^{\infty} e^{-(\frac{\overline{\gamma}_{\mathrm{E}} r-\overline{\gamma}_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}\overline{\gamma}_{\mathrm{E}}})\gamma_{\mathrm{E}}} (1-e^{-\frac{\gamma_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}})^{L-1} d\gamma_{\mathrm{E}}. \end{aligned} \tag{4.22}$$

by using the following based on [56, Eq. 3.312.1]

$$\int_0^{\infty} \left(1-e^{-\frac{x}{\beta}}\right)^{\nu-1} e^{-\mu x} dx = \beta \mathrm{B}(\beta\mu, \nu), \quad [\mathrm{Re} \quad \beta, \nu, \mu > 0], \tag{4.23}$$

where Re depicts the real part of the imaginary numbers and the beta function $\mathrm{B}(.,.)$ can be represented as follows [56, Eq. 8.384.1]:

$$\mathrm{B}(x,y) = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)} \tag{4.24}$$

where $\Gamma(z) = \int_0^{\infty} t^{z-1} e^{-t} dt$ is the gamma function [56, Eq. 8.310.1]. Therefore, our simplified expression for the average secrecy throughput is given by:

$$T_{\mathrm{s}} \approx \frac{bL}{n} e^{\frac{1-r}{\overline{\gamma}_{\mathrm{B}}}} \mathrm{B}(z, L), \tag{4.25}$$

with $z = \frac{\overline{\gamma}_{\mathrm{E}} r + \overline{\gamma}_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}}$. For the case of single antenna Alice and single antenna single Eve, we set $L = 1$ to (4.25) and we can further simplify the average secrecy throughput as follows

$$T_{\mathrm{s1}} \approx \frac{b\overline{\gamma}_{\mathrm{B}} e^{\frac{1-r}{\overline{\gamma}_{\mathrm{B}}}}}{n(\overline{\gamma}_{\mathrm{E}} r + \overline{\gamma}_{\mathrm{B}})}. \tag{4.26}$$

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 (4.26) can be determined by solving*

$$\left(\frac{Q^{-1}(\delta)}{2\sqrt{n}} + \frac{b}{n}\log(2)\right)\left(r + \frac{\overline{\gamma}_E \overline{\gamma}_B r}{\overline{\gamma}_E r + \overline{\gamma}_B}\right) - \overline{\gamma}_B = 0, \tag{4.27}$$

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.

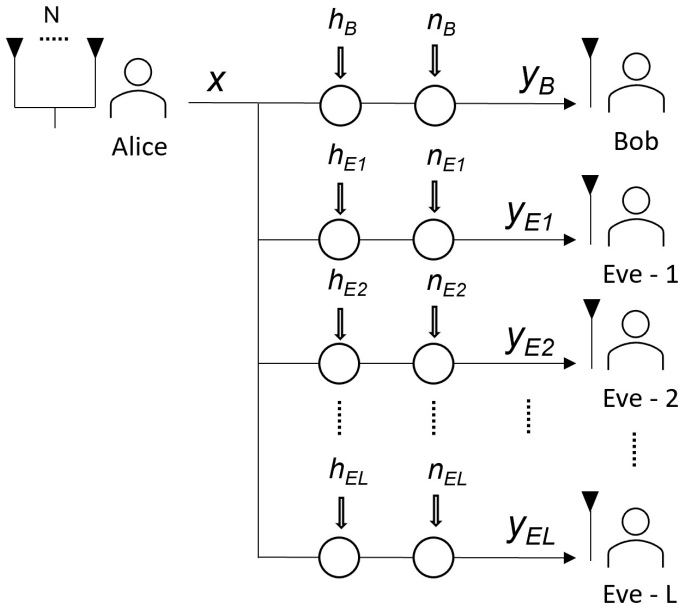

Fig. 4.2 Multi-antenna transmitter system model

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 (4.25) is obtained by finding a positive root of the following expression by setting it to zero.*

$$\frac{1}{n\overline{\gamma}_B}\Big(Mr\Big(1+\overline{\gamma}_E\big(\psi_0(z+L)-\psi_0(z)\big)\Big)-\overline{\gamma}_B\Big)=0, \tag{4.28}$$

where $\psi_0(.)$ is the digamma function [57, 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.

4.2.3 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. 4.2. 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 [23], [58], [59]. 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

$$\mathbf{x}=[\mathbf{w}_t \quad \mathbf{W}_a][x_t \quad \mathbf{x}_a]^T=\mathbf{w}_t x_t+\mathbf{W}_a\mathbf{x}_a. \tag{4.29}$$

The received signal at Bob

$$\begin{aligned} y_\mathrm{B}&=\mathbf{h}_\mathrm{B}\mathbf{x}+n_\mathrm{B}\\ y_\mathrm{B}&=\mathbf{h}_\mathrm{B}\mathbf{w}_t x_t+\mathbf{h}_\mathrm{B}\mathbf{W}_a\mathbf{x}_a+n_\mathrm{B}\\ y_\mathrm{B}&=\mathbf{h}_\mathrm{B}\mathbf{w}_t x_t+n_\mathrm{B}. \end{aligned} \tag{4.30}$$

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 (4.30) 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

$$\begin{aligned} y_{\mathrm{E}_k}&=\mathbf{h}_{\mathrm{E}_k}\mathbf{x}+n_{\mathrm{E}_k}\\ y_{\mathrm{E}_k}&=\mathbf{h}_{\mathrm{E}_k}\mathbf{w}_t x_t+\mathbf{h}_{\mathrm{E}_k}\mathbf{W}_a\mathbf{x}_a+n_{\mathrm{E}_k}, \quad k=1,2,..,L. \end{aligned} \tag{4.31}$$

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

$$\overline{\gamma}_{\mathrm{B}} = \frac{P}{{\sigma_{\mathrm{B}}}^2}, \tag{4.32}$$

and the instantaneous received SNR at Bob

$$\gamma_{\mathrm{B}} = \phi \overline{\gamma}_{\mathrm{B}} ||\mathbf{h}_{\mathrm{B}}||^2. \tag{4.33}$$

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

$$f_{\gamma_{\mathrm{B}}}(\gamma) = \frac{\gamma^{N-1} e^{-\frac{\gamma}{\phi \overline{\gamma}_{\mathrm{B}}}}}{(\phi \overline{\gamma}_{\mathrm{B}})^N \Gamma(N)}. \tag{4.34}$$

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

$$\begin{aligned} F_{\gamma_{\mathrm{B}}}(\gamma) &= 1 - \frac{\Gamma(N, \frac{\gamma}{\phi \overline{\gamma}_{\mathrm{B}}})}{\Gamma(N)}, \quad \text{or} \\ F_{\gamma_{\mathrm{B}}}(\gamma) &= 1 - e^{-\frac{\gamma}{\phi \overline{\gamma}_{\mathrm{B}}}} \sum_{k=0}^{N-1} \frac{1}{k!} \Big(\frac{\gamma}{\phi \overline{\gamma}_{\mathrm{B}}} \Big)^k. \end{aligned} \tag{4.35}$$

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

$$\overline{\gamma}_{\mathrm{E}_k} = \frac{P}{\sigma^2_{\mathrm{E}_k}}, \tag{4.36}$$

and the instantaneous received SINR at the kth Eve is

$$\begin{aligned} \gamma_{\mathrm{E}_k} &= \frac{\phi P ||\mathbf{h}_{\mathrm{E}_k} \mathbf{w}_t||^2}{\frac{1-\phi}{N-1} P ||\mathbf{h}_{\mathrm{E}_k} \mathbf{W}_a||^2 + \sigma^2_{\mathrm{E}_k}}, \quad \text{or} \\ \gamma_{\mathrm{E}_k} &= \frac{\phi \overline{\gamma}_{\mathrm{E}_k} ||\mathbf{h}_{\mathrm{E}_k} \mathbf{w}_t||^2}{\frac{1-\phi}{N-1} \overline{\gamma}_{\mathrm{E}_k} ||\mathbf{h}_{\mathrm{E}_k} \mathbf{W}_a||^2 + 1}. \end{aligned} \tag{4.37}$$

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

$$f_{\gamma_{\mathrm{E}}}(\gamma) = L\Big(1-\tau^{1-N}e^{-\frac{\gamma}{\phi\bar{\gamma}_{\mathrm{E}}}}\Big)^{L-1}e^{-\frac{\gamma}{\phi\bar{\gamma}_{\mathrm{E}}}}\left(\frac{\tau^{1-N}}{\phi\bar{\gamma}_{\mathrm{E}}}+\frac{(1-\phi)}{\phi\tau^{N}}\right), \tag{4.38}$$

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 (3.9). For simplicity, first, $S(\gamma_{\mathrm{E}})$ as in (3.11) is approximated, and then this result is used in (3.10). The following shows the steps of the approximation process for $S(\gamma_{\mathrm{E}})$

$$\begin{aligned} S(\gamma_{\mathrm{E}}) &= \int_0^{\infty}(1-\varepsilon_{\gamma_{\mathrm{B}}|\gamma_{\mathrm{E}}}(x))\frac{x^{N-1}e^{-\frac{x}{\phi\bar{\gamma}_{\mathrm{B}}}}}{(\phi\bar{\gamma}_{\mathrm{B}})^{N}\Gamma(N)}dx \\ &= 1-\int_0^{\infty}\varepsilon(x)\frac{x^{N-1}e^{-\frac{x}{\phi\bar{\gamma}_{\mathrm{B}}}}}{(\phi\bar{\gamma}_{\mathrm{B}})^{N}\Gamma(N)}dx. \end{aligned} \tag{4.39}$$

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

$$\begin{aligned} S(y) = 1-\Big(&\underbrace{\int_0^{\alpha+u}\frac{x^{N-1}e^{-\frac{x}{\phi\bar{\gamma}_{\mathrm{B}}}}}{(\phi\bar{\gamma}_{\mathrm{B}})^{N}\Gamma(N)}dx}_{\mathrm{S1}} \\ &+\underbrace{\int_{\alpha+u}^{\alpha-u}(\beta(x-\alpha)+1/2)\frac{x^{N-1}e^{-\frac{x}{\phi\bar{\gamma}_{\mathrm{B}}}}}{(\phi\bar{\gamma}_{\mathrm{B}})^{N}\Gamma(N)}dx}_{\mathrm{S2}}\Big). \end{aligned} \tag{4.40}$$

where β, α have been defined in (3.16), (3.13), respectively. The calculation of $S1$ is based on the following

$$S1 = \frac{1}{(\phi\bar{\gamma}_{\mathrm{B}})^{N}\Gamma(N)}\int_0^{\alpha+u}x^{N-1}e^{-\frac{x}{\phi\bar{\gamma}_{\mathrm{B}}}}dx, \tag{4.41}$$

and $S2$ is obtained as calculating the following expression

$$S2 = \frac{1}{(\phi\bar{\gamma}_{\mathrm{B}})^{N}\Gamma(N)}\int_{\alpha+u}^{\alpha-u}(\beta(x-\alpha)+1/2)x^{N-1}e^{-\frac{x}{\phi\bar{\gamma}_{\mathrm{B}}}}dx. \tag{4.42}$$

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

$$S(\gamma_{\mathrm{E}}) \approx (1-F_{\gamma_{\mathrm{B}}}(\alpha)), \tag{4.43}$$

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

$$F_{\gamma_{\mathrm{B}}}(\alpha) = 1 - e^{-\frac{\alpha}{\phi\overline{\gamma}_{\mathrm{B}}}} \sum_{k=0}^{N-1} \frac{1}{k!} \Big(\frac{\alpha}{\phi\overline{\gamma}_{\mathrm{B}}}\Big)^k. \tag{4.44}$$

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

$$\begin{aligned} S(\gamma_{\mathrm{E}}) \approx & 1 - \Big[1 - \frac{\Gamma(N, \frac{\alpha}{\phi\overline{\gamma}_{\mathrm{B}}})}{\Gamma(N)}\Big], \quad \text{or} \\ S(\gamma_{\mathrm{E}}) \approx & e^{-\frac{\alpha}{\phi\overline{\gamma}_{\mathrm{B}}}} \sum_{k=0}^{N-1} \frac{1}{k!} \Big(\frac{\alpha}{\phi\overline{\gamma}_{\mathrm{B}}}\Big)^k. \end{aligned} \tag{4.45}$$

The approximation in (4.43) also overlaps with the approximation given in [44]

$$S(\gamma_{\mathrm{E}}) \approx 1 + \beta \int_{\alpha+u}^{\alpha-u} F_{\gamma_{\mathrm{B}}}(x)dx, \tag{4.46}$$

Then T_s becomes

$$T_{\mathrm{s}} \approx \frac{b}{n} \int_0^{\infty} (1 - F_{\gamma_{\mathrm{B}}}(\alpha)) f(\gamma_{\mathrm{E}}) d(\gamma_{\mathrm{E}}). \tag{4.47}$$

It is hard to obtain a closed-form formula for (4.47) due to the complexity of the integral. However, we obtained a closed form approximation by transforming (4.38) into the following by setting $L = 2$

$$f_{\gamma_{\mathrm{E}}}(\gamma) = \Big(2e^{-\frac{\gamma}{\phi\overline{\gamma}_{\mathrm{E}}}} - 2e^{-\frac{2\gamma}{\phi\overline{\gamma}_{\mathrm{E}}}} \tau^{1-N}\Big) \left(\frac{\tau^{1-N}}{\phi\overline{\gamma}_{\mathrm{E}}} + \frac{(1-\phi)}{\phi\tau^N}\right), \tag{4.48}$$

Then, (4.47) is simplified with the help of (4.44) and (4.48)

$$\begin{aligned} T_{\mathrm{s}} \approx & \frac{2b}{n} \sum_{k=0}^{N-1} \frac{e^{\frac{1-r}{\phi\overline{\gamma}_{\mathrm{B}}}}}{k!} \sum_{j=0}^{k} \binom{k}{j} \Big(\frac{r-1}{\phi\overline{\gamma}_{\mathrm{B}}}\Big)^{k-j} \Big(\frac{r}{\phi\overline{\gamma}_{\mathrm{B}}}\Big)^k G^{-\lambda} \Gamma(\lambda) \times \\ & \Big[\frac{1}{\phi\overline{\gamma}_{\mathrm{E}_k}} (\psi(\lambda, \lambda+2-N, \Theta_1) - \psi(\lambda, \lambda+3-2N, \Theta_2)) + \\ & G(1-N)(\psi(\lambda, \lambda+2-2N, \Theta_2) - \psi(\lambda, \lambda+1-N, \Theta_1))\Big], \end{aligned} \tag{4.49}$$

for $\lambda = (k+1)$, $\Theta_1 = \frac{\frac{r}{\phi\overline{\gamma}_{\mathrm{B}}} + \frac{1}{\phi\overline{\gamma}_{\mathrm{E}_k}}}{G}$ and $\Theta_2 = \frac{\frac{r}{\phi\overline{\gamma}_{\mathrm{B}}} + \frac{2}{\phi\overline{\gamma}_{\mathrm{E}_k}}}{G}$ and $G = \frac{1-\phi}{\phi(N-1)}$.
We obtained simulation results of the formula in (4.49) for the special case of 2 antenna transmitter and 2 eavesdroppers. In the next section, both the general formula for T_{s} in (4.47)

and closed-form approximation (4.49) are numerically evaluated and presented with the other numerical results.

4.3 Numerical 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 4.1 for the simulations. The values of these parameters were derived from the studies in [44, 58, 59]. 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 4.1 System Parameters

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

4.3.1 Single Antenna Transmitter and Multiple Eavesdroppers

First, we investigate the accuracy of the approximation derived in (4.25) by comparing it with Monte Carlo simulation results.

In Fig. 4.3, we evaluate the average achieved secrecy throughput by Monte Carlo simulation and compare it with our closed-form approximation in (4.25) for various blocklength values n. In this comparison, we consider various numbers of eavesdroppers. By observing Fig. 4.3, 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 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. 4.4, 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

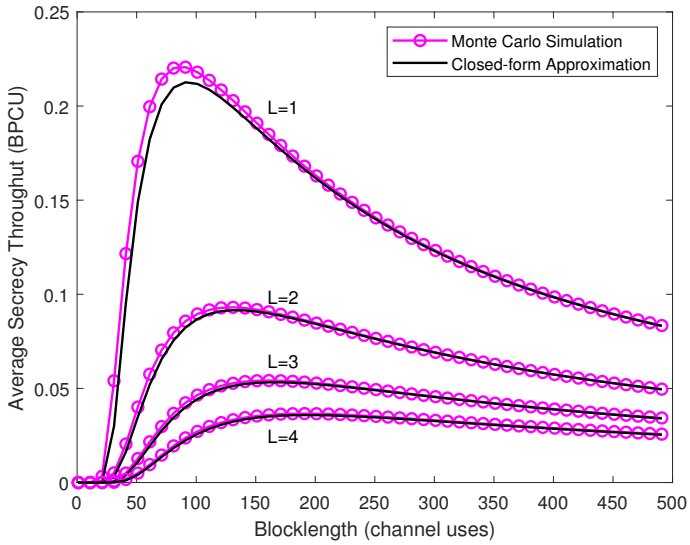

Fig. 4.3 Average Achievable Secrecy Throughput with respect to different Blocklength values for various numbers of eavesdroppers.

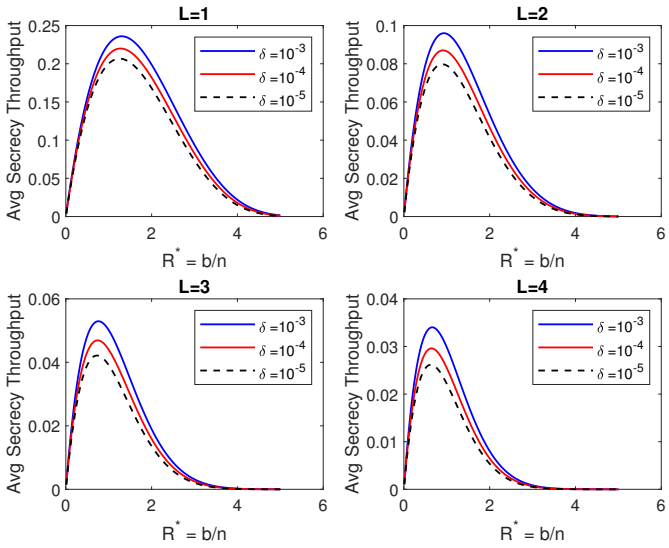

Fig. 4.4 Average Achievable Secrecy Throughput with respect to R^* = b/n for various numbers of eavesdroppers, L, and information leakage probabilities δ.

of information bits b takes values up to 500 bits. This evaluation confirms the trend we reported in Fig. 4.3, 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

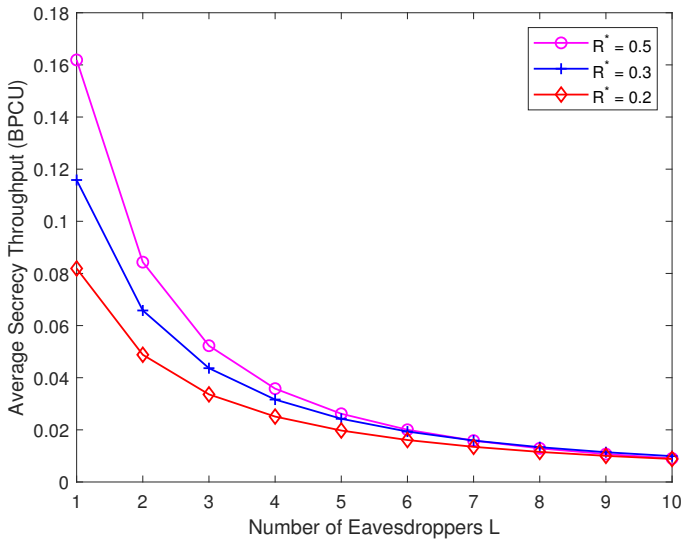

Fig. 4.5 Average Achievable Secrecy Throughput with respect Number of Eavesdroppers for various transmission rates R^*.

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. 4.5, 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, we observe that as the number of eavesdroppers increases, it causes a considerable loss in average secrecy throughput. The reason is that the presence of multiple eavesdroppers can lead to each eavesdropper channel being affected by different fading parameters. As a result, as the number of eavesdroppers increases, there is a higher possibility that one eavesdropper may have a stronger SNR than the others. This may cause a greater decline in the 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. 4.6, 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. 4.6 is that the average secrecy throughput for the examined information leakage probabilities

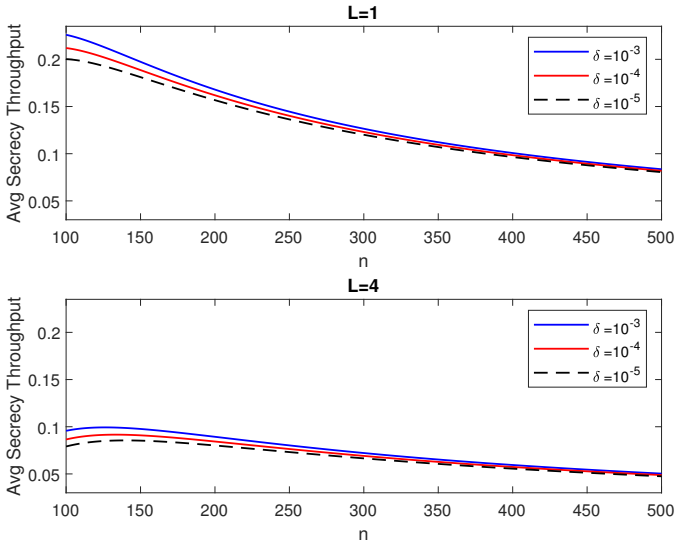

Fig. 4.6 Average Achievable Secrecy Throughput with respect to various Blocklength values for various number of eavesdroppers L and information leakage probabilities values δ.

(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. 4.7. 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. 4.7. By observing this figure, we can see that the optimal average secrecy throughput is lower when the transmitted messages are shorter.

Finally, Fig. 4.8 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 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

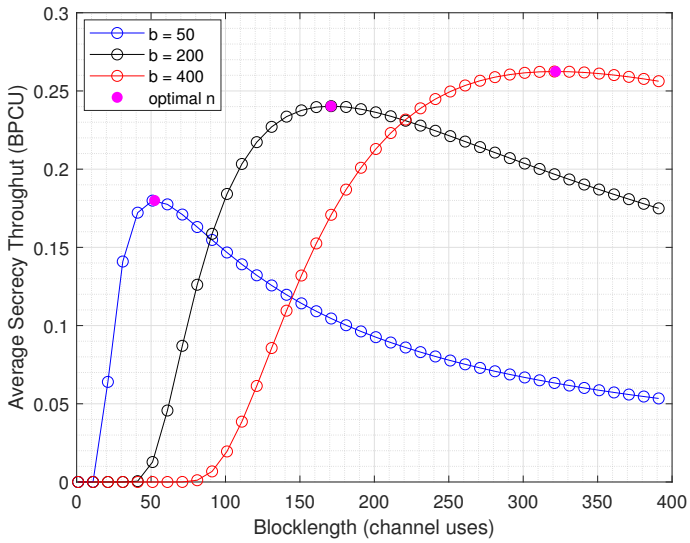

Fig. 4.7 Average Achievable Secrecy Throughput with respect to different Blocklength values and a single eavesdropper. Different number of information bits b are considered. The optimal value is calculated as described in Theorem 1.

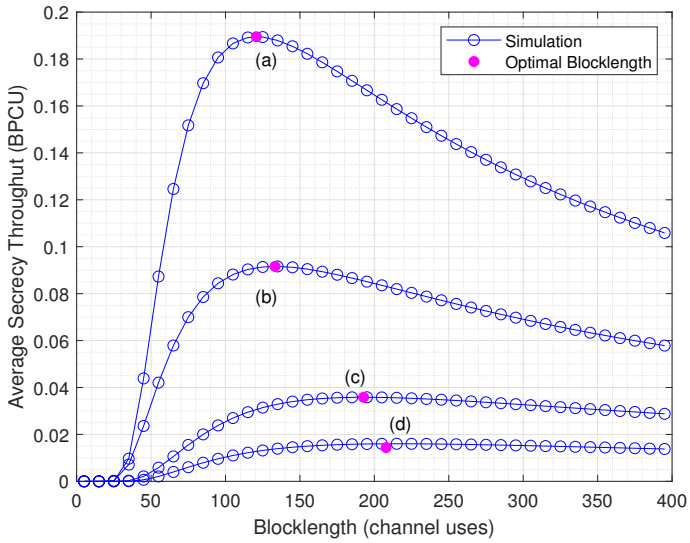

Fig. 4.8 Average Achievable Secrecy Throughput with respect to different Blocklength values for multiple eavesdroppers. The optimal value is calculated as described in Theorem 2. Settings: (a) $L = 4$, $\overline{\gamma}_{\mathrm{B}} = 10$ dB, $\overline{\gamma}_{\mathrm{E}} = 5$ dB, (b) $L = 2$, $\overline{\gamma}_{\mathrm{B}} = \overline{\gamma}_{\mathrm{E}} = 10$ 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.

eavesdropper, when several eavesdroppers exist, the average secrecy throughput is in the lowest level.

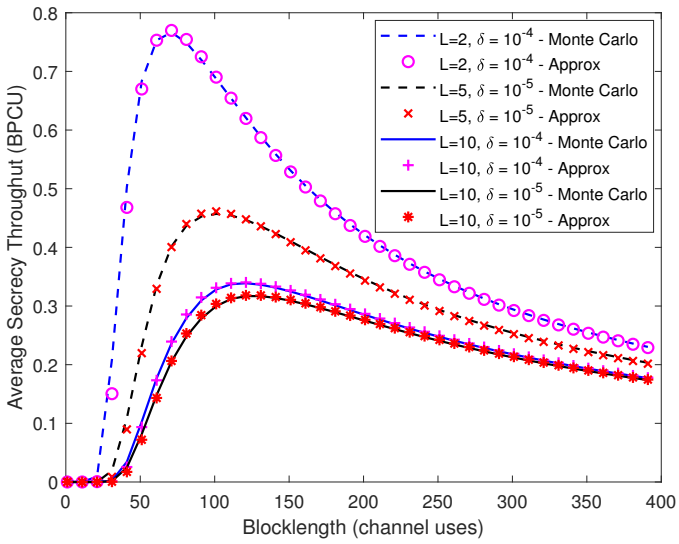

Fig. 4.9 Average Achievable Secrecy Throughput with respect to different Blocklength values for various number of eavesdroppers and the information leakage probability values.

4.3.2 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 (4.47) and (4.49), which quantify the average secrecy throughput when the transmitter has multiple antennas.

In Fig. 4.9, 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 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 (4.47).

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 4.49). The results are depicted in Fig. 4.10 where the evaluation of (4.49) is compared with the general expression presented in (4.47) 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

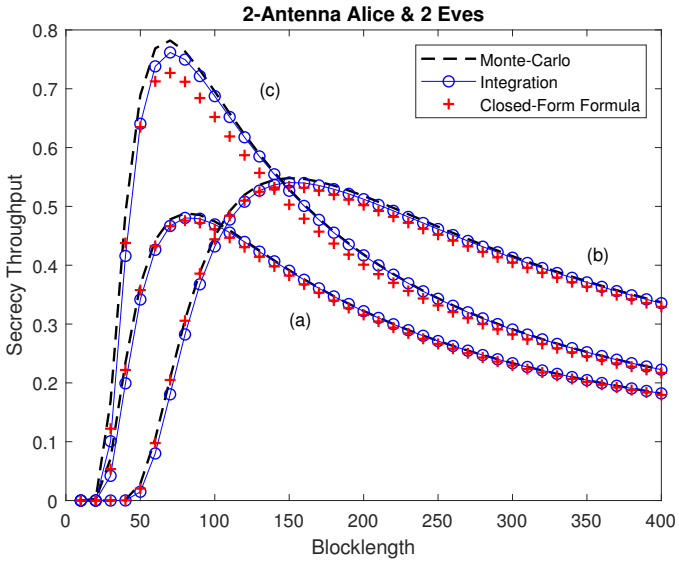

Fig. 4.10 Average Achievable Secrecy Throughput with respect to Blocklength. Settings: (a) b = 100 bits, (b) b = 200 bits, (c) $\overline{\gamma}_{\mathrm{E}} = 5$ dB.

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. 4.11 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. As the number of eavesdroppers increases, having more antennas leads to higher throughput for the same number of eavesdroppers. From this figure, we can also observe that the throughput almost halves if the transmission rate decreases by half ($R^* = b/n = 0.5$). Furthermore, we can observe that the impact of the number of antennas on the throughput becomes less significant when the transmission rate decreases. Additionally, the power allocation ratio has a more effect on the system when the number of channel uses is small. However, when the power allocation ratio of the AN becomes larger, it leads to a drop in the average secrecy throughput. In other words, if the transmitter allocates more of its power to inject AN, the average secrecy throughput decreases.

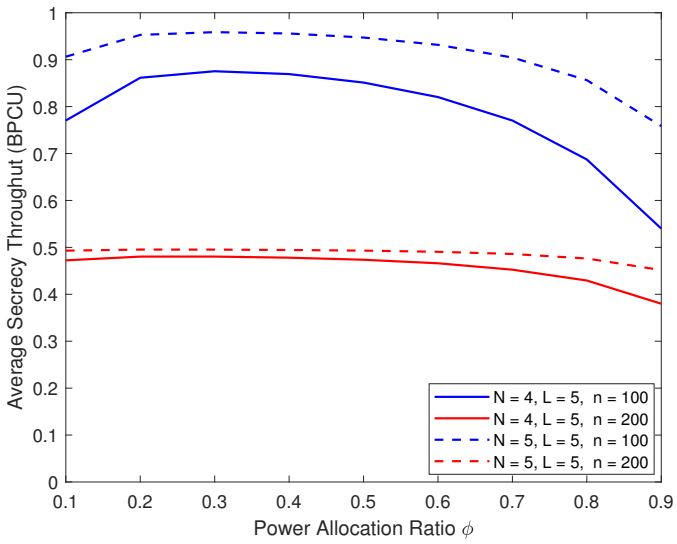

Fig. 4.11 Average Achievable Secrecy Throughput with respect to Power Allocation Ratio.

4.4 Summary

In this study, we provide a novel approximation of the average secrecy throughput for a wiretap channel under Rayleigh fading with multiple eavesdroppers for SPC. 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 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.

Next, we take one further step to extend the wiretap channel model by adding multiple receivers and discusses how eavesdroppers collaboration impact the system security performance.

Chapter 5

Secrecy Analysis of Multiple Receivers and Multiple Eavesdroppers

In this chapter, we study the secrecy performance of short packet secure communications in large-scale networks. Therefore, we investigated a fading wiretap channel when there are not only multiple eavesdroppers, but also receivers. In particular, we also compare the performance of colluding and non-colluding eavesdropping modes to find whether cooperation is still beneficial for eavesdroppers to intercept secure communication.

5.1 Background Information

The emergence of 5G and beyond networks possesses new challenges for secure communication as they are expected to provide services for large-scale networks that contain multiple users and possible several eavesdroppers. This calls for reassessing the theoretical principles of PLS to measure the performance of 5G networks for short packet blocklengths for various wiretap scenarios.

5.1.1 Motivation and Contributions

From the above, it is clear that only a few works investigate multiple-user networks and there is a lack of studies for multiple eavesdroppers perspective.

In this study, the aim is to investigate the security performance of SPC in large-scale networks, which contain multiple users against several malicious eavesdroppers. Specifically, we consider external eavesdroppers in two scenarios, that have not yet been studied in the literature. In the first scenario, the eavesdroppers are assumed to be independent of each other, which is the non-colluding case. In contrast, in the second scenario, the eavesdroppers

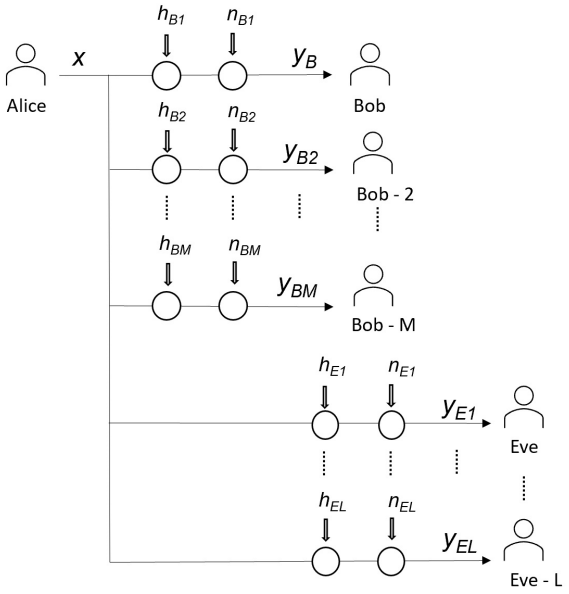

Fig. 5.1 The system model

are assumed to be colluding, which means that they are working together. Each eavesdropper shares the information that they have gained with the other eavesdroppers. The main contributions of this study are as follows:

- We study two eavesdropper modes, i.e., non-colluding and colluding, and obtain closed-form formulas of average secrecy throughput for each mode when all transmitter, receivers and eavesdroppers have single antennas.
- We then perform Monte Carlo simulations to evaluate the performance of the system. We compare the simulated results by evaluating the derived closed-form formulas.

5.2 System Model and Problem Description

As illustrated in Fig. 5.1, single antenna transmitter, Alice, wants to communicate securely with one of the M single-antenna legitimate receivers, Bobs, in the presence of L number of single antenna eavesdroppers, Eves. All the channels are affected by Rayleigh fading and are independent of each other. The transmitter encodes the messages into the codeword x and the jth legitimate receiver, Bob, receives the codeword as

$$y_{\mathrm{B}_j}(i) = h_{\mathrm{B}_j}(i)x(i) + n_{\mathrm{B}_j}(i), \quad j = 1,2,..,M, \tag{5.1}$$

where $h_{\mathrm{B}_j}(i)$ characterizes the small-scale fading coefficient with zero mean and unit variance for main channel at time i of the jth Bob and $n_{\mathrm{B}_j}(i)$ is the Additive White Gaussian Noise (AWGN) experienced during transmission with $n_{\mathrm{B}} \sim \mathcal{N}(0, \sigma_{\mathrm{B}}^2)$, which has zero mean and variance of σ_{B}^2. The main channel transmission is overheard by the kth eavesdropper, who receives a message

$$y_{\mathrm{E}_k}(i) = h_{\mathrm{E}_k}(i)x(i) + n_{\mathrm{E}_k}(i), \quad k = 1, 2, .., L. \tag{5.2}$$

where $h_{\mathrm{E}_k}(i)$ corresponds to the fading coefficient with zero mean and unit variance at time i of the kth eavesdropper that is corrupted by AWGN noise of $n_{\mathrm{E}_k}(i) \sim \mathcal{N}(0, \sigma_{\mathrm{E}}^2)$ with zero mean and variance σ_{E}^2. The time index, i, of the channels coefficients is omitted, because we assume that it remains constant over a block and varies across other blocks independently. The instantaneous and average SNR of a receiver and an eavesdropper are given respectively as

$$\gamma_{\mathrm{B}_j} = \frac{P|h_{B_j}|^2}{\sigma_B^2}, \quad \overline{\gamma}_{\mathrm{B}_j} = \frac{\mathbb{E}\{|h_{\mathrm{B}_j}|^2\}P}{\sigma_{\mathrm{B}}^2}, \tag{5.3}$$

$$\gamma_{\mathrm{E}_k} = \frac{P|h_{E_k}|^2}{\sigma_E^2}, \quad \overline{\gamma}_{\mathrm{E}_k} = \frac{\mathbb{E}\{|h_{\mathrm{E}_k}|^2\}P}{\sigma_{\mathrm{E}}^2}, . \tag{5.4}$$

where P is the transmit power at Alice. Under the considered setting, the secrecy capacity can be computed as [60]

$$C_{\mathrm{s}} = \begin{cases} C_{\mathrm{B}} - C_{\mathrm{E}}, & \text{when} \quad \gamma_{\mathrm{B}_j} > \gamma_{\mathrm{E}_k}, \\ 0, & \text{when} \quad \gamma_{\mathrm{B}_j} \leq \gamma_{\mathrm{E}_k}, \end{cases} \tag{5.5}$$

where the capacity of the main channel is [25]

$$\begin{aligned} C_{\mathrm{B}} &= \log_2(1 + \min_j \quad \gamma_{\mathrm{B}_j}) \\ &= \log_2(1 + \gamma_{\mathrm{B}}). \end{aligned} \tag{5.6}$$

and the capacity of the strongest eavesdropper's channel equals to [25]

$$\begin{aligned} C_{\mathrm{E}} &= \log_2(1 + \max_k \quad \gamma_{\mathrm{E}_k}) \\ &= \log_2(1 + \gamma_{\mathrm{E}}). \end{aligned} \tag{5.7}$$

Since we assume multiple receivers and eavesdroppers, secure communication can only be guaranteed when the instantaneous SNR of weakest legitimate receiver, γ_{B}, is larger than that of the strongest eavesdropper, γ_{E}. In other words, we consider the worst case scenario to obtain secure communication. Therefore, the maximum secure transmission rate is limited by the worst channel condition of one of any receivers and by the best channel conditions among the eavesdroppers.

5.2.1 Average Secrecy Throughput Analysis

In this section, we apply the average secrecy throughput analysis for our considered scenarios. The defined decoding error probability expression ε in (3.6) is valid in these calculations, as well as the average achievable secrecy throughput T_s (3.7). In order to obtain a closed-form approximation, the expression in (3.9) is solved with the help of the linearization technique in (3.12).

Average Secrecy Throughput for L Non-Colluding Eavesdroppers

First, we assume the eavesdroppers are non-colluding, which means they do not cooperate. We are interested in finding the CDF of each node. The CDF of Bob is obtained as follows

$$\begin{aligned} F_{\gamma_{\mathrm{B}}}(x) &= \Pr(\gamma_{\mathrm{B}} < x) = \Pr\{\min_{M} \gamma_{\mathrm{B}_M} < x\} \\ &= 1 - \Pr\{\min_{M} \gamma_{\mathrm{B}_M} > x\} \\ &= 1 - \Pr\{\gamma_{\mathrm{B}_1} > x, \gamma_{\mathrm{B}_2} > x, .., \gamma_{\mathrm{B}_M} > x\} \\ &= 1 - \Big[\int_{x}^{\infty} f_{\gamma_{\mathrm{B}}}(\gamma) d\gamma\Big]^{M}. \end{aligned} \tag{5.8}$$

Thus,

$$\begin{aligned} F_{\gamma_{\mathrm{B}}}(x) &= 1 - \Big[\int_{x}^{\infty} \frac{1}{\overline{\gamma}_{\mathrm{B}}} e^{-\frac{\gamma_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}}}\Big]^{M}, \\ &= 1 - (e^{-\frac{x}{\overline{\gamma}_{\mathrm{B}}}})^{M}. \end{aligned} \tag{5.9}$$

According to the above, PDF of Bob equals to

$$f(\gamma_{\mathrm{B}}) = \frac{M}{\overline{\gamma}_{\mathrm{B}}} e^{-\frac{M\gamma_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}}}. \tag{5.10}$$

Whereas the CDF of Eve is found with the following

$$\begin{aligned} F_{\gamma_{\mathrm{E}}}(x) &= \Pr(\gamma_{\mathrm{E}} < x) = \Pr\{\max_{L} \gamma_{\mathrm{E}_L} < x\} \\ &= \Pr\{\gamma_{\mathrm{E}_1} < x, \gamma_{\mathrm{E}_2} < x, .., \gamma_{\mathrm{E}_L} < x\} \\ &= \Big[\int_0^x f_{\gamma_{\mathrm{E}}}(\gamma) d\gamma\Big]^L. \end{aligned} \tag{5.11}$$

Then PDF of Eve is easy to calculate

$$\begin{aligned} f(\gamma_{\mathrm{E}}) &= \frac{dF_{\gamma_{\mathrm{E}}}(x)}{dx} = L f_{\gamma_{\mathrm{E}}}(x)\Big[\int_0^x f_{\gamma_{\mathrm{E}}}(\gamma) d\gamma\Big]^{L-1} \\ &= L\Big(1 - e^{-\frac{\gamma_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}}\Big)^{L-1} \frac{1}{\overline{\gamma}_{\mathrm{E}}} e^{-\frac{\gamma_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}}. \end{aligned} \tag{5.12}$$

In order to evaluate the expression in (3.10) for a non-colluding case, we insert $f(\gamma_{\mathrm{B}})$, which is defined in (5.10), into (3.11)

$$S(\gamma_{\mathrm{E}}) = \int_0^{\infty} (1 - \varepsilon_{\gamma_{\mathrm{B}}|\gamma_{\mathrm{E}}}) \frac{M}{\overline{\gamma}_{\mathrm{B}}} e^{-\frac{M\gamma_{\mathrm{B}}}{\overline{\gamma}_{\mathrm{B}}}} d\gamma_{\mathrm{B}}. \tag{5.13}$$

For given values of $\gamma_{\mathrm{B}} = x$ and $\gamma_{\mathrm{E}} = y$, the integral becomes

$$S(y) = 1 - \Big(\underbrace{\int_0^{\alpha+u} \frac{M}{\overline{\gamma}_{\mathrm{B}}} e^{-\frac{Mx}{\overline{\gamma}_{\mathrm{B}}}} dx}_{\mathrm{S}_1} + \underbrace{\int_{\alpha+u}^{\alpha-u} (\beta(x-\alpha) + 1/2) \frac{M}{\overline{\gamma}_{\mathrm{B}}} e^{-\frac{Mx}{\overline{\gamma}_{\mathrm{B}}}} dx}_{\mathrm{S}_2}\Big). \tag{5.14}$$

where,

$$\mathrm{S}_1 = 1 - e^{-\frac{M(\alpha+u)}{\overline{\gamma}_{\mathrm{B}}}}, \tag{5.15}$$

and

$$\begin{aligned} \mathrm{S}_2 = &\frac{\beta}{M}(M(\alpha+u) + \overline{\gamma}_{\mathrm{B}}) e^{-\frac{M(\alpha+u)}{\overline{\gamma}_{\mathrm{B}}}} - \frac{\beta}{M}(M(\alpha-u) + \overline{\gamma}_{\mathrm{B}}) e^{-\frac{M(\alpha-u)}{\overline{\gamma}_{\mathrm{B}}}} \\ &+ \Big(\frac{1}{2} - \beta\alpha\Big)[e^{-\frac{M(\alpha+u)}{\overline{\gamma}_{\mathrm{B}}}} - e^{-\frac{M(\alpha-u)}{\overline{\gamma}_{\mathrm{B}}}}]. \end{aligned} \tag{5.16}$$

Thus, we get

$$S(\gamma_{\mathrm{E}}) = \frac{\beta\overline{\gamma}_{\mathrm{B}}}{M} e^{-\frac{M\alpha}{\overline{\gamma}_{\mathrm{B}}}} [e^{\frac{Mu}{\overline{\gamma}_{\mathrm{B}}}} - e^{-\frac{Mu}{\overline{\gamma}_{\mathrm{B}}}}]. \tag{5.17}$$

For high SNR values, the expression in (5.17) is approximated as

$$S(\gamma_{\mathrm{E}}) \approx e^{-\frac{M\alpha}{\overline{\gamma}_{\mathrm{B}}}}. \tag{5.18}$$

Then, by replacing (5.18) into (3.10), and by also using $f(\gamma_{\mathrm{E}})$ in (5.12) we get

$$\begin{aligned} T_{\mathrm{s}} &\approx \frac{b}{n}\int_0^{\infty} e^{-\frac{M\alpha}{\overline{\gamma}_{\mathrm{B}}}} L\Big(1-e^{-\frac{\gamma_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}}\Big)^{L-1}\frac{1}{\overline{\gamma}_{\mathrm{E}}}e^{-\frac{\gamma_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}}d\gamma_{\mathrm{E}} \longrightarrow \\ T_{\mathrm{s}} &\approx \frac{bL}{n\overline{\gamma}_{\mathrm{E}}}e^{\frac{M-Mr}{\overline{\gamma}_{\mathrm{B}}}}\int_0^{\infty} e^{-\gamma_{\mathrm{E}}\left(\frac{Mr}{\overline{\gamma}_{\mathrm{B}}}+\frac{1}{\overline{\gamma}_{\mathrm{E}}}\right)}\Big(1-e^{-\frac{\gamma_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}}\Big)^{L-1}d\gamma_{\mathrm{E}}. \end{aligned} \tag{5.19}$$

According to [56], we can use the following equation

$$\int_0^{\infty}\big(1-e^{-\frac{x}{\beta}}\big)^{v-1}e^{-\mu x}dx = \beta \mathrm{B}(\beta\mu, v), \quad [\mathrm{Re} \quad \beta, v, \mu > 0], \tag{5.20}$$

to find a solution. Re depicts the real part of the imaginary numbers. Finally, the secrecy throughput in closed-form formula is derived for L non-colluding eavesdroppers (T_{ncol} stands for T_s for non-colluding Eves scenario)

$$T_{\mathrm{ncol}} \approx \frac{bL}{n}exp\Big(\frac{M-Mr}{\overline{\gamma}_{\mathrm{B}}}\Big)\mathrm{B}\Big(\frac{\overline{\gamma}_{\mathrm{E}}Mr}{\overline{\gamma}_{\mathrm{B}}}+1, L\Big). \tag{5.21}$$

where the beta function $\mathrm{B}(.,.)$ is represented in the form of gamma function ($\Gamma(x) = \int_0^{\infty} t^{x-1}e^{-t}dt$) as in [56]

$$\mathrm{B}(x,y) = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)}. \tag{5.22}$$

Average Secrecy Throughput for L Colluding Eavesdroppers

According to [24], [25], all eavesdroppers can perform joint processing and by using maximal ratio combining (MRC) they can obtain a joint SNR with the sum of at all the Eves. Alternatively, L number of colluding Eves can be modelled as L antenna single Eve. Therefore, the PDF of Eve is represented as

$$f(\gamma_{\mathrm{E}}) = \frac{{\gamma_{\mathrm{E}}}^{L-1}e^{-\frac{\gamma_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}}}{{\overline{\gamma}_{\mathrm{E}}}^{L}\Gamma(L)}. \tag{5.23}$$

The first steps of the formula derivation for average secrecy throughput of colluding eavesdroppers are similar to the non-colluding case. Since the legitimate receivers part remains the same, the approximation for $S(\gamma_{\mathrm{E}})$ in (5.18) is also valid for this scenario. Therefore, (5.23) is replaced in (3.10) and we derive

$$
\begin{aligned}
T_{\mathrm{s}} &\approx \frac{b}{n}\int_0^{\infty} e^{-\frac{M\alpha}{\overline{\gamma}_{\mathrm{B}}}} \frac{{\gamma_{\mathrm{E}}}^{L-1} e^{-\frac{\gamma_{\mathrm{E}}}{\overline{\gamma}_{\mathrm{E}}}}}{{\overline{\gamma}_{\mathrm{E}}}^{L}\Gamma(L)} d\gamma_{\mathrm{E}} \longrightarrow \\
T_{\mathrm{s}} &\approx \frac{b e^{\frac{M-Mr}{\overline{\gamma}_{\mathrm{B}}}}}{n{\overline{\gamma}_{\mathrm{E}}}^{L}\Gamma(L)} \int_0^{\infty} e^{-\gamma_{\mathrm{E}}\left(\frac{Mr}{\overline{\gamma}_{\mathrm{B}}}+\frac{1}{\overline{\gamma}_{\mathrm{E}}}\right)} {\gamma_{\mathrm{E}}}^{L-1} d\gamma_{\mathrm{E}}.
\end{aligned}
\tag{5.24}
$$

By using [56]

$$
\int_0^{\infty} x^{v-1} e^{-\mu x} dx = \frac{\Gamma(v)}{\mu^{v}} \quad [\mathrm{Re} \quad \mu > 0, \quad \mathrm{Re} \quad v > 0]. \tag{5.25}
$$

The closed-form formula for colluding Eves is presented below (T_{col} symbolizes the average secrecy throughput for colluding Eves scenario)

$$
T_{\mathrm{col}} \approx \frac{b}{n\overline{\gamma}_{\mathrm{E}}^{L}} exp\Big(\frac{M-Mr}{\overline{\gamma}_{\mathrm{B}}}\Big)\Big(\frac{1}{\overline{\gamma}_{\mathrm{E}}}+\frac{Mr}{\overline{\gamma}_{\mathrm{B}}}\Big)^{-L}. \tag{5.26}
$$

5.3 Numerical Results

Numerical results show the performance of the proposed approximations. Specifically, Monte Carlo simulations are conducted to verify the accuracy of the closed-form expressions. Then, the impact of the average SNR's, and the number of receivers and eavesdroppers on the secrecy performance of SPC are examined. Unless otherwise specified, throughout the simulations, information leakage probability is set as $\delta = 10^{-4}$ and the information bits parameter is $b = 200$. All Monte Carlo simulations are the average of 10^5 trials.

Fig. 5.2 shows the average secrecy throughput with respect to various blocklengths obtained by Monte Carlo simulations. It also depicts the derived closed-form formula approximations given by (5.21) and (5.26). Note that theoretical results match very well with the simulated outcome for both non-colluding and colluding eavesdroppers cases. The average secrecy throughput for both cases first increases and then slightly decreases as the blocklength increases. The reason is that ε is a monotonically decreasing function of blocklength n for a fixed number of information bits b. Furthermore, for the same number of eavesdroppers, colluding mode negatively affects the average secrecy throughput due to their ability to gather the received information.

Fig. 5.3 plots the average secrecy throughput versus the average SNR of the main channel for selected values of L the number of eavesdroppers) and M (the number of receivers). For evaluation purposes, both L and M are assigned the values of 2 and 6. The average secrecy throughput is significantly low if the average SNR of the eavesdropper channel is more powerful than the main channel. To obtain average secrecy throughput, $\overline{\gamma}_{\mathrm{B}}$ should be high,

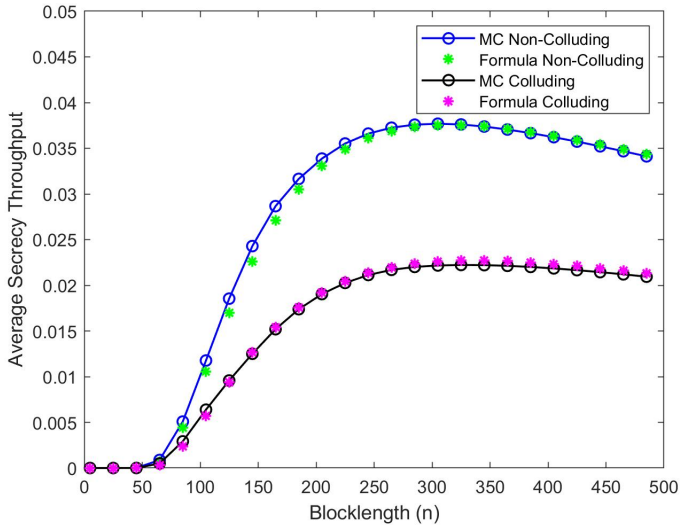

Fig. 5.2 Average Achievable Secrecy Throughput vs. Blocklength. L=M=2, $\overline{\gamma}_{\mathrm{B}} = \overline{\gamma}_{\mathrm{E}} = 10$ dB.

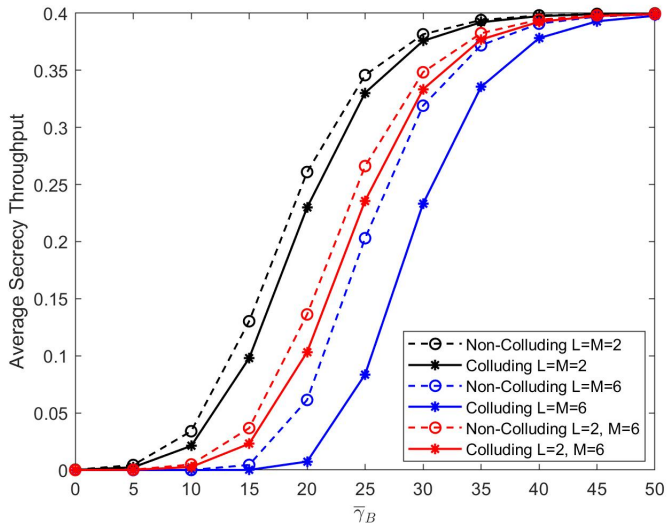

Fig. 5.3 Average Achievable Secrecy Throughput vs average SNR of Bob. n = 500, $\overline{\gamma}_{\mathrm{E}} = 10$ dB.

when the number of eavesdroppers increases. Moreover, when any of the receivers have a higher SNR than any of the eavesdroppers, the maximal achievable throughput reaches a maximum value that can not be exceeded irrespective of the number of the eavesdroppers. It is also clear that the eavesdroppers reduce the average secrecy throughput when colluding rather than acting individually.

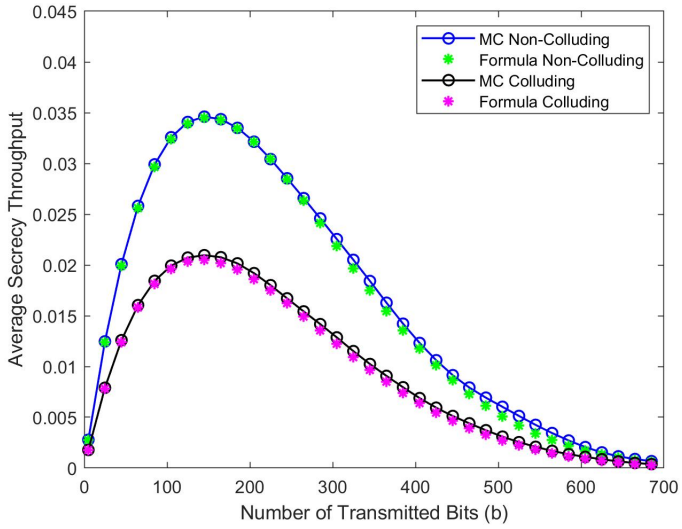

Fig. 5.4 Average Achievable Secrecy Throughput vs. Bits. L=M=2, n=200, $\overline{\gamma}_{\mathrm{B}} = \overline{\gamma}_{\mathrm{E}} = 10$ dB.

In Fig. 5.4, the plotted average secrecy throughput with respect to transmitted bits shows again a great fit between the derived theoretical value and the Monte Carlo simulation results. As expected, colluding eavesdroppers are more harmful to the system performance. Average secrecy throughput increases first and then decreases with the increase of the message size b for both colluding and non-colluding modes. When n is fixed, the large change on b affects obtaining the secure transmission, then average secrecy throughput results in zero.

Lastly, the effect of the number of receivers and eavesdroppers on the average secrecy throughput is demonstrated in Fig. 5.5. Different from the previous comparisons, the number of information bits is set to be 100 and 500 bits while keeping the packet length at 600 channel uses. For the upper part of Fig. 5.5, the number of receivers varies when the number of eavesdroppers is set to 2. For the lower part of Fig. 5.5, the number of receivers remains 2, while the number of eavesdroppers varies. For both cases, transmitting more information bits using the same blocklength helps maintain high average secrecy throughput. However, increasing the number of receivers helps to achieve higher secrecy throughput up to a point and then it gradually drops to the level of zero. Particularly, it does not help to accommodate more receivers to eliminate the eavesdropper impact on the secrecy performance. The reason is that the receivers are more likely to be affected by the different fading channel conditions when their number increases. Therefore, according to our assumption, the minimum received SNR of the channel between the transmitter and the receiver may be much lower. Differently, eavesdroppers affect significantly the throughput

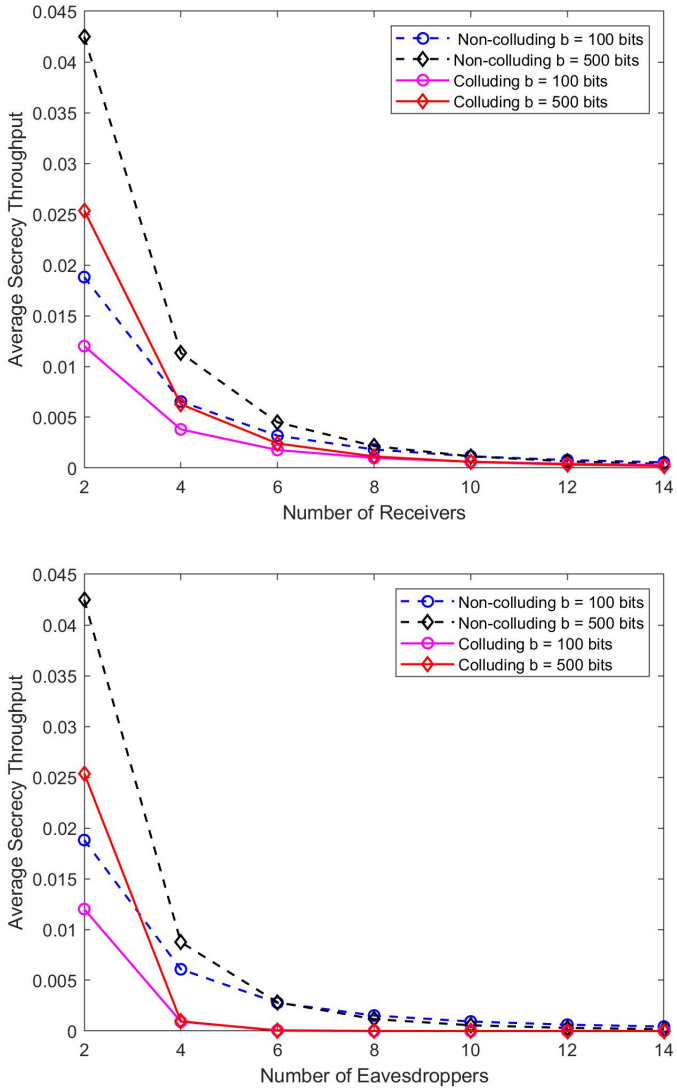

Fig. 5.5 Average Achievable Secrecy Throughput vs. No of Receivers (M)/No of Eavesdroppers (L). n=600, $\overline{\gamma}_{\mathrm{B}} = \overline{\gamma}_{\mathrm{E}} = 10$ dB.

even for the smaller numbers. The secrecy throughput deteriorates and falls sharply with the growing number of eavesdroppers, especially for the colluding case.

5.4 Summary

In this work, we considered a wiretap channel model in which the transmission happens between a transmitter and multiple legitimate receivers in the presence of multiple non-colluding and colluding eavesdroppers. All nodes have a single antenna and all the channels

are affected by the Rayleigh fading. We characterized the average secrecy throughput for colluding and non-colluding adversary modes while transmitting short packets. Monte Carlo simulations validate closed-form expressions for each of the considered scenarios. Numerical results show that colluding eavesdroppers turn out to affect the average secrecy throughput more seriously than the non-colluding adversaries and that they are more powerful when their numbers increase. Setting a large blocklength for transmitting a message results in higher average secrecy throughput for both cases, but based on the evaluations, it is discernible that there is an upper-level value for the throughput. Interestingly, increasing the number of legitimate receivers negatively affects the secrecy performance of the system due to the possibility to be exposed to harsh fading parameters.

Chapter 6

Conclusion

6.1 Thesis Conclusion

In this thesis, we investigated secure communication in several different wiretap channel settings from the aspect of short packet transmission.

In Chapter 3, we explored the security performance of short packet transmission over a wiretap channel under the existence of an active eavesdropper for two different topologies, namely line and triangular. Novel approximations are proposed for the average secrecy throughput expressions for a Rayleigh fading wiretap channel with an active eavesdropper, which operates either in half duplex or full duplex mode. The obtained approximations are validated by Monte Carlo simulations. Our analysis show that while an active eavesdropper affects more the secrecy throughput compared to a passive adversary case, the full-duplex mode is more harmful than a half-duplex one. In addition, the distance and location of the eavesdropper on the topology play an important role on the achieved secrecy throughput as well as the jamming power level of the eavesdropper.

Chapter 4 studies secure SPC for large-scale networks under the presence of multiple independent adversaries. Novel closed-form approximations of the average secrecy throughput are obtained for the case where the transmitter either single or multiple antennas and the validity of these approximations is confirmed with MC simulations. We are also be able to study extensively the impact of the AN, the number of transmitter antennas and the number of eavesdroppers on system security performance. We observed that although an increased number of antennas leads to higher average secrecy throughput, higher transmission rates are more effective in obtaining high average secrecy throughput. In addition, the optimal blocklength value that maximizes the average secrecy throughput is obtained for the single antenna transmitter scenario.

Finally, in Chapter 5 we considered a wiretap channel setting similar to the one in Chapter 4, but differs in the sense that there are also multiple legitimate receivers. Specifically, external eavesdroppers are analysed in two scenarios, i.e., non-colluding and colluding. We characterized the average secrecy throughput for colluding and non-colluding adversary modes while transmitting short packets and Monte Carlo simulations performed to show the accuracy of the closed form expressions for each of the considered scenarios. Numerical results show that colluding eavesdroppers are more harmful than the non-colluding ones, especially if their numbers increase. Interestingly, growing number of legitimate receivers do not help to maintain high average secrecy throughput, because they are more likely to be exposed to harsh fading parameters.

6.2 Future Research

The work presented in this thesis has potential to be extended in the following research directions.

Chapter 3 covered the topic about how to combat eavesdropping and jamming attacks in SPC and analysed the overall system in the context of average secrecy throughput. While the legitimate transmitter aims to maintain a non-negative secrecy rate, eavesdropper either listen or jam the ongoing transmission to gain benefit. This conflicting behaviour can be formulated in a game theoretic aspect to find out what strategy on resource allocation can lead to maximization of the secrecy output. More importantly, resource allocation is also essential when it comes to large-scale networks which multiple users, because they involve massive resource-constrained nodes such as in IoT networks.

Although it is very common to assume the channel statistics are available at the transmitter in PLS literature, this assumption may seem too much idealistic when it comes to passive adversaries. A promising future direction is to investigate the scenario with user and eavesdroppers having non-identical distribution channel statistics due to different distances from the transmitter. In particular, we may extend the findings in Chapter 4 to consider the distances from transmitter to receivers and eavesdroppers are different. In addition, the assumption of unknown CSI of eavesdroppers is another issue to be considered.

The work in Chapter 5 can be extended to a multiple-antenna setting and as well as taking into account randomly scattered eavesdroppers, which will be representative of a more of practical scenario. Thereby, the system performance can be analyzed according to the location of the eavesdropper and the antenna number impact can be explored. These eavesdroppers do not necessarily have to be passive adversaries, they can actively try to disrupt the main channel communication as well as being a part of the network as regular

users. Therefore, a complex scenario with malicious activities, which may involve the mixture of passive and active eavesdroppers, is a potential aspect to explore.

As wireless networks continue to play an increasingly critical role in modern world, the demand for secure and reliable communication will only continue to grow. Several challenges must be addressed to fully exploit the physical layer security in short packet communications. Despite these challenges, PLS in SPC remains an active area of research that is expected to yield new avenues for enhancing wireless security in the near future.

Appendix A

A.1 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 (4.26) :

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

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:

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

$\Delta(n)$ 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 (A.2) in order to find out whether the function concave or convex :

$$\frac{\partial \Delta(n)}{\partial n} = \frac{1}{n(\overline{\gamma}_{\mathrm{E}} r + \overline{\gamma}_{\mathrm{B}})} \underbrace{\Big(\frac{M^2\overline{\gamma}_{\mathrm{E}}^2\overline{\gamma}_{\mathrm{B}} D}{(\overline{\gamma}_{\mathrm{E}} r + \overline{\gamma}_{\mathrm{B}})} - r(\overline{\gamma}_{\mathrm{E}}\overline{\gamma}_{\mathrm{B}} + \overline{\gamma}_{\mathrm{E}} r + \overline{\gamma}_{\mathrm{B}})(M^2 + H)\Big)}_{\Delta_1} \tag{A.3}$$

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 (A.3) $\frac{1}{n(\overline{\gamma}_{\mathrm{E}} r + \overline{\gamma}_{\mathrm{B}})} > 0$, therefore the sign of the equation depends on the expression inside the brackets.

$$\Delta_1 = \underbrace{\frac{M^2\overline{\gamma}_{\mathrm{E}}^2\overline{\gamma}_{\mathrm{B}} D}{(\overline{\gamma}_{\mathrm{E}} r + \overline{\gamma}_{\mathrm{B}})}}_{\mathrm{J1}} - \underbrace{r(\overline{\gamma}_{\mathrm{E}}\overline{\gamma}_{\mathrm{B}} + \overline{\gamma}_{\mathrm{E}} r + \overline{\gamma}_{\mathrm{B}})(M^2 + H)}_{\mathrm{J2}}. \tag{A.4}$$

Since $\log(\mathrm{J1}) < \log(\mathrm{J2})$, the second derivative in (A.3) is negative and hence T_{s1} is concave.

A.2 PROOF OF LEMMA 2

To find the optimal blocklength value that maximizes the secrecy throughput in (4.25), we take the partial derivative of the logarithm of T_s with respect to n :

$$\frac{\partial \log T_s}{\partial n} = \frac{\partial \Omega(n)}{\partial n} = \frac{\partial \log\left(\frac{bL}{n} e^{\frac{1-e^{\frac{Q^{-1}(\delta)}{\sqrt{n}}+\frac{b}{n}\log(2)}}{\overline{\gamma}_{\mathrm{B}}}} \mathrm{B}\left(\frac{\overline{\gamma}_{\mathrm{E}} e^{\frac{Q^{-1}(\delta)}{\sqrt{n}}+\frac{b}{n}\log(2)}}{\overline{\gamma}_{\mathrm{B}}}+1, L\right)\right)}{\partial n} \tag{A.5}$$

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

$$\Omega(n) = \frac{1}{\overline{\gamma}_{\mathrm{B}} n}\left[Mr\Big(1+\overline{\gamma}_{\mathrm{E}}\big(\psi_0(z,L)-\psi_0(z)\big)\Big)-\overline{\gamma}_{\mathrm{B}}\right]. \tag{A.6}$$

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 :

$$\frac{\partial \Omega(n)}{\partial n} = \frac{1}{\overline{\gamma}_{\mathrm{B}} n^2}\Big(\frac{\overline{\gamma}_{\mathrm{E}}^2 DM^2}{\overline{\gamma}_{\mathrm{B}}} g_1 + r(M^2+H+M)\big(\overline{\gamma}_{\mathrm{E}} g_2 - 1\big)\Big) + \frac{1}{n^2}. \tag{A.7}$$

where the trigamma function is denoted by $\psi_1(.)$ [57, Eq. 6.4.1] and the substitutions of $g_1 = \big(\psi_1(z)-\psi_1(z+L)\big)$, $g_2 = \big(\psi_0(z)-\psi_0(z+L)\big)$ are applied. This expression is always negative and the proof is complete.

A.3 DERIVATION OF the CDF of γ_{E}

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

$$\begin{aligned} F_{\gamma_{\mathrm{E}}}(\gamma) &= \Pr(\gamma_{\mathrm{E}} < \gamma) = \Pr(\max_k \gamma_{\mathrm{E}_k} < \gamma) \\ &= \Pr\{\gamma_{\mathrm{E}_1} < \gamma, \gamma_{\mathrm{E}_2} < \gamma, ..., \gamma_{\mathrm{E}_k} < \gamma\} \\ &= \Big[\int_0^{\gamma} f_{\gamma_{\mathrm{E}}}(x)dx\Big]^L. \end{aligned} \tag{A.8}$$

According to [58], [59], the CDF of the instantaneous SINR at an Eve under AN is given by

$$F_{\gamma_{\mathrm{E}}}(\gamma) = 1 - \Big(1+\frac{(1-\phi)\gamma}{\phi(N-1)}\Big)^{1-N} e^{-\frac{\gamma}{\phi\overline{\gamma}_{\mathrm{E}}}}. \tag{A.9}$$

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

$$F_{\gamma_{\mathrm{E}}}(\gamma) = \left(1 - \Big(1+\frac{(1-\phi)\gamma}{\phi(N-1)}\Big)^{1-N} e^{-\frac{\gamma}{\phi\overline{\gamma}_{\mathrm{E}}}}\right)^L. \tag{A.10}$$

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

$$f_{\gamma_{\mathrm{E}}}(\gamma) = \frac{dF_{\gamma_{\mathrm{E}}}(\gamma)}{d\gamma} = L f_{\gamma_{\mathrm{E}}}(\gamma)\Big[\int_0^{\gamma} f_{\gamma_{\mathrm{E}}}(x)dx\Big]^{L-1} \tag{A.11}$$

and

$$\begin{aligned} f_{\gamma_{\mathrm{E}}}(\gamma) = L\Bigg(1-\Big(1+\frac{(1-\phi)\gamma}{\phi(N-1)}\Big)^{1-N} e^{-\frac{\gamma}{\phi\overline{\gamma}_{\mathrm{E}}}}\Bigg)^{L-1} \\ \times\Bigg(\frac{\Big(1+\frac{(1-\phi)\gamma}{\phi(N-1)}\Big)^{1-N} e^{-\frac{\gamma}{\phi\overline{\gamma}_{\mathrm{E}}}}}{\phi\overline{\gamma}_{\mathrm{E}}} - \frac{(1-\phi)(1-N)e^{-\frac{\gamma}{\phi\overline{\gamma}_{\mathrm{E}}}}}{\phi(N-1)\Big(\frac{(1-\phi)\gamma}{\phi(N-1)}+1\Big)^{N}}\Bigg). \end{aligned} \tag{A.12}$$

If we set $\tau = 1+\frac{(1-\phi)\gamma}{\phi(N-1)}$ in (A.12), the PDF of $f(\gamma_{\mathrm{E}})$ simplifies to:

$$f_{\gamma_{\mathrm{E}}}(\gamma) = L\Big(1-\tau^{1-N}e^{-\frac{\gamma}{\phi\overline{\gamma}_{\mathrm{E}}}}\Big)^{L-1} e^{-\frac{\gamma}{\phi\overline{\gamma}_{\mathrm{E}}}}\left(\frac{\tau^{1-N}}{\phi\overline{\gamma}_{\mathrm{E}}}+\frac{(1-\phi)}{\phi\tau^{N}}\right). \tag{A.13}$$

References

[1] Nan Yang, Lifeng Wang, Giovanni Geraci, Maged Elkashlan, Jinhong Yuan, and Marco Di Renzo. Safeguarding 5G wireless communication networks using physical layer security. IEEE Commun. Mag., 53(4):20–27, Apr. 2015.

[2] Aylin Yener and Sennur Ulukus. Wireless physical-layer security: Lessons learned from information theory. Proc. of the IEEE, 103(10):1814–1825, 2015.

[3] H Vincent Poor and Rafael F Schaefer. Wireless physical layer security. Proc. Natl. Acad. Sci. (PNAS), 114(1):19–26, 2017.

[4] 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., 26(5):6–11, Oct. 2019.

[5] Giuseppe Durisi, Tobias Koch, and Petar Popovski. Toward massive, ultra-reliable, and low-latency wireless communication with short packets. Proc. IEEE, 104(9):1711–1726, 2016.

[6] Claude E Shannon. Communication theory of secrecy systems. The Bell system technical journal, 28(4):656–715, Oct. 1949.

[7] Aaron D Wyner. The wire-tap channel. Bell system technical journal, 54(8):1355–1387, Oct. 1975.

[8] Imre Csiszár and János Körner. Broadcast channels with confidential messages. IEEE Trans. Inf. Theory, 24(3):339–348, May 1978.

[9] Wei Huang, Wei Chen, Bo Bai, Shidong Zhou, and Zhu Han. Physical layer security game with full-duplex proactive eavesdropper. In Proc. IEEE Global Conf. on Signal and Inf. Processing (GlobalSIP), pages 992–996, Washington, DC, USA, Dec. 2016.

[10] Xiao Tang, Pinyi Ren, and Zhu Han. Combating full-duplex active eavesdropper: A game-theoretic perspective. In Proc. IEEE Int. Conf. Commun. (ICC), pages 1–6, Kuala Lumpur, Malaysia, May 2016.

[11] Xiao Tang, Pinyi Ren, and Zhu Han. Power-efficient secure transmission against full-duplex active eavesdropper: A game-theoretic framework. IEEE Access, 5:24632–24645, Oct. 2017.

[12] Wei Huang, Wei Chen, Bo Bai, and Zhu Han. Wiretap channel with full-duplex proactive eavesdropper: A game theoretic approach. IEEE Trans. Veh. Technol., 67(8):7658–7663, Aug. 2018.

[13] Wei Wang, Kah Chan Teh, Sheng Luo, and Kwok Hung Li. Secure transmission in MISOME wiretap channels with half and full-duplex active eavesdroppers. In Proc. IEEE Global Commun. Conf. (GLOBECOM), pages 1–6, Singapore, Dec. 2017.

[14] Sujatha Allipuram, Parthajit Mohapatra, and Saswat Chakrabarti. Secrecy performance of an artificial noise assisted transmission scheme with active eavesdropper. IEEE Wireless Commun. Lett., 24(5):971–975, May 2020.

[15] Chenxi Liu, Jemin Lee, and Tony QS Quek. Secure transmission in the presence of full-duplex active eavesdropper. In
Proc. IEEE Global Commun. Conf. (GLOBECOM), pages 1–6, Singapore, Dec. 2017.

[16] Long Kong, Jiguang He, Georges Kaddoum, Satyanarayana Vuppala, and Lin Wang. Secrecy analysis of a MIMO full-duplex active eavesdropper with channel estimation errors. In Proc. IEEE Veh. Technol. Conf. (VTC-Fall), pages 1–5, Montreal, QC, Canada, Sep. 2016.

[17] Mounir Ghogho and Ananthram Swami. Physical-layer secrecy of MIMO communications in the presence of a Poisson random field of eavesdroppers. In Proc. IEEE Int. Conf. Commun. (ICC), pages 1–5, Kyoto, Japan, Jun. 2011.

[18] Liyun Zhang, Haixia Zhang, Dalei Wu, and Dongfeng Yuan. Improving physical layer security for MISO systems via using artificial noise. In Proc. IEEE Global Commun. Conf. (GLOBECOM), pages 1–6, Dec. 2015.

[19] Tong-Xing Zheng, Hui-Ming Wang, Jinhong Yuan, Don Towsley, and Moon Ho Lee. Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers. IEEE Trans. on Commun., 63(11):4347–4362, Nov. 2015.

[20] Qiang Li and Wing-Kin Ma. Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization. IEEE Trans. Signal Process., 61(10):2704–2717, May 2013.

[21] Zongmian Li, Pengcheng Mu, Bo Wang, and Xiaoyan Hu. Optimal semi adaptive transmission with artificial-noise-aided beamforming in MISO wiretap channels. IEEE Trans. Veh. Technol., 65(9):7021–7035, Sep. 2016.

[22] Zheng Chu, Hong Xing, Martin Johnston, and Stéphane Le Goff. Secrecy rate optimizations for a MISO secrecy channel with multiple multiantenna eavesdroppers. IEEE Trans. Wireless Commun., 15(1):283–297, Jan. 2016.

[23] Wei Wang, Kah Chan Teh, and Kwok Hung Li. Secrecy throughput maximization for MISO multi-eavesdropper wiretap channels. IEEE Trans. Inf. Forensics Secur., 12(3):505–515, Mar. 2017.

[24] Giovanni Geraci, Sarabjot Singh, Jeffrey G Andrews, Jinhong Yuan, and Iain B Collings. Secrecy rates in broadcast channels with confidential messages and external eavesdroppers. IEEE Trans. Wirel. Commun., 13(5):2931–2943, May 2014.

[25] Yongjue Chen, Wei Li, and Huixi Shu. Wireless physical-layer security with multiple receivers and eavesdroppers: Outage probability and average secrecy capacity. In Proc. IEEE Int. Symp. Pers. Indoor Mob. Radio Commun. (PIMRC), pages 662–667, Hong Kong, China, Aug. 2015.

[26] Anish Prasad Shrestha, Jaijin Jung, and Kyung Sup Kwak. Secure wireless multicasting in presence of multiple eavesdroppers. In Proc. Int. Symp. Commun. Inf. Technol. (ISCIT), pages 814–817, Surat Thani, Thailand, Sep. 2013.

[27] Jinxiao Zhu, Yin Chen, Yoshitaka Nakamura, Xiaohong Jiang, Osamu Takahashi, and Norio Shiratori. Outage performance of secure multicasting in the presence of multiple eavesdroppers. In Proc. Int. Conf. Mob. Comput. Ubiquitous Netw. (ICMU), pages 138–142, Hakodate, Japan, Jan. 2015.

[28] Yury Polyanskiy, H Vincent Poor, and Sergio Verdú. Channel coding rate in the finite blocklength regime. IEEE Trans. Inf. Theory, 56(5):2307–2359, May 2010.

[29] Yury Polyanskiy and Sergio Verdú. Scalar coherent fading channel: Dispersion analysis. In Proc. IEEE Int. Symp. Inf. Theory, pages 2959–2963, St. Petersburg, Russia, Jul. 2011.

[30] Wei Yang, Giuseppe Durisi, Tobias Koch, and Yury Polyanskiy. Diversity versus channel knowledge at finite block-length. In Proc. IEEE Inf. Theory Workshop (ITW), pages 572–576, Lausanne, Switzerland, Sep. 2012.

[31] Christopher Potter, Kurt Kosbar, and Adam Panagos. On achievable rates for MIMO systems with imperfect channel state information in the finite length regime. IEEE Trans. Commun., 61(7):2772–2781, Jun. 2013.

[32] Wei Yang, Giuseppe Durisi, Tobias Koch, and Yury Polyanskiy. Quasi-static simo fading channels at finite blocklength. In Proc. IEEE Int. Symp. Inf. Theory, pages 1531–1535, Istanbul, Turkey, Jul. 2013.

[33] Wei Yang, Giuseppe Durisi, Tobias Koch, and Yury Polyanskiy. Quasi-static multiple-antenna fading channels at finite blocklength. IEEE Trans. Inf. Theory, 60(7):4232–4265, Apr. 2014.

[34] Philippe Mary, Jean-Marie Gorce, Ayse Unsal, and H Vincent Poor. Finite blocklength information theory: What is the practical impact on wireless communications? In IEEE Glob. Commun. Conf. (GC Wkshps), pages 1–6, Washington, DC, USA, Dec. 2016.

[35] Wei Yang, Giuseppe Caire, Giuseppe Durisi, and Yury Polyanskiy. Finite-blocklength channel coding rate under a long-term power constraint. In Proc. IEEE Int. Symp. Inf. Theory, pages 2067–2071, Honolulu, HI, USA, Jun. 2014.

[36] Giuseppe Durisi, Tobias Koch, Johan Östman, Yury Polyanskiy, and Wei Yang. Short-packet communications over multiple-antenna Rayleigh-fading channels. IEEE Trans. Commun., 64(2):618–629, Dec. 2015.

[37] Matthieu Bloch and Joao Barros.
Physical-layer security: from information theory to security engineering. Cambridge University Press, Cambridge, U.K., 1st ed. edition, 2011.

[38] Vincent YF Tan. Achievable second-order coding rates for the wiretap channel. In IEEE Int. Conf. Commun. Syst. (ICCS), pages 65–69, Singapore, Nov. 2012.

[39] C. Cao, H. Li, Z. Hu, W. Liu, and X. Zhang. Physical-layer secrecy performance in finite blocklength case. In Proc. IEEE Global Commun. Conf. (GLOBECOM), pages 1–6, San Diego, CA, USA, Dec. 2015.

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

[41] W. Yang, R. F. Schaefer, and H. V. Poor. Secrecy-reliability tradeoff for semi-deterministic wiretap channels at finite blocklength. In Proc. IEEE Int. Symp. Inf. Theory (ISIT), pages 2133–2137, Aachen, Germany, Jun. 2017.

[42] W. Yang, R. F. Schaefer, and H. V. Poor. Wiretap channels: Nonasymptotic fundamental limits. IEEE Trans. Inf. Theory, 65(7):4069–4093, Jul. 2019.

[43] L. Zhang and Y. Liang. Average throughput analysis and optimization in cooperative IoT networks with short packet communication. IEEE Trans. Veh. Technol., 67(12):11549–11562, Dec. 2018.

[44] H. Wang, Q. Yang, Z. Ding, and H. V. Poor. Secure short-packet communications for mission-critical IoT applications. IEEE Trans. Wireless Commun., 18(5):2565–2578, May 2019.

[45] 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., 19(5):3405–3420, May 2020.

[46] Tian Yu, Xiaoli Sun, and Yueming Cai. Secure short-packet transmission in uplink massive MU-MIMO IoT networks. In Proc. Int. Conf. Wirel. Commun. Signal Process. (WCSP), pages 50–55, Nanjing, China, Oct. 2020.

[47] Lai Wei, Yuli Yang, and Bingli Jiao. Secrecy throughput in full-duplex multiuser MIMO short-packet communications. IEEE Wireless Commun. Lett., 10(6):1339–1343, Jun. 2021.

[48] Xiazhi Lai, Tuo Wu, Qi Zhang, and Jiayin Qin. Average secure BLER analysis of NOMA downlink short-packet communication systems in flat Rayleigh fading channels. IEEE Trans. Wireless Commun., 20(5):2948–2960, May 2021.

[49] Chen Feng, Hui-Ming Wang, and H. Vincent Poor. Reliable and secure short-packet communications. IEEE Trans. Wireless Commun., 21(3):1913–1926, Mar. 2022.

[50] Nihan Arı, Nikolaos Thomos, and Leila Musavian. Average secrecy throughput analysis with multiple eavesdroppers in the finite blocklength. In Proc. IEEE Int. Symp. Pers. Indoor Mob. Radio Commun. (PIMRC), pages 1–5, London, UK, Aug. 2020.

[51] Nihan Arı, Nikolaos Thomos, and Leila Musavian. Performance analysis of short packet communications with multiple eavesdroppers. IEEE Transactions on Communications, 2022.

[52] Nihan Arı, Nikolaos Thomos, and Leila Musavian. Secrecy performance of short packet communications: Wiretap channel with multiple receivers and eavesdroppers. In Int. Wirel. Commun. Mob. Comput. Conf. (IWCMC), pages 395–400, Dubrovnik, Croatia, Jun. 2022.

[53] Nihan Arı, Nikolaos Thomos, and Leila Musavian. Active eavesdropping in short packet communication: Average secrecy throughput analysis. In Proc. IEEE Int. Conf. on Commun. Workshops (ICC Workshops), pages 1–6, Montreal, QC, Canada, Jun. 2021.

[54] B. Makki, T. Svensson, and M. Zorzi. Finite block-length analysis of the incremental redundancy HARQ. IEEE Wireless Commun. Lett., 3(5):529–532, Oct. 2014.

[55] Peiya Wang, Guanding Yu, and Zhaoyang Zhang. On the secrecy capacity of fading wireless channel with multiple eavesdroppers. In Proc. IEEE Int. Symp. Inf. Theory (ISIT), pages 1301–1305, Nice, France, Jun. 2007.

[56] I. S. Gradshteyn and I. M. Ryzhik. Table of Integrals, Series, and Products. Academic press, New York, NY, USA, 7th ed. edition, 2007.

[57] Milton Abramowitz and Irene A Stegun. Handbook of mathematical functions with formulas, graphs, and mathematical tables. US Government printing office, Washington D.C., USA, 1964.

[58] Nan Yang, Shihao Yan, Jinhong Yuan, Robert Malaney, Ramanan Subramanian, and Ingmar Land. Artificial Noise: Transmission optimization in multi-input single-output wiretap channels. IEEE Trans. on Commun., 63(5):1771–1783, May 2015.

[59] Shihao Yan, Nan Yang, Ingmar Land, Robert Malaney, and Jinhong Yuan. Three artificial-noise-aided secure transmission schemes in wiretap channels. IEEE Trans. Veh. Technol., 67(4):3669–3673, Apr. 2017.

[60] Bloch, Matthieu and Barros, JoÃo and Rodrigues, Miguel R. D. and McLaughlin, Steven W. Wireless information-theoretic security. IEEE Trans. Inf. Theory, 54(6):2515–2534, Jun. 2008.