Physical Layer Security of Cognitive Radio Networks

Thesis submitted for the award of the Degree
of

Doctor of Philosophy

in the Department of Electrical Engineering

by

Shilpa Thakur
(2018REE0051)

Under the supervision of

Dr. Ajay Singh

भारतीय प्रौद्योगिकी
संस्थान जम्मू
INDIAN INSTITUTE OF
TECHNOLOGY JAMMU

Indian Institute of Technology Jammu
Jammu 181221

January 2022

Declaration

I hereby declare that the matter embodied in this thesis entitled **"Physical Layer Security of Cognitive Radio Networks"** is the result of investigations carried out by me in the Department of Electrical Engineering, Indian Institute of Technology Jammu, India, under the supervision of **Dr. Ajay Singh** (IIT Jammu) and it has not been submitted elsewhere for the award of any degree or diploma, membership etc. In keeping with the general practice in reporting scientific observations, due acknowledgements have been made whenever the work described is based on the findings of other investigators. Any omission that might have occurred due to oversight or error in judgment is regretted. A complete bibliography of the books and journals referred in this thesis is given at the end of the thesis.

January 2022
Indian Institute of Technology Jammu

Shilpa Thakur
(2018REE0051)

In the memory of my beloved father

Acknowledgements

First and foremost, I would express my deep sense of gratitude to my thesis supervisor Dr. Ajay Singh for his continuous support, expert guidance, harmony, and patience throughout these years of the Ph.D. program. He has always given me the time, technical feedback, and moral support I needed during my research. I benefited greatly from his research experience, constructive suggestions, disciplines, and principles to accomplish my research work. It is due to his belief in me that today I am submitting this thesis. I cannot find the words to thank him for everything he has done, and he is doing, helping me achieve my goals and succeed in my research career.

My profound thanks to student research committee members Dr. Sudhakar Modem and Dr. Tanmay Sarkar for their valuable time to discuss and critically examine the research work carried out during this course. I express my sincere regards to all my teachers, who have taught me fantastic subjects at IIT Jammu. I am also grateful to Dr. Ankit Dubey, Head of the Department, all faculty members, and the Department of Electrical Engineering staff for their fantastic help throughout the course. During these inspiring years at IIT Jammu, I made many good friends. I acknowledge all my friends at IIT Jammu: Mr. Gaurav Sharma, Mr. Mohit Kumar, Ms. Sapna Thapar, Ms. Shalini Tripathi, and Mr. Shashi Bhushan for their enormous support in different ways. My special thanks to Mr. Gaurav Sharma for discussion whenever required.

I want to express my love to my mother, Mrs. Asha Thakur, for her support and care for me whenever I need her. To make my life comfortable, I want to mention my deep sense of respect to my in-laws, Mr. Vijay Kumar Jaswal and Mrs. Saroj Jaswal. Without their support and moral encouragement, this achievement was impossible. I also would like to mention somebody who played a significant role during this journey. She is constantly with me in all my good and challenging times. I am incredibly fortunate to have his company. She is none other than my younger sister Mrs. Neha Thakur. Finally, I would like to thank my husband, Dr. Gaurav Jaswal, for his patience, help, and encouragement during all those difficult phases. His never-ending inspiration is still my powerhouse. His hard-working attitude and genuine love for humanity changed my view of life. Special mention to my daughter Amayra whose innocent talks and activities relax me whenever I get stressed and tired.

Last but not least, I would like to thank Science and Engineering Research Board (SERB), Department of Science and Technology (DST), Government of India, for funding support un-

der the project ”Physical Layer Security of Cognitive Radio Networks” (Project Ref. no. YSS/2015/001738).

Abstract

With the emergence of future heterogeneous networks and high multi-media applications, the demand for the radio spectrum has increased day by day. However, the popularity of growing wireless systems makes it difficult for spectrum agencies to manage the available electromagnetic radio spectrum, thus necessitating intelligent ways to detect the unused spectrum. Cognitive radio is a powerful tool to deal with spectrum scarcity problems and improves the spectrum's utilization. Based upon the type of available network-side information, along with the regulatory constraint, cognitive users (secondary users or unlicensed users) seek to underlay, overlay, or interweave their signals with primary users (licensed users) without affecting their communication significantly. Among these approaches, the underlay approach is preferable due to its low implementation complexity in the dense areas where the secondary users are permitted to use the primary user's spectrum if the interference to the primary user is below a predefined threshold. In such a complex environment, information security is one of the most vital issues because of the broadcasting nature of their channel. Although the conventional cryptographic techniques have proven their effectiveness to ensure information, they become vulnerable against potential eavesdroppers with limited computational power. Moreover, the broadcast nature of wireless channels offers different challenges in terms of key (public/private) exchange and distributions. In contrast, information-theoretic-based physical layer security emerges as a promising security approach that complements and supports the conventional cryptographic techniques. Physical layer security is an efficient tool for protecting legitimate users against eavesdropping attacks by exploiting the physical characteristics of the channel. By now, many research works have explained the fundamental performance limits of physical layer security under different wiretap channel models. Notably, the fading channel model is essential for efficiently capturing the basic time-varying properties of wireless channels among other wiretap channel models. This thesis, therefore, concentrates on the analysis of physical layer security for underlay cognitive radio networks over fading channels.

We first examine the secrecy performance of an underlay cognitive radio network in a perfect channel state information scenario. We consider that the secondary transmitter is equipped with multiple antennas, and the optimal and sub-optimal antenna selection schemes are utilized to find the single best antenna among available ones to improve secrecy performance. A generalized selection combining strategy that reduces the network's hardware complexity

is employed at the secondary receiver, and the maximal ratio combining scheme is utilized at the eavesdropper. It is assumed that the primary transmitter lies very far from the secondary receivers, but the primary receiver is in the proximity of the secondary networks. The novel closed-form expressions for secrecy outage probability and intercept probability are derived in the presence of multiple primary receivers. The secrecy performance gap between optimal and sub-optimal antenna selection schemes is studied. We present comprehensive simulation and numerical results to describe the theoretical analysis's validity and demonstrate our theoretical findings.

Next, we evaluate the secrecy performance of an underlay cognitive radio network for an imperfect channel state information environment. For this, we consider two practical scenarios, i.e., scenario 1: passive eavesdropping, i.e., the channel state information of an eavesdropper's channel is unavailable at the secondary transmitter, and scenario II: active eavesdropping, i.e., the channel state information of eavesdropper's link is known to the secondary transmitter. The secondary receiver, eavesdropper, and primary receiver are equipped with multiple antennas, and the selection combining and maximal ratio combining techniques has been adopted at the secondary receiver, while the latter has been employed at the maximal ratio combining scheme. The new closed-form expressions of exact and asymptotic secrecy outage probability, intercept probability, and ε-outage secrecy capacity are derived for the scenario I. Likewise, a comprehensive analysis of average secrecy capacity is performed in scenario II. New closed-form expressions for exact and asymptotic average secrecy capacity are derived, valid for an arbitrary number of antennas at the secondary receiver and eavesdropper.

Following, we investigate the secrecy performance of an underlay cognitive radio network in the presence of a dominant interferer, primary transmitter, under peak interference power constraints. Depending upon the availability of global channel state information of an eavesdropper channel, we analyze the secrecy performance of the proposed network in the Rayleigh fading environment for both passive and active eavesdropping scenarios. Further, the impact of outdated CSI of the Alice-primary receiver link on the various performance metrics with the concept of interference-outage is also studied. Monte Carlo simulation is performed to verify the validation of our analytical results.

Finally, we study the secrecy performance of the receive antenna selection scheme in an interference-limited underlay cognitive radio network. Exact and asymptotic expressions for the secrecy outage probability, intercept probability, and average secrecy capacity are derived

over a general fading scenario (i.e., primary network undergoes Rayleigh fading and secondary network undergoes Nakagami-m fading). The impact of outdated channel state information on the secrecy performance of an interference-limited cognitive radio network is also analyzed when interference from the primary transmitter to secondary receivers exits under peak interference power constraint. The extreme value theorem is used to find the asymptotic expressions of various performance metrics for a large number of antennas at the secondary receiver and eavesdropper.

We validate our entire framework through extensive simulation and numerical results and demonstrate the effects of system/channel parameters on the secrecy performance of the considered systems.

Contents

List of Figures

List of Tables

List of Symbols

Symbol	Description
$\bar{I}_P$	Peak Interference Power
$\bar{P}_A$	Power at Alice
$\bar{P}_T$	Maximum Transmit Power
I_P	Normalized Peak Interference Power
I_{pav}	Average Interference Power
P_A	Normalized Power at Alice
P_T	Normalized Maximum Transmit Power
$\|h_0\|$	Fading Coefficients of Alice-PR Channel
$\|h_i\|$	Fading Coefficients of Main Channel
$\|h_0\|^2$	Channel Power Gain of Alice-PR channel
$\|h_i\|^2$	Channel Power Gain of Main Channel
N_A	Number of Antennas at Alice
$\varphi(b)$	Digamma Function
N_B	Number of Antennas at Bob
$\mathbb{E}(.)$	Expectation Operator
$\mathbb{C}$	Field of Complex Number
N_E	Number of Antennas at Eve
$I(X;Y)$	Mutual Information Between X and Y
N_R	Number of Antennas at Primary Receiver
N_P	Number of Primary Receivers
N_c	Fixed Number of Selected Antennas
ρ_R	Correlation Coefficient of Interference Channel
ρ_B	Correlation Coefficient of Main Channel

Symbol	Description
ρ_E	Correlation Coefficient of Eavesdropper's Channel
$F_R(.)$	CDF of Random Variable R
$f_R(.)$	PDF of Random Variable R
R_e	Equivocation Rate
$\mathbb{H}(S^k\|Z^n)$	Conditional Entropy of S^k given Z^n
S^k	Data Sequence of Secret Message
R_s	Target Rate
$R_s, \max$	Largest Secrecy Rate
N_M	Complex Gaussian Noise of Main Channel
N_E	Complex Gaussian Noise of Wiretap Channel
N_0	Noise Variance
α_l	Weighting factors
α_I	Phase Margin
β_1	Variance of the Main channel
β_2	Variance of the Wiretap channel
λ	Variance of PT-Bob link
η	Variance of PT-Eve link
Ω_0	Variance of the Interference Channel
κ	Index of Best Selected Antenna
Φ_M	SINR of the Main Channel
Φ_E	SINR of the Wiretap Channel
ϕ_M	SIR of the Main Channel
ϕ_E	SIR of the Wiretap Channel
γ_M	SNR of the Main channel
γ_E	SNR of the Wiretap channel
C_M	Capacity of the Main channel
C_E	Capacity of the Wiretap channel
C_s	Secrecy Capacity
p	Channel Coefficient of Alice-PR channel with Outdated Constraint

Symbol	Description
ϕ_i	SIR of i^{th} Antenna of Bob
ϕ_j	SIR of j^{th} Antenna of Eve
$U(m,n,z)$	Tricomi Confluent Hypergeometric Function
${}_2F_1(m,n;p;x)$	Gauss Hypergrometric Function
h_{j0}	Channel Gain between j^{th} Antenna of Alice and PR
h_{p0}	Channel Gain between Alice and p^{th} PR
α	Path Loss Exponent

List of Abbreviations

Abbreviation	Description
AF	Amplify-and-Forward
AN	Artificial Noise
ASC	Average Secrecy Capacity
AWGN	Additive White Gaussian Noise
CBS	Cognitive Base Station
CDF	Cumulative Distribution Function
CR	Cognitive Radio
CRN	Cognitive Radio Network
CSI	Channel State Information
CJ	Cooperative Jamming
DF	Decode-and-Forward
DSA	Dynamic Spectrum Access
EGC	Equal Gain Combining
FCC	Federal Communication Commission
GSC	Generalized Selection Combining
IoT	Internet of Things
MISO	Multiple-Input-Single-Output
MIMO	Multiple-Input-Single-Output
MRC	Maximal Ratio Combining
NOMA	Non-Orthogonal Multiple Access
OAS	Optimal Antenna Selection
PDF	Probability Density Function

Abbreviation	Description
PNZC	Probability of Non-zero Secrecy Capacity
PLS	Physical Layer Security
PR	Primary Receiver
PT	Primary Transmitter
PU	Primary User
QoS	Quality of Service
RF	Radio Frequency
RAS	Receive Antenna Selection
SAS	Sub-optimal Antenna Selection
SC	Selection Combining
SISO	Single-Input-Single-output
SOP	Secrecy Outage Probability
SINR	Signal-to-Interference Plus Noise Ratio
SNR	Signal-to-Noise Ratio
SIR	Signal-to-Interference Ratio
SR	Secondary Receiver
ST	Secondary Transmitter
SU	Secondary User
TAS	Transmit Antenna Selection
TBF	Transmit Beamforming
V2X	Vehicle-to-Everything

Chapter 1

Introduction

The scarcity of the radio frequency (RF) spectrum rises day by day with the progress in the number of intelligent wireless devices along with new applications such as streaming video, the internet of things (IoT), and device-to-device communication. It is because the traditional fixed-spectrum allocation schemes do not utilize the spectrum resources efficiently. Many investigations have revealed that most of the authorized RF spectrum bands are not used efficiently in the time and space domain [1, 2], which results in unused "white spaces" or "spectrum holes" in the time-frequency grid at any particular location. According to the Federal Communications Commission (FCC), temporal and geographical variations in the assigned spectrum's utilization range from 15% to 85% [3]. Additionally, the fixed spectrum allocation policies do not allow the unlicensed user (secondary user or SU) to utilize the rarely used spectrum of the licensed user (primary user or PU). This problem, associated with the rapidly increasing radio spectrum demand for wireless services, has led to spectrum scarcity for wireless applications. Hence, it has required a new communication model, i.e., cognitive radio (CR), to utilize the radio spectrum efficiently, and it allows SUs to use the vacant spectral bands of PUs opportunistically [4]. Although, this opportunistic access should be in a way that does not infringe any process of PUs in the band. Therefore, SUs must be cognizant of the PU's activity in the target band. SUs should recognize the spectrum holes and the idle state of the PUs to utilize the free bands and hastily leave the spectrum band as soon as the PU becomes active. CR embraces this experience by dynamically cooperating with the environment and modifying the operating parameters to exploit the unused spectrum without interfering with the PU [4, 5]. It is an intelligent wireless communication introduced by J. Mitola in 1999 [5] in which a transmitter can sense the radio frequency environment, adjust its transmit parameters (i.e., carrier frequency,

bandwidth, and transmission power) to optimize spectrum usage, and modify its transmission and reception accordingly. Spectrum pooling is an example of an opportunistic spectrum access method that provides public access to authorized frequency bands [6]. The broadcasting nature of the cognitive radio causes various difficulties for guaranteeing secure communications in the presence of sturdy eavesdroppers. Due to its broadcasting nature, it becomes tough to shield the transmitted signals from unauthorized receivers. The eavesdropper tries to elicit the confidential information transmitted by the secondary transmitter (ST) to the legitimate receiver [7]. Traditionally, in all communication systems, the issues of authentication, confidentiality, and privacy are controlled in the upper layers of the protocol stack using variations of private-key and public-key cryptosystems. These cryptosystems are generally based upon mathematical operations, believed challenging to perform for an attacker with limited computational power; hence, we refer to the security provided by these systems as computational security. While computational security has proven its effectiveness to secure data, it may not be easy to implement in some emerging network architectures with limited computational power. In contrast with the established practice of computational security, many results from information theory and cryptography suggest that there is much secrecy to be gained by accounting for the imperfections of the physical layer when designing secure systems. The study of models, methods, and algorithms that aim at strengthening the security of communication networks by utilizing the properties of the physical layer has developed into a dynamic research area, colloquially known as physical layer security (PLS) [8]. PLS also complements and supports the existing cryptographic techniques. This chapter presents an overview of a cognitive radio network (CRN), fundamental aspects of PLS, and main contributions of the thesis.

1.1 Cognitive Radio Network

Conventionally, the wireless systems employ a static spectrum allocation policy, which means that government agencies allocate spectrum bands to PUs for large geographical regions. However, these allocated spectrum bands are not adequately utilized by PUs. Hence, this policy faces a spectrum scarcity problem due to the rise in spectrum demand. It necessitates the development of dynamic spectrum access techniques (DSA) that allow SUs to temporally use the unused licensed spectrum and solve the spectrum scarcity issue [9]. Hence, more manageable and comprehensive utilization of available spectrum is possible by using CR technology [1]. CR

permits the wireless networks to utilize the radio spectrum more efficiently in an opportunistic manner without interfering with PU's activities. CR can adjust its transmission parameters according to the interactions with the environment in which it works. It can provide cognitive capability and reconfigurability to users [4, 9]. Cognitive capability refers to sensing and gathering information such as transmission frequency, bandwidth, power, modulation, etc., from the surrounding environment. With this capability, SUs can recognize the best available spectrum. Reconfigurability refers to immediately adjusting the operational parameters according to the sensed information to attain optimal performance. By opportunistically exploiting the spectrum, CR allows SUs to sense which portion of the spectrum is available or not, pick the best available channel, coordinate spectrum access with other users, and vacate the channel when a PU reclaims the spectrum usage [10].

1.1.1 Cognitive Radio: Definitions

The concept of CR was introduced by J. Mitola [5]. It was a novel technique to define intelligent radios that can automatically make decisions utilizing gathered information about the RF environment through model-based reasoning and learn and adapt according to their experiences. Since its introduction, various regulatory bodies have provided different definitions of the CR. J. Mitola defines the CR in [11] as:

"*A really smart radio that would be self-RF- and user-aware, and that would include language technology and machine vision along with a lot of high-fidelity knowledge of the radio environment*."

S. Haykin defined CR in [4]:

"*Cognitive radio is an intelligent wireless communication system that is aware of its surrounding environment (i.e., outside world), and uses the methodology of understanding-by-building to learn from the environment and adapt its internal states to statistical variations in the incoming RF stimuli by making corresponding changes in certain operating parameters (e.g., transmit-power, carrier-frequency, and modulation strategy) in real-time, with two primary objectives in mind: (i) highly reliable communications whenever and wherever needed; (ii) efficient utilization of the radio spectrum.*"

CRs can generally sense their operating environment and adjust their parameters to attain the best performance. In this thesis, we assume that a CRN permits the concurrency of primary and secondary networks in the same frequency band while fulfilling spectrum sharing constraints.

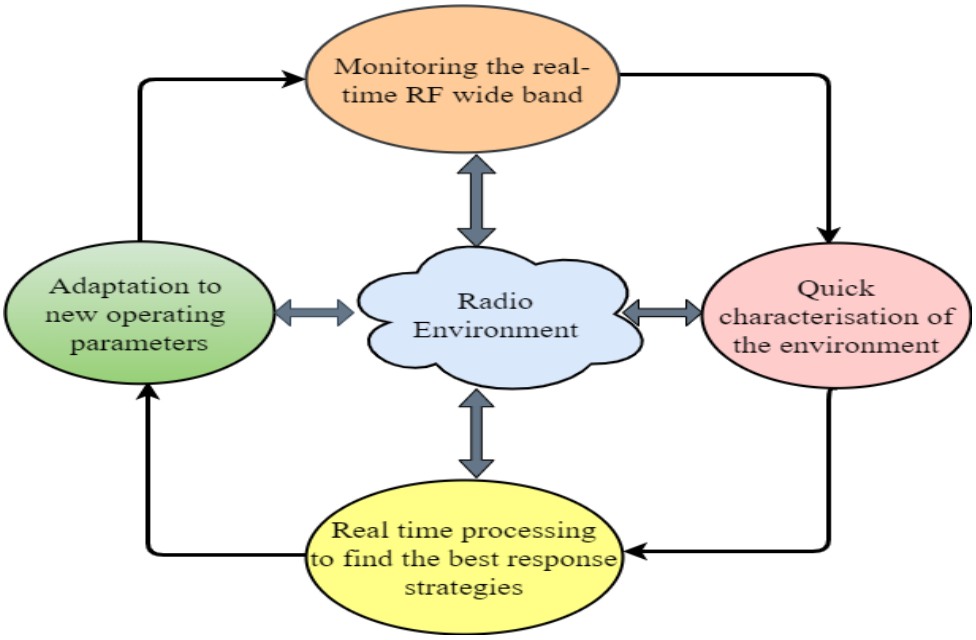

Figure 1.1: Basic cognitive cycle (adapted from [12])

1.1.2 Functions of Cognitive Radio

The main functions of CR are detecting the white space of the spectrum, picking the best frequency bands, organizing spectrum access with other users, and relinquishing the frequency band when a PU appears, as demonstrated by Figure 1.1. The following functions support a cognitive cycle:

- spectrum sensing and analysis;
- spectrum management and handoff;
- spectrum allocation and sharing.

CR can detect the spectrum hole and utilize that frequency band for its communication. On the other hand, when PU begins using the licensed spectrum again, CR can identify their activity through sensing to generate no interference from SUs' transmission. After recognizing the spectrum holes through sensing, spectrum management and handoff function of CR allows SUs to determine the most suitable spectral band according to the time-varying channel characteristics to satisfy various quality of service (QoS) requirements [12]. For example, when a PU reclaims its spectral band, the SU using that band can shift its transmission to another available spectral band, according to the channel capacity determined by the noise and interference levels, path loss, channel error rate, and holding time. In DSA, a SU may share the spectrum resources

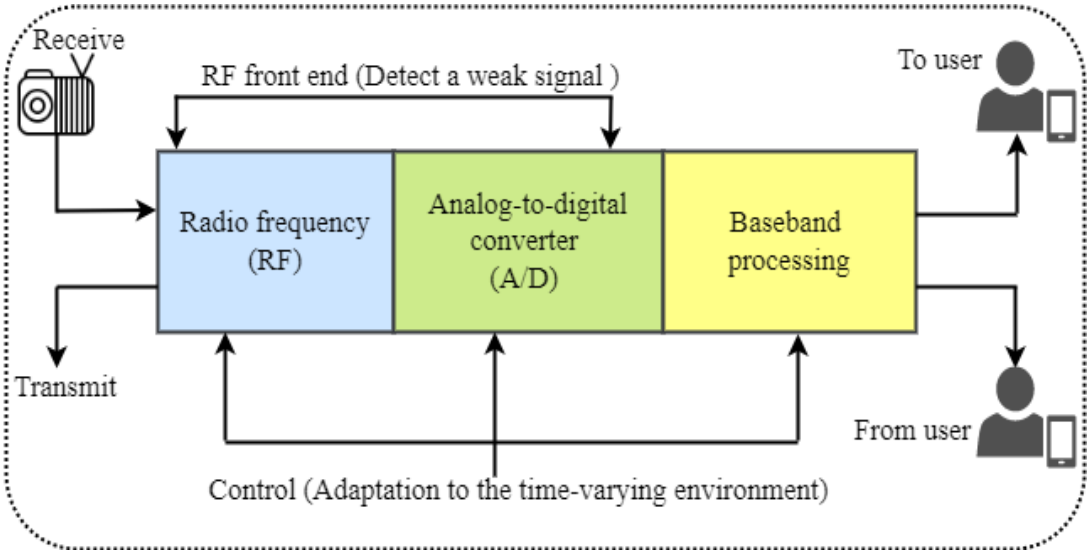

Figure 1.2: Cognitive radio transceiver architecture (adapted from [9, 13])

with PUs, other SUs, or both. Hence, a flexible spectrum allocation and sharing mechanism are essential to achieving high spectrum efficiency. Since PUs own the spectrum rights, when SUs co-exist in a licensed band with PUs, the interference level due to SUs to PUs should be limited by a certain threshold.

To perform these functions, CR needs an RF transceiver. The main elements of a CR transceiver are the RF front-end and the baseband processing unit, as shown in Figure 1.2. The received signal is amplified, mixed, and analog-to-digital (A/D) converted in the RF front-end, then it is modulated/demodulated in the baseband processing unit. All elements of the CR transceiver can be reconfigured via a control bus to adapt to the time-varying RF environment. The main segment of the CR transceiver is the wideband RF front-end that can simultaneously sense the white space over a wide frequency range. This functionality is associated mainly with RF hardware technologies, such as a wideband antenna, power amplifier, and adaptive filter. The RF hardware for the CR should be tuned to any part of an extensive range of the spectrum. However, because the CR transceiver acquires signals from various transmitters operating at different power levels, bandwidths, and locations, the RF front-end should have the ability to identify a weak signal in an extended dynamic range is a significant challenge in CR transceiver design [2].

1.1.3 Spectrum Access Techniques

DSA technique permits the SUs to access the primary spectrum either without rendering any interference to the PUs or the interference caused by the SU to the PU is kept below a prede-

termined interference limit [14]. Depending on the spectrum access policy and applications, DSA approaches can be broadly categorized into three access mechanisms [4, 14], namely, exclusive use mechanism, open sharing mechanism, and hierarchical access mechanism as shown in Figure 1.3.

1.1.3.1 Exclusive Use Mechanism

The exclusive use mechanism supports the current spectrum regulation policy and includes flexibility to enhance spectrum utilization efficiency. Usually, the licensed spectrum is not fully utilized by authorized users all the time. Thus, the licensees can lease those underutilized spectra to a third party under an agreement. The dynamic exclusive use mechanism can be implemented by employing two approaches, i.e., spectrum property rights and dynamic spectrum allocation [14]. The spectrum property rights procedure permits licensees to sell and trade spectrum, driving the most booming economy and market of the limited radio resources. Although licensees can share the spectrum for profit, the regulatory policies do not mandate this spectrum-sharing approach. The dynamic spectrum allocation aims to enhance spectrum utilization using DSA by exploiting various spatial and temporal traffic statistics services.

1.1.3.2 Open Sharing Mechanism

The open sharing mechanism is also known as spectrum commons, where anyone can access any range of spectrum without any approval under consideration of a minimum set of rules from technical standards required for sharing spectrum. However, the usage of this mechanism can render unmanageable interference among users.

1.1.3.3 Hierarchical Access Mechanism

The hierarchical access mechanism aims to open licensed spectrum to SUs while restricting destructive interference to the PUs. This mechanism has an access priority between the PUs and SUs. Compared to the exclusive use and open sharing mechanisms, the hierarchical mechanism may be the most favorable solution for improving spectrum utilization. In this context, three spectrum sharing approaches have been considered, i.e., overlay, underlay and interweave techniques [16].

i) **Overlay Mode:** The PUs share their signal codebooks and messages in overlay mode with the SUs. Additionally, the SUs may use these messages to improve the performance

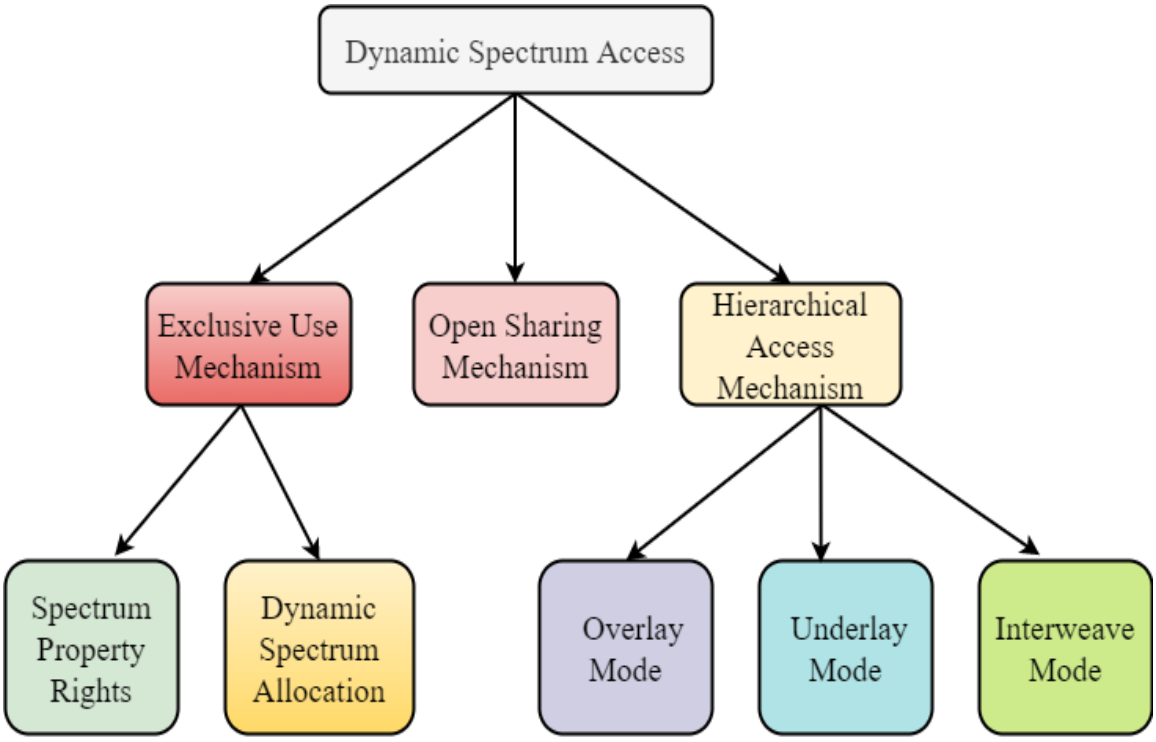

Figure 1.3: Schematic diagram of different dynamic spectrum access approaches (adapted from [15])

of the primary transmission through relaying the primary message to the primary receiver (PR). The overlay mode can enhance the performance of both primary and secondary networks. However, in practice, a technical challenge of the overlay paradigm is the required knowledge of the PU messages at the ST and the encoding and decoding complexity associated with SUs transmissions in the system. Moreover, sharing PU's private information with the SUs increases the security concerns for the primary system.

ii) **Underlay Mode:** The underlay mode of spectrum sharing is based on interference management, where an interference constraint is levied on the SUs' transmit power. Both PU and SU are allowed to communicate in the same frequency band as long as the interference rendered by SUs to the primary receiver is held below a predefined threshold [16, 12]. Our thesis focuses on the underlay approach since it is the most flexible and satisfies interference constraints. In practice, the underlay spectrum sharing technique may be executed through band manager coordination [17] or under a regulator's supervision [18]. Although, the secondary communication range is limited due to the constraints on its transmission power.

iii) **Interweave Mode :** In the interweave paradigm, the SUs access the licensed spectrum

during idle periods of the PUs. The SU must stop its transmission when the PU is active to avoid destructive interference to the PU. The interweave mode depends on spectrum sensing techniques where SUs need to sense the licensed frequency band and detect the spectrum holes. Once a spectrum hole is identified, the SU can transmit with maximum power. However, in the highly time-variant radio environment, sensing imperfections may happen because of channel uncertainty, noise uncertainty, sensing interference, and limited observation time. In this case, a false alarm may result in lost chances and thus lower spectrum utilization. In addition, the ST may cause destructive interference to the PR in case of missed detection, which results in degradation of primary network performance. Moreover, the interweave approach does not allow SUs to coexist with PUs in the underutilized spectrum. Nevertheless, this paradigm is inadequate in dense areas due to the scarcity of spectrum holes.

1.1.4 Applications of Cognitive Radio Networks

CRN aims at enhancing spectrum utilization by allowing a SU to utilize underutilized spectrum resources held by government and commercial users. RF bands allotted to PUs could be shared with SUs under certain restrictions. CR technology is already being applied to some communication systems like WiFi networks and Bluetooth [12, 19]. However, there is growing demand for such opportunities to include other specific frequency bands employed for other services. Some applications of CRN are summarized as follows:

1. **Cellular Networks:** The traffic load of current wireless networks increased with the arrival of smartphones, social networks, and media websites. It provides both an opportunity and a challenge for cellular service operators [20]. Allowing cellular networks like WCDMA and LTE to dynamically access the TV bands can facilitate cellular networks to fulfill traffic demand. It can be implemented, for instance, by using cognitive femtocells [21] and licensed shared access [12].

2. **Mesh Networks:** Wireless mesh networks are developing as a cost-effective solution for providing broadband connectivity [22]. The challenge for traditional wireless mesh networks is the higher bandwidth required to meet the applications as the network density increases. Since the CR technology alleviates the bandwidth scarcity, cognitive mesh networks can provide broadband access in dense urban areas.

3. **Military Communication:** In military communication networks, attaining reliable and secure communications is challenging. Also, the capacity of military networks is limited because of requirements of significant bandwidth for communications between soldiers, armed vehicles, and other units on the battlefield amongst themselves and with the headquarters. The CRN is a promising technology to satisfy bandwidth and reliability needs for such densely deployed networks [23], [24].

4. **Public Safety and Emergency Networks:** Natural disasters may temporarily terminate existing communication infrastructure because some base stations of cellular networks fall, and existing WLANs are broken. Consequently, the connectivity between sensor nodes and the sink node in wireless sensor networks is lost. Thus, an emergency network needs to be established. In addition, this emergency communication also requires a significant amount of radio spectrum for carrying a volume of traffic, including voice, video and data. Since a CR can identify spectrum availability and reconfigure itself, CRNs can be used for such emergency networks [12], [25]. Further, CRNs can promote interoperability between different communication systems by adapting another network's requirements and conditions.

5. **Leased Networks:** Dynamic spectrum leasing presumes a monetary reward for PUs for accepting spectrum sharing with the SUs [26]. Here, a primary network can benefit from leasing a fraction of its licensed spectrum to secondary networks. As a CR is a radio device capable of learning and adapting to its RF environment, it makes an ideal platform for leased networks.

1.2 Underlay Cognitive Radio Networks

An underlay cognitive radio network consists of a primary network and secondary network that coexist in the same spectrum band. A primary network is an existing licensed network operating in a particular spectrum band. Primary networks can either be a centralized infrastructure or distributed ad-hoc in nature. The PUs have priority to spectrum access. On the other hand, the SUs opportunistically access the primary spectrum while adhering to the restrictions imposed by the PUs [15]. In underlay CRNs, for reliable communication in the primary network, the transmit power of ST is constrained so that it could not cause any interference to the primary network.

1.2.1 Spectrum Sharing Constraint

In an underlay CRN, the efficiency of spectrum utilization can be improved by allowing the SU and PU to transmit concurrently in the same frequency band provided that the interference caused by the ST to PR is maintained under a predefined acceptable interference constraint [16]. The allocation of ST's transmit power is the most important concern to meet the interference power constraints. In general, the ST power control needs knowledge of the channel state information (CSI) between the ST and PR link. In the context of the interference power concept and depending on the availability of the PR's CSI at the ST, two main categories of interference constraints have been studied in the underlay CRN literature, namely, peak interference power constraint [27, 28, 29] and PU outage constraint [30].

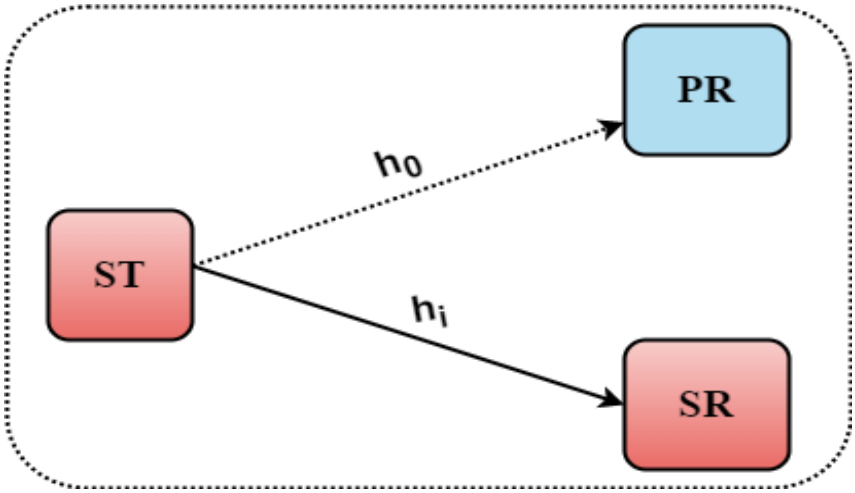

Figure 1.4: The basic model of underlay CRN, (Solid line represents the main channel, dotted line represents the interference channel)

1.2.1.1 Interference Power Constraint

In an underlay CRN, the SU transmits concurrently in the same spectrum band with PU as shown in Figure 1.4. In Figure 1.4, $|h_0|$ denotes the channel fading coefficient of ST-PR link, $|h_0|^2$ denotes the channel power gain of the ST-PR link. Further, $|h_i|$ denotes the channel fading coefficient of the main channel (the channel between ST-secondary receiver (SR)), and $|h_i|^2$ is the channel power gain of the main channel. In Figure 1.4, the primary transmitter (PT) is assumed to be located far away from SR as in [27, 28], and hence the PT does not cause interference to the SR. For reliable communication, the transmit power of ST must not exceed the interference threshold at the PR. This threshold is expressed in terms of the peak (short-term) or average (long-term) power that can be tolerated by the PR [28]. In the case of the peak

interference constraint, we have [31]

$$\bar{P}_A\left(|h_0|^2,|h_i|^2\right)|h_0|^2 \leq \bar{I}_P, \tag{1.1}$$

where $\bar{P}_A\left(|h_0|^2,|h_i|^2\right)$ is the instantaneous transmit power of the ST for the channel gain pair $\left(|h_0|^2,|h_i|^2\right)$ and $\bar{I}_P$ denotes tolerable peak interference power at the PR. (1.1) indicates that the ST's transmit power is restricted by peak interference power for reliable communication in underlay CNRs. In average power constraint, we have

$$\mathbb{E}\left[\bar{P}_A\left(|h_0|^2,|h_i|^2\right)|h_0|^2\right] \leq I_{pav}, \tag{1.2}$$

where I_{pav} is the average interference power at the PR and $\mathbb{E}(.)$ is the expectation operator.

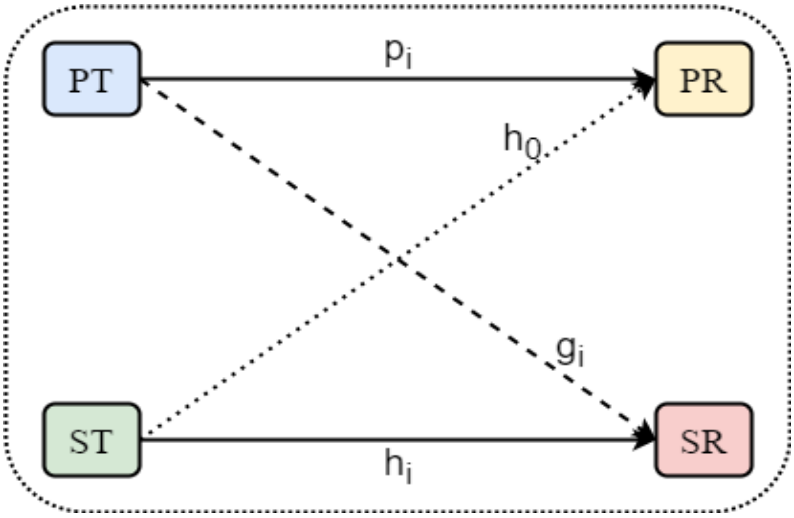

Figure 1.5: A schematic diagram of an underlay CRN where interference from primary transmitter to secondary receivers exist.

In practice, the average interference power constraint can be used to ensure a long-term QoS for the PU if the primary network provides delay-insensitive applications. On the other hand, the peak interference power may be more suitable if the service provided by the PU has an immediate QoS requirement. Using these constraints and assuming that the ST has perfect CSI of PU, the performance analysis of the secondary network in terms of achievable capacity has been investigated in [29]. The availability of $|h_0|$ at the ST can be obtained through a band manager [17] or can be directly fed back from the PR to the SU. The collaboration between primary and secondary networks may be limited; hence, obtaining full CSI of ST-PR channel at the ST is tough.

1.2.1.2 PU Outdated Constraint

In Figure 1.5, an underlay CRN is shown, i.e., PU and SU both transmit in the same spectrum band. The primary network consists of one PT, one PR, and the secondary network consists of an ST-SR pair. In this figure, p_i, h_0, h_i, and g_i represent channel gains of PT-PR, ST-PR, ST-SR, and PT-SR channels, respectively. The peak interference power or average interference power constraints may be helpful when $|h_0|^2$ gains are perfectly known at the ST. Nevertheless, when signal variations for the PT to the PR are random, outage probability becomes a more reliable measure. In particular, the primary outage probability occurs when the signal-to-interference plus noise ratio (SINR) at the PR falls below a certain threshold (different to the peak interference power or average interference power constraints) [32]. As such, the spectrum sharing constraint is based on the acceptable outage threshold at the PR [30, 33]. The PU outage probability in the presence of the SU transmission can be expressed as [33]

$$P_{out}^{PU} = \Pr\left\{\frac{P_P|p_i|^2}{\bar{P}_A|h_0|^2+N_0} \leq \vartheta_T\right\}, \tag{1.3}$$

where P_P denote the PT's transmit power, N_0 is the noise power, P_{out}^{PU} denotes primary outage probability and ϑ_T is the desired SINR at the PR. To protect the PU, the P_{out} must not be greater than its tolerable target denoted by Θ. Thus, the achievable capacity of secondary network subject to the PU outage constraint is expressed as

$$C = \mathbb{E}\left[\log_2\left(1+\frac{\bar{P}_A|h_i|^2}{P_P|g_i|^2+N_0}\right)\right] \tag{1.4}$$

$$\text{subject to } P_{out}^{PU} \leq \Theta. \tag{1.5}$$

The outage constraint may be more practical for PU protection since obtaining the perfect CSI of the ST-PR link is very challenging due to the time-varying property of the ST-PR link. This thesis examines the secrecy performance of underlay CRN under both peak interference power constraint and PU outdated constraint.

1.3 Spatial Diversity Techniques: Basic Concept

In wireless networks, transmission malfunctions happen primarily when the wireless channel in the deep fade, resulting in the so-called communication outage. The wireless network's

performance can be magnified by utilizing diversity techniques in space, time, and frequency domains. These techniques are considered as an effective mechanism to combat the fading in the wireless channel. Spatial diversity can be exploited when the transmitter and receiver have multi-antennas. Spatial diversity techniques are divided into two categories; 1) transmit combining techniques 2) receive combining techniques.

1.3.1 Transmit Combining Techniques

When Alice is equipped with multiple antennas, the data symbols can be distributed among multiple antennas to exploit the spatial diversity at Alice. Here, we assume that Alice is equipped with N_A antennas. Let $\{x[n]\}$ be the sequence of data to be transmitted and assume that the data symbols are independent and identically distributed (i.i.d) over time with zero mean and unit variance. The data is first pre-processed to form transmit symbol vectors $\{s[n]\}$ according to the different transmit combining schemes, where $s[n] = [[s_1[n], s_2[n], ...s_{N_A}[n]]^T$ is the vector of symbols to be transmitted over the N_A antenna in the combining techniques symbol period. The transmitted symbols are assume to satisfy the sum power constraint as

$$\mathbb{E}[|s|^2] = \sum_{l=1}^{N_A} [|s_l[n]|]^2 \leq 1. \tag{1.6}$$

The signal obtained at Bob during the n^{th} symbol period is expressed as

$$y[n] = \sum_{l=1}^{N_A} \sqrt{\bar{P}_A} h_l s_l[n] + w[n], \tag{1.7}$$

where $h_l \sim \mathscr{CN}(0, \sigma_l^2)$ is the channel coefficient between the l^{th} transmit antenna of Alice and Bob, and $w[n] \sim \mathscr{CN}(0, N_0)$ is the additive white Gaussian noise (AWGN). Based upon the availability of the CSI at transmitter, various signal processing schemes can be employed at transmitter to exploit spatial diversity. These are as follows:

1.3.1.1 Transmit Beamforming

In transmit beamforming (TBF), the data in each symbol period is multiplied by a set of weighting coefficients that precompensate for the channel effect before transmission. Let $\alpha_1, \alpha_2 ..... \alpha_{N_A}$ be the weighting factors imposed on the N_A, respectively. The signal transmitted on the l^{th} an-

tenna can be expressed as

$$s_l[n] = \alpha_l x_l[n], \tag{1.8}$$

where the transmission power is $P_l = P_A|\alpha_l|^2$. With the linearly precoding at Alice, the signal received at Bob can be expressed as

$$y[n] = \sum_{l=1}^{N_A} \sqrt{\bar{P_A}} h_l \alpha_l x_l[n] + w[n]. \tag{1.9}$$

The signal-to-noise ratio (SNR) at the Bob is then expressed as

$$\gamma_M = \frac{\bar{P_A}|\sum_{l=1}^{N_A} h_l \alpha_l|^2}{N_0}. \tag{1.10}$$

When the information of channel coefficients $\{h_l\}_{l=1}^{N_A}$) is available at Alice, the set of weighting coefficients $\{\alpha_k\}_{l=1}^{N_A}$ can be picked to maximize the γ_M in (1.10) subject to the power constraint expressed [34]. The optimization problem can be formulated as follows [35]:

$$\max_{\alpha_1 ... \alpha_{N_A}} \frac{|\bar{P_A} \sum_{l=1}^{N_A} h_l \alpha_l|^2}{N_0} \tag{1.11}$$

$$\text{subject to} \sum_{l=1}^{N_A} |\alpha_l|^2. \tag{1.12}$$

By utilizing the Cauchy-Schwartz inequality, we have

$$|\sum_{l=1}^{N_A} h_l \alpha_l|^2 \leq \left(\sum_{l=1}^{N_A} |h_l|^2 \right) \left(\sum_{l=1}^{N_A} |\alpha_l|^2 \right) = \left(\sum_{l=1}^{N_A} |h_l|^2 \right), \tag{1.13}$$

where the equality holds when $\alpha_l = c.h_l^*$, for $l = 1...N_A$. The power constraint in (1.12) can be satisfied by choosing appropriate value of c. Then we have

$$\alpha_l = \frac{h_l^*}{\sqrt{\sum_{l'}^{N_A} |h_{l'}|^2}}, \text{ for } l = 1.....N_A. \tag{1.14}$$

The SNR at Bob with TBF is re-expressed as

$$\gamma_M^{TBF} = \sum_{l=1}^{N_A} \frac{\bar{P_A}|h_l|^2}{N_0}. \tag{1.15}$$

The SNR achieved with TBF is equal to the sum of SNRs between N_A antennas of Alice and Bob, as if each transmit antenna transmits to Bob at different time instants and utilizes the full power $\bar{P}_A$ in each transmission slot. Hence, we can say that TBF achieves an N_A-fold performance gain related to a single-input-single-output (SISO) system. Although TBF can achieve a significant gain in SNR, the need for instantaneous CSI at Alice has limited its use in practical systems.

1.3.1.2 Transmit Antenna Selection

It is assumed that Alice can only get the channel amplitude information very smoothly compared to the channel phase information. Since the phase changes much faster than the channel amplitude; thus, it is more challenging to estimate it. Furthermore, it is not accessible to co-phase all the signals transmitted by the different antennas at Bob without the exact knowledge of phase information. In this situation, it may be more advisable to communicate only on a single antenna with the best channel to circumvent detrimental interference. It is referred to as transmit antenna selection (TAS) scheme [36, 37].

Assume that the $l^{*\text{th}}$ antenna of Alice experiences the highest instantaneous SNR, i.e.,

$$l^* = \arg\max_l \frac{\bar{P}_A |h_l|^2}{N_0} \tag{1.16}$$

and is picked to send signal to Bob so that $\alpha_l = 1$, for $l^* = l$, and $\alpha_l = 0$, for $l^* \neq l$,. The signal received at Bob is

$$y[n] = \sqrt{\bar{P}_A} h_{l^*} x[n] + w[n] \tag{1.17}$$

and the resulting SNR with TAS scheme is given by

$$\gamma_M^{TAS} = \frac{\bar{P}_A |h_{l^*}|^2}{N_0} = \max_l \frac{\bar{P}_A |h_l|^2}{N_0}$$

In the TAS scheme, the channel estimation and antenna selection are performed at Bob, and the index of the best antenna is only carried back to Alice. Depending upon the availability of the CSI at Alice, the TAS is classified as an optimal antenna selection and sub-optimal antenna selection schemes, which are discussed later in this thesis.

1.3.2 Receive Combining Techniques

We can benefit from Bob's spatial diversity to increase the system's performance when Bob is outfitted with multiple antennas. Consider a scenario where single-antenna Alice sends a signal to Bob equipped with N_B antenna. Let $x[n]$ be the transmitted symbol in the n^{th} symbol period and assume that $\mathbb{E}[|x[n]|^2] = 1$. The signal received at the l^{th} antenna of Bob can be expressed as

$$y_l[n] = \sqrt{\bar{P}_A} h_l x[n] + w_l[n]. \tag{1.18}$$

The SNR at l^{th} antenna of Bob is expressed as $y_l = \frac{\bar{P}_A |h_l|^2}{N_0}$. It is assumed that the instantaneous value of the set of channel coefficients is available at Bob. Before making signal detection, Bob will linearly combine the received symbols $y_1[n], y_2[n]..y_{N_B}[n]$ with the corresponding weighting factors $a_1, a_2...a_{N_B}$, to receive the signal $z[n] = \sum_{l=1}^{N_B} a_l y_l[n]$. The value of weighting factors can be measured according to the different combining techniques [35, 38, 39]. Some of these techniques are described as follows:

1.3.2.1 Equal-Gain Combining

In equal gain combining (EGC), signals received at N_B antennas are multiplied by a complex weighting factor that compensates for the phase rotation of the channel [40]. The complex weighting factors are expressed as $a_l = e^{-j\rho_l}$ for $l = 1, 2, ...N_B$. EGC achieves phase coherence at Bob and thus, strengthens the received signal. In the EGC scheme, the magnitude of the weighting factors $|a_l|_{l=1}^{l=N_B}$ are equal and do not depend on SNRs of all links. Hence, it reduces the hardware complexity of the EGC compared to the maximal ratio combining (MRC) method to be discussed later on. The output of the combiner with EGC scheme is expressed as

$$\begin{aligned} z[n]^{EGC} &= \sum_{l=1}^{N_B} a_l y_l[n] = \sum_{l=1}^{N_B} e^{-j\rho_l} \left[\sqrt{\bar{P}_A} |h_l| e^{j\rho_l} x[n] + w_l[n] \right] \\ &= \sqrt{\bar{P}_A} \left(\sum_{l=1}^{N_B} |h_l| \right) x[n] + \sum_{l=1}^{N_B} e^{-j\rho_l} w_l[n]. \end{aligned} \tag{1.19}$$

Hence, the resulting SNR at EGC combiner is written as

$$\gamma_M^{EGC} = \frac{\mathbb{E}\left[|\sqrt{\bar{P}_A} \left(\sum_{l=1}^{N_B} |h_l| \right) x[n]|^2 \right]}{\mathbb{E}\left[|\sum_{l=1}^{N_B} e^{-j\rho_l} w_l[n]|^2 \right]} = \frac{\left(\bar{P}_A \sum_{l=1}^{N_B} |h_l| \right)^2}{N_0}. \tag{1.20}$$

1.3.2.2 Selection Combining

Although the EGC scheme enhances the received SNR at Bob by co-phasing all the signals, in practice, it is usually tough to accomplish due to the rapid change in the phase with time and is hard to track. When the received signals are not perfectly co-phased, their summation may result in harmful interference and loss in spatial diversity. Hence, the alternative strategy is to use the selection combining (SC) scheme where a single antenna with the maximum SNR among available N_B antennas is selected for detection. In this case, the weighting factors can be expressed as

$$a_l = \begin{cases} 1, & \text{if } `\gamma_l > \gamma_l^{'},\ l \neq l^{'} \\ 0 & \text{otherwise} \end{cases} \tag{1.21}$$

. where $\gamma_l = \bar{P_A}|h_l|^2/N_0$. The weight associated with highest SNR antenna is equal to 1 otherwise it is zero. The output SNR at Bob with SC scheme is given by

$$\gamma^{SC} = \max_{l=1,2,.....N_B} \gamma_l. \tag{1.22}$$

The outage performance of the SC scheme in a single-input-multiple-output (SIMO) network is the same as the TAS scheme in a multiple-output-single-input system (MISO) since they get the same output SNR [35].

1.3.2.3 Maximal Ratio Combining

Even though EGC and SC schemes use the CSI to get their weighting factors, they are not optimized in any sense. Hence, to completely utilize the spatial diversity provided by multiple antennas, it is more beneficial to pick weighting factors that maximize the output SNR at Bob, reducing the outage probability. The technique that accomplishes this task is called maximal ratio combining (MRC). The weighting factors with MRC scheme are expressed as

$$a_l = |h_l|^2 e^{-j\phi_l}/\sigma_l^2, \quad \text{for } l = 1,2,...N_B. \tag{1.23}$$

In MRC, the signals are weighted according to their local channel quality and are co-phased to perform coherent addition of the signals at Bob. The output SNR with MRC scheme at Bob is

expressed as

$$\gamma_M^{MRC} = \sum_{l=1}^{N_B} \gamma_l, \tag{1.24}$$

where γ_l is the sum of the received SNRs of all antennas. Thus, we can say that the MRC scheme attains the maximum SNR among all combining schemes.

1.3.2.4 Generalized Selection Combining

The complexity of the MRC and EGC schemes depends on the number of available paths, which can be high for a large number of antennas. Furthermore, MRC is very sensible to channel errors, and these errors serve to be more critical when the instantaneous SNR is low. On the other hand, SC utilizes only one path out of the available ones and hence, does not thoroughly utilize the amount of diversity given by the channel. Therefore, a hybrid technique called generalized selection combining (GSC) is proposed that bridges the gap between SC, EGC, and MRC [39]. It adaptively combines the fixed number of N_c $(N_c \leq N_B)$ high SNR paths among available N_B paths [41]. The output SNR with GSC scheme at Bob is given as

$$\gamma_M^{GSC} = \sum_{l=1}^{N_c} \gamma_l, \;\; l = 1, 2, ...N_B. \tag{1.25}$$

This thesis analyzes the secrecy performance of the SC, MRC, and GSC schemes adopted at either Bob or Eve that will study in the subsequent chapters.

1.4 Physical Layer Security

The wireless networks are extensively employed in civilian and military applications. The transmission of confidential messages has been kept secret from unauthorized users in these networks. However, the security of data transfer in wireless networks is a challenging issue due to the broadcasting nature of their channel. Opponents may try to get illegal access to interrupt the information. Thus, privacy and security are considered a new QoS constraint in wireless network design [42, 43]. Conventionally, the security of wireless communications is mainly handled at the upper layer of the protocol stack using cryptographic techniques. Nevertheless, these cryptographic techniques have become more complex and challenging to implement with the development of ad-hoc and decentralized networks. Therefore, there has been a significant

interest in studying the inherent ability of the PLS to provide secure communications. This paradigm is known as physical layer security. What distinguishes PLS from other high layers cryptographic techniques is that it exploits the wireless channel's randomness and fluctuations to achieve security at a remarkably reduced computational complexity. It incorporates many disciplines and topics, from multiple-input multiple-output signalling techniques minimizing the probability of interception to error-control codes providing information-theoretic secrecy. Information-theoretic security reports back to 1949 when Shannon introduced his pioneer work on cipher systems [44]. Shannon [44] analyses the secure transmission of a secret message when a random secret key is shared between the legitimate parties, and an eavesdropper is trying to intercept the communication. Shannon revealed that the entropy of the shared secret key should exceed the entropy of the transmitted message to attain perfect secrecy. Later on, in 1975, Wyner's work [45] came to sprinkle some positive light on information-theoretic security. Wyner's model, called a wiretap channel, benefits the channel's imperfections to secure transmission at the physical layer without requiring a shared secret key. Since then, investigations of the wiretap channel have increased and have extended to more general communication systems, including broadcast channels, fading channels, multiuser networks, and many other wireless communication models. In particular, the security of fading channels against potential wiretapping attacks is essential, especially regarding the unprecedented growth of wireless communication applications and devices. The fading wiretap channel has uncovered new research objectives for information-theoretic security. What is unique about the fading model is that it benefits from the channel's randomness to secure the transmission against potential Eve at the physical layer itself. Consequently, despite the eavesdropper having a better average SNR than the legitimate receiver, PLS can still be achieved over fading channels without sharing a secret key. To understand the general concept of PLS, we consider a three-node wireless network as shown in Figure 1.6 where the communication between transmitter (Alice) and legitimate receiver (Bob) is being intercepted by an unauthorized node eavesdropper (Eve). The Alice-Bob link is called the main channel, whereas the communication channel between Alice and Eve is referred to as the eavesdropper channel or wiretap channel. When Alice transmits information to Bob, Eve may eavesdrop on their transmission due to the broadcast nature of the wireless medium. Since today's wireless systems are incredibly standardized, Eve can promptly acquire the transmission parameters, including the signal waveform, coding and modulation scheme, and encryption algorithm. Thus, the information could be interpreted at Eve by decoding its

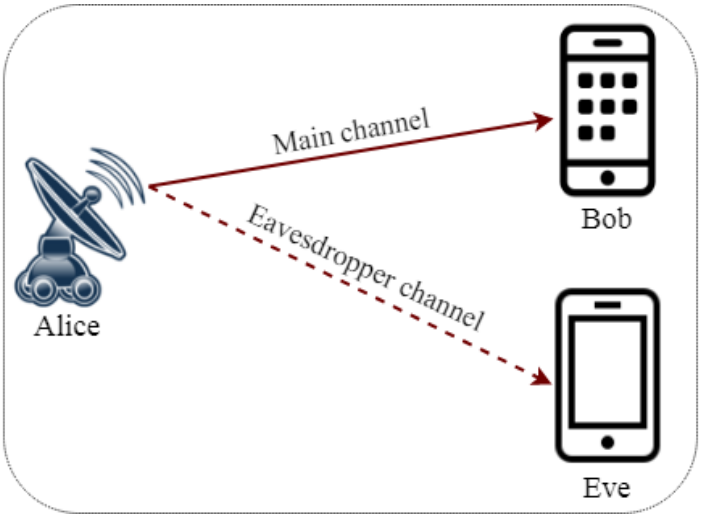

Figure 1.6: A schematic diagram of an eavesdropping scenario in wireless networks

eavesdropped signal, leading to the insecurity of the legitimate transmission. The number of research works on PLS has progressed over the last few years [46]. In the PLS literature, a so-called secrecy capacity is developed and presented as the difference between the capacities of the main link and the wiretap link. It has been confirmed that perfect secrecy is reached if the secrecy capacity is positive, implying that when the main channel capacity is higher than the wiretap channel capacity, the transmission from Alice to Bob can be secure. It can be well described by using the Shannon coding theorem from which Bob cannot recover the signal from Alice if the capacity of the Alice-Bob link is less than the data rate. Therefore, given a positive secrecy capacity, the data rate can be fixed between the capacities of the main and wiretap channels so that Bob successfully decodes the signal transmitted by Alice and Eve fails to decode it. Nevertheless, if the secrecy capacity is negative (i.e., the main channel capacity falls below the wiretap channel capacity), Eve is more likely than Bob to succeed in decoding the transmitted by Alice. In an information-theoretic sense, when the main channel capacity becomes smaller than the wiretap channel capacity, it is difficult to assure that Bob succeeds and Eve fails to decode the signal transmitted by Alice.

1.4.1 Background and Basic model

PLS models usually build upon the model called the wiretap channel studied in [45]. The PLS model is shown in Figure 1.7 consists of a source (Alice) who wants to send information to a legitimate receiver (Bob) while maintaining this information confidential from wire-tapper or eavesdropper (Eve). The Wyner model assumes that the eavesdropper channel or wiretap

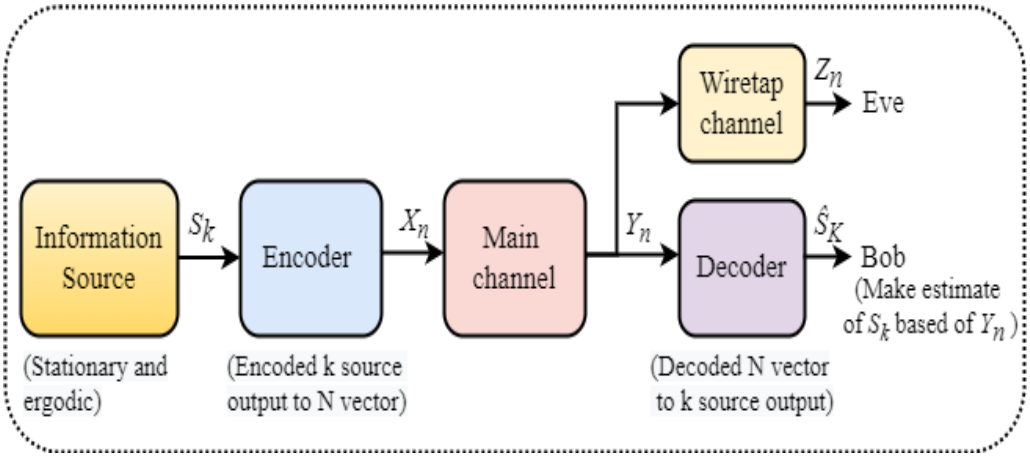

Figure 1.7: The wiretap channel model (adapted from [47])

channel is a degraded version of the main channel. Wyner demonstrated a positive information rate with perfect secrecy if the wiretap channel is noisier than the main channel. The idea in [45] was to utilize the noise of the communication channel along with proper physical layer coding to ensure secure communication. The source is stationary and ergodic and has a finite alphabet. The first k source output S_k encoded into an n vector X_n which is input to the main channel. The legitimate receiver makes an estimate $\hat{S}_k$ of S_k based on the output Y_n of the main channel, incurring a error probability $P_e = \Pr(S_k \neq \hat{S}_k)$, where $\Pr(.)$ denoted the probability. Z_n denotes the observation of wiretapper N-length codewords Y_n gets through the wiretap channel, and Y_n is the output of the main channel. Wyner in [45] proved that reliable and secure communication between Alice and Bob could be made viable by using the corresponding qualities of the main channel and wiretap channel. [45] defined the discrete memoryless wiretap channel, where Eve obtained a degraded version of the legitimate receiver's received signal through a cascaded discrete memoryless channel. The goal of the wiretap channel is to design a coding scheme that makes it possible to communicate both reliably and securely. In this structure, the performance of the coding scheme can be measured in terms of average error probability and equivocation rate [48]. The average error probability indicates the level of secure communication between Alice and Bob. The equivocation rate at Eve marks the secrecy level of confidential message [47]. The uncertainty about the secret message at Eve is measured by the equivocation rate R_e, which is defined as

$$R_e = \lim_{n\to\infty} \frac{1}{n} \mathbb{H}(S_k|Z_n), \tag{1.26}$$

where $\mathbb{H}(S_k|Z_n)$ is the entropy of S_k given the output information Z_n at Eve. The higher the equivocation rate, the less information that Eve obtains about the confidential message S_k. Throughout this thesis, we only focus on the information theoretic perfect secrecy which requires the equivocation rate R_e to be equal to the rate of the message $R_s = \lim_{n\to\infty} \frac{1}{n}\mathbb{H}(S_k)$ as in [48, 49]. Csiszar *et al.,* [49] generalized Wyner's wiretap channel to a large class of channels and obtained the full characterization of the rate-equivocation region.

A critical point on the rate-equivocation region of the wiretap channel is the point where $R = R_e$. It is the largest rate at which Eve receives no information about the message transmitted between Alice and Bob after observing Z_n, i.e.,

$$\lim_{N\to\infty} \frac{1}{n} I(S_k; Z_n) = 0, \tag{1.27}$$

and is called the secrecy capacity, where $I(.;.)$ denotes the mutual information. (1.27) is also referred to as the weak secrecy constraints for the reason that it requires the vanishing only of the rate of the information Eve's observations gets about the message. This constraints can be strengthened to one that vanishes the mutual information

$$\lim_{n\to\infty} I(S_k; Z_n) = 0 \tag{1.28}$$

i.e., the strong secrecy constraint, for variety of channels included in [50]. The secrecy capacity for the general wiretap channel is given as [51]

$$C_s = \max_{p(v,x)} I(V_n; Y_n) - I(V_n; Y_n), \tag{1.29}$$

where $p(v,x)$ denoted the joint probability density function of V and X and V must be satisfy the Markov relation $V_n \to X_n \to (Y_n, Z_n)$.

1.4.1.1 Gaussian Wiretap Channel

The Gaussian broadcast channel in the presence of a potential eavesdropper, Eve, is shown in Figure 1.8. This model is a specific example of the broadcast channel in which the codewords transmitted by Alice are corrupted by additive Gaussian noise under the malicious attempt of Eve. The relationships between inputs and outputs of the channel with Gaussian noise are

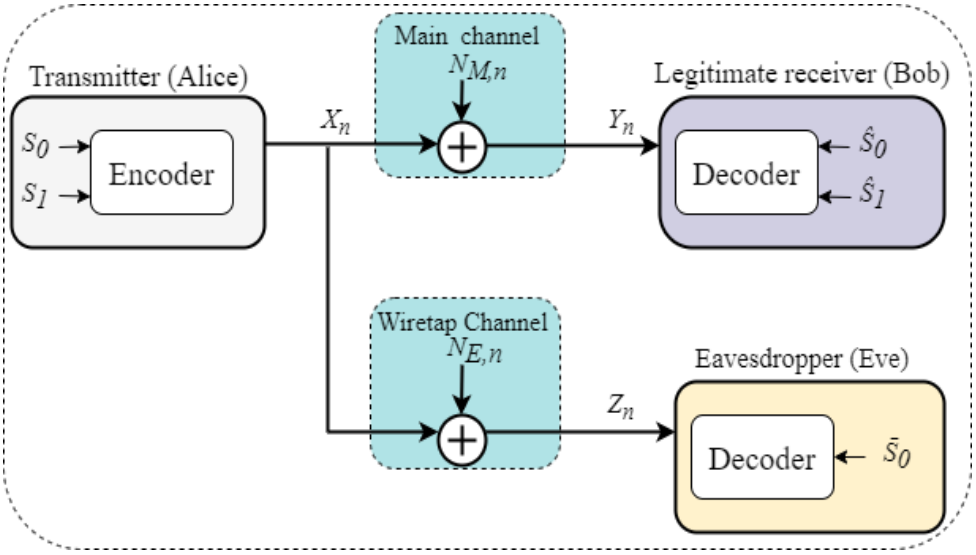

Figure 1.8: Schematic diagram of Gaussian broadcast channel model with secure message [47]

expressed as

$$Y_l = X_l + N_{M,l} \text{ and } Z_l = X_l + N_{E,l}, \tag{1.30}$$

where noise processes $\{N_{M,l}\}_{l\geq 1}$ and $\{N_{E,l}\}_{l\geq 1}$ independent and identically distributed (i.i.d) and

$$N_{M,l} \sim \mathcal{N}(0,\sigma_M^2) \text{ and } N_{E,l} \sim \mathcal{N}(0,\sigma_E^2) \tag{1.31}$$

It is assumed that the statistics of $N_{M,l}$ and $N_{E,l}$ are known to Alice, Bob and Eve before transmission. The input to the channel is subject to a power constraint $\frac{1}{n}\sum_{l=1}^{n} E[X_l^2] \leq \bar{P}_A$, where $\bar{P}_A$ is the transmit power of Alice. The main feature of the Gaussian broadcast channel that makes it more tractable to study than the general broadcast channel is that either wiretap channel is stochastically degraded with respect to (w.r.t) to the main channel or the main channel is stochastically degraded w.r.t to wiretap channel [52]. In the concrete, if $\sigma_E^2 \geq \sigma_M^2$, the channel is characterized as

$$Y_l = X_l + N_{M,l} \text{ and } Z_l = X_l + N_l^{'}, \quad \text{with } N_l^{'} \sim \mathcal{N}\left(0,\sigma_E^2 - \sigma_M^2\right). \tag{1.32}$$

Similarly, if $\sigma_E^2 < \sigma_M^2$, the channel is characterized as

$$Y_l = X_l + N_{M,l} \text{ and } Z_l = X_l + N_l^{''}, \quad \text{with } N_l^{''} \sim \mathcal{N}\left(0,\sigma_M^2 - \sigma_E^2\right). \tag{1.33}$$

The secrecy capacity, C_s of the Gaussian wiretap channel is expressed as [47]

$$C_s = (C_M - C_E)^+ = \left[\frac{1}{2}\log\left(\frac{\bar{P}_A}{\sigma_M^2}\right) - \frac{1}{2}\log\left(\frac{\bar{P}_A}{\sigma_E^2}\right)\right]^+, \tag{1.34}$$

where C_M denotes the capacity of the main link, and C_E denotes the capacity of the eavesdropper channel. The notation $(a)^+$ denotes $\max(0,a)$ and C_s is zero when $\sigma_E^2 < \sigma_M^2$. (1.34) signifies that secure communication is possible if the main channel has better SNR than the eavesdropper's channel. This is likely to happen when Eve is located far away from Alice than Bob. It is noted that C_s does not grow unbounded as $\bar{P}_A \to \infty$ i.e.,

$$\lim_{\bar{P}_A \to \infty} C_s(\bar{P}_A) = \left(\frac{1}{2}\log\left(\frac{\sigma_M^2}{\sigma_E^2}\right)\right)^+. \tag{1.35}$$

Hence, rising P_A results in only marginal secrecy gains beyond a certain point. (1.34) also extend to the complex Gaussian wiretap channel, for which the noise processes are complex and circular symmetric, i.e., $N_{M,l} \sim \mathscr{CN}\left(0,\sigma_M^2\right)$ and $N_{E,l} \sim \mathscr{CN}\left(0,\sigma_E^2\right)$ and can account for constant multiplicative coefficients $h_M \in \mathbb{C}$ (field of complex number) and $h_E \in \mathbb{C}$ in the main and wiretap channels, respectively. A complex Gaussian wiretap channel is equivalent to two parallel real Gaussian channels with power constraint $\bar{P}_A/2$. The secrecy capacity, C_s, of complex Gaussian wiretap channel is given by

$$C_s = \left(\log\left(1 + \frac{|h_M|^2\bar{P}_A}{\sigma_M^2}\right) - \log\left(1 + \frac{|h_E|^2\bar{P}_A}{\sigma_E^2}\right)\right)^+. \tag{1.36}$$

1.4.1.2 Wireless Channel

For ease of exposition, we concentrate on a transmission of a single source message and characterization of the secrecy capacity, but all results expressed there-after generalize to introduce a common message for Bob and Eve. The channel between Alice and Bob is modeled as a fading channel, characterized by a complex coefficient h_M and independent complex AWGN $N_M(N_M \sim \mathscr{CN}(0,\sigma_M^2)$ as shown in Figure 1.9. The coefficient h_M accounts for the multipath interference occurring in wireless transmission and is called a fading coefficient. The square of the magnitude of h_M is called fading gain. Similarly, the eavesdropper's channel is modeled as another fading model with fading coefficients h_E and independent AWGN

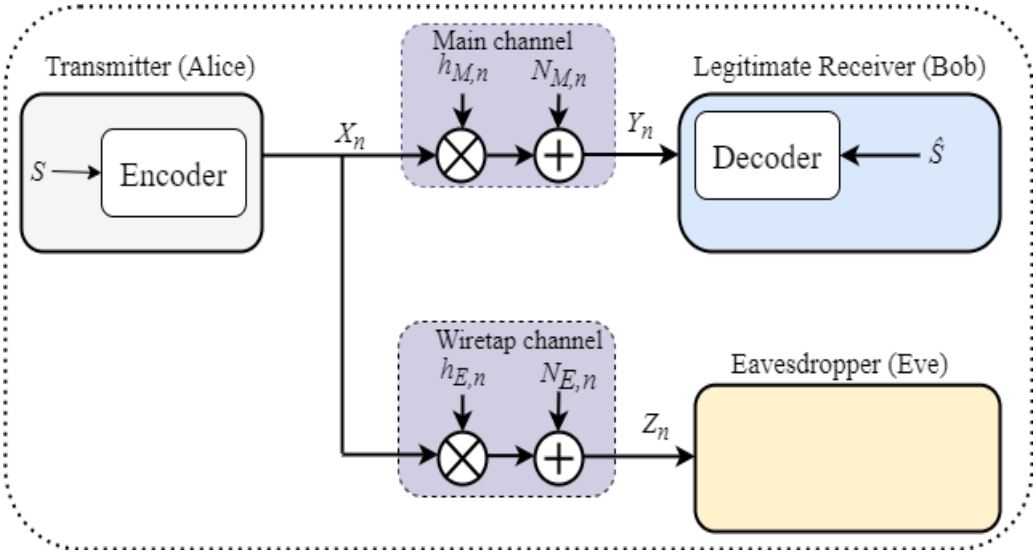

Figure 1.9: A schematic diagram of wireless channel in the presence of an eavesdropper, Eve [48, 53]

$N_E (N_E \sim \mathscr{CN}(0, \sigma_E^2)$. The received signals at Bob and Eve for each channel, l are given by

$$Y_l = h_{M,l} X_l + N_{M,l} \text{ and } Z_l = h_{E,l} X_l + N_{E,l}, \tag{1.37}$$

where $h_{M,l}$, $h_{E,l}$, $N_{M,l}$ and $N_{E,l}$ are mutually independent. Different types of fading can be modeled by selecting the statistics of $\{h_{M,l}\}_{l\geq 1}$ and $\{h_{E,l}\}_{l\geq 1}$ suitably.

Lets consider a particular case of i.i.d Rayleigh fading, for which $\{h_{M,l}\}_{l\geq 1}$ and $\{h_{E,l}\}_{l\geq 1}$ are mutually i.i.d complex Gaussian processes with $h_{M,l} \sim \mathscr{CN}\left(0, \beta_1^2\right)$ and $h_{E,l} \sim \mathscr{CN}\left(0, \beta_2^2\right)$. The fading gains $G_{M,l}$ and $G_{E,l}$ are exponentially distributed random variables with means $\mu_{M,l}$ and $\mu_{E,l}$, respectively which is given as

$$\mu_{M,l} \triangleq \mathbb{E}\left[G_{M,l}\right] = \beta_1^2 \text{ and } \mu_{E,l} \triangleq \mathbb{E}\left[G_{E,l}\right] = \beta_2^2. \tag{1.38}$$

It is assumed that the statistics of $N_{M,l}$ and $N_{E,l}$ is known to Alice, Bob and Eve before transmission. Bob has least instantaneous access to main channel coefficients, $h_{M,l}$ and detects the symbols coherently. Moreover, Eve has access to both $h_{M,l}$ and $h_{E,l}$, so that the information leakage is defined implicitly as

$$\mathbf{L}(\mathscr{C}^n) = \frac{1}{n} I\left(S_k; Z_n | h_{M,n} h_{E,n} \mathscr{C}^n\right), \tag{1.39}$$

where $\mathscr{C}^n$ is the code utilized by Alice.

1.4.2 Relevance of the Wiretap Channel Model

This section addresses the implicit theories essential in the wiretap channel model.

1. **Availability of Channel State Information:** The equivocation of Eve is ensured, provided that the wiretap code used for communication is ideally meant to the main channel. It needs the CSI about the main and the eavesdropper channels to be known at the emitter. The assumption that the CSI of the main channel is correctly known is reasonable since Alice and Bob can always cooperate in characterizing their channel, requiring the CSI of the eavesdropper's channel is more problematic; however, in situations where Alice is a wireless base station, and Eve is a user in the network, the CSI is known at the emitter. Moreover, one can replace the exact CSI with a conservative estimation based on geographical information.

2. **Authentication:** The wiretap channel model inherently believes that the main channel is authenticated. In principle, this assumption is not restrictive since authentication mechanisms can be executed in the upper layers of the protocol stack. It is possible to assure unconditionally secure authentication [54] if a short secret key is available. Typically, the critical size required for authentication scales as the logarithm of the message size; therefore, only a tiny fraction of secrecy capacity needs to be sacrificed to exchange secret keys.

3. **Passive Eavesdropping:** The range of the wiretap channel is restricted to passive eavesdropping policies where the adversary does not tamper with the main or eavesdropper channels. Supplementary techniques are also needed to cope with jamming.

4. **Availability of Random Generator:** Unlike conventional encoders, which are deterministic functions, wiretap encoders are stochastic encoders and rely on the availability of perfect random generators. In general, pseudo-random generators could be used, although their initialization mechanism should be thoroughly considered.

5. **Weak Secrecy:** Security is defined in terms of the equivocation rate $\frac{1}{n}\mathbb{H}(S_k;Z_n)$ and a more satisfying criterion would be to use the absolute equivocation $\mathbb{H}(S_k;Z_n)$. The former notion of information-theoretic security is called weak secrecy, while the latter is referred to as strong secrecy. It is shown in [55] that strong and weak secrecy capacity are equal.

1.5 Motivation

Cognitive radio networks have been considered a promising technique for dealing with spectrum scarcity issues and proving spectrum utilization efficiency by allowing the SUs to transmit simultaneously with the PUs on the same bandwidth via employing overlay, underlay and interweave mechanisms [16, 56, 57]. Among these mechanisms, the underlay CRN is preferable due to its low implementation complexity in the dense areas where the SU are permitted to use the PU's spectrum if the interference to the PUs is below a predefined threshold [12]. The performance of the secondary network is substantially restricted due to the power constraint at the primary network and the impact of large-scale fading. These networks become weaker to severe security attacks and security threats of eavesdropping due to the broadcasting nature of their channel. Traditionally, higher layer cryptographic techniques are used to secure these networks. However, due to the dynamic nature of these CRNs, higher-layer cryptographic authentication and identification have become more expensive and unsafe to potential attacks. In cryptography, codes based on keys are secret sequences of bits only known to Alice or Bob to guarantee the confidentiality of the information transmitted by Alice. The purpose of Eve is to crack the codes used by Alice and Bob, that is, to recover messages from codewords without knowing the keys. The security of encryption schemes is traditionally evaluated in terms of computational security [8] and relies on assumptions restricting the computing resources of Eves. Essentially, computational security guarantees that the amount of computing time or memory required to break a code is unreasonable with today's technology. Usually, a code is regarded as secure if the computational complexity of Eve's decoding algorithm is equivalent to that required for solving complicated mathematical problems. This notion of security is widely used in current cryptographic protocols, but despite being satisfactory in many situations, it fails to guarantee security in the long term. For example, many codes regarded as secure twenty years ago are now easily breakable with modern computers [58]. Consequently, encoding algorithms have to be frequently updated to face the increasing power of modern computers [59]. The advent of wireless networks has fostered mobile ad-hoc networks comprised of many devices with heterogeneous capabilities; the wide range of computing power available in the devices makes it challenging to deploy a public-key infrastructure [60].

In contradiction with the established practice of computational security, many results from information theory and cryptography suggest that much protection is to be obtained by account-

ing for the physical layer's imperfections when designing secure systems. For example, white noise and fading are generally treated as impairments in wireless communications; information-theoretic results confirm that they can be harnessed to protect messages from a potential eavesdropper without requiring a shared secret key [8]. Hence, PLS deals with the study of models, methods, and algorithms that aim at strengthening the security of communication systems by exploiting the characteristics of the physical layer. In addition, PLS is the only solution to secure data transmission without complex cryptographic operations in the enlightenment of the circumstances. It can be acquired by statistically improving the main channel while corrupting all eavesdropper channels. Furthermore, PLS is also a solution to supplement and strengthen the existing cryptographic techniques. Hence, this thesis examines the secrecy performance of the underlay CRN by utilizing different PLS techniques.

1.6 Performance Metrics

The secrecy performance evaluation of the CRN over fading channels may be presented in terms of performance metrics. This section briefly introduces some performance metrics as shown in Table 1.1 that are used in this thesis to analyze the PLS of underlay CRNs.

1.6.1 Secrecy Capacity

The secrecy capacity C_s is the maximum achievable perfect secrecy rate R such that $R = R_e$ [59, 61]. It is defined as the difference between the capacity of the main channel and the capacity of the wiretap channel [48, 43]. The instantaneous secrecy capacity in terms of the SNR of the main channel, γ_M, and the wiretap channel γ_E is given as

$$C_s = \begin{cases} C_M - C_E = \log_2\left(\frac{1+\gamma_M}{1+\gamma_E}\right) & \text{if } \gamma_M > \gamma_E, \\ 0 & \text{if } \gamma_M \leq \gamma_E, \end{cases} \tag{1.40}$$

where C_M is the capacity of the main channel and C_E is the capacity of the wiretap channels. In the case where Bob has no CSI of Eve, C_s can be characterized in terms of secrecy outage probability (SOP) [62], which is discussed in the next subsection. Moreover, from (1.40) it follows that the C_s is positive when $\gamma_M > \gamma_E$. Thus, it is important to compute the probability of non-zero secrecy capacity (PNZC), which is discussed later.

1.6.2 Secrecy Outage Probability

SOP is considered a key performance metric to analyze the PLS in the scenario where CSI of wiretap channel is unavailable at Alice. In this scenario, perfect secrecy is guaranteed when the target rate is less than secrecy capacity, i.e., $R_s \leq C_s$. On the other hand, the information-theoretic security is compromised when $R_s > C_s$ [62, 63]. Hence, SOP is defined as the probability that the C_s falls below the target rate, R_s. Mathematically, one can say

$$P_{out}(R_s) = Pr(C_s < R_s) = \int_0^\infty \int_0^\infty F_{\gamma_M}\left(2^{R_s}(1+x)-1\right) f_{\gamma_E}(x)dx, \tag{1.41}$$

where P_{out} is the SOP, $F_{\gamma_M}(.)$ is the cumulative distribution function (CDF) of γ_M, $f_{\gamma_E}(.)$ is the probability density function (PDF) of γ_E.

Table 1.1: Performance Metrics for Physical Layer Security

Type	Definition	CSI Requirement
Instantaneous performance metrics	Secrecy rate [64, 65]: the rate difference of the main and wiretap channel	Full instantaneous CSI, deterministic outdated CSI
	Secrecy capacity [47]: Maximum achievable secrecy rate	
Statistical performance metrics	Average secrecy capacity (ASC) [66], [67]: the average of the secrecy rate over channel distributions	Statistical CSI, indeterministic outdated CSI
	SOP [62, 68]: the probability that the secrecy capacity drops below some predetermined rate	
	Intercept Probability [69], [70]: the probability that the SNR of main channel drops below the SNR of wiretap channel	
	PNZC [67, 71]: the probability that the SNR of the main channel is greater than the wiretap channel	
Asymptotic performance metrics	Secrecy diversity order [62]: the high SNR slope of the SOP	indeterministic outdated CSI
	Number of degree of freedom [68]: the high SNR slope of average secrecy capacity	

1.6.3 Probability of Non-Zero Secrecy Capacity

It is depicted from (1.40) that C_s is positive when $\gamma_M > \gamma_E$ and is zero when $\gamma_M \leq \gamma_E$ [63]. With the assumption that the main channel and wiretap channel are independent, according to (1.40), PNZC is defined as the probability that the SNR of the main channel is greater than the SNR of the wiretap channel. The PNZC can be expressed as [71]

$$Pr(C_s > 0) = Pr(\gamma_M > \gamma_E) = \int_0^{\infty} \int_0^{\gamma_M} f_{\gamma_M}(x) f_{\gamma_E}(y) dxdy, \tag{1.42}$$

where $f_{\gamma_M}(.)$ is the PDF of γ_M. Note that when $\gamma_M >> \gamma_E$ then $\Pr(C_s > 0) \approx 1$. Contrariwise, when $\gamma_E << \gamma_M$ then $\Pr(C_s > 0) \approx 0$ [63].

1.6.4 Intercept Probability

An intercept event happens when the capacity of the wiretap channel is greater than the main channel's capacity. In this case, an eavesdropper can efficiently decode the source message. In [69], intercept probability is defined as probability that the capacity of legitimate link falls below that of eavesdropper's link i.e.,

$$P_{int} = Pr(C_M < C_E) \ = Pr(\gamma_M < \gamma_E) \ = 1 - Pr(C_s > 0). \tag{1.43}$$

In contrast, SOP is defined as the probability of the difference between C_M and C_E. Hence, the intercept probability is a special case of SOP for $R_s = 0$.

1.6.5 ε-Outage Secrecy Capacity

For a typical delay-limited wireless communication network, ε-outage secrecy capacity is a relevant metric to measure the secrecy performance of the wiretap channels. It is defined as the largest secrecy rate $R_{s,max}$ such that the SOP is equal to ε [67, 72]. Mathematically, it can be expressed as

$$C_{out}(\varepsilon) = R_{s,max}, \tag{1.44}$$

where $P_{out}(R_{s,max}) = \varepsilon$.

1.6.6 Average Secrecy Capacity

ASC is taken as a fundamental performance metric in an active eavesdropping scenario, i.e., CSI of the wiretap channel is known at Alice. It is the average of secrecy capacity C_s over γ_M and γ_E [73]. By recalling the definition of C_s in (1.40), ASC can be expressed as

$$\bar{C}_s = \int_0^\infty \int_y^\infty [\log_2(1+x) - \log_2(1+y)] f_{\gamma_E}(y) f_{\gamma_M}(x) dy dx. \tag{1.45}$$

Using integration by parts, and performing some simple mathematical manipulation, ASC can be written as [67, 66]

$$\bar{C}_s = \frac{1}{\ln 2} \int_0^\infty \frac{F_{\gamma_E}(y)}{1+y} \left[\int_y^\infty f_{\gamma_M}(x) dx \right] dy = \frac{1}{\ln 2} \int_0^\infty \frac{F_{\gamma_E}(y)}{1+y} \left[1 - F_{\gamma_M}(y) \right] dy, \tag{1.46}$$

where $F_{\gamma_E}(.)$ is the CDF of γ_E.

1.7 Contributions and Outline of Thesis

In this thesis, an effort has been made to examine the secrecy performance of underlay CRNs. This thesis has only considered the analysis of the PLS of underlay CRN over different fading models without additional power costs, aiming to increase the main channel's capacity while degrading the capacity of the wiretap channel. This thesis aims to evaluate the secrecy performance of underlay CRNs analytically under spectrum sharing constraints with different diversity combining techniques at Alice, Bob, and Eve. Distinct Alice's transmit power policies are presented, and various interference constraints such as outage constraint or peak interference power constraint imposed by Alice to PR are considered. The channel gains between transmitters and receivers follow either the Rayleigh distribution or Nakagami-m distribution. Numerical analysis and simulations are also carried out to evaluate the secrecy performance of the considered system models. This thesis consists of seven chapters and the main contributions of the remaining chapters are summarized as follows:

Chapter 2 presents the literature review on different physical layer security techniques viz. multiple-input-multiple-output (MIMO) diversity, multiuser diversity, and cooperative diversity. Also, it finds the research gap between these techniques and discusses some well-known work on various PLS techniques such as game theory and machine learning aided PLS.

Chapter 3 considers an underlay CRN consisting of multi-antenna Alice, single-antenna Bob, single-antenna Eve, and single-antenna multiple PRs. Depending upon the availability of the CSI, optimal and sub-optimal antenna selection schemes are adopted at Alice. GSC and MRC schemes are adopted at Bob and Eve, respectively. This chapter analyses underlay CRN's secrecy performance in the presence of multiple PRs under peak interference power constraint in a passive eavesdropping scenario. Closed-form expressions for SOP and intercept probability for the proposed model are derived with the assumption of perfect CSI. The secrecy performance gap between optimal and sub-optimal antenna selection with the GSC scheme is also studied in this chapter.

Chapter 4 considers an underlay CRN that consists of single-antenna Alice and a multi-antenna Bob, multi-antenna Eve, and multi-antenna PR. We assume that the primary channel, main channel, and wiretap channel are outdated in this chapter. We consider SC and MRC scheme at Bob and compare their secrecy performance. MRC scheme is adopted at both PR and Eve. In this chapter, we ignore the interference caused by PT to Bob and Eve. This chapter analyzes the secrecy performance of underlay CRN with peak power constraint for two eavesdropping scenarios, i.e., 1) passive eavesdropping and 2) active eavesdropping. We derive closed-form expressions for SOP, intercept probability, probability of non-zero secrecy capacity, and ε-outage secrecy capacity for passive eavesdropping. On the other hand, for active eavesdropping, we derive a closed-form expression for average secrecy capacity.

Chapter 5 presents the analysis of the secrecy performance of underlay CRN with peak interference power constraint and PU outage constraint. We assume that PT lies in the proximity of the secondary receivers; hence the interference from PT to secondary receives exist, and the quality of interest is SINR. The proposed underlay CRN consists of multi-antenna Alice, single-antenna Bob, Eve, and PR in the presence of a dominant interfere called PT. The optimal antenna scheme is adopted at Alice and secrecy performance for active and passive eavesdropping scenarios analyzed over Rayleigh fading environment. However, CSI on the Alice-PR channel may be outdated due to the time-varying properties or feedback latency from the PU. PR's interference constraint will not be satisfied if Alice allocates transmission power using this outdated CSI. Therefore, we investigate the consequences of the imperfect CSI of the Alice-PR link on the mathematical analysis of various performance metrics by considering the concept of interference outage. Moreover, we also study the PLS of the proposed network when the secondary network's channels are also outdated with an optimal antenna selection scheme at

Alice.

Chapter 6 considers an interference-limited scenario, i.e., the interference from PT is more dominant than noise at the receivers. Hence, the quality of interest is the signal-to-interference ratio (SIR), and these CRNs are called interference-limited CRNs. We examine the secrecy performance of the receive antenna selection scheme in interference-limited CRN, where the antenna that results in the highest SIR at the Bob is chosen to improve the secrecy performance of the secondary transmission. Exact and asymptotic expressions for the SOP and intercept probability are derived over a general fading (i.e., the primary network undergoes Rayleigh fading and the secondary network undergoes Nakagami-m fading) scenario assuming that the CSI on the Alice-PR link is perfect. Extreme value theorem is used to drive asymptotic expression of SOP and intercept probability for a large number of antennas at Bob and Eve. Moreover, the impact of outdated CSI on the secrecy performance of the optimal antenna selection scheme is also studied in this chapter.

Chapter 7 presents the summary of main contributions of this thesis and briefly outlines some possible future directions.

Chapter 2

Literature Review

An eavesdropper can easily hear the communication between legitimate users for the interception in wireless systems, making the wireless transmission extremely defenseless to eavesdropping attacks. Due to the distributed nature of broadcasting channels, security concerns are further intensified and have played a more critical role in spectrum-sharing networks. In underlay CRNs, the primary network and the secondary network can communicate in the same spectrum band simultaneously [29]. In such complicated circumstances, security and protecting the broadcast channel against eavesdropping is a more difficult task. In addition, due to the dynamic nature of these environments, higher layer cryptographic authentication and identification have become more costly and vulnerable to attacks [62]. In the light of the circumstances mentioned above, there has been significant interest in the PLS to secure data transmission without the necessity for complicated cryptographic operations. It enables secure communications by only utilizing the properties of wireless channels, e.g., fading, noise, and interferences, to avoid the use of extra spectral resources and to reduce signaling overhead [49, 74]. PLS techniques aim to strengthen the main channel of the legitimate receiver comparative to the eavesdropper channel for accomplishing perfect secrecy. For this purpose, many diversity combining techniques have been proposed in the open literature to improve the quality of the main channel. Hence, in this chapter, we present various diversity techniques to improve the PLS against potential eavesdroppers. Traditionally, diversity techniques are exploited to increase transmission reliability, which can intensify wireless security. We present the PLS improvement through MIMO, multiuser diversity, and cooperative diversity, respectively. Furthermore, we discuss other PLS techniques like game theory and machine learning aided PLS that shield confidential messages from the wicked attempt of eavesdroppers.

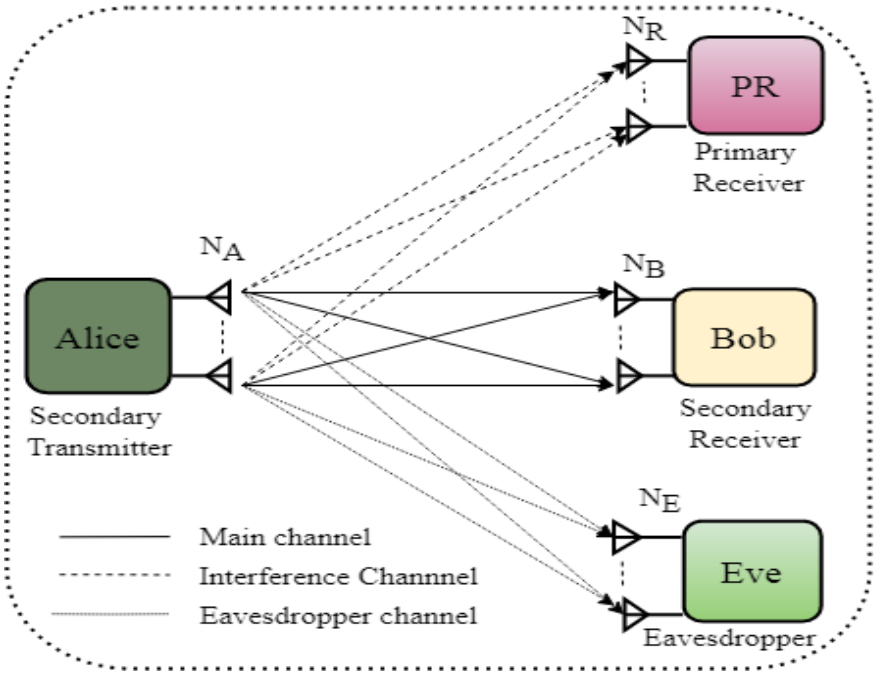

Figure 2.1: An underlay cognitive radio network consisting of a primary receiver (PR), a secondary transmitter (Alice) and a legitimate receiver (Bob) in the presence of an eavesdropper (Eve)

2.1 MIMO Diversity

This subsection shows the MIMO diversity scheme for PLS of underlay CRN against potential eavesdropping attacks. As pointed in Figure 2.1, all the network's nodes are equipped with multiple antennas, where N_R, N_A, N_B, and N_E indicate the number of antennas at the PR, Alice, Bob, and Eve, respectively. MIMO has been acknowledged as an efficacious mechanism to combat wireless fading and enhance the capacity of wireless channels. However, Eve can also utilize the MIMO structure to enhance the capacity of the wiretap channel from Alice to Eve. Hence, it may not be possible to improve a wireless network's secrecy capacity with MIMO without a proper design. For example, if traditional open-loop space-time block coding is considered, Bob should first estimate the main channel matrix H_m and then do the space-time decoding process with an estimated $\hat{H}_m$, the diversity gain to be realized for the main channel. Likewise, Eve can also estimate the wiretap channel matrix H_w and then do the corresponding space-time decoding to achieve diversity gain for its channel. Consequently, the traditional space-time block coding is not sufficient to improve PLS against eavesdropping attacks.

Usually talking, if Alice transmits its signal to Bob with N_A antennas, Eve will also receive N_A signal copies for interception purposes. To shield against a potential eavesdropper, Alice should utilize a preprocess that necessitates being adapted to the main and wiretap channels so

that the diversity gain can only be achieved at Bob, whereas Eve avails nothing from the multiple antennas at Alice. Alice should include an adaptive transmit process to improve the main channel capacity while lowering the wiretap channel capacity. Ideally, such a process points to maximizing MIMO transmission's secrecy capacity, requiring the CSI of the main channel and wiretap links. However, Eve's CSI may be unavailable in practice since Eve is customarily passive and keeps silent. If only Bob's CSI is known, the adaptive transmit process can be devised to maximize the capacity of the main channel, which does not require CSI knowledge of the wiretap channel. Since the adaptive transmit process is optimized based on the main channel's CSI, the main channel's capacity increases with MIMO significantly. The wiretap channel is independent of the main channel; hence, no improvement is achieved in its capacity. As for the adaptive process mentioned above, various transmit combining techniques like transmit beamforming (TBF), transmit antenna selection (TAS) are presented in the open literature. At Alice, TBF and TAS schemes are adopted to enhance the SNR of the main channel. Similarly, at receivers, the different receive combining techniques (e.g., SC, MRC, GSC) combine the multiple signals transmitted through different transmitting paths called diversity branches into a single improved signal. These diverse branches carry the same information with uncorrelated multipath fading. Hence, receive combining techniques are used to decrease the fading effect and improve the SNR of the main channel, which enhances the secrecy performance of the network.

2.1.1 Transmit Beamforming

Transmit beamforming is a signal processing method that combines many transmit antennas at Alice so that desired signals transmit in a particular direction to Bob [75, 76]. Assuming that Eve and Bob usually lie in separate directions corresponding to Alice, the desired signals with TBF received at Eve will undergo disruptive interference and become very vulnerable. Thus, the TBF persuasively defends against eavesdropping attacks by reducing the signal strength at Eve by making use of spatial degrees of freedom [77]. A proper design of TBF is needed to utilize the advantages of multiple-antenna techniques for guaranteeing PLS effectively. When the main and wiretap channels are approximately orthogonal, it is easy to intensify the strength of the main channel and weaken the intercepted signal concurrently by some means. Nevertheless, in general, the signals to Bob and Eve are generated from Alice and pass through the same channel simultaneously; it is impossible to separate them in time and frequency domains. A feasible approach is to utilize the spatial degrees of freedom given by multiple antennas at Alice. As a

simple example, if Alice has global and perfect CSI, it is possible to send a secret message in the null space of the wiretap channel, such that Eve cannot overhear any information [78].

Both linear and non-linear TBF techniques are promising techniques in multi-antenna enabled PLS. Although the beamformer's design can be done according to various criteria, a fundamental purpose is to direct the signal toward Bob's direction while reducing the signal strength at Eve [79]. For example, cooperative secure beamforming is designed to maximize the information rate at Bob while reducing information leakage to Eves [80]. Additionally, cooperative jamming plays an essential role in ensuring data security in two-hop relay systems. In particular, Bob and Alice act as jammers in the first and second hops, respectively [81]. It is commonly comprehended that beamformer and jamming signal designs in multiple-antenna systems depend on the availability of CSI at Alice [82, 83]. Unlike traditional systems without considering PLS, permitting PLS via multiple antennas requires complete knowledge of CSI. Remarkably, the CSI of the main channel and the wiretap channel is needed to facilitate the design of an adequate beamformer since the secrecy rate is determined by the main and the wiretap channels jointly. In other words, the amount of CSI available at the Alice decides the secrecy performance.

It is very challenging to design an optimal beamformer to enable secure communications under general system settings since the objective function of the secrecy capacity is unlikely to be a convex function of the transmit beamformer. Thus, Khisti *et al.* [84] considered a special case, where all three nodes Alice, Bob, and Eve are equipped with multiple antennas, and the capacity of the Gaussian wiretap channel model was analyzed. The associated channel matrices are fixed and known to all three nodes. The characterization of the secrecy capacity is established as the saddle point solution to a minimax problem. To get more insights, Fakoorian *et al.* [85] calculated the rank of the optimal input covariance matrix. In particular, the authors revealed the relationship between rank and channel matrices for Bob and Eve. Furthermore, the authors determined the necessary and sufficient conditions that an optimal input covariance matrix is full rank and presented a method for characterizing the resulting covariance matrix. Even if full CSI is available, it is not easy to design an optimal transmit beamformer. In order to obtain a tractable solution, alternative optimization schemes are proposed accordingly. In [86], the objective function is divided into two components, namely the main channel capacity and the wiretap channel capacity. A suboptimal beamforming scheme was presented by maximizing the main channel capacity subject to a constraint on the wiretap channel capacity. Moreover,

Cumanan *et al.* [87] approximated the secrecy capacity based on a Taylor series expansion and thus transformed the original problem into a tractable convex optimization problem. By considering practical finite-alphabet input, Wu *et al.* [88] developed an iterative algorithm for finding an optimal precoding matrix based on a gradient descent method with a backtracking line search. The main difficulty in designing the optimal beamformer lies in the non-convexity of the secrecy capacity. Another possible way to design a suboptimal beamformer is to replace the nonconvex objective function with other relevant convex performance metrics. The concept of diversity-multiplexing trade-off was also introduced into multiple-antenna secure communications [89]. In the works, as mentioned earlier [87, 87, 89], a design of beamformer was based on the assumption of full CSI at Alice. However, in a practice scenario, Alice typically obtains only partial CSI through information feedback from Bob [96, 97] in frequency division duplex systems or directly using channel reciprocity [98] in time division duplex systems. Indeed, the exactness of CSI has a significant impact on the performance of multiple antenna systems. There are high chances of information leakage to Eve when Alice has imperfect CSI, resulting in secrecy performance degradation [99]. Thus, it is necessary to design robust beamforming schemes to conquer performance degradation. Chu *et al.* [90] proposed a robust beamforming scheme to maximize the secrecy rate, subject to maximum SOP and maximum transmit power constraints with the assumption that partial CSI of Eve is available. Furthermore, a semidefinite programming approach was used to solve a robust beamforming optimization problem in a scenario that both Bob and Eve CSI are imperfect [91].

According to the definition of secrecy capacity given in (1.40), the secrecy capacity is a decreasing function of the interception distance between Alice and Eve. A challenging issue in ensuring PLS occurs if Eve is located closer to Alice than Bob, namely short-distance interception. In these circumstances, even if spatial beamforming is used, the secrecy performance may not be sufficient. Hence, artificial noise (AN) is incorporated in the transmit signal deliberately to distract Eve, enhancing the data security further [100]. The main principle of AN design is to avoid interference leakage to Bob while impairing the intercepted signal at Eve. Hence, the AN is adopted in association with multiple-antenna techniques to enhance PLS. Particularly by exploiting spatial degrees of freedom granted by multiple transmit antennas, it is possible to adapt the directions of AN and the transmit signal jointly through spatial beamforming to optimize the secrecy performance [101], [102]. The accuracy of CSI determines the performance of AN at Alice. If Alice has full CSI, maximum spatial degrees of freedom are available to design the

Table 2.1: Transmit Beamforming Techniques for Secure Communication

Type of beamforming	Authors	System Model	Contribution
Beamforming with full CSI	A. Khisti *et al.* [84]	Multi-antenna Alice Bob and Eve	Transmit signal is coded based on Gaussian wiretap codebooks
	S.Fakoorian *et al.* [85]	Multi-antenna Alice, Bob and Eve	Derived the rank of optimal solution to achieve the secrecy capacity under power constraint
	Y.Wu *et al.* [88]	Multi-antenna Alice, Bob and Eve	Investigated linear precoding design to maximize the secrecy rate under constraint of finite alphabet input
	Z Rezki *et al.* [89]	Multi-antenna Alice, Bob and Eve	Achieved finite SNR diversity multiplexing trade off with zero forcing transmit scheme
	K Cumanan *et al.* [87]	Multi-antenna Alice, Bob and Eve	Proposed iterative algorithm to solve secrecy rate optimization problems
Robust Beamforming	Z Chu *et al.* [90]	Multi-antenna Alice, Bob and Eve	Optimized the secrecy rate with robust beamforming technique
	Q. Li *et al.* [91]	Multi-antenna Alice & Eves and single antenna Bob and Eve	Developed a robust transmit design by semi-definite programming
	S Bashar *et al.* [92]	Multi-antenna Alice & Eve, and single antenna Bob	Investigated the effect of codebook based transmit beamforming
Artificial-noise-aided beamforming	X Zhou *et al.* [93]	Multi-antenna Alice, single antenna Bob and multiple Eves	Obtained expression of achievable secrecy rate
	X Zhang *et al.* [94]	Multi-antenna Alice, single antenna Bob and Eve	Provided power allocation rate parameter of wiretap code for achieving maximal throughput
	Y Yang *et al.* [95]	Multi-antenna Alice, Bob and Eve	Investigated the impact of delayed CSI on PLS by using TBF and AN schemes

beamformer. However, in practice, Eve's CSI is usually imperfect or even unavailable. Tang *et al.* [103] proposed a robust beamforming scheme to maximize the worst-case secrecy rate via semidefinite programming with imperfect CSI of the main and wiretap channel. Further, to relax the assumptions of an imperfect CSI, Wang *et al.* [66] considered a case of perfect CSI of the main channel and statistical distribution of the wiretap channel for MISO secure communications. They suggested a beamforming scheme and the corresponding optimal power allocation between the transmit signal and AN to maximize the achievable secrecy rate. Zhou *et al.* [93] and Zhang *et al.* [94] analyzed the secrecy performance and designed the corresponding power allocation scheme over fast and slow fading channels, respectively. In slow fading channels, the channel coherence time is usually longer than the length of a codeword. In such a scenario, SOP is adopted as the performance metric. In contrast, in fast fading channels, the channel coherence time is much shorter than the length of a codeword, and the ergodic secrecy rate becomes a more appropriate performance metric. It is worth noting out that AN does not have to be necessarily sent by Alice. In practice, AN can also be transmitted by Bob [104]. In this scenario, the CSI feedback for AN's design is not required, significantly lessening overhead. A problem of this scheme is the self-interference caused by Bob, which reduces the signal reception performance. Fortunately, since Bob knows the AN signal prior, it may cancel the interference in the received signal via successive interference cancellation. Moreover, it is possible to transmit the AN from both Alice and Bob to enhance communication security. Table 2.1 gives a summary of all beamforming techniques that are used to enhance data security capability.

2.1.2 Transmit Antenna Selection

As discussed above, the TBF scheme mandates the precise CSI of the wiretap channel or the main channel. It acquires high feedback overhead, and computational cost of signal processing, particularly for a large number of antennas at Alice [105]. Against this background, TAS is applied at multi-antenna Alice to improve security with reduced hardware complexity. TAS is a low-cost, less complex technique to exploit spatial diversity in multiple antenna settings [36, 37]. Bob informs Alice about the best antenna index through an open (non-secure) channel and low rate return channel in the TAS scheme. Although Eve can access the open return channel, it will not exploit this information since Eve has access uniquely to the antenna index and has no CSI of the main channel. This antenna index is optimum for the main link only.

Therefore, Eve is not capable of exploiting any additional diversity from the multiple transmit antenna at Alice [106]. Hence, TAS is adopted at Alice to enhance the PLS with low feedback overhead. Yang *et al.* [107] analyzed the impact of antenna correlation on PLS of MIMO wiretap channel where TAS is employed at Alice and closed-form expressions for exact and asymptotic SOP were derived. In extension to this, [71] analyzed the PLS with TAS scheme in Nakagami-m fading environment with non-identical fading parameters for the main and wiretap channel and derived closed-form expressions for PNZC, SOP, and ε-outage secrecy capacity. [107, 71] considered that the main channel and the wiretap channel are independent. However, when both Bob and Eve are close, the eavesdropper channel is correlated to the main channel. Hence, Ferdinand *et al.* [108] investigated the secrecy performance of MISO wiretap channels with TAS scheme when the eavesdropper channel is correlated with the main channel. The works mentioned above did not consider the impact of the interference caused by the primary network on the secondary network. However, in the practical CRN, the interference from the primary network to the secondary network will affect the performance of the secondary networks. Hence, Hanif *et al.* [109] investigated the performance of TAS with both continuous and discrete power adaptation schemes and derived closed-form expressions for outage probability and diversity order under interference constraints. The secrecy performance of TAS on multiple-input-single-output wiretap channels with correlated main and eavesdropper channels was investigated in [108]. The CSI is outdated or imperfect due to feedback delays, feedback errors, and electromagnetic wave spreading. Therefore, [111] investigated the effect of outdated CSI on the secrecy performance of the MIMO wiretap channel using TAS in a Rayleigh fading environment. Different from the works as mentioned above, [67] proposed a general order TAS instead of best antenna TAS in outdated CSI scenario due to the reason that Sometimes the best channel may be unavailable and busy in other services. In this case, it is possible to transmit on another antenna instead of the best antenna to avoid service interruption. Moreover, general order TAS can reduce the processing complexity at the receiver because the only subset of CSI is sufficient to decide on the suitable transmit antenna to satisfy the QoS.

It is worth mentioning that all studies mentioned above assume the CSI of the main channel available at Alice without knowing the CSI of Eve and select the best antenna that maximizes the capacity of the main channel. This TAS scheme is called sub-optimal antenna selection (SAS) scheme. In contrast to this, Sadeque *et al.* [115] employed the TAS scheme that selects the antenna that provides the maximum secrecy rate with the assumption that instantaneous

Table 2.2: Transmit Antenna Selection Schemes for PLS

Authors	System Model	Contribution
Yang *et al.*[107]	Multi-antenna Alice, Bob and Eve	Analyzed the impact of antenna correlation on PLS of MIMO wiretap channel and derived closed-form expressions for exact and asymptotic SOP
Yang *et al.*[71]	Multi-antenna Alice, Bob and Eve	Considered Nakagami-m fading of main and wiretap channel and derived closed-form expression for SOP and ε-outage secrecy capacity
Ferdinand *et al.*[108]	Multi-antenna Alice, single antenna Bob and Eve	Investigated the secrecy performance MISO wiretap channel when Eve's channel is correlated with main channel
Wang *et al.*[68]	Multi-antenna Alice, Bob and Eve	Derive closed-form expression of SOP for two realistic scenarios:1) Bob is located near Alice, and 2) Bob and Eve located near Alice
Zhu *et al.*[110]	Multi-antenna Alice, Bob and Eve	Proposed OAS and SAS schemes, depending on whether Alice has global CSI of main link and wiretap link for MIMO wireless system
Huang *et al.*[67]	Multi-antenna Alice, multi-antenna Bob and multiple multi-antenna Eve	Proposed general order TAS scheme to improve the PLS of MIMOME wireless system with outdated CSI
Xiong *et al.*[111]	Multi-antenna Alice, multi-antenna Bob and multi-antenna Eve	Investigated secrecy performance of TAS scheme in MIMO wireless network with imperfect feedback
Hanif *et al.*[109]	Multi-antenna Alice, single-antenna Bob, PT and PR	Investigated performance of TAS scheme for power adaptive underlay CR with instantaneous interference constraint
Hanif *et al.*[112]	Multi-antenna Alice, single-antenna Bob, PT and PR	Investigated performance of TAS scheme for discrete power adaptive underlay CR with PT's interference
Blagojevic *et al.*[113]	Multi-antenna Alice, single-antenna Bob, and single-antenna PU	Analyzed performance of underlay CRN with TAS scheme
Lei *et al.*[114]	Multi-antenna Alice, Bob and Eve and multi-antenna PR	Investigated OAS and SAS schemes for MIMO underlay CRN over Nakagami-m channels and also compare them with STT

CSI of both the main channel and the eavesdropper's channel is assumed to be available at Alice. This assumption is required since the construction of codes that ensure secrecy requires the knowledge of the instantaneous capacities of both channels. This scheme is called optimal antenna selection scheme (OAS). Further, [110] explored the OAS and SAS for secrecy performance analysis of MIMO wireless networks and considered PNZC as a performance metric to evaluate the secrecy performance of OAS and SAS schemes. The traditional space-time transmission (STT) scheme is considered as a bench mark and compare the OAS and SAS schemes with STT. Le *et al.* [114] extended this analysis to analyze the PLS of underlay CRNs over Nakagami-m fading scenario and derive the closed-form expressions for SOPs with OAS and SAS schemes.

2.1.3 Receive Combining Techniques

The receiver combining techniques combine the multiple signals received from different paths into a single improved signal. These techniques are used to minimize the fading effect and enhance the SNR at SRs. The most commonly used receive combining techniques used at SRs to enhance the PLS are SC, MRC, GSC. The TAS schemes combines with receive combining scheme improves the PLS of wireless network to great extend.

In SC, the received signal from the antenna that experiences the highest SNR is chosen for processing at the receiver. It is also called receive antenna selection (RAS). SC, unlike TAS, does not require a feedback path from Bob to Alice. SC is the most commonly used technique because it requires a single receive amplifier or allows a single-chip implementation for power and cost reduction. For example, SC is an option in IEEE 802.11n standard for WLANs [116] and is compatible with IEEE 802.16 standard for WiMAX [117]. Elkashlan *et al.* in [62] analyzed the secrecy performance of underlay CRN by adopting SC at both Bob and Eve and presented new closed-form expressions for the exact and asymptotic SOP under peak interference power constraint. Hanif *et al.* [118] studied the performance of underlay CRN for the general and interference-limited scenarios with SC scheme and derived closed-form expressions for SOP. However, SC is not the optimal solution as all the available diversity paths are not utilized. It gives the motivation to use maximal-ratio combining for better security. In MRC, each signal branch is multiplied by a weight factor proportional to the signal amplitude. It is an optimal technique, as signal combining from all branches are co-phased and added to maximize the combined SNR at the receiver. Yang *et al.* [71] adopted either MRC or SC at

Bob and Eve to combined the received signals and derived closed-form expressions for SOP, PNZC, and ε-outage secrecy capacity. The authors in [71] concluded that the highest level of secrecy is achieved when MRC is employed at Bob and SC is adopted at Eve, and the lowest level of secrecy is achieved when SC is employed at Bob and MRC is employed at Eve. Furthermore, [71] also examined the following fundamental question: *"1) What is the performance gap between MRC and SC in MIMO wiretap channels?" and 2) What are the explicit network parameters that determine this gap in Nakagami-m fading?".* Xiong *et al.* in [111], adopted the MRC technique at both Bob and Eve and analyzed the secrecy performance of MIMO wiretap with imperfect feedback. [111] derived closed-form expressions for PNZC and SOP in the case of imperfect feedback due to feedback delay. Prabhu *et al.* in [72] considered a single-input-single-output-multiple eavesdropper (SIMOME) wireless communications system in slow flat Rayleigh fading conditions, where the Eve is equipped with multiple antennas and the SOPs for MRC and SC schemes at Eve are compared. It was revealed that SC at one multi-antenna Eve would have the same effect as that at multiple non-colluding single-antenna Eve. Furthermore, He *et al.* in [119] considered the MRC scheme at both Bob and Eve and derived closed-form expression for SOP in Rayleigh fading environment. The secrecy performance of correlated multi-antenna wiretap channels with SC and MRC are analyzed in [120] and found that when the SNR of Bob is much greater than Eve, the correlation between Bob and Eve has a positive impact on secrecy. In extension to this, [121] investigated the secrecy performance for TAS/MRC scheme in a multi-input multi-output multi-antenna eavesdropper (MIMOME) system assuming that both the antenna correlation and the channel correlation between Bob and Eve. Unlike the existing works, the correlated main channels and eavesdropper channels experience Nakagmai- m fading with distinct fading parameters and are modeled as a combination of conditionally independent channel gains and independent channel gains. [122] analyzed the impact of antenna correlation for a single-input-multiple-output system with the MRC scheme and illustrated that antenna correlation at Bob degrades the secrecy performance, especially in the low average channel gain regime. Singh *et al.* [69] adopted either MRC or SC at Bob and MRC at Eve and analyzed the PLS of underlay CRNs in the presence of multiple PUs with spectrum sharing constraints. [69] also compared the performance gap between SC and MRC schemes in the presence of multiple PR. The presence of multiple PRs induced new challenges to PLS investigation compared with the traditional single PR-based CRN. Recently, Chopra *et al.,* in [123] investigated the secrecy performance of threshold-based CRN under interference

constraint when SC scheme is employed at Eve and derived the outage probability of Optimal relay Selection scheme for a multi-relay system when either the instantaneous channel state information (ICSI) or the statistical channel state information (SCSI) is available. The works, as discussed above, have ignored the interference caused by PT to secondary receivers. However, in a practical scenario, this interference exists and affects the secondary networks' performance to a great extent. When this interference is much larger than the noise at the secondary receivers, the quality of interest is the signal-to-interference ratio (SIR). [118] analyzed the performance of the SC scheme employed at Bob and Eve for general and interference-limited scenarios over general fading and derived closed-form expressions for bit error rate and outage probability.

The complexity of the MRC scheme depends upon the number of available paths available, which can be high, especially for multi-path diversity. In addition, MRC is very sensitive to channel errors, and these tend to be more critical when the instantaneous SNR is low. On the other hand, SC uses only one path out of the available ones and hence, do not fully exploit the amount of diversity offered by the channel. Thus, comparing with SC and MRC, a hybrid technique called generalized selection combining (GSC) is proposed which bridges the gap between SC and MRC [39]. The primary idea of the GSC scheme is to pick a subset of the best diversity branches and then combine them in the MRC fashion to lessen the complexity and the energy dissipation. The GSC scheme provides a performance/implementation trade-off between MRC and SC schemes. In addition, the GSC scheme is expected to be more sturdy toward channel estimation errors since the weakest SNR paths are not included in the combining process. Chen *et al.* [124] analyzed the GSC/MRC scheme to enhance the PLS of a wireless system consisting of a single antenna Alice, a multi-antennas Bob, and a multi-antennas Eve. The GSC scheme is implemented to Bob while the MRC scheme is utilized to Eve in order to maximize its instantaneous SNR. Deng *et al.* in [125] considered GSC for cognitive decode-and-forward (DF) relaying in Nakagami-m fading channels. More importantly, authors in [125] obtained a high SNR approximation of the ergodic capacity for two scenarios: 1) proportional interference power and 2) fixed interference power constraint. Wang *et al.* in [66] considered GSC at Bob and Eve for secure communication at MIMO wiretap channel over Nakagami-m fading. [66] derived closed-form for SOP at high SNR for two realistic scenarios: 1) Bob is located near to Alice, and 2) Bob and Eve is located close to Alice. Furthermore, [68] extended this to two eavesdropping scenarios and presented new closed-form expressions for several key performance indicators:1) the average capacity slope and power offset of the asymptotic average

secrecy rate, and 2) the secrecy diversity order and the the secrecy array gain of the asymptotic SOP.

2.2 Cooperative Diversity

Cooperative diversity has been recognized as an adequate solution for combating the shadowing effects to enhance transmission reliability [126], [127]. In this subsection, we are mainly studied different cooperative diversity techniques that are utilized for PLS enhancement. Figure 2.2 shows an underlay CRN that is comprised of Alice, N relays, Bob, and Eve. N relays are employed to improve the quality of the signal transmitted from Alice to Bob. Specifically, Alice first sends its signal to N relays, then relays forward it to Bob. At present, there are two basic relay protocols: amplify-and-forward (AF) and decode-and-forward (DF). A relay node amplifies and retransmits its received noisy version of the Alice signal to Bob in the AF protocol. In contrast, the DF protocol requires the relay node to decode its received signal and forward its decoded signal to Bob. It is concluded that the multiple relays-assisted signal transmission from Alice consists of two steps: 1) Alice broadcasts its signal, and 2) relay nodes retransmit their received signals [127]. Each of the two transmission steps is vulnerable to eavesdropping attack and needs to be carefully designed to prevent an eavesdropper from intercepting information sent by Alice to Bob. Cooperative beamforming can significantly improve the main channel's capacity with multiple relays. Ding *et al.* [128] introduced cooperative transmission to the secrecy communication system and showed that outage probability approaching zero could be achieved by introducing cooperative communication. Jin *et al.* [129] studied a multi-pair massive MIMO two-way relay network, in which a relay station serves multiple pairs of users with a large number of antennas, which uses MRC/maximum ratio transmission schemes. Furthermore, [130] presented an analytical characterization of the ergodic capacity of AF MIMO dual-hop relay channels, assuming that the CSI is available at Bob only and investigated the impact of the system and channel characteristics based upon these expressions. Dong *et al.* in [131] addressed secure communications of one Alice-Bob pair with the help of multiple cooperating relays in the presence of one or more Eve and considered three cooperative schemes DF, AF, and cooperative jamming (CJ). They proposed a design for relay weight and allocation of transmit power that meets the following goals: 1) maximize the attainable secrecy rate subjected to a total transmit power constraint, or 2) minimize the total transmit power subjected to a secrecy

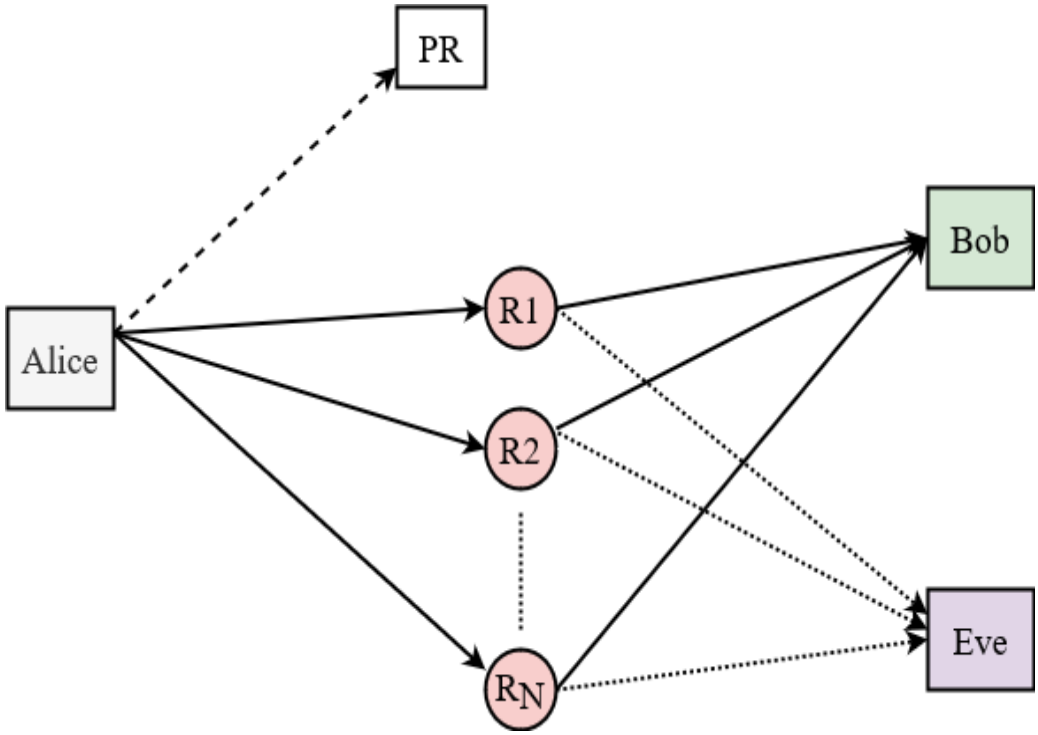

Figure 2.2: An underlay cognitive radio network consisting of PR, Alice, Bob and *N* cooperative relays in the presence of Eve.

rate constraint. [132] used relays opportunistically for secret communications and proposed two transmission schemes: 1) opportunistic cooperative jamming and (2) relay chatting that do not require the knowledge of Eve's CSI. [132] also demonstrated that an opportunistic relay chatting scheme could achieve an outage probability close to zero, whereas the outage probability achieved by the cooperative jamming scheme becomes constant at high SNR. [133] investigated joint relay and jammer selection in two-way cooperative networks, consisting of two sources, many intermediate nodes, and one Eve, with the constraints of PLS and the proposed algorithms which choose two or three intermediate nodes to intensify PLS against the wicked Eve. The first picked node works in the traditional relay mode and supports the sources to deliver their data to the corresponding destinations using an AF protocol. The second and third nodes are employed in different phases as jammers to produce interference upon Eve deliberately. Liu *et al.* in [134] analyzed the security of cognitive relay networks where the transmit power of the cognitive relay is restrained, and pair of cognitive relays are elected. The first relay acts as a supporter and sends the secret information to the authorized receiver under the malicious attempt of Eve. The second reply acts as a trusted jammer and sends a jamming signal to mislead Eve's received signals. [134] proposed and compared four relay selection policies, namely random relay, and random jammer, random jammer and best relay, best relay and best jammer,

Table 2.3: Various Cooperative Diversity Schemes

Authors	System Model	Performance Metrics	Contributions
Jin *et al.* [129]	Single-antenna Alice, multi-antenna relay and single-antenna Bob	Ergodic rate	Considered a multi-pair relay system with massive antenna arrays and analyzed ergodic rate when MRC scheme is utilized at relay with consideration of imperfect CSI
Jin *et al.* [130]	Multi-antenna Alice, multi-antenna AF relay and multi-antenna Bob	Ergodic Capacity	Analyzed the ergodic capacity of AF MIMO dual-hop relay channel and investigated the impact of the system channel characteristics
Dong *et al.* [131]	One Alice-Bob pair, multiple relays and multiple Eves	Secrecy rate	Proposed novel design of relays weights and the allocation of transmit power that maximize the achievable secrecy rate subject to a transmit power constraint, or, minimize the transmit power subject to a secrecy rate constraint.
Ding *et al.* [132]	One Alice-Bob pair, one Eve and multiple Eves	SOP	Two secrecy transmission schemes were proposed in opportunistic relaying
Chen *et al.* [133]	Two Alice, many intermediate nodes, and one Eve,	SOP, Ergodic secrecy rate	Considered two- way AF relay networks where jamming was considered as a useful approach to resist security attacks.
Liu *et al.* [134]	One Alice, many DF cognitive relays, one PU, one Bob and one Eve	SOP	Proposed several relay selection policies for secure communication in cognitive DF relay networks, where a pair of cognitive relays is opportunistically selected for PLS enhancement against Eve.
Zou *et al.* [135]	CRN with one Alice, one Bob and multiple relays and one Eve	SOP, Intercept probability	Investigated the security-reliability trade-off of cognitive relay transmission in the presence of realistic spectrum sensing
Fan *et al.* [136]	Two-way relay network, with multiple AF relays	Symbol error rate	Studied the effect of relay selection based on outdated CSI on system performance in Rayleigh fading channels
Fan *et al.* [137]	Multi-antenna Alice, multiple relays, single-antenna Bob and Eve	SOP	Quantified the impact of correlated fading on secure communication of multiple AF relaying networks.

and best relay and no jammer; and characterized the collective influence of the proposed relay selection policies and interference power constraint on the secrecy performance by determining new exact closed-form expressions for SOP. Fan *et al.* in [136] considered a two-way relay network with AF relays, out of which the best relay is selected based on the outdated CSI and studied the outdated CSI effect on the system performance in Rayleigh fading channels. [135] explored the PLS of a CRN comprised of Alice communicating with Bob with the aid of multiple secondary relays in the presence of Eve. [135] proposed two relay selection schemes, namely both single-relay and multi-relay selection, for protecting the secondary transmission against eavesdropping attacks and investigated the security reliability trade-off of the cognitive relay in the realistic spectrum sensing. Furthermore, [138] proposed AF and DF-based optimal relay selection to enhance the PLS of the wireless networks. Moreover, Wu *et al.* [139] analyzed PLS with AF over generalized-K fading channels and derived some lower bounds on outage probability, ASC, and PNZC in closed-form. Shah *et al.* [140] proposed a cooperative diversity-based relay and subchannel-selection scheme in CRNs, which decides a relay and subchannel to obtain the maximum secrecy rate while maintaining the energy consumed under a specific limit. More recently, Fan *et al.* in [137] investigated the impact of correlation on secure multiple AF relaying networks, where full relay selection and partial relay selection were used to choose the best relay.

2.3 Multiuser Diversity

Multiuser diversity is considered an attractive option for increasing the throughput in wireless networks [146]. Multiuser diversity is a kind of diversity that is generally integrated into systems with numerous users who share the same spectrum band via an access mechanism. This diversity originates from the fact that different users in a system typically have immensely different SNRs and that the total throughput can be maximized by assigning only the user(s) with the highest instantaneous SNR transmit at a given time [147]. Alice requires access to the channel quality measurements and the ability to schedule transmission among the users based on the channel quality to employ multiuser diversity [148]. In this section, we discuss the multiuser diversity for improving PLS. Figure 2.3 shows an underlay CRN with one Alice, multiple Bobs, one Eve, and one PR. In a multiuser environment, when channels are independent, it is more likely to find a strong channel as users become large. Hence, multiuser diversity can be exploited

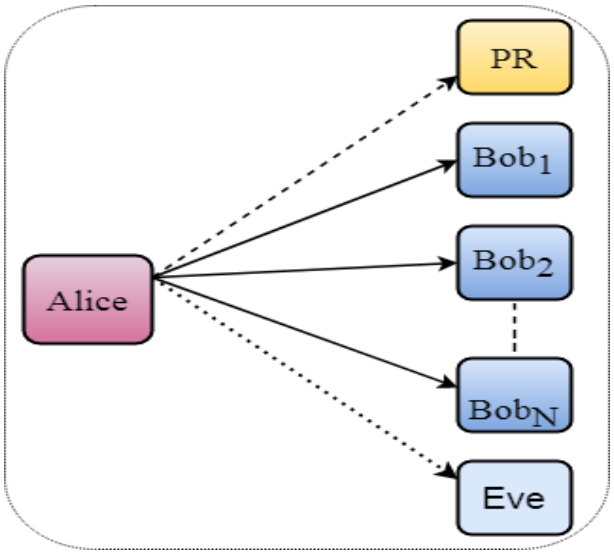

Figure 2.3: An underlay cognitive radio network consisting of one PR, one Alice, *N* Bobs and one Eve.

Table 2.4: Multiuser Diversity Scheme for PLS

Authors	System Model	Performance Metrics	Contributions
Ban *et al.* [141]	Multiple Alice, one Bob and one PR	Capacity	Showed that multiuser diversity gain in a CRN increases differently according to conditions given by the transmit power of SUs and a predetermined interference temperature
Aghazadeh *et al.*[142]	One PR, multiple Alice and one Bob	Average achievable channel capacity and outage probability	Presented optimal and sub-optimal multiuser selection. schemes
Zhang *et al.*[143]	One Alice-Bob pair coexist with one PT-PR pair	Multiuser diversity gain and ergodic throughput	Analyzed the multiuser diversity gain and ergodic throughput for different types of CRNs and compared against those in the conventional networks without the PR link.
Zou *et al.* [8]	One base station, multiple legitimate users and multiple Eves	Secrecy rate and intercept probability	Proposed the user scheduling scheme for improving the PLS of CRN with a primary QoS constraint
L Fan *et al.* [144]	One base station, *M* legitimate users and *N* DF relays	Secrecy outage probability	Investigated two criteria for user and relay selection
Badarneh *et al.*[145]	One PT-PR pair, one Alice and multiple Bobs	Average and effective throughput, average bit error rate and outage probability	Used extreme value theorem to analyze the asymptotic performance of k^{th} best SU selection scheme for arbitrary number of SUs

by scheduling users to communicate when they have favorable channel conditions. As a result, the system performance increases with the increase in the number of users [31]. The effects of multiuser diversity in a spectrum sharing system where SUs restrictively utilize a spectrum licensed to PUs only if interference perceived at PUs is regulated below a predetermined level is investigated in [141], [149]. This interference regulation affects the characteristics of multiuser diversity gains. [8] considered a CRN that consists of one cognitive base station (CBS), multiple cognitive users (CUs) in the presence of multiple eavesdroppers, where CUs transmit their data packet to CBS under a PUs'QoS constraint while eavesdroppers attempt to intercept their communication. [8] investigated the PLS against potential eavesdropping attacks in the CRN and proposed the user scheduling scheme to achieve multiuser diversity for improving the security level of cognitive transmission with primary QoS constraint and analyzed the achievable secrecy rate and intercept probability of the traditional and proposed multiuser scheduling schemes as well as artificial noise scheme in Rayleigh fading environments. [150], [151] and [142] analysed the performance of multiuser diversity for uplink underlay CRNs without taking the interference from the primary network into consideration. In particular, Ekin *et al.* in [150] analyzed the achievable capacity gain of uplink multiuser CRN over dynamic fading environment, and the outage probability and effective capacity were analyzed for opportunistic spectrum sharing in Rayleigh fading environment in [151]. Aghazadeh *et al.* in [142] a performance analyzed the performance of a multiuser selection diversity in a SIMO spectrum sharing system, and closed-form expressions are ASC, and outage probability were derived. The presence of multiple SUs in spectrum sharing networks needs a proper user scheduling scheme such as an opportunistic user selection scheme. It can achieve multiuser diversity. Multiuser interference diversity was investigated for opportunistic communications in CRNs by exploiting the mutual interference between the secondary channel and the primary link in [143] and diversity gain and ergodic throughput were analyzed for different types of CRN. [31] analyzed the ergodic capacity of various multiuser scheduling schemes in downlink CRNs with interference from the primary network under the outage constraint of multiple PUs and the SU maximum transmit power limit. Fan *et al.* in [144] introduced two PLS schemes for multiuser multi-relay networks, where the communication from M users to the base station is aided by direct links and by N DF relays and derived the asymptotic SOP at high transmit SNRs and high main-to-eavesdropper ratios for both schemes. More recently, the asymptotic performance of a generalized multiuser diversity scheme for an interference-limited underlay CRN was analyzed in

[145]; here, authors used extreme value theorem to show that k^{th} highest signal-to-interference ratio converges to uniformly in distribution to an inverse gamma random variable for fixed k and large SUs.

2.4 Other PLS Techniques

There are some other PLS techniques that are used to protect the confidential information against potential eavesdropper. These are given as follows:

2.4.1 Game Theory

Game theory [152] is a formal structure with a set of mathematical mechanisms to examine some complex interactions among interdependent rational players. Basar *et al.* in [153] adopted the research method of game theory to study the impact of intruders who aim to destroy communication on the system transmission performance under the limit of transmitting power. Mukherjee *et al.* [154] considered a MIMO communication link in the presence of a more sophisticated adversary: the wiretapper can act either as a passive eavesdropper or as an active jammer, and secrecy rate was chosen as the game payoff function. In addition to this, [155] modeled the network as a zero-sum game in strategic form with the MIMO secrecy rate as the payoff function and carried out a detailed analysis of the various rate outcomes that result from the possible actions of the agents. Han *et al.* in [156] studied static Game with incomplete information between Alice and relay; and solved problems of favorable interference with auction theory. Saad *et al.* in [157] designed a shared game-theoretical structure that allows single-antenna transmitters to autonomously make judgments to cooperate and make implicit MIMO alliances while considering the inherent benefit-cost tradeoff involved in this configuration. Houjeij *et al.* [158] formulated a non-cooperative game between the SUs and the eavesdroppers in cognitive radio networks. This game consists of two levels of competition: 1) the SUs require to pick their fancied channel to optimize the trade-off between interference (due to channel jam), availability (due to PUs' activity), and secrecy rate (due to the potential of being overheard), and 2) the eavesdroppers are imperative and require to pick the channels that allow them to reduce the overall secrecy rate of the network.

2.4.2 Machine Learning Based PLS

Machine learning (ML) based strategies can be implemented to resolve a vast range of problems in wireless networks, from radio access technology selection [159] to different resource optimization problems [160], as well as channel estimation and signal detection problems [161]. In the following, a literature survey of PLS with ML is provided. Recently, ML methods have been implemented extensively as an explication way to solve many challenging predicaments that have very complex structures with rigorous constraints on computational time [162]. Moreover, artificial intelligence has developed as one of the booming techniques in numerous research issues [163]. Various ML methods can achieve their practical implementations. These methods permit machines to learn from their computations and make decisions according to the environment [164, 165]. Several ML algorithms are open in the literature [166], such as linear regression, logistic regression, and neural networks. A neural network is a popular ML method because it can realize different relationships in complex and statistical data sets [167, 168]. In current years, many research interests have been promoted to employ the neural network to design and optimize wireless systems, where the researchers think that neural network will be the core method for 5 G and beyond wireless systems [169, 170, 171]. The different optimization strategies with various approximations methods have been widely employed in secure transmission designs. These approaches solve complex and mathematically intractable resource allocation problems [172, 173]. Nevertheless, these techniques are usually developed based on iterative methods to generate either optimal or sub-optimal solutions [174, 175]. The computational complexities incorporated with these traditional optimization techniques are neither affordable in low-powered devices in Internet-of-Things (IoT) nor fit for ultra-reliability applications and low-latency in future wireless networks. Further, these optimization methods generate different complications in delay-sensitive systems as the dynamic nature of real-time parameters needs regular updates in a little time [176]. It includes stringent delay requirements in modernizing those design parameters, challenging to reach by standard optimization approaches. ML procedures can be recognized as the potential solution strategies to determine these real-time update issues. Among several ML approaches, the deep learning approach has several advantages.

Several works have described that ML techniques can be utilized in different real-time wireless communication applications in the literature. For instance, deep learning-based channel estimation and signal detection methods in orthogonal frequency division multiplexing systems are investigated in [161]. A deep neural network-based method for effective online configu-

ration of reconfigurable intelligent surfaces is proposed in [177], where the transmitted signal focusing is improved under the indoor environment. The deep reinforcement learning-based joint transmit beamforming and phase shift matrix design for reconfigurable intelligent surface aided MISO systems is examined in [178]. The neural network-based spectrum and energy efficiency maximization techniques are proposed for the CRN [160]. A learning-based approach for wireless resource management is performed in [176], whereas a reinforcement learning-based resource allocation technique is developed for vehicle-to-vehicle communications in [179]. A deep neural network is utilized to learn the interference management over interference-limited channels in [180], whereas the authors design a deep neural network for channel calibration between the uplink and downlink directions in generic massive in [170]. Nevertheless, none of these works has considered applying ML techniques to solve resource allocation problems concurrently with perfect and imperfect CSI in secure communication systems. Hence, [181] investigated power allocation an ML-based power allocation design with both perfect and imperfect CSI for secure transmission, and a neural network-based approach is introduced to maximize the secrecy rate of the SR under the constraints of total transmit power of ST and the interference leakage to the PR, in which several regularization designs are produced.

2.5 Important Findings

This chapter presents several physical layer security techniques for improving data security against eavesdropping attacks. We discuss MIMO, multi-user diversity, cooperative diversity, and other PLS techniques such as game theory and machine learning to increase the secrecy capacity of the wireless network. We study different transmit combining schemes in MIMO diversity, such as TBF and TAS schemes. We noted that the TAS scheme is a less complex and less expensive technique than TBF and provides the same diversity gain as TBF. Moreover, the TAS scheme does not mandate the instantaneous CSI of the eavesdropper channel at Alice. In addition, we explore various receive combining schemes such as SC, MRC, and GSC schemes and conclude that the GSC scheme is more generalized relatives to SC and MRC. GSC scheme bridges the gap between SC and MRC schemes. While the MRC scheme is optimal, it increases the network's hardware complexity. We also study different cooperative diversity schemes like AF, DF, and cooperative jamming schemes to enhance the PLS of wireless communication.

The MIMO and cooperative diversity mechanism require modifications to protect the PUs'QoS while maximizing the secondary network security. Hence, a multi-user scheduling scheme is utilized to find the best user and improve the PLS. Lastly, we discuss other PLS techniques like game theory and machine learning-aided PLS.

Chapter 3

Secrecy Performance for Perfect CSI Scenario

This chapter presents a method of utilization diversity combining to improve secrecy performance of underlay CRN with multiple PRs over Rayleigh fading environment in a perfect CSI scenario. We investigate the secrecy performance of underlay CRN consisting of an Alice, a Bob, and N_P primary receivers in the presence of an eavesdropper, Eve. Alice, Bob, and Eve are outfitted with N_A, N_B, and N_E antennas, respectively. Alice transmits a confidential message to Bob, and Eve tries to intercept their communication in a passive eavesdropping scenario, i.e., CSI of eavesdropper channel is not available at Alice. A GSC scheme which is a more generalized scheme, is applied at Bob. The MRC scheme is optimal as it maximizes the output SNR at the receiver. Hence, to make Eve a powerful candidate to extract more information, i.e., worst-case scenario, we adopt the MRC scheme at Eve. Depending upon the availability of the global CSI of main and eavesdropper channels at Alice, we employ optimal antenna selection and sub-optimal antenna selection schemes at Alice. In addition, multiple PRs bring new challenges to examining the PLS of CRN compared with the traditional single PR-based network. Hence, we determine the impact of multiple PRs on the secrecy performance of the proposed network. Firstly, we derive closed-form expressions for SOP and intercept probability for single-antenna-based Alice and single PR. Further, we investigate the impact of multiple PRs on SOP and intercept probability. Lastly, we adopt SAS and OAS schemes at multi-antenna Alice and derive closed-form expressions for SOP and intercept probability with SAS and OAS schemes in the presence of multiple PRs. We also study the performance gap between SAS and OAS schemes. The impact of the GSC scheme with OAS and SAS schemes on PLS is also

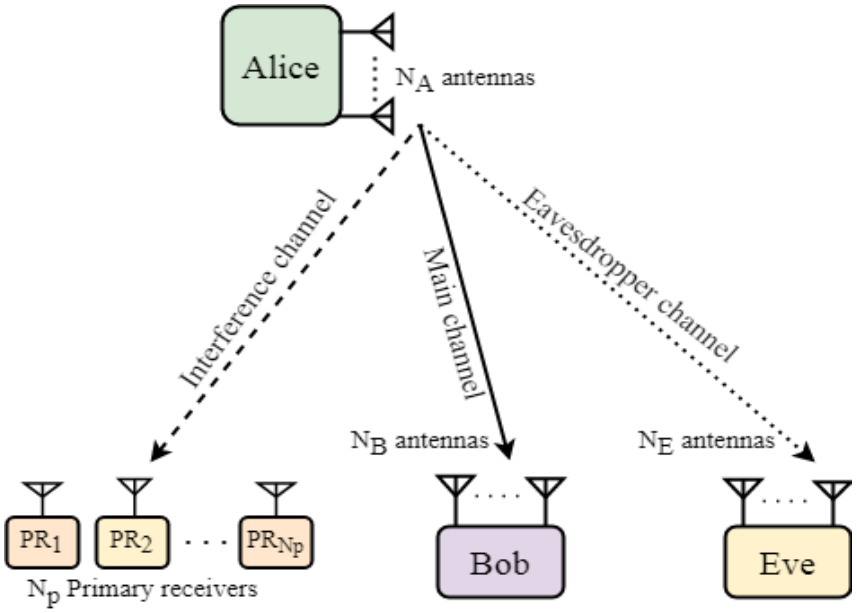

Figure 3.1: An underlay CRN with multi-antenna Alice, Bob and Eve and N_P primary receivers

characterized in this chapter.

3.1 System and Channel Model

We consider a wiretap underlay cognitive radio network as shown in Figure 3.1, where Alice sends a cryptic message to the legitimate receiver, Bob and Eve want to intercept their transmission. In more general form, we assume that our proposed system consists of single-antenna based N_P $(N_P \geq 1)$ primary receivers, N_A $(N_A \geq 1)$ antennas-based Alice, N_B $(N_B \geq 1)$ antennas-based Bob and N_E $(N_E \geq 1)$ antennas-based Eve. In this case, we assume that PT lies very far away from the secondary receivers. Hence, we neglect the interference caused by PT to the secondary receivers. We concentrate on passive eavesdropping, where the CSI of Eve is not known at Alice. In such a situation, Alice has no alternative but to encode the secret data into codewords of a steady rate R_s [62]. Our proposed system model is defined for three possible cases :

- Single PR with single antenna based Alice
- Multiple PRs with single antenna based Alice
- Multiple PRs with multi-antenna based Alice

The PR-Alice link is called the interference channel, the Alice-Bob link is the main channel, and the Alice-Eve link is the wiretap or eavesdropper channel. All channels i.e., interference

channel, main channel, and wiretap or eavesdropper channel are experiencing independent and identically distributed (i.i.d.) Rayleigh fading. Let $h_{jB_d} \sim \mathscr{CN}(0,\beta_1)$ is the channel gain of the channel between $j^{\text{th}}(j = 1,2,....N_A)$ antenna of Alice, and $d^{th}(d = 1,2.....N_B)$ antenna of Bob with zero mean and variance β_1 and $h_{jE_l} \sim \mathscr{CN}(0,\beta_2)$ is the channel gain of the channel between $j^{\text{th}}(j = 1,2,....N_A)$ antenna of Alice, and $l^{\text{th}}(l = 1,2.....N_E)$ antenna of Eve with zero mean and variance β_2. The channel gain and variance of interference channel are $\{h_{p0}\}_{p=1}^{N_p}$ and Ω_0 respectively. The GSC scheme is adopted at Bob, which means that Bob combines N_c $(1 \leq N_c \leq N_B)$ best (in term of SNR) receive antennas based upon the perfect CSI estimation via pilot signals transmitted by Alice. Based upon these pilot signals, Bob perfectly estimate the CSI and then arranges the order statistics $|h_{jB_d}|^2$ in descending order such that $|h_{jB_1}|^2, \geq ||h_{jB_2}|^2..... \geq ||h_{jB_{N_B}}|^2$. The instantaneous SNR at Bob can be written as

$$\gamma_M = \frac{\bar{P_A}}{N_0}\sum_{d=1}^{N_c}|h_{jB_d}|^2 = P_A\sum_{d=1}^{N_c}|h_{jB_d}|^2, \tag{3.1}$$

where $\bar{P_A}$ is Alice's transmit power, N_0 is the noise variance and $P_A = \frac{\bar{P_A}}{N_0}$ is the normalised transmit power of Alice. Eve adopted the MRC scheme, hence, the instantaneous SNR at Eve can be written as

$$\gamma_E = \sum_{l=1}^{N_E}\frac{\bar{P_A}}{N_0}|h_{jE_l}|^2 = \sum_{l=1}^{N_E}P_A|h_{jE_l}|^2. \tag{3.2}$$

3.1.1 Peak Interference Power Constraints

We are considering an underlay spectrum sharing cognitive network, i.e., both PU and SU are transmitting in the same spectrum concurrently band provided the interference caused by Alice to PRs is below some threshold [182]. The underlay CRNs have obtained more recognition due to their high efficiency and requiring no information of the primary signal [183]. In underlay CRN, for secure transmission, Alice's transmit power $\bar{P_A}$ should be kept below the peak interference power, $\bar{I_P}$. Furthermore, we assume that instantaneous CSI of the PR-Alice channel is valid and up-to-date at PRs [184]. The transmit power of Alice is bounded by maximum transmit power $\bar{P_T}$ and $\bar{I_P}$ at PRs as

$$\bar{P_A} = \min\left(\frac{\bar{I_P}}{\{h_{p0}\}_{p=1}^{N_p}}, \bar{P_T}\right), \tag{3.3}$$

from which the instantaneous SNR at Bob and Eve can be rewritten as

$$\gamma_M = \min\left(\frac{\gamma_p}{Y}, \gamma_0\right) X_M, \tag{3.4}$$

$$\gamma_E = \min\left(\frac{\gamma_p}{Y}, \gamma_0\right) X_E, \tag{3.5}$$

respectively, where $\gamma_p = \frac{\bar{I_P}}{N_0}, \gamma_0 = \frac{\bar{P_T}}{N_0}, Y = |\{h_{p_i}\}_{p_i=1}^{N_p}|^2, X_M = \sum_{d=1}^{N_c} |h_{jB_d}|^2$ and $X_E = \sum_{l=1}^{N_E} |h_{jE_l}|^2$. For ease of exposition and mathematical tractability, we denote $\gamma_1 = \beta_1\gamma_0 = \frac{\beta_1\gamma_p}{\sigma}$ and $\gamma_2 = \beta_2\gamma_0 = \frac{\beta_2\gamma_p}{\sigma}$. Here, γ_1 denotes the average SNR of the main channel, and γ_2 denotes the average SNR of the wiretap channel or eavesdropper channel. If $X_M = \sum_{d=1}^{N_c} X_d$, where $X_d = |h_{jB_d}|^2$ is i.i.d. exponential random variable (R.V.) with parameter β_1, then the CDF of $\gamma_M = \min\left(\frac{\gamma_p}{Y}, \gamma_0\right) X_M$ conditioned on Y is given as

$$\begin{aligned} F_{\gamma_M|Y}(\gamma_M) = &\binom{N_B}{N_c}\left[1 - e^{\frac{-\gamma_M}{\mu(y)\beta_1}} \sum_{a=0}^{N_c-1} \frac{1}{a!}\left(\frac{\gamma_M}{\mu(y)\beta_1}\right)^a + \sum_{n=1}^{N_B-N_c} (-1)^{N_c+n-1} \binom{N_B - N_c}{n}\right. \\ &\left(\frac{N_c}{n}\right)^{N_c-1}\left[\left(1+\frac{n}{N_c}\right)^{-1}\left(1 - e^{-\frac{\left(1+\frac{n}{N_c}\right)\gamma_M}{\mu(y)\beta_1}}\right) - \sum_{a=0}^{N_c-2}\left(\frac{n}{N_c}\right)^m\left(1 - e^{\frac{-\gamma_M}{\mu(y)\beta_1}}\right.\right. \\ &\left.\left.\left.\sum_{k=0}^{a}\frac{1}{k!}\left(\frac{\gamma_M}{\mu(y)\beta_1}\right)^a\right)\right]\right], \end{aligned} \tag{3.6}$$

where $\mu(y) = \min\left(\frac{\gamma_p}{Y}, \gamma_0\right)$. When $X_E = \sum_{l=1}^{N_E} X_l$, where $X_l = |h_{jE_l}|^2$ is i.i.d exponential R.V. with parameter β_2, then the CDF and PDF of $\gamma_E = \min\left(\frac{\gamma_p}{Y}, \gamma_0\right) X_E$ conditioned on Y can be written as

$$F_{\gamma_E|Y}(\gamma_E) = 1 - e^{-\frac{\gamma_E}{\mu(y)\beta_2}} \sum_{k=0}^{N_E-1} \frac{1}{k!}\left(\frac{\gamma_E}{\mu(y)\beta_2}\right)^k, \tag{3.7}$$

$$f_{\gamma_E|Y}(\gamma_E) = \frac{\gamma_E^{N_E-1} e^{\frac{-\gamma_E}{\mu(y)\beta_2}}}{(\mu(y)\beta_2)^{N_E}(N_E-1)!}, \tag{3.8}$$

respectively.

3.1.2 Optimal Antenna Selection Scheme

In all TAS scheme, only the best antenna among available N_A antennas available at Alice is selected to transmit a signal from Alice to Bob. When the global CSI of main and wiretap channel is available, the OAS scheme that maximizes the secrecy capacity be employed at Alice. This assumption is required since the construction of wiretap codes that ensure secrecy

requires the knowledge of the instantaneous capacities of both channels. Alice in turn uses the CSI of the main and wiretap channel to construct codes that achieve secrecy [49]. Eve might be another legitimate user who wants to tap other user's communication, which can be active in the network. Hence, the CSI of Eve's channel is estimated by monitoring Eve's transmission, which has been proposed in [185]. Without the loss of generality, we assume that the transmit antenna j is selected as the best antenna to send the signal from Alice to Bob with power P_A. Considering the use the GSC scheme at Bob, the capacity of the main channel C_{jM} from transmit antenna j^{th} to Bob can be expressed as

$$C_{jM} = \log_2 \left(1 + \bar{P}_A \sum_{d=1}^{N_c} |h_{jB_d}|^2 \right). \tag{3.9}$$

Similarly, the capacity of the eavesdropper channel, C_{jE} from j^{th} transmit antenna to Eve can be represented as

$$C_{jE} = \log_2 \left(1 + \bar{P}_A \sum_{l=1}^{N_E} |h_{jE_l}|^2 \right). \tag{3.10}$$

In the OAS scheme, the transmit antenna that maximizes the secrecy capacity C_s is considered as the "best" transmit antenna. Hence, the OAS criterion can be written as

$$\kappa = \arg\max_{j \varepsilon N_A} \left(C_{jM} - C_{jE} \right) = \arg\max_{j \varepsilon N_A} \frac{1 + \bar{P}_A \sum_{d=1}^{N_C} |h_{jB_d}|^2}{1 + \bar{P}_A \sum_{l=1}^{N_E} |h_{jE_l}|^2} = \arg\max_{j \varepsilon N_A} \left(\frac{1 + \gamma_{jM}^{OAS}}{1 + \gamma_{jE}^{OAS}} \right), \tag{3.11}$$

where κ signifies the best selected antenna. Therefore, once the global CSI of the main and wiretap channel h_{jB_d} and h_{jE_l} are available at Alice, the best antenna could be determined at Alice by (3.11).

3.1.3 Sub-optimal Antenna Selection Scheme

As mentioned above, the global CSI of the main and Eve channels should be available at Alice in the OAS scheme. Though, in some instances where CSI of Eve's channels is not available, the OAS is not performing correctly. Therefore, the best solution in this case is the SAS scheme, which maximizes the main channel's capacity instead of the secrecy capacity when the CSI of Eve's channel is unavailable at Alice. The antenna selection criterion at Alice in the SAS

scheme can be written as

$$\kappa = \arg\max_{j\varepsilon N_A} C_{jM} = \arg\max_{j\varepsilon N_A} \sum_{d=1}^{N_C} |h_{jB_d}|^2 = \arg\max_{j\varepsilon N_A} \left(\ln\left(1+\gamma_{jM}^{SAS}\right)\right), \tag{3.12}$$

where $\gamma_{jM}^{SAS} = \frac{\bar{P}_A}{N_0} X_{jM}^{SAS}$ is the SNR received at Bob from j^{th} antenna at Alice and κ denotes the best selected antenna.

3.2 Secrecy Performance Analysis

This section comprehensively investigates the secrecy performance of the proposed networks in the passive eavesdropping scenario for all three possible cases: 1) single PR and single-antenna based Alice, 2) multiple PRs and single-antenna based Alice, and 3) multiple PRs and multi-antenna based Alice. The closed-form expressions for SOP and intercept probability for all three cases are derived.

3.2.1 Case I: Single PR and Single-Antenna Based Alice

This subsection investigates the secrecy performance of an underlay CRN consisting of single-antenna Alice, multi-antenna Bob and multi-antenna Eve, and a single PR. This section derives exact closed-form expressions for SOP and intercept probability for single PR and single-antenna-based Alice. Furthermore, this subsection also examines the SOP and the intercept probability asymptotically at high SNR region, i.e., $\gamma_1 \approx \infty$.

Proposition 3.1. *The closed-form expressions of exact SOP of underlay CRN with a single PR and single-antenna based Alice can be expressed as*

$$\begin{aligned} P_{out_1} = &\binom{N_B}{N_c}\Bigg[\left(1-e^{-\frac{\sigma}{\Omega_0}}\right)\left[1-\mathscr{B}_1\sum_{a=0}^{N_c-1}\alpha_1\zeta_1+\mathscr{B}_2-\lambda_3\left(1-\beta_1\sum_{a=0}^{m}\alpha_1\zeta_1\right)\right]+e^{\frac{-\sigma}{\Omega_0}} \\ &-\mathscr{H}_0\sum_{a=0}^{N_c-1}\sum_{r=0}^{a-z}\alpha_2\zeta_2\lambda_4+\lambda_5\left(e^{\frac{-\sigma}{\Omega_0}}-\frac{\lambda_2 e^{-\left(\frac{\mathscr{C}_3(2^{R_s}-1)}{\gamma_1}+\frac{\sigma}{\Omega_0}\right)}}{\left(\frac{\mathscr{C}_3 2^{R_s}}{\sigma\gamma_1}+\frac{1}{\sigma\gamma_2}\right)^{N_E}}\right)-\sum_{l=1}^{N_B-N_c}\lambda_3\Bigg(e^{\frac{-\sigma}{\Omega_0}} \\ &-\mathscr{B}_2\sum_{a=0}^{m}\sum_{r=0}^{a-z}\alpha_2\zeta_2\lambda_4\Bigg)\Bigg], \end{aligned} \tag{3.13}$$

where

$$\mathscr{C}_2=(-1)^{N_c+l-1}\frac{(N_B-N_c)!}{(N-N_c-l)!l!}\left(\frac{N_B}{l}\right)^{N_c-1},\ \mathscr{C}_3=\left(1+\frac{l}{N_c}\right),\mathscr{C}_4=\left(\frac{-l}{N_c}\right)^m,$$
$$\lambda_5=\sum_{l=1}^{N_B-N_c}\frac{\mathscr{C}_2}{\mathscr{C}_3}\zeta_1=\frac{(z+N_E-1)!}{\left(\frac{2^{R_s}}{\gamma_1}+\frac{1}{\gamma_2}\right)^{z+N_E}},\ \sigma=\frac{I_P}{P_T},\ \alpha_1=\sum_{z=0}^{a}\binom{a}{z}\frac{1}{a!}\left(\frac{2^{R_s}-1}{\gamma_1}\right)^{a-z}\left(\frac{2^{R_s}}{\gamma_1}\right)^{z},$$
$$\mathscr{H}_0=\frac{1}{\Omega_0(\sigma\gamma_2)^{N_E}},\ \lambda_1=\frac{1}{(\gamma_2)^{N_E}\left(\frac{\mathscr{C}_3 2^{R_s}}{\gamma_1}+\frac{1}{\gamma_2}\right)^{N_E}},\ \alpha_2=\sum_{z=0}^{a}\binom{a}{z}\frac{1}{a!}\left(\frac{2^{R_s}-1}{\sigma\gamma_1}\right)^{a-z}\left(\frac{2^{R_s}}{\sigma\gamma_1}\right)^{z},$$
$$\lambda_3=\sum_{l=1}^{N_B-N_c}\sum_{m=0}^{N_c-2}\mathscr{C}_2\mathscr{C}_4\lambda_2=\frac{1}{\Omega_0(\sigma\gamma_2)^{N_E}\left(\frac{\mathscr{C}_3(2^{R_s}-1)}{\sigma\gamma_1}+\frac{1}{\Omega_0}\right)},\ \zeta_2=\frac{(z+N_E-1)!}{\left(\frac{2^{R_s}}{\sigma\gamma_1}+\frac{1}{\sigma\gamma_2}\right)^{z+N_E}}\frac{(a-z)!}{r!},$$
$$\mathscr{B}_1=\frac{e^{\frac{-(2^{R_s}-1)}{\gamma_1}}}{(N_E-1)!\gamma_2^{N_E}},\lambda_4=\frac{(a-z)!\sigma^r e^{-\left(\frac{(2^{R_s}-1)}{\gamma_1}+\frac{\sigma}{\Omega_0}\right)}}{r!\left(\frac{(2^{R_s}-1)}{\gamma_1}+\frac{\sigma}{\Omega_0}\right)^{a-z-r+1}},\ \mathscr{B}_2=\sum_{l=1}^{N_B-N_c}\frac{\mathscr{C}_2}{\mathscr{C}_3}\left(1-\lambda_1 e^{\frac{-\mathscr{C}_3(2^{R_s}-1)}{\gamma_1}}\right).$$

Proof: The proof of Proposition (3.1) is given in the Appendix A.1.

Some useful observations can be made from (3.13). These are as follows:

1. For $N_c=1$, (3.13) reduces to

$$P_{out_2}=\left(1-e^{-\frac{\sigma}{\Omega_0}}\right)N_B\sum_{l=0}^{N_B-1}(-1)^l\binom{N_B-1}{l}\left[1-\frac{1}{(\gamma_2)^{N_E}}\frac{e^{-\frac{(1+l)(2^{R_s}-1)}{\gamma_1}}}{\left(\frac{(1+l)2^{R_s}}{\gamma_1}+\frac{1}{\gamma_2}\right)^{N_E}}\right]+N_B$$
$$\sum_{l=0}^{N_B-1}(-1)^l\binom{N_B-1}{l}\left[e^{\frac{-\sigma}{\Omega_0}}-\frac{1}{\Omega_0(\gamma_2)^{N_E}}\frac{1}{\left(\frac{(1+l)2^{R_s}}{\gamma_1}+\frac{1}{\gamma_2}\right)^{N_E}}\frac{e^{-\left(\frac{(1+l)(2^{R_s}-1)}{\gamma_1}+\frac{\sigma}{\Omega_0}\right)}}{\left(\frac{(1+l)(2^{R_s}-1)}{\sigma\gamma_1}+\frac{1}{\Omega_0}\right)}\right].\tag{3.14}$$

(3.14) is corresponding to the SOP of underlay CRN consist of a single PR and single-antenna based Alice with peak interference power constraints when SC scheme is adopted at Bob, and MRC scheme is employed at Eve.

2. When $N_B=N_E=1$, (3.13) reduces to

$$P_{out_3}=\left(1-e^{-\frac{\sigma}{\Omega_0}}\right)\left[1-\frac{e^{\frac{-(2^{R_s}-1)}{\gamma_1}}}{\frac{2^{R_s}\gamma_2}{\gamma_1}+1}\right]+\left[e^{\frac{-\sigma}{\Omega_0}}-\frac{1}{\left[\frac{2^{R_s}\gamma_2}{\gamma_1}+1\right]}\frac{e^{-\left(\frac{(2^{R_s}-1)}{\gamma_1}+\frac{\sigma}{\Omega_0}\right)}}{\left(\frac{(2^{R_s}-1)}{\sigma\gamma_1}+\frac{1}{\Omega_0}\right)}\right].\tag{3.15}$$

(3.15) is SOP corresponding to single-antenna Alice and single-antenna Bob with peak interfer-

ence power constraints and (3.15) is equivalent to [69, eq.11]. The SOP given in (3.15) reduces to [186, eq.9] without peak interference power constraints.

Proposition 3.2. *The intercept probability for the single PR and single antenna based Alice can be written as*

$$P_{int_1} = \binom{N_B}{N_c}\left[1-\Gamma_1\sum_{a=0}^{N_c-1}\Gamma_2+\lambda_5\left(1-\frac{1}{\eta_2^{N_E}}\right)-\lambda_3\left(1-\Gamma_1\sum_{a=0}^{m}\Gamma_2\right)\right], \tag{3.16}$$

where

$$\eta_1 = \left[\left(\frac{\gamma_1}{\gamma_2}\right)^{\frac{1}{1+\frac{N_E}{a}}}+\left(\frac{\gamma_2}{\gamma_1}\right)^{\frac{1}{1+\frac{a}{N_E}}}\right],\ \eta_2 = \left(\frac{\mathscr{C}_3\gamma_2}{\gamma_1}+1\right)$$
$$\Gamma_1 = \frac{1}{(N_E-1)!},\ \Gamma_2 = \frac{(a+N_E-1)!}{a!\eta_1^{a+N_E}}.$$

Proof: The proof of Proposition (3.2) given in the Appendix A.2.

From (3.16), it is clear that intercept probability degrades with increasing $\frac{\gamma_1}{\gamma_2}$ (i.e main link is better than Eve's link) for constant value of $\frac{a}{N_E}$ and improves with increasing $\frac{\gamma_2}{\gamma_1}$ (i.e Eavesdropper channel is better than main channel) for constant value of $\frac{a}{N_E}$, where a is varying from 0 to N_c-1. For $N_B = N_c$, (3.16) reduces to

$$P_{int_1} = 1-\sum_{n=0}^{N_B-1}\binom{n+N_E-1}{n}\frac{\gamma_1^{N_E}\gamma_2^n}{(\gamma_1+\gamma_2)^{n+N_E}} \tag{3.17}$$

We can say that for $N_B = N_c$, intercept probability given in (3.17) reduces to [119, eq.3] without interference power constraint and also reduces to [69, eq.12] with power constraint.

Next, we identify the asymptotic behavior of SOP in the high SNR regime of γ_1, i.e., $\gamma_1 \to \infty$. It allows us to find the secrecy diversity order and secrecy diversity gain, which are the two factors governing SOP at $\gamma_1 \to \infty$. We first expand the exponential terms of (3.6) using Maclaurain series expansion [187, eq. 1.211.1]. Neglecting the other higher terms, the first order expansion of $F_{\gamma_M}(x)$ can be written as

$$F^{\infty}_{\gamma_M|Y}(\gamma_M) = \begin{cases} \frac{1}{(N_c)!N_c^{N_B-N_c}}\left(\frac{\gamma_M}{\mu(y)\beta_1}\right)^{N_B}, & Y \le \frac{\gamma_p}{\gamma_0} \\ \frac{1}{(N_c)!N_c^{N_B-N_c}}\left(\frac{\gamma_M Y}{\sigma\mu(y)\beta_1}\right)^{N_B}, & Y > \frac{\gamma_p}{\gamma_0}. \end{cases} \tag{3.18}$$

By utilizing (3.18), the asymptotic SOP for multiple primary receivers and single-antenna based

Alice is derived in Proposition 3.3.

Proposition 3.3. *The asymptotic SOP for an underlay CRN with single PR and single antenna based Alice can be expressed as*

$$P_{out_1}^{\infty} = \mathscr{N}_1(\gamma_1)^{-N_B}\left[\left(1-e^{\frac{-\sigma}{\Omega_0}}\right)+e^{\frac{-\sigma}{\Omega_0}}\sum_{n=0}^{N_B-q}\frac{(N_B-q)!}{n!}\left(\frac{\Omega_0}{\sigma}\right)^{N_B-n-q}\right], \tag{3.19}$$

where

$$\mathscr{N}_1 = \frac{1}{N_c!{N_c}^{N_B-N_c}}\sum_{q=0}^{N_B}\binom{N_B}{q}\left(2^{R_s}-1\right)^{N_B-q}\left(2^{R_s}\right)^{q}\frac{(q+N_E-1)!}{(N_E-1)!}{\gamma_2}^{q}.$$

Proof : The proof of (3.19) is given in Appendix (A.3).

The asymptotic SOP given in (3.19) can also be written as

$$P_{out_1}^{\infty} = (G_A\gamma_1)^{-G_D} + O(\gamma_1^{-G_D}). \tag{3.20}$$

where secrecy diversity order is

$$G_D = N_B, \tag{3.21}$$

secrecy array gain is

$$G_A = \left[\mathscr{N}_1\left(\left(1-e^{\frac{-\sigma}{\Omega_0}}\right)+e^{\frac{-\sigma}{\Omega_0}}\sum_{n=0}^{N_B-q}\frac{(N_B-n)!}{n!}\left(\frac{\Omega_0}{\sigma}\right)^{N_B-n-q}\right)\right]^{\frac{-1}{N_B}}. \tag{3.22}$$

According to (3.20), (3.21) and (3.22) we have following remark to provide insight into the use of generalized selection combining scheme at Bob.

- The asymptotic result affirm that G_D is independent of N_E and γ_2, as mention in (3.21).
- SOP increases with the increasing N_E and γ_2. This confirms that the G_A in (3.22) is a decreasing function of N_E and γ_2.
- As indicated in (3.21), G_D is also independent of choice of N_c. It is dependent on N_B at the Bob.

3.2.2 Case II: Multiple PRs and Single-Antenna Based Alice

In this case, we analyze the secrecy performance of an underlay CRN with multiple primary receivers. We drive closed-form expressions for the SOP and intercept probability for underlay CRN consists of N_P primary receivers, and Alice is equipped with a single antenna .

Proposition 3.4. *The exact SOP of the proposed system with N_P PRs and single antenna Alice can be expressed as*

$$P_{out_4} = \binom{N_B}{N_c}\Bigg[\tau_1\left(1-e^{-\frac{p\sigma}{\Omega_0}}\right)\left[1-\beta_1\sum_{a=0}^{N_c-1}\alpha_1\zeta_1+\beta_2-\lambda_3\left(1+\beta_1\sum_{a=0}^{m}\alpha_1\zeta_1\right)\right] + \tau_1 e^{\frac{-p\sigma}{\Omega_0}}\left(1+\lambda_5-\lambda_3\right) - \frac{1}{(N_E-1)!}\sum_{a=0}^{N_c-1}\sum_{z=0}^{a}\sum_{s=0}^{a-z}\frac{\tau_1\zeta_2\alpha_2 p}{\Omega_0}e^{-\left(\frac{(2^{Rs}-1)}{\gamma_1}+\frac{p\sigma}{\Omega_0}\right)} \frac{(\sigma)^q(1-\lambda_3)}{\left(\frac{(2^{Rs}-1)}{\sigma\gamma_1}+\frac{(p)}{\Omega_0}\right)^{a-z-s+1}} - \frac{\lambda_5\tau_1\tau_2 p}{\Omega_0}\frac{e^{-\left(\frac{C_3(2^{Rs}-1)}{\gamma_1}+\frac{p\sigma}{\Omega_0}\right)}}{\left(\frac{C_3(2^{Rs}-1)}{\sigma\gamma_1}+\frac{p}{\Omega_0}\right)}\Bigg], \tag{3.23}$$

where $\tau_1 = \sum_{p=0}^{N_P}\binom{N_P}{p}(-1)^{(p+1)}$, $\tau_2 = \frac{1}{\left(\frac{C_3(2^{Rs})}{\sigma\gamma_1}+\frac{1}{\sigma\gamma_2}\right)^{N_E}(\sigma\gamma_2)^{N_E}}$.

Proof: The proof of Proposition 3.4 is given in Appendix A.1.

For a single PR i.e., N_P = 1, (3.22) reduces to (3.13). For $N_B = N_c$ and N_P = 1, (3.22) reduces to [69, eq.15] and for $N_B = 1$ and $N_P = 1$, (3.22) reduces to [69, eq.17]. The closed-form expression of intercept probability with N_P primary receivers and single antenna based Alice is obtained in the following proposition.

Proposition 3.5. *The intercept probability for GSC/MRC based underlay CRN with multiple PUs and single antenna based Alice is expressed as*

$$P_{int_2} = \tau_1\binom{N_B}{N_c}\left[1-\Gamma_1\sum_{a=0}^{N_C-1}\Gamma_2+\lambda_5\left(1-\frac{1}{\eta_2^{N_E}}\right)-\lambda_3\left(1-\Gamma_1\sum_{a=0}^{m}\Gamma_2\right)\right]. \tag{3.24}$$

Proof: The proof of Proposition 3.5 is given Appendix (A.2).

For N_P = 1, (3.24) reduces to (3.16). For $N_B = N_c$ and $N_P = 1$, (3.22) reduces to [69, eq.16] and for $N_B = 1$ and $N_P = 1$, (3.22) reduces to [69, eq.19].

Proposition 3.6. *The expression for asymptotic SOP with multiple PRs can be written as*

$$P_{out_2}^{\infty} = \kappa_1(\gamma_1)^{-N_B}\tau_1\left[\left(1-e^{\frac{-p\sigma}{\Omega_0}}\right)+e^{\frac{-p\sigma}{\Omega_0}}\sum_{n=0}^{N_B-q}\frac{(N_B-q)!}{n!}\left(\frac{\Omega_0}{p\sigma}\right)^{N_B-n-q}\right]. \tag{3.25}$$

Proof: The proof of Proposition 3.6 is given in Appendix A.3.

For a single primary receiver, i.e., $N_P = 1$, (3.25) reduces to (3.19).

3.2.3 Case III: Multiple PRs and Multi-Antenna Based Alice

In this subsection, we consider multiple antennas at Alice in the presence of multiple PRs. It is challenging to co-phase all the signals transmitted by different antennas of Alice without accurate knowledge of the phase information because phase estimation is very complex compared to channel magnitude estimation. Hence, it is more beneficial to transmit on a single best antenna to avoid adverse interference in this case. It is referred to as an antenna selection scheme. Depending upon the availability of global CSI of main and Eve's channel at Alice, we utilize OAS and SAS schemes at Alice. The expression for SOP and intercept probability with OAS and SAS schemes are investigated in this subsection.

3.2.3.1 SOP with OAS scheme

The secrecy capacity with OAS scheme can be written as

$$C_s^{OAS} = \max_{j\varepsilon N_A}\{C_j^{OAS}\}, \tag{3.26}$$

where, $C_j^{OAS} = \ln(1+\gamma_{jM}^{OAS}) - \ln(1+\gamma_{jE}^{OAS})$ is the secrecy capacity, when Alice and all PUs are equipped with single antenna while Bob and Eve are employed with arbitrary number of antennas. Hence, the SOP with OAS scheme can be written as

$$P_{out}^{OAS} = Pr\{C_s^{OAS} \le R_s\} = \{\max\{C_i^{OAS}\} \le R_s\} = \prod_{j=1}^{N_A} Pr\{C_j^{OAS} \le R_s\}. \tag{3.27}$$

We assume that all the fading coefficients are i.i.d. random variables (R.Vs), then the closed-form expression for SOP with optimal antenna selection scheme can be written as

$$P_{out_5}^{OAS} = \prod_{j=1}^{N_A} Pr\{C_j^{OAS} \le R_s\} = (P_{out_4}))^{N_A}, \tag{3.28}$$

where P_{out_4} is the SOP, when Alice is equipped with single antenna while Bob and Eve are equipped with multiple antennas in the presence of N_P PRs.

3.2.3.2 SOP with SAS Scheme

Here, we derive a closed-form expression of SOP with sub-optimal antenna selection scheme.

Proposition 3.7. *The closed-form expression of SOP with sub-optimal antenna selection scheme can be written as*

$$P_{out_6}^{SAS} = \binom{N_B}{N_c}^{N_A} \sum_{k_1+k_2+k_3+k_4+k_5=N_A} \sum_{j=0}^{N_C-1} \sum_{l=1}^{N_B-1} \sum_{c=0}^{k_3} \sum_{v=1}^{N_B-N_C} \sum_{m=0}^{N_C-2} \sum_{k=0}^{m} \frac{\mathscr{Z}_1\mathscr{Z}_2\mathscr{Z}_3\mathscr{Z}_4}{(N_E-1)!\gamma_2^{N_E}}$$
$$\binom{N_A}{k_1,k_2,k_3,k_4,k_5} \frac{(b+d+N_E-1)!}{\left(\frac{2^{R_S}\mathscr{A}}{\gamma_1}+\frac{1}{\gamma_2}\right)^{b+d+N_E}} \left[e^{-\frac{(2^{R_S}-1)\mathscr{A}}{\gamma_1}} \left(1-e^{-\frac{\sigma}{\Omega_0}}\right)^{N_P} + \sum_{p=0}^{N_P} \binom{N_P}{p} \right.$$
$$\left. (-1)^p e^{-\left(\frac{(2^{R_S}-1)\mathscr{A}}{\gamma_1}+\frac{p\sigma}{\Omega_0}\right)} \sum_{m=0}^{g} \frac{g!}{m!} \frac{\sigma^{b+m}}{\left(\frac{(2^{R_S}-1)\mathscr{A}}{\sigma\gamma_1}+\frac{p}{\Omega_0}\right)^{g-m+1}} \right] \tag{3.29}$$

where $\mathscr{A} = b+c, \mathscr{C}_3+k_5, g = b-d, \mathscr{Z}_1 = \left(\frac{1}{j}\right)^{k_2} \binom{jk_2}{b} \left(\frac{2^{R_S}-1}{\gamma_1}\right)^{jk_2-b} \left(\frac{2^{R_S}}{\gamma_1}\right)^{b}, \mathscr{Z}_2 = \left(\frac{\mathscr{C}_2}{\mathscr{C}_3}\right)^{k_3}$ $\binom{k_3}{c}(-1)^c, \mathscr{Z}_3 = (-1)^{k_4}(\mathscr{C}_2\mathscr{C}_4)^{k_4}, \ \mathscr{Z}_4 = (\mathscr{C}_2\mathscr{C}_4)^{k_5} \left(\frac{1}{k}\right)^{k_5} \binom{kk_5}{d} \left(\frac{2^{R_S}-1}{\gamma_1}\right)^{kk_5-d} \left(\frac{2^{R_S}}{\gamma_1}\right)^{d}$.

Proof: The proof of Proposition 3.5 can be seen in Appendix A.4.

For $N_c = 1$, the SOP with SAS scheme reduces to

$$P_{out_7}^{SAS} = N_B^{N_A} \sum_{a=0}^{N_B-1} \left((-1)^a \binom{N_B-1}{a} \frac{1}{1+a} \right)^{N_A} \sum_{i=0}^{N_A} \binom{N_B}{i} (-1)^i \frac{1}{\left(\frac{(1+a)i(2^{R_S})\gamma_2}{\gamma_1}+1\right)^{N_E}}$$
$$\left\{ e^{-\frac{(1+a)i(2^{R_S}-1)}{\gamma_1}} \left(1-e^{-\frac{\sigma}{\Omega_0}}\right)^{N_P} + \tau_1 \frac{e^{-\left(\frac{(1+a)i(2^{R_S}-1)}{\gamma_1}+\frac{p\sigma}{\Omega_0}\right)}}{\left(\frac{(1+a)i(2^{R_S}-1)}{\sigma\gamma_1}+\frac{p}{\Omega_0}\right)} \right\} \tag{3.30}$$

.

3.2.3.3 Intercept Probability with OAS and SAS Scheme

The closed form expression of intercept probability with optimal antenna selection scheme can be written as

$$P_{int_3}^{OAS} = Pr\left(\max_{l=1,2....N_A} C_{s_l} < 0 \right) = \prod_{l=1}^{N_A} Pr(C_{s_l} < 0) = (P_{int_2}))^{N_A}. \tag{3.31}$$

The closed form expression of intercept probability with sub-optimal antenna selection is obtained by putting $R_s = 0$ in (3.29) as

$$P_{int_4}^{SAS} = \sum_{k_1+k_2+k_3+k_4=N_A} \binom{N_B}{N_c} (-1)^{k_2} \sum_{s=0}^{N_c-1} \lambda_5^{k_3} \sum_{a}^{k_3} \binom{k_3}{a} (-1)^a \sum_{m=0}^{N_C-2} (C_2C_3)^{k_4} \sum_{b=0}^{k_4} (-1)^b \sum_{s=0}^{m} \left(\frac{1}{\gamma_1}\right)^{k_2k+bs} \left(\frac{1}{s!}\right)^{k_2+b} \frac{1}{\gamma^{N_E}(N_E-1)} \frac{M!}{\left(\frac{N}{\gamma_1}+\frac{1}{\gamma_2}\right)^{M+1}}, \tag{3.32}$$

where $M = sk_2 + kb + N_E - 1$, $N = k_2 + aC_3 + b$. For $N_c = 1$ i.e., SC scheme is adopted at Bob, (3.32) reduces to

$$P_{int_5}^{SAS} = \sum_{n=0}^{N_BN_A} \binom{N_BN_A}{n} \frac{(-1)^n}{\left(\frac{n\gamma_2}{\gamma_1}+1\right)^{N_E}}. \tag{3.33}$$

and for $N_B = 1$, (3.33) reduces to [106, eq.12].

3.2.3.4 Asymptotic SOP with OAS and SAS Schemes

The expression of asymptotic SOP with OAS scheme for this case can be written as

$$\begin{aligned} P_{out_3}^{\infty} &= \left(P_{out_2}^{\infty}\right)^{N_A} \\ &= \left\{ \kappa_1 (\gamma_1)^{-N_B} \tau_1 \left[\left(1 - e^{\frac{-p\sigma}{\Omega_0}}\right) + e^{\frac{-p\sigma}{\Omega_0}} \sum_{n=0}^{N_B-q} \frac{(N_B-q)!}{n!} \left(\frac{\Omega_0}{p\sigma}\right)^{N_B-n-q} \right] \right\}^{N_A}. \end{aligned} \tag{3.34}$$

At high SNR, the CDF of the main channel with SAS scheme can be written as

$$F_{\gamma_M|(Y=y)}^{SAS^{\infty}}(x) = \left[\frac{1}{(N_c)!N_c^{N_B-N_c}} \left(\frac{x}{\gamma_1}\right)^{N_B} \right]^{N_A}. \tag{3.35}$$

By utilizing (3.35), the expression for asymptotic SOP with SAS scheme and multiple PRs can be written as

$$P_{out_4}^{\infty} = \left(\frac{1}{(N_c)!N_c^{N_B-N_c}} \right)^{N_A} \gamma_1^{-N_AN_B} \sum_{q=0}^{N_BN_A} \kappa_2 \tau_1 \left\{ \left(1 - e^{-\frac{p\sigma}{\Omega_0}}\right) + e^{\frac{-(p\sigma)}{\Omega_0}} \sum_{t=0}^{N_AN_B-1} \frac{(N_AN_B-q)!}{t!} \left(\frac{\Omega_0}{p\sigma}\right)^{N_AN_B-q-t} \right\}, \tag{3.36}$$

where

$$\kappa_2 = \frac{(q+N_E-1)!}{(N_E-1)!}\binom{N_BN_A}{q}\left(2^{R_s}-1\right)^{N_AN_B-q}(2^{R_s})^q\gamma_2^q.$$

The asymptotic SOP with OAS and SAS scheme given in (4.29) and (3.36) can also be written as

$$\begin{aligned} P_{out_3}^{\infty} &= (G_A{}^{OAS}\gamma_1)^{-G_D^{OAS}} + O(\gamma_1^{-G_D^{OAS}}), \\ P_{out_4}^{\infty} &= (G_A{}^{SAS}\gamma_1)^{-G_D^{SAS}} + O(\gamma_1^{-G_D^{SAS}}), \end{aligned} \tag{3.37}$$

where secrecy diversity order is

$$G_D{}^{OAS} = G_D{}^{SAS} = N_BN_A. \tag{3.38}$$

secrecy array gains with OAS and SAS schemes can be calculated as

$$G_A{}^{OAS} = \left[\kappa_1\tau_1\left\{\left(1-e^{\frac{-p\sigma}{\Omega_0}}\right)+e^{\frac{-p\sigma}{\Omega_0}}\sum_{n=0}^{N_B-q}\frac{(N_B-q)!}{n!}\left(\frac{\Omega_0}{p\sigma}\right)^{N_B-n-q}\right\}\right]^{\frac{-1}{N_AN_B}}, \tag{3.39}$$

and,

$$G_A{}^{SAS} = \left[\left(\frac{1}{(N_c)!N_c^{N_B-N_c}}\right)^{N_A}\sum_{q=0}^{N_BN_A}\kappa_2\tau_1\left\{\left(1-e^{-\frac{p\sigma}{\Omega_0}}\right)+e^{-\frac{p\sigma}{\Omega_0}}\sum_{t=0}^{N_AN_B-1}\frac{(N_AN_B-q)!}{t!}\left(\frac{p\sigma}{\Omega_0}\right)^{N_AN_B-q-t}\right\}\right]^{\frac{-1}{N_AN_B}}, \tag{3.40}$$

respectively. Based on (3.38), (3.39) and (3.40), we find that $G_D{}^{OAS}$ & $G_D{}^{SAS}$ totally dependent upon antenna configuration of secondary transmitter Alice and legitimate receiver Bob.

In order to recognize the effect of GSC on SOP, we quantify the secrecy outage trade off between N_c+k and N_c, $k = 1,2,.....N_B-N_c$. From (3.38), it is clear that N_c+k and N_c have same diversity order. As such, we may conclude that the SNR gap between N_c+k and N_c is determined from (3.39) & (3.40) and written as

$$\frac{G_A{}^{OAS}(N_c+k)}{G_A{}^{OAS}(N_c)} = \left[\frac{N_c!(N_c)^k}{(N_c+k)!(1+\frac{k}{N_c})^{N_B-N_c-k}}\right]^{\frac{-1}{N_BN_A}}, \tag{3.41}$$

$$\frac{{G_A}^{SAS}(N_C+k)}{{G_A}^{SAS}(N_c)} = \left[\frac{N_c!(N_c)^k}{(N_c+k)!(1+\frac{k}{N_c})^{N_B-N_c-k}}\right]^{\frac{-1}{N_A}}. \tag{3.42}$$

Based on (3.41) & (3.42), it is confirm that $\frac{{G_A}^{OAS}(N_c+1)}{{G_A}^{OAS}(N_c)} \geq 1$ and $\frac{{G_A}^{SAS}(N_c+1)}{{G_A}^{SAS}(N_c)} \geq 1$. From this, we conclude that both ${G_A}^{OAS}$ and ${G_A}^{SAS}$ are an increasing function of N_c. Further,

$$\left(\frac{{G_A}^{OAS}(N_C+k+1){G_A}^{OAS}(N_c+1)}{{G_A}^{OAS}(N_c+k){G_A}^{OAS}(N_c)}\right) < 1,$$
$$\left(\frac{{G_A}^{SAS}(N_c+k+1){G_A}^{SAS}(N_c+1)}{{G_A}^{SAS}(N_c+k){G_A}^{SAS}(N_c)}\right) < 1.$$

This also confirm that SNR gap is a decreasing function of N_c. For $k = l$ and $N_A = 1$, (3.41) reduces to [68, eq.49].

3.3 Numerical Examples and their Illustration

Numerical results show the impact of GSC/MRC on the secrecy performance of underlay CRN for all three possible cases. In this section, we consider $\Omega_0 = 1$ and $R_s = 1$ throughout the analysis. The exact analytical curves of the SOP are supremely matched with simulation curves, and the asymptotic analytical lines of the SOP are perfectly matching with the exact curves at the high regime of γ_1.

Figure 3.2 plots SOP for different values of N_c as a function of γ_1. We have taken parameters set as $\sigma = 0.5$, $N_A = 1$, $N_E = 1$, $N_B = 5$ and γ_2 = 10 dB. Figure 3.2 confirm that the SOP decreases as N_c increasing from 1 to 5. It indicates that the number of selected antenna N_c has a positive impression on the secrecy of the proposed network. For $N_c = 1$, this curve resembles SC/MRC (i.e. SC at Bob and MRC at Eve) scheme, and for $N_c = N_B = 5$, this curve resembles the MRC/MRC (MRC at both Bob and Eve) scheme. Figure 3.2 also shows the performance gap between the SC and MRC at Bob and depicts that the MRC scheme performs much better than the SC scheme.

Figure 3.3 plots intercept probability versus γ_1/γ_2. From Figure 3.3, it is also clear that intercept probability improves with increasing γ_1/γ_2. Intercept probability progresses with the increase in the number of antennas at eavesdropper and decreases with the increment in the number of antennas at Bob. Similar inferences can be made from Table 3.1.

Figure 3.4 shows SOP and intercept probability with OAS and SAS schemes for $\gamma_2 = 10$

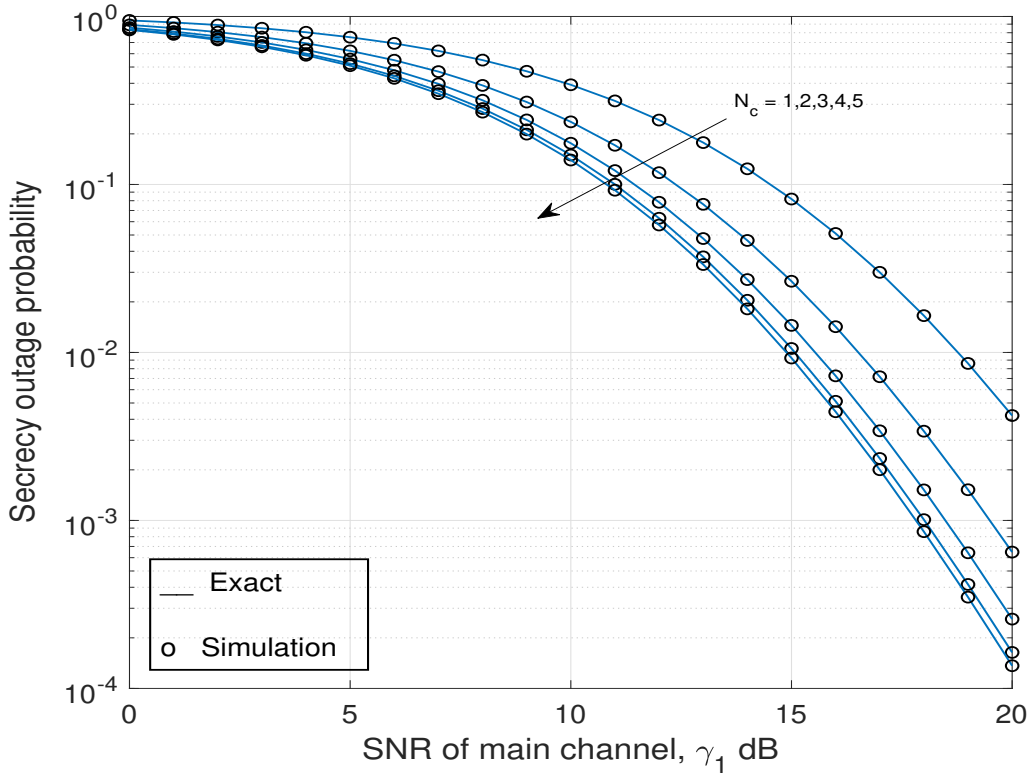

Figure 3.2: SOP versus γ_1 for $\sigma = 0.5$, $\gamma_2 = 10$ dB, $N_P = 5$, $N_A = 1$, $R_s = 1$, $N_B = 5$ and $N_E = 1$

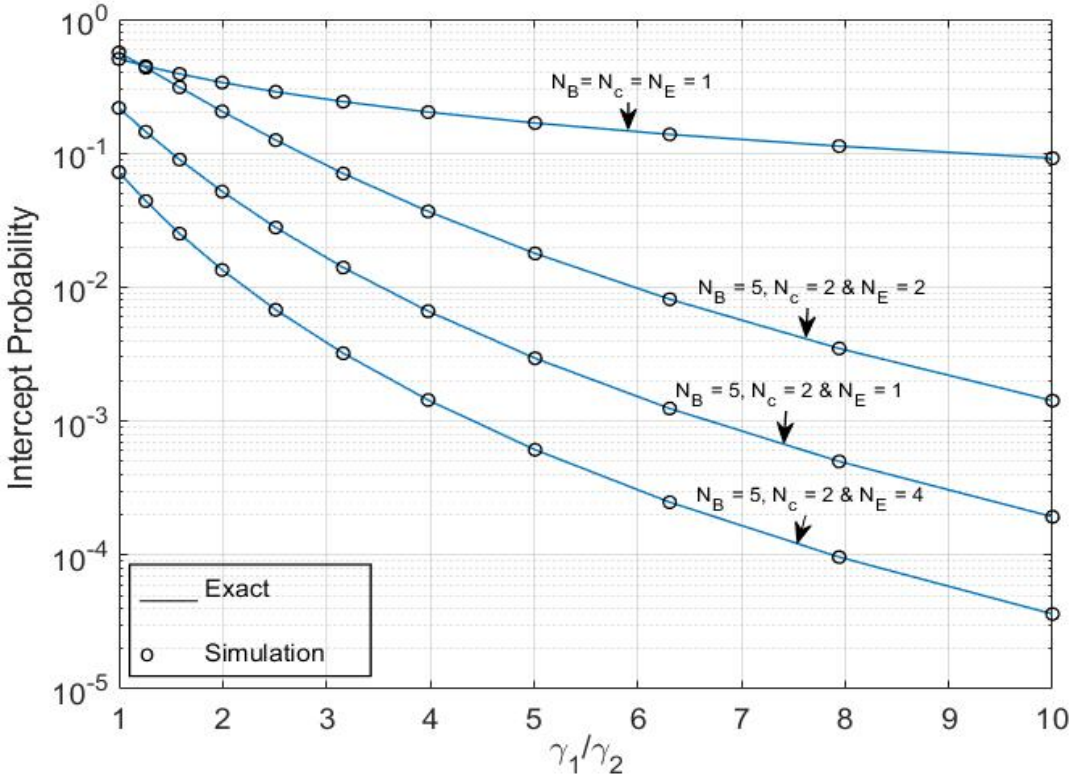

Figure 3.3: Intercept probability versus γ_1/γ_2 for $\sigma = 0.5$, $N_P = 5$, and $N_A = 1$

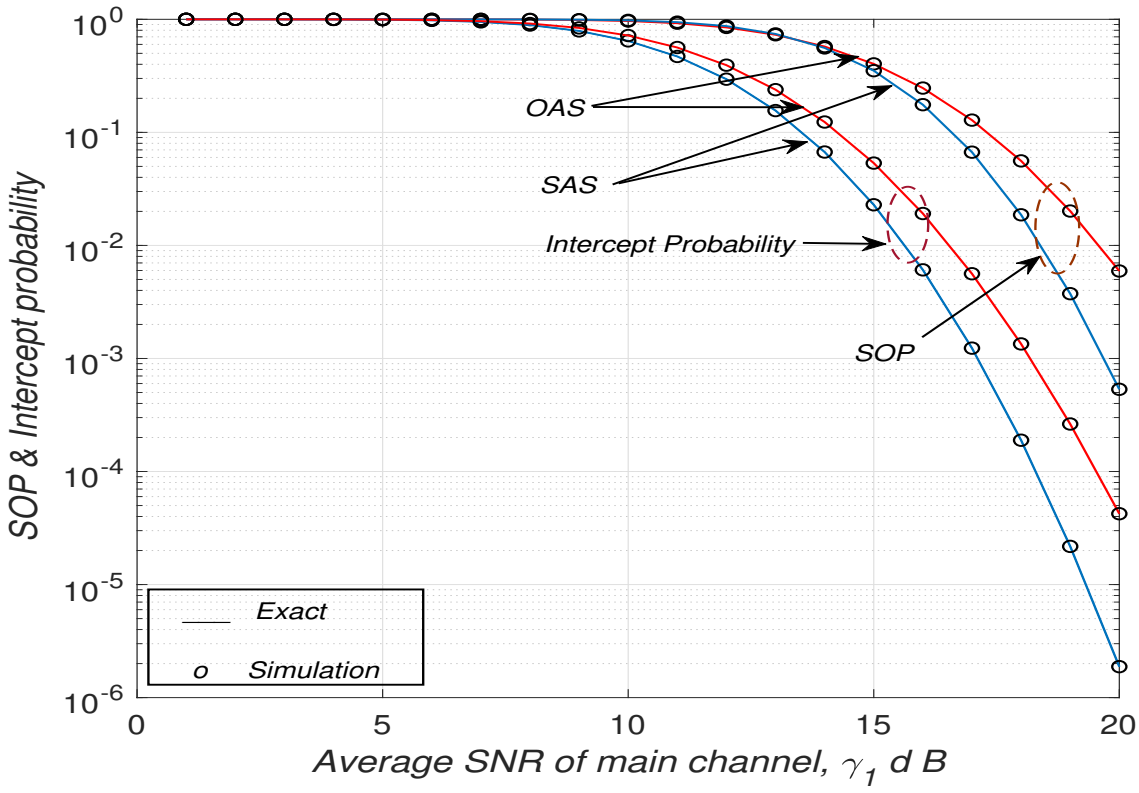

Figure 3.4: Secrecy outage probability and intercept probability versus γ_1 for $N_A = 3$, $\gamma_2 = 10$ dB, $\sigma = 0.01$, $N_P = 1$, $N_B = 5$, $N_E = 5$ and $N_c = 2$

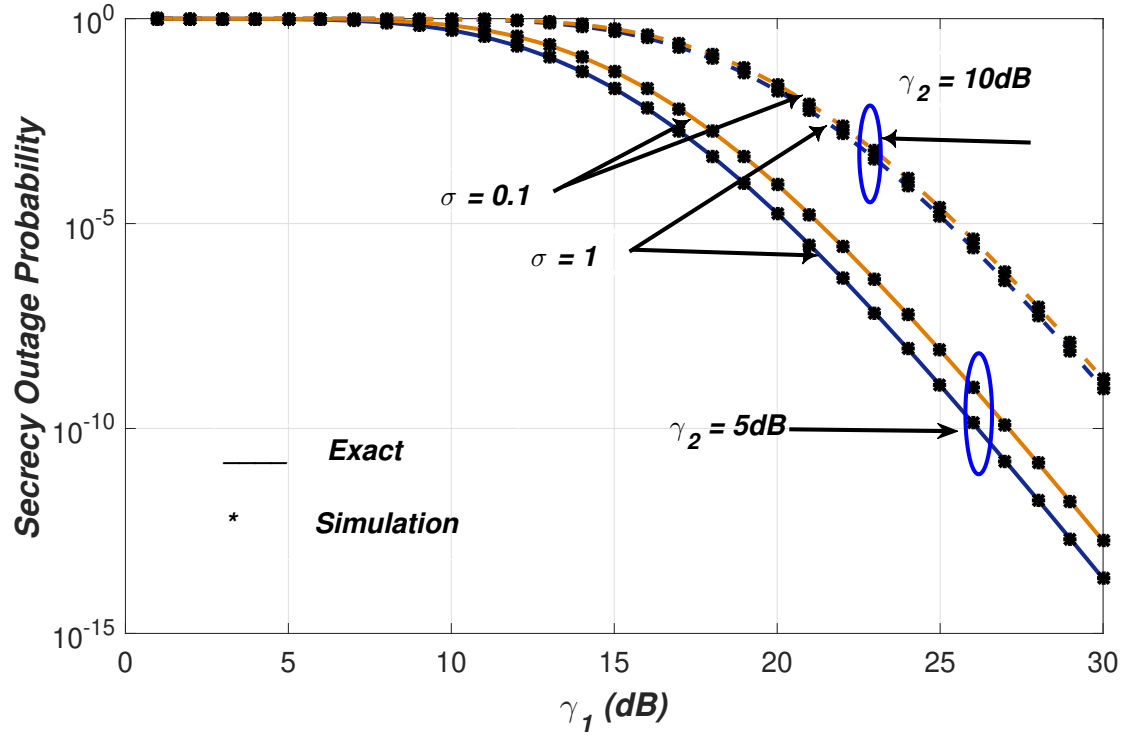

Figure 3.5: SOP versus γ_1 with $N_A = 2$, $N_P = 1$, $N_B = 5$, $N_E = 5$ and $N_c = 1$

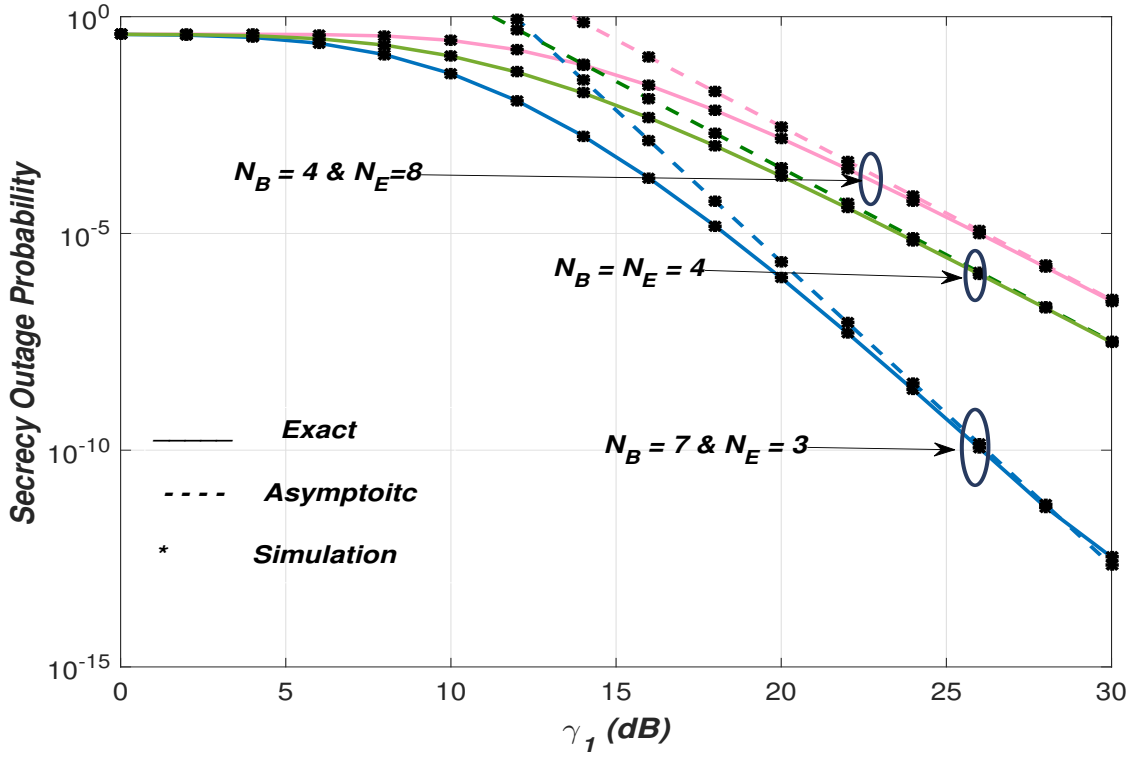

Figure 3.6: Exact and asymptotic SOP versus γ_1 with $N_c = 3$, $N_P = 1$, $\sigma = 0.5$ and $N_A = 2$

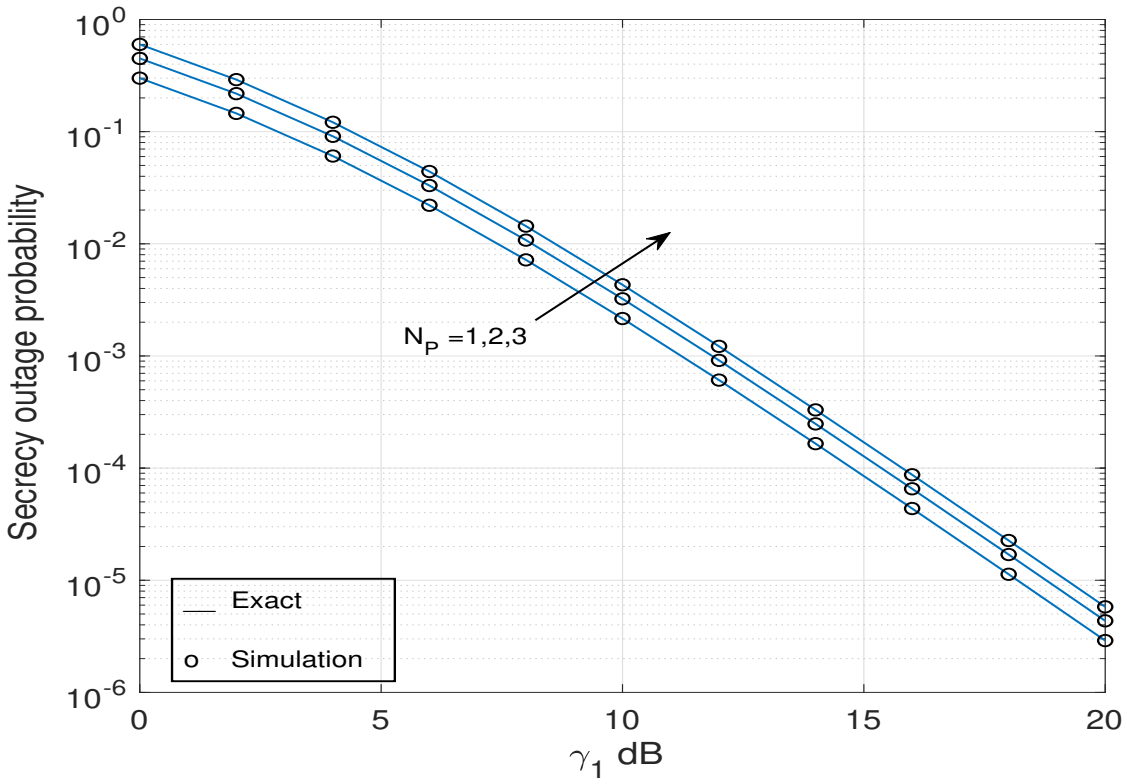

Figure 3.7: SOP versus γ_1 for multiple primary receivers with $\gamma_2 = 0$ dB, $\sigma = 0.01$, $N_B = 3$ and $N_c = 2$

Table 3.1: Improvement in Intercept Probability

S.No	Number of antenna at Alice, N_A	Number of antenna at Bob, N_B	Selected number of antenna at Bob, N_c	Number of antenna at Eve, N_E	γ_1/γ_2	Intercept Probability
1	1	5	2	1	2	0.0216
2.	1	5	3	1	2	0.0110
3.	1	5	3	2	2	0.0456
4.	1	5	3	5	2	0.3282

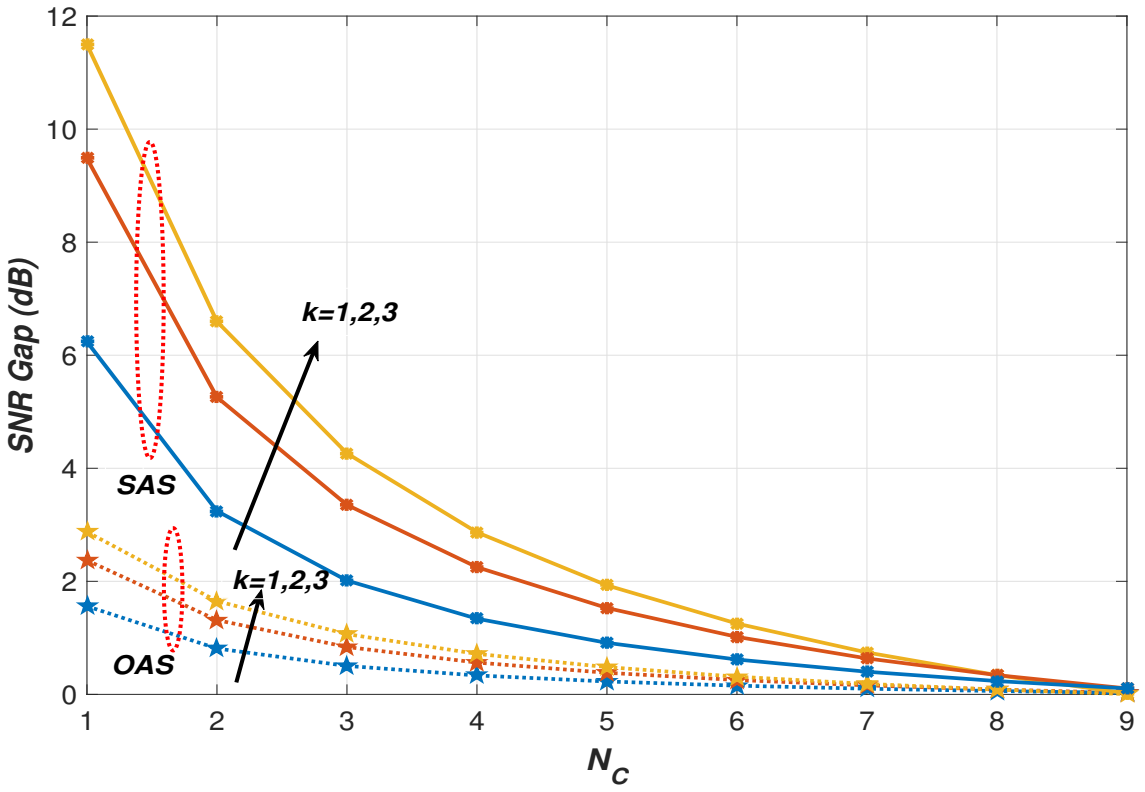

Figure 3.8: Signal to noise ratio for $N_B = 10$

dB, $N_P = 1$, $N_B = 5$, $N_E = 5$ and $N_c = 2$. As N_A increases, both SOP and intercept probability significantly decrease. It is because of an increasing number of transmit antenna N_A improved the power gain of Alice through receiver diversity, and Eve cannot obtain it. In Figure 3.4, one can also see the OAS scheme performs better than the SAS scheme.

Figure 3.5 shows the variation in SOP with σ and SNR of Eve's channel γ_2. From figure 3.5, it is observed that SOP decreases with increase in σ. This is due to relaxing the peak interference power constraint $\sigma = \frac{\gamma_p}{\gamma_0} = \frac{I_P}{P_T}$, which leads to increase in the transmit power $\bar{P}_A$ given by (1.28). Also, SOP increase with γ_2.

Figure 3.6 plots both exact and asymptotic SOP different number of N_B and N_E antennas. The parallel lines show that secrecy diversity order is only depend on antenna at Bob, N_B and

transmit antennas, N_A. It is independent of choice of antenna, N_c and Eve's antennas, N_E as indicated by (3.38). From figure 3.6, we also observed that SOP increases with increasing γ_2 and N_E. This confirm that secrecy array gain given in (3.39) is deceasing function of γ_2 and N_E.

Figure 3.7 shows loss in secrecy and increase in SOP as PR is increasing from 1 to 3 i.e., N_P = 1 to N_P = 3 for γ_2 = -10 dB. This can be explained by the fact, for very low SNR in Eve's channel i.e $\gamma_2 << 1$, secrecy capacity reduces to $C_s = \log_2(1+\gamma_M)$. The SNR of main channel decreases with increasing the number of primary users N_P. At $\gamma_2 << 1$, secrecy capacity only depends upon the main channel's capacity. This mean that SOP increases with increasing the number of primary users N_P.

Figure 3.8 plots signal to noise ratio gap indicated by (3.41) versus N_c for different value of k and N_B = 10. From Figure 3.8, it is clear that SNR gap increase with increasing k and decreasing with increasing N_c. It confirm that G_A in (3.39) is increasing function of N_c and SNR gaps in (3.41) & (3.42) are decreasing function of N_c.

3.4 Conclusion

In this chapter, we have analyzed the secrecy performance of an underlay cognitive radio network for three different cases: 1) single PR and single antenna based Alice, 2) multiple PRs and single antenna based Alice, and 3) multiple PRs and multi-antenna based Alice. For multi-antenna Alice, depending upon whether global CSI of main and Eve's channels is available at Alice, we have proposed OAS and SAS scheme and concluded that the OAS scheme performs better than the SAS scheme. We have adopted the GSC scheme at Bob and MRC technique at Eve. We have derived closed-form expression for exact and asymptotic SOP and intercept probability in the Rayleigh fading environment for three cases. Our results are also applicable for an arbitrary number of primary receivers and antennas at Alice, Bob, and Eve. Our numerical results also confirmed that the secrecy performance of the proposed network degrades with increasing multiple primary receivers, the number of antennas at Eve, and the SNR of the eavesdropper channel. On the other hand, secrecy performance improves with and by increasing the number of transmitting antennas, antenna at Bob, SNR of the main channel, and σ. We also compared the SOP and intercept probability performance and found that intercept probability outperforms the SOP.

Chapter 4

Secrecy Performance for Imperfect CSI Scenario

In a practical scenario, the CSI may be outdated or imperfect due to the complexity of electromagnetic wave spreading and transmitting delay, which causes estimation error at the receivers. This chapter examines the secrecy performance of underlay CRN in an imperfect CSI scenario. We consider an underlay CRN consisting of single-antenna Alice, multi-antenna Bob, multi-antenna Eve, and multi-antenna PR. The secrecy performance gap between SC and MRC schemes adopted at Bob is examined when all channels are outdated CSI. The MRC scheme is employed at Eve to make it a potential candidate to intercept more and more information (i.e., worst case). Furthermore, we adopted the MRC scheme at PR, which is a worst-case to restrict Alice's transmit power. To examine the impact of outdated CSI on the secrecy performance of underlay CRN, we consider two practical eavesdropping scenarios. That is Scenario I (i.e., passive eavesdropping): the CSI of a wiretap's channel is not available at Alice, and Scenario II (i.e., Active eavesdropping): the CSI of wiretap channel is known to Alice. For Scenario I, we investigate the secrecy performance of an underlay CRN in terms of SOP, intercept probability and, ε- outage secrecy capacity as CSI of wiretap channel is not available. For Scenario II, when the CSI of Eve's channel is available, the secrecy performance is measured in terms of average secrecy capacity since the Alice adjusts its transmission rate based on the global CSI of main and wiretap channels to achieve perfect secrecy. Furthermore, the asymptotic analysis of secrecy outage probability and average secrecy capacity is carried out in the high SNR regime to find further insights.

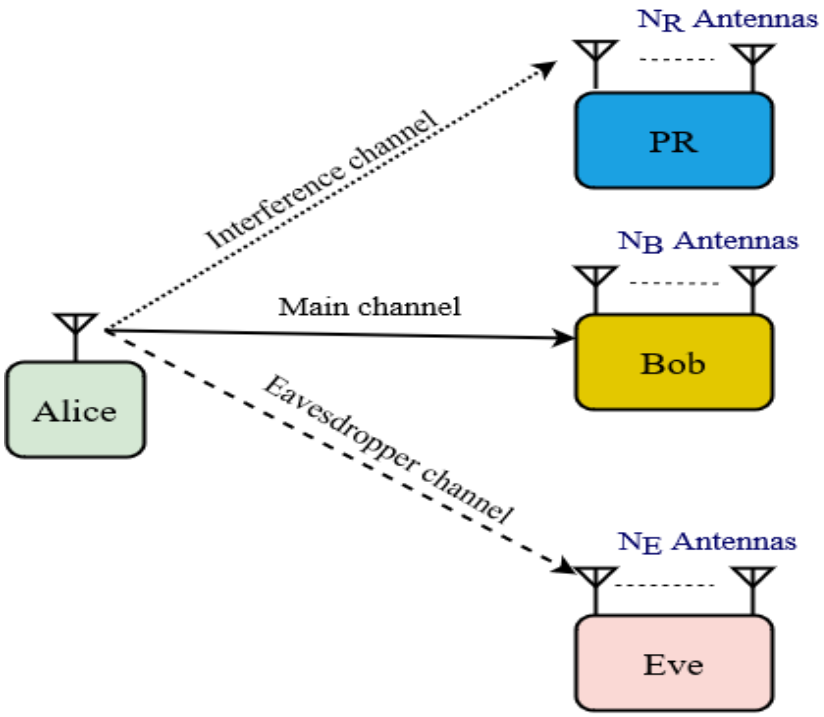

Figure 4.1: An underlay CRN consists of multi-antenna PR, single-antenna Alice, multi-antenna Bob and multi-antenna Eve

4.1 System and Channel Model

We consider an underlay CRN that consists of single-antenna Alice, multi-antenna Bob, multi-antenna Eve, and multi-antenna PR displayed in Figure 4.1. It is assumed that the primary transmitter, PT is not in the proximity of Alice while PR lies close to Alice [114, 188]. The secret information is sent from Alice to Bob in the presence of Eve, and Eve tries to decode these messages from its received vector. The PR, Bob, and Eve are outfitted with N_R, N_B, and N_E antennas. It is believed that all channels undergo spatially independent Rayleigh fading with average SNR γ_R, γ_1, and γ_2, respectively. The channel fading coefficients of between Alice-PR, Alice-Bob, and Alice-Eve channels with estimation errors are given as [189]

$$\tilde{h}_l^{i_l} = \sqrt{\rho_l} h_l^{i_l} + \sqrt{1-\rho_l} g_l^{i_l}, \tag{4.1}$$

where $l \in$ (PR (R), Bob (B) and Eve (E)), $h_l^{i_l}$ represents the channel gains of the channel between Alice and the i^{th} antenna of the PR, Bob and Eve and these are the Gaussian R.Vs. with zero mean and variances Ω_0, β_1 and β_2 respectively. $g_l^{i_l}$ is the channel estimate error, which is a complex Gaussian R.V. with zero mean. Both $h_l^{i_l}$ and $g_l^{i_l}$ have same variances. ρ_l is the power

correlation coefficient of varies from 0 to 1. The instantaneous SNR can be written as

$$\gamma_l = \frac{\bar{P}_A}{N_0}\tilde{H}_l, \tag{4.2}$$

where $\tilde{H}_l$ represents the combined channel power gains between Alice-$l \in$ PR, Bob, Eve. In underlay CRN, for reliable communication, Alice's transmit power, $\bar{P}_A$ is strictly constrained by $\bar{P}_T$ and $\bar{I}_P$ and given by

$$\bar{P}_A = \min\left(\frac{\bar{I}_P}{\sum_{k=1}^{N_R}|\tilde{h}_{R_k}|^2}, \bar{P}_T\right), \tag{4.3}$$

where $|\tilde{h}_{R_k}|^2$ is the channel gain of the interference channel. We employ the MRC technique at PR, which is the worst case to limit the transmit power at Alice. From (4.3), the instantaneous SNRs at Bob and Eve can be rewritten as

$$\gamma_M = \min\left(\frac{\gamma_p}{\sum_{k=1}^{N_R}|\tilde{h}_{R_k}|^2}, \gamma_0\right)\sum_{j=1}^{N_B}|\tilde{h}_{B_j}|^2, \tag{4.4}$$

$$\gamma_E = \min\left(\frac{\gamma_p}{\sum_{k=1}^{N_R}|\tilde{h}_{R_k}|^2}, \gamma_0\right)\sum_{i=1}^{N_E}|\tilde{h}_{E_i}|^2, \tag{4.5}$$

respectively, where $\gamma_p = \frac{\bar{I}_P}{N_0}$, $\gamma_0 = \frac{\bar{P}_T}{N_0}$, $|\tilde{h}_{B_j}|^2$ and $|\tilde{h}_{E_i}|^2$ are the channel gains of the main channel and eavesdropper channel with estimation errors, respectively. For ease of explanation and analytical tractability, we denote $\gamma_1 = \beta_1\gamma_0 = \frac{\beta_1\gamma_p}{\sigma}$ and $\gamma_2 = \beta_2\gamma_0 = \frac{\beta_2\gamma_p}{\sigma}$ and $\sigma = \frac{\gamma_p}{\gamma_0}$.

4.1.1 Channel Statistics with Maximal Ratio Combining Scheme

Let $\tilde{H}_l^{MRC} = \sum_{u_l=1}^{N_l}|\tilde{h}_{l,u_l}|^2$, $l \in$ (R, B and E) denotes the combined channel gain with MRC scheme. The CDF and PDF of $\tilde{H}_l^{MRC}$ with estimation errors can be written as [190]

$$F_{\tilde{H}_l^{MRC}}(x) = \sum_{u_l=1}^{N_l} A_l(u_l)\left(1 - e^{-\frac{x}{\gamma_l}}\sum_{a=0}^{u_l-1}\frac{x^a}{a!\gamma_l^a}\right), \tag{4.6}$$

$$f_{\tilde{H}_l^{MRC}}(x) = \sum_{u_l=1}^{N_l} A_l(u_l)\frac{x^{u_l-1}e^{-\frac{x}{\gamma_l}}}{(u_l-1)!\gamma_1^{u_l}}, \tag{4.7}$$

respectively, where $A_l(u_l) = \binom{N_l-1}{u_1-1}(1-\rho_l)^{N_l-u_l}{\rho_l}^{u_l-1}$.

4.1.2 Channels Statistics with Selection Combining Scheme

The channel gain with SC scheme can be expressed as $\tilde{H}_l^{SC} = \max_{u_l \in \{1,2.....N_l\}} |\tilde{h}_{l,u_l}|^2$. The CDF and PDF of $\tilde{H}_l^{SC}$ can be written as

$$F_{\tilde{H}_l^{SC}}(x) = \sum_{u_l=0}^{N_l-1} \frac{\phi_l}{\xi_l} \left(1 - e^{-\frac{x\xi_l}{\gamma_l}}\right), \tag{4.8}$$

$$f_{\tilde{H}_l^{SC}}(x) = \sum_{u_l=0}^{N_l-1} \frac{\phi_l}{\gamma_l} e^{-\frac{x\xi_l}{\gamma_l}}, \tag{4.9}$$

respectively, where $\phi_l = \frac{N_l(-1)^{u_l}\binom{N_l-1}{u_l}}{(1-\rho_l)\zeta_l}$, $\zeta_l = \frac{\rho_l}{1-\rho_l} + u_l + 1$ and $\xi_l = \frac{1}{1-\rho_l} - \frac{\rho_l}{\zeta_l(1-\rho_l)^2}$.

4.2 Secrecy Performance Analysis in Passive Eavesdropping Scenario

This section analyzes the secrecy performance in the passive eavesdropping scenario, i.e., the CSI of wiretap channels is inaccessible at Alice. In this scenario, we study three necessary performance metrics such as SOP, intercept probability, and ε- outage secrecy capacity to evaluate the secrecy performance of the proposed system.

4.2.1 Secrecy Outage Probability

The secrecy capacity, C_s in (1.40) can be rewritten as

$$C_s = \log_2\left(\frac{1+\gamma_M}{1+\gamma_E}\right) < R_s, \tag{4.10}$$

which is analogous to $\varepsilon(\gamma_E) = 2^{R_s}(1+\gamma_E) - 1 > \gamma_M$.

For secure transmission, the target rate R_s should be less than secrecy capacity C_s, otherwise, it leads to the compromising of the information-theoretic security. SOP is defined as the probability that secrecy capacity C_s falls under R_s, and can be expressed as

$$P_{out} = P_r\left(C_s < R_S\right) = P_r\big(\gamma_M \leq \gamma_E\big) + P_r\big(\gamma_M > \gamma_E\big) P_r\big(C_s < R_S \mid \gamma_M > \gamma_E\big). \tag{4.11}$$

which can be simplified to [62]

$$P_{out} = \int_0^{\infty} \int_0^{\infty} F_{\gamma_M|\{Y=y\}}(\varepsilon(\gamma_E)) f_{\gamma_E|\{Y=y\}}(\gamma_E) f_Y(y) d\gamma_E dy, \tag{4.12}$$

where $f_Y(y)$ is the PDF of Y, $f_{\gamma_E|\{Y=y\}}(.)$ is the PDF of γ_E conditioned on Y, and $F_{\gamma_M|Y=y}(.)$ is the CDF of γ_M conditioned on Y. The SOP given in (4.12) can be rewritten as [62]

$$\begin{aligned} P_{out} = & \underbrace{\int_0^{\frac{\gamma_p}{\gamma_0}} \int_0^{\infty} F_{\gamma_M|(Y=y)}(\varepsilon(\gamma_E)) f_{\gamma_E|(Y=y)}(\gamma_E) f_Y(y) d\gamma_E dy}_{\mathscr{J}_1} \\ & + \underbrace{\int_{\frac{\gamma_p}{\gamma_0}}^{\infty} \int_0^{\infty} F_{\gamma_M|(Y=y)}(\varepsilon(\gamma_E)) f_{\gamma_E|(Y=y)}(\gamma_E) f_Y(y) d\gamma_E dy}_{\mathscr{J}_2}. \end{aligned} \tag{4.13}$$

4.2.1.1 MRC/MRC Scheme at Bob/Eve and MRC Scheme at PR

In this subsection, we investigate the SOP when MRC scheme is employed at PR, Bob and Eve. The CDF of γ_M with MRC scheme can be expressed as

$$F_{\gamma_M|(Y=y)}(\varepsilon(\gamma_E)) = \sum_{b=1}^{N_B} A(b) \left(1 - e^{-\frac{\varepsilon(\gamma_E)}{\lambda\beta_1}} \sum_{a=0}^{b-1} \frac{(\varepsilon(\gamma_E))^a}{a!(\lambda\beta_1)^a}\right), \tag{4.14}$$

where

$$\lambda = \begin{cases} \gamma_0, & X \leq \frac{\gamma_p}{\gamma_0} \\ \frac{\gamma_p}{X}, & X \geq \frac{\gamma_p}{\gamma_0}, \end{cases} \tag{4.15}$$

and $A(b) = \binom{N_B}{b} (1-\rho_B)^{N_B-b} \rho_B^{b-1}$. The PDF at Eve with MRC scheme can be written as

$$f_{\gamma_E|(Y=y)}(\gamma_E) = \sum_{d=1}^{N_E} A(d) \frac{\gamma_E^{d-1} e^{-\frac{\gamma_E}{\lambda\beta_2}}}{(d-1)!(\lambda\beta_2)^d}, \tag{4.16}$$

where $A(d) = \binom{N_E}{d} (1-\rho_E)^{N_E-d} \rho_E^{d-1}$. Similarly, the PDF of Y with MRC scheme can be given by

$$f_Y(y) = \sum_{r=1}^{N_R} A(r) \frac{y^{r-1} e^{-\frac{y}{\gamma_R}}}{(r-1)!\gamma_R^r}, \tag{4.17}$$

where $A(r) = \binom{N_R}{r}(1-\rho_R)^{N_R-r}\rho_R^{r-1}$. By substituting (4.14), (4.16) and (4.17) in (4.13) and performing some mathematical manipulation; $\mathscr{J}_1^{MRC/MRC}$ and $\mathscr{J}_2^{MRC/MRC}$ can be calculated as

$$\mathscr{J}_1{}^{MRC/MRC} = \sum_{b=1}^{N_B}\sum_{d=1}^{N_E}\sum_{r=1}^{N_R} A(r)A(b)A(d)\left[1-\frac{e^{-\left(\frac{2^{R_s}-1}{\gamma_1}\right)}}{(d-1)!\gamma_2^d}\sum_{a=0}^{b-1}\sum_{n=0}^{a}\alpha_1\right]\left[1-e^{-\frac{\sigma}{\gamma_R}}\sum_{h=0}^{r-1}\frac{1}{h!}\left(\frac{\sigma}{\gamma_R}\right)^h\right], \quad (4.18)$$

and

$$\mathscr{J}_2{}^{MRC/MRC} = \sum_{b=1}^{N_B}\sum_{d=1}^{N_E}\sum_{r=1}^{N_R}\frac{A(b)A(d)A(r)}{\gamma_R}\left[\sum_{h=0}^{r-1}\frac{e^{-\frac{\sigma}{\gamma_R}}}{h!}\left(\frac{\sigma}{\gamma_R}\right)^h - \alpha_2 e^{-\sigma\left(\frac{2^{R_s}-1}{\sigma\gamma_1}+\frac{1}{\gamma_R}\right)}\sum_{m=0}^{r-1+a-n}\Delta_1\right], \quad (4.19)$$

respectively, where $\alpha_1 = \frac{1}{a!}\binom{a}{n}\left(\frac{2^{R_s}-1}{\gamma_1}\right)^{a-n}\left(\frac{2^{R_s}}{\gamma_1}\right)^n\frac{(n+e-1)!}{\left(\frac{2^{R_s}}{\gamma_1}+\frac{1}{\gamma_2}\right)^{n+e}}, \Delta_1 = \frac{(r-1+a-n)!}{m!}\frac{\sigma^m}{\left(\frac{2^{R_s}-1}{\sigma\gamma_1}+\frac{1}{\gamma_R}\right)^{r+a-n-m}}$, $\alpha_2 = \frac{1}{(d-1)!(r-1)!(\sigma\gamma_2)^d}\frac{1}{a!}\binom{a}{n}\left(\frac{2^{R_s}-1}{\sigma\gamma_1}\right)^{a-n}\left(\frac{2^{R_s}}{\sigma\gamma_1}\right)^n\frac{(n+d-1)!}{\left(\frac{2^{R_s}}{\sigma\gamma_1}+\frac{1}{\sigma\gamma_2}\right)^{n+d}}$. Hence, by substituting (4.18) and (4.19) in (4.13), the closed-form expressions for SOP with MRC scheme at PR, Bob and Eve can be calculated in the following subsections.

4.2.1.2 SC/MRC Scheme at Bob/Eve and MRC scheme at PR

This subsection considers the SC scheme at Bob and the MRC scheme adopted at both Eve and PR. Before going into the detail, we first calculate the statistical properties of γ_M and γ_E. The CDF of γ_M when SC scheme is applied at Bob can be expressed as

$$F_{\gamma_M|(Y=y)}(\varepsilon(\gamma_E)) = \sum_{b=0}^{N_B-1}\frac{\phi_B}{\xi_B}\left(1-e^{-\frac{\varepsilon(\gamma_E)\xi_B}{\lambda\Omega_1}}\right), \quad (4.20)$$

where $\phi_B = \frac{N_B(-1)^b\binom{N_B-1}{b}}{(1-\rho_B)\zeta_B}$, $\zeta_B = \frac{\rho_B}{1-\rho_b}+b+1$, and $\xi_B = \frac{1}{1-\rho_B}-\frac{\rho_B}{\zeta_B(1-\rho_B)^2}$. By substituting (4.20), (4.16) and (4.17) in (4.13); $\mathscr{J}_1$ and $\mathscr{J}_2$ for SC/MRC scheme at Bob/Eve and the MRC scheme at PR can be calculated as

$$\mathscr{J}_1{}^{SC/MRC} = \sum_{b=0}^{N_B-1}\sum_{d=1}^{N_E}\sum_{r=1}^{N_R}\frac{A(r)A(d)\Phi_B}{\xi_B}\left(1-\frac{e^{-\frac{\xi_B(2^{R_s}-1)}{\gamma_1}}}{\left(\frac{2^{R_s}\xi_B\gamma_2}{\gamma_1}+1\right)^d}\right)\left(1-e^{-\frac{\sigma}{\gamma_R}}\sum_{h=0}^{r-1}\frac{1}{h!}\left(\frac{\sigma}{\gamma_R}\right)^h\right) \quad (4.21)$$

and

$$\mathscr{J}_2{}^{SC/MRC} = \sum_{b=0}^{N_B-1}\sum_{d=1}^{N_E}\sum_{r=1}^{N_R}\sum_{h=0}^{r-1}\frac{\Phi_B}{\xi_B}A(d)A(r)\frac{e^{-\frac{\sigma}{\gamma_R}}}{h!}\left[\left(\frac{\sigma}{\gamma_R}\right)^h - \frac{e^{-\left(\frac{\xi_B(2^{R_s}-1)}{\gamma_1}+\frac{\sigma}{\gamma_R}\right)}}{\left(\frac{2^{R_s}\xi_B\gamma_2}{\gamma_1}+1\right)^d}\frac{\sigma^r}{\left(\frac{\xi_B(2^{R_s}-1)}{\sigma\gamma_1}+\frac{1}{\gamma_R}\right)^{r-h}}\right], \quad (4.22)$$

respectively. Hence, by substituting (4.21) and (4.22) in (4.13), the closed-form expressions of SOP for SC scheme is adopted at Bob, and the MRC scheme is employed at Eve, and PR can be calculated.

4.2.2 Intercept Probability

An intercept probability is an important performance metric in a passive eavesdropping scenario. Intercept probability is special case of SOP for $R_s = 0$, that means $\varepsilon(\gamma_E) = \gamma_E$. This subsection examines the intercept probability of the underlay CRN for SC and MRC schemes employed at Bob.

4.2.2.1 Intercept Probability with MRC/MRC Scheme

In this case, the MRC scheme is adopted by PR, Bob, and Eve. By substituting $R_s = 0$ and (4.18) and (4.19) in (4.13), after performing some simple mathematical manipulation the expressions for intercept probability with MRC scheme at PR, Bob and Eve can be calculated as

$$P_{int}^{MRC/MRC} = \sum_{b=1}^{N_B} \sum_{d=0}^{N_E} A(b)A(d) \left[1 - \sum_{a=0}^{b-1} \binom{a+d-1}{d-1} \left(\frac{\gamma_2}{\gamma_1}\right)^a \frac{1}{\left(1+\frac{\gamma_2}{\gamma_1}\right)^{a+d}} \right]. \tag{4.23}$$

4.2.2.2 Intercept Probability with SC/MRC Scheme

In this case, we adopt the SC scheme at Bob and the MRC scheme at both Eve and PR. By substituting (4.20), (4.16) and (4.17) in (4.13) and taking $R_s = 0$, the intercept probability for this case can be calculated as

$$P_{int}^{SC/MRC} = \sum_{b=0}^{N_B-1} \sum_{d=1}^{N_E} \frac{\Phi_B A(d)}{\xi_B} \left(1 - \frac{1}{\left(\frac{\xi_B \gamma_2}{\gamma_1} + 1\right)^d} \right). \tag{4.24}$$

It is worth noting that (4.23) and (4.24) involve only finite summations of exponentials, powers and thus can be computed in closed form. These expressions serve as a necessity for other metrics such as the PNZC and can be computed as

$$Pr(C_s > 0) = Pr(\gamma_M > \gamma_E) = 1 - P_{out}(0) = 1 - P_{int}. \tag{4.25}$$

4.2.3 Asymptotic Secrecy Outage Probability

It is very challenging to find insights from the exact expressions of SOP given above. Hence, the asymptotic nature of SOP in a high SNR regime of γ_1, i.e., $\gamma_1 \to \infty$, is a key point of consideration in this

subsection. As $\gamma_1 \to \infty$, it means Bob is located very near to Alice in comparison to the eavesdropper. When $\gamma_1 \to \infty$, the asymptotic CDF of γ_M with MRC and SC schemes can be written as

$$F_{\gamma_M}^{\infty\, MRC} = \frac{(1-\rho_B)^{N_B-1}\,\gamma_M}{\gamma_1}, \tag{4.26}$$

$$F_{\gamma_M}^{\infty\, SC} = \sum_{b=0}^{N_B-1} \frac{\Phi_B \gamma_M}{\gamma_1}, \tag{4.27}$$

respectively. In the following subsections, we investigate the asymptotic SOPs for MRC/MRC and SC/MRC schemes.

4.2.3.1 Asymptotic SOP with MRC/MRC Scheme at Bob/Eve and MRC Scheme at PR

This subsection investigates the asymptotic expression of secrecy outage probability for underlay CRN in an imperfect CSI scenario when the MRC scheme is adopted at PR, Bob, and Eve. To this end, by substituting (4.26), (4.16) and (4.17) in (4.13) and performing some simple mathematical manipulation; the asymptotic expression for SOP with MRC scheme can be calculated as

$$\begin{aligned} P_{out}^{\infty\, MRC/MRC} = (1-P_B)^{N_B-1} \sum_{d=1}^{N_E} \frac{A(d)}{\gamma_1} \Bigg[\left(2^{R_s}-1+d2^{R_s}\gamma_2\right) \sum_{r=1}^{N_R} A(r) \Bigg[1 - e^{-\frac{\sigma}{\gamma_R}} \sum_{h=0}^{r-1} \frac{1}{h!} \\ \left(\frac{\sigma}{\gamma_R}\right)^h \Bigg] + \sum_{d=1}^{N_E}\sum_{r=1}^{N_R} A(d)A(r) e^{-\frac{\sigma}{\gamma_P}} \left(\frac{d2^{R_s}\gamma_2}{\gamma_1} \sum_{h=0}^{r-1} \frac{1}{h!} \left(\frac{\sigma}{\gamma_R}\right)^h + \frac{(2^{R_s}-1)}{\sigma\gamma_1} \\ \sum_{z=0}^{r} \frac{1}{\Gamma(r)} \frac{\sigma^h \gamma_R^{1-z} r!}{z!} \right) \Bigg]. \end{aligned} \tag{4.28}$$

4.2.3.2 Asymptotic SOP with SC/MRC Scheme at Bob/Eve and MRC Scheme at PR

This subsection investigates the asymptotic SOPs when the SC scheme is adopted at Bob, and the MRC scheme is employed at PR and Eve. By substituting (4.27), (4.16) and (4.17) in (4.13) and performing some mathematical manipulation; the asymptotic expression for SOP with SC at Bob and the MRC scheme at Eve can be expressed as

$$\begin{aligned} P_{out}^{\infty\, SC/MRC} = \sum_{b=0}^{N_B-1} \sum_{d=1}^{N_E} \frac{\Phi_B A(d)}{\gamma_1} \Bigg[\left(2^{R_s}-1+2^{R_s}d\gamma_2\right) \sum_{r=1}^{N_R} A(r) \left(1 - e^{-\frac{\sigma}{\gamma_R}} \sum_{h=0}^{r-1} \frac{1}{h!} \left(\frac{\sigma}{\gamma_R}\right)^h \right) \\ + \sum_{b=0}^{N_B-1} \sum_{d=1}^{N_E} \sum_{r=1}^{N_R} \Phi_B A(d)A(r) e^{-\frac{\sigma}{\gamma_P}} \left(\frac{d2^{R_s}\gamma_2}{\gamma_1} \sum_{h=0}^{r-1} \frac{1}{h!} \left(\frac{\sigma}{\gamma_R}\right)^h + \frac{(2^{R_s}-1)}{\sigma\gamma_1} \sum_{z=0}^{r} \\ \frac{1}{\Gamma(r)} \frac{r!}{z!} \sigma^h \gamma_R^{1-z} \right) \Bigg]. \end{aligned} \tag{4.29}$$

The asymptotic SOPs given in (4.28) and (4.29) can be rewritten as

$$P_{out}^{\infty\ MRC/MRC} = \left(G_A^{MRC/MRC}\gamma_1\right)^{-G_D^{MRC/MRC}} + O\left(\gamma_1^{-G_D^{MRC/MRC}}\right), \tag{4.30}$$

$$P_{out}^{\infty\ SC/MRC} = \left(G_A^{SC/MRC}\gamma_1\right)^{-G_D^{SC/MRC}} + O\left(\gamma_1^{-G_D^{SC/MRC}}\right), \tag{4.31}$$

where $G_D^{MRC/MRC}$ and $G_D^{SC/MRC}$ are unity and the secrecy array gains are

$$G_A^{MRC/MRC} = \Bigg[(1-\rho_B)^{N_B-1}\sum_{d=1}^{N_E}A(d)\Bigg(\left(2^{R_s}-1+2^{R_s}d\gamma_2\right)\sum_{r=1}^{N_R}A(r)\Bigg(1-e^{-\frac{\sigma}{\gamma_R}}\sum_{h=0}^{r-1}\frac{1}{h!}\left(\frac{\sigma}{\gamma_R}\right)^h\Bigg)+\sum_{d=1}^{N_E}\sum_{r=1}^{N_R}A(d)A(r)e^{-\frac{\sigma}{\gamma_R}}\Bigg(\frac{d2^{R_s}\gamma_2}{\gamma_1}\sum_{h=0}^{r-1}\frac{1}{h!}\left(\frac{\sigma}{\gamma_R}\right)^h+\frac{(2^{R_s}-1)}{\sigma}\sum_{z=0}^{r}\frac{1}{\Gamma(r)}\frac{\sigma^h\gamma_R^{1-z}r!}{z!}\Bigg)\Bigg)\Bigg]^{-1}, \tag{4.32}$$

$$G_A^{SC/MRC} = \Bigg\{\sum_{b=0}^{N_B-1}\sum_{d=1}^{N_E}\Phi_B A(d)\Bigg[\left(2^{R_s}-1+2^{R_s}d\gamma_2\right)\sum_{r=1}^{N_R}A(r)\Bigg(1-e^{-\frac{\sigma}{\gamma_R}}\sum_{h=0}^{r-1}\frac{1}{h!}\left(\frac{\sigma}{\gamma_R}\right)^h\Bigg)+\sum_{b=0}^{N_B-1}\sum_{d=1}^{N_E}\sum_{r=1}^{N_R}\Phi_B A(d)A(r)e^{-\frac{\sigma}{\gamma_R}}\Bigg(\frac{d2^{R_s}\gamma_2}{\gamma_1}\sum_{h=0}^{r-1}\frac{1}{h!}\left(\frac{\sigma}{\gamma_R}\right)^h+\frac{(2^{R_s}-1)}{\sigma}\sum_{z=0}^{r}\frac{1}{\Gamma(r)}\frac{\sigma^h\gamma_R^{1-z}r!}{z!}\Bigg)\Bigg]\Bigg\}^{-1}. \tag{4.33}$$

Based on equations (4.32) and (4.33), the following observations can be made.

- MRC/MRC and SC/MRC schemes has same diversity order of unity. $G_D^{MRC/MRC}$ and $G_D^{SC/MRC}$ both are independent of N_B, N_E and N_R.
- MRC/MRC scheme offers lower SOP than SC/MRC scheme. It is explained by the fact that $G_A^{MRC/MRC} \geq G_A^{SC/MRC}$.
- The performance difference between MRC and SC at legitimate receiver Bob can be characterized by ratio of their array gain and it can be written as

$$\frac{G_A^{MRC/MRC}}{G_A^{SC/MRC}} = \left[\frac{(1-\rho_B)^{N_B-1}}{\sum_{b=0}^{N_B}\phi_B}\right]^{-1}. \tag{4.34}$$

  From (4.34), it is clear that for the same value of N_B and ρ_B, MRC/MRC scheme is better than SC/MRC scheme by an SNR gap of $-10\log\left[\frac{(1-\rho_B)^{N_B-1}}{\sum_{b=0}^{N_B}\phi_B}\right]$ dB.

4.2.4 ε-Outage Secrecy Capacity

ε-outage secrecy capacity is a vital secrecy performance metric. It can be calculated by using the numerical evaluation method. However, we utilize the Gaussian approximation approach to find the closed expressions for ε-outage secrecy capacity for MRC/MRC and SC/MRC schemes in this subsection in order to avoid numerical roots finding. Firstly, we calculate the k^{th} order moment of γ_M and γ_E. The k^{th} order moment of γ_M with MRC and SC schemes can be calculated as

$$\mathbb{E}[\gamma_M^k] = \int_0^\infty (\gamma_M)^k f_{\gamma_M}(\gamma_M) d\gamma_M, \tag{4.35}$$

where $f_{\gamma_M}(\gamma_M)$ is the PDF of γ_M and for MRC and SC schemes which can be expressed as

$$f_{\gamma_M}^{MRC}(\gamma_M) = \sum_{b=1}^{N_B} \frac{(\gamma_M)^{b-1} e^{-\frac{\gamma_M}{\gamma_1}}}{(b-1)!\gamma_1^b}, \tag{4.36}$$

$$f_{\gamma_M}^{SC}(\gamma_M) = \sum_{b=0}^{N_B-1} \frac{\phi_B}{\gamma_1} e^{-\frac{\gamma_M \xi_B}{\gamma_1}}, \tag{4.37}$$

respectively. By utilizing (4.36) and (4.37) in (4.35), k^{th} order moment of γ_M with MRC and SC schemes can be written as

$$\mathbb{E}^{MRC}[\gamma_M^k] = \sum_{b=1}^{N_B} A(b) \frac{(k+b-1)!}{(b-1)!} \gamma_1^k, \tag{4.38}$$

$$\mathbb{E}^{SC}[\gamma_M^k] = \frac{\phi_B k! \gamma_1^k}{\xi_B^{k+1}}, \tag{4.39}$$

respectively. Similarly, k^{th} order moment of γ_E with MRC scheme can be expressed as

$$\mathbb{E}[\gamma_E^k] = \sum_{d=1}^{N_E} A(d) \frac{(k+d-1)!}{(d-1)!} \gamma_2^k. \tag{4.40}$$

By utilizing [191], C_M can be expanded in Taylor series in term of γ_M as

$$C_M(\gamma_M) = \log_2(1+\mathbb{E}[\gamma_M]) + \log_2(e) \sum_{h=1}^{\infty} (-1)^{h-1} \frac{(\gamma_M - \mathbb{E}[\gamma_M])^h}{h(1+\mathbb{E}[\gamma_M])^h}. \tag{4.41}$$

By applying expectation operator to (4.41), the approximation of C_M can be written as

$$\mathbb{E}(C_M) \approx \log_2(1+\mathbb{E}[\gamma_M]) - \frac{\log_2 D[\gamma_M]}{2(1+\mathbb{E}(\gamma_M))^2}, \tag{4.42}$$

where $D[\gamma_M]$ is the variance of γ_M. By expanding C_M^2 in Taylor series about γ_M and using expectation operator, the second moment of C_M is approximated as

$$\mathbb{E}(C_M^2) = (\log_2(1+\mathbb{E}[\gamma_1]))^2 + \frac{D[\gamma_M]\log_2 e}{(1+\mathbb{E}[\gamma_M])^2}\log_2\left(\frac{e}{1+\mathbb{E}[\gamma_M]}\right). \tag{4.43}$$

According to (4.42) and (4.43), the variance of C_M can be written as

$$D[C_M] = \frac{(\log_2 e)^2 D[\gamma_M]}{(1+\mathbb{E}[\gamma_M])^2} - \frac{(\log_2 e)D^2[\gamma_M]}{4(1+\mathbb{E}[\gamma_M])^4}. \tag{4.44}$$

We can find the expectation and variance of C_E by putting the corresponding parameters into (4.42) and (4.43) respectively. Since C_s is a linear combination of two independent Gaussian R.Vs i.e., C_M and C_E, it is also a Gaussian R.V. Hence, we can say that $\mathbb{E}[C_s] = \mathbb{E}[C_M] - \mathbb{E}[C_E]$ and $D[C_s] = D[C_M] - D[C_E]$, where $\mathbb{E}[.]$ is the expectation and $D[.]$ is the variance. The Gaussian approximation of CDF of C_s can be written as

$$F_{C_s}(x) \approx 1 - \frac{1}{2}\text{erfc}\left(\frac{x-\mathbb{E}[C_s]}{\sqrt{2D[C_s]}}\right), \tag{4.45}$$

where erfc(.) is complementary error function. Thus, according to definition of ε-outage secrecy capacity and using (4.45), we have

$$\begin{aligned} C_{out}(\varepsilon) =& \log_2 e\left[\ln\left(\frac{\mu_M}{\mu_E}\right) - \frac{\sigma_M^2}{2\mu_M^2} + \frac{\sigma_E^2}{2\mu_E^2}\right] + \sqrt{2}\log_2 e\left[\frac{\sigma_M^2}{\mu_M^2} - \frac{\sigma_M^2}{4\mu_M^2} + \frac{\sigma_E^2}{\mu_E^2} - \frac{\sigma_E^2}{4\mu_E^2}\right] \\ & \times \text{erfc}^{-1}(2-2\varepsilon). \end{aligned} \tag{4.46}$$

where $\mu_l = 1+\mathbb{E}[\gamma_l]$, $l \in \{Bob(M), Eve(E)\}, \sigma_l^2 = \mathbb{E}[\gamma_l^2] - \mathbb{E}^2[\gamma_l]$.

4.3 Secrecy Performance Analysis in Active Eavesdropping Scenario

This section assumes an active eavesdropping scenario, i.e., the CSI of the eavesdropper channel is known to Alice. In this case, ASC is considered as a significant performance metric since Alice can accommodate its transmission rate according to the CSI of the main and wiretap channels to achieve perfect secrecy. We calculate the exact and asymptotic expressions of ASC for MRC/MRC and SC/MRC schemes in the succeeding subsections. Furthermore, we characterize the asymptotic ASC in terms of high SNR slope and high SNR power offset.

4.3.1 Average Secrecy Capacity

By remembering the definition of achieved secrecy rate defined in (1.45), we have [68]

$$\bar{C}_s = \int_0^{\infty} \int_{\gamma_E}^{\infty} [\log_2(1+\gamma_M) - \log_2(1+\gamma_E)]\, f_{\gamma_E}(\gamma_E) f_{\gamma_M}(\gamma_M) d\gamma_E d\gamma_M. \tag{4.47}$$

To solve the above integral, first, we perform integration by parts on inner integral and apply some algebraic manipulation; the ASC can be calculated as

$$\bar{C}_s = \frac{1}{\ln 2} \int_0^{\infty} \frac{F_{\gamma_E}(\gamma_E)}{1+\gamma_E} \left(\int_{\gamma_E}^{\infty} f_{\gamma_M}(\gamma_M) d\gamma_M \right) d\gamma_E. \tag{4.48}$$

4.3.1.1 Average Secrecy Capacity for MRC/MRC Scheme

The CDF of γ_E with MRC scheme can be given by

$$F_{\gamma_E}(\gamma_E) = \sum_{d=1}^{N_E} A(d) \left(1 - e^{-\frac{\gamma_E}{\gamma_2}} \sum_{a=0}^{d-1} \frac{\gamma_E^a}{a! \gamma_2^a} \right). \tag{4.49}$$

By inserting (4.36) and (4.49) in (4.48) and using [187, eq.3.353.5], the ASC for MRC/MRC scheme can be calculated as

$$\begin{aligned} C^{MRC/MRC} = \sum_{d=1}^{N_E} \sum_{b=1}^{N_B} \sum_{k=0}^{b-1} \frac{A(b)A(d)}{k! \gamma_1^k} \Bigg[& \left((-1)^{(k-1)} e^{\frac{1}{\gamma_1}} \mathrm{Ei}\left(-\frac{1}{\gamma_1} \right) + \sum_{c=1}^{k} (c-1)! (-1)^{k-c} \left(-\frac{1}{\gamma_1} \right)^c \right) \\ & + \sum_{a=0}^{d-1} \frac{1}{a! \gamma_2^a} \Bigg((-1)^{a+k-1} e^{\left(\frac{1}{\gamma_1}+\frac{1}{\gamma_2}\right)} \mathrm{Ei}\left(-\left(\frac{1}{\gamma_1} + \frac{1}{\gamma_2} \right) \right) + \sum_{t=1}^{a+k} (t-1)! (-1)^{a+k-t} \\ & \times \left(\frac{1}{\gamma_1} + \frac{1}{\gamma_2} \right)^{-t} \Bigg) \Bigg], \end{aligned} \tag{4.50}$$

where $\mathrm{Ei}(x) = -\int_{-x}^{\infty} \frac{e^{-t}}{t}$ is exponential integral.

4.3.1.2 Average Secrecy Capacity for SC/MRC Scheme

By inserting (4.49) and (4.37) in (4.48) and using [187, eq.3.353.1], the ASC for SC/MRC scheme can be written as

$$\begin{aligned} C_{SC/MRC} = \sum_{d=1}^{N_E} A(d) \frac{\Phi_B}{\xi_B} \left(-e^{\frac{\xi_B}{\gamma_1}} \right) Ei\left(-\frac{\xi_B}{\gamma_1} \right) + \sum_{d=1}^{N_E} \sum_{a=0}^{j-1} \frac{A(d)}{a!} \frac{1}{\gamma_2^a} \frac{\Phi_B}{\xi_B} \Bigg[& (-1)^{a-1} e^{\left(\frac{\xi_B}{\gamma_1}+\frac{1}{\gamma_2}\right)} \\ & \times \mathrm{Ei}\left(-\left(\frac{\xi_B}{\gamma_1} + \frac{1}{\gamma_2} \right) \right) + \sum_{c=1}^{a} (c-1)! (-1)^{(a-c)} \left(\frac{\xi_B}{\gamma_1} + \frac{1}{\gamma_2} \right)^{-c} \Bigg]. \end{aligned} \tag{4.51}$$

4.3.2 Asymptotic Average Secrecy Capacity

In order to analyze the consequences of the system's parameters on the secrecy performance of the proposed network, we examine the ASC in the high SNR regime. We calculate asymptotic expressions of average secrecy capacity for MRC/MRC and SC/MRC schemes in the preceding subsections. Furthermore, we also provide two metrics, i.e., high SNR slope and the high SNR power offset for MRC/MRC and SC/MRC schemes, which characterize the impact of main parameters such as correlation coefficients (ρ_B, ρ_E and ρ_R), number of antennas (N_B, N_E and N_R) and average SNRs (γ_1, γ_2, and γ_R), on average secrecy capacity.

4.3.2.1 Asymptotic Average Secrecy Capacity for MRC/MRC Scheme

For $\sum_{d=1}^{N_E} A(d) = 1$, (4.49) can be written as $F_{\gamma_E}(\gamma_E) = 1 - T_{\gamma_E}(\gamma_E)$, where

$$T_{\gamma_2}(\gamma_E) = \sum_{d=1}^{N_E} A(d) \exp\left(-\frac{\gamma_E}{\gamma_2}\right) \sum_{a=0}^{d-1} \frac{1}{a!} \left(\frac{\gamma_E}{\gamma_2}\right)^a. \tag{4.52}$$

Taking this into consideration, the asymptotic ASC can be expressed as

$$\begin{aligned} C_{MRC/MRC} =& \frac{1}{\ln 2} \int_0^\infty \left[\int_0^{\gamma_M} \frac{1 - T_{\gamma_2}(\gamma_E)}{1+\gamma_E} d\gamma_E \right] f_{\gamma_M}(\gamma_M) d\gamma_M \\ =& \tau_1 - \tau_2, \end{aligned} \tag{4.53}$$

where τ_1 and τ_2 can be calculated as

$$\tau_1 = \frac{1}{\ln 2} \int_0^\infty \ln(1+\gamma_M) f_{\gamma_1}(\gamma_M) d\gamma_M, \tag{4.54}$$

$$\tau_2 = \frac{1}{\ln 2} \int_0^\infty \frac{T_{\gamma_2}(\gamma_E)}{1+\gamma_E} f_{\gamma_1}(\gamma_M) d\gamma_E d\gamma_M. \tag{4.55}$$

Now, we investigate τ_1 and τ_2 in the high SNR regime respectively. Hence, $\gamma_M \to \infty$, $\ln(1+\gamma_M) \approx \ln(\gamma_M)$. Hence, by substituting (4.36) in (4.54) and using [187, eq.4.352.1], we have

$$\tau_1^\infty = \frac{1}{\ln 2} \sum_{b=1}^{N_B} A(b) \psi(b) + \sum_{b=1}^{N_B} A(b) \log_2 \gamma_1, \tag{4.56}$$

where $\psi(b) = \frac{d}{db} \ln(\Gamma(b))$ is the digamma function. According to [68, eq.19], the asymptotic expression for τ_2 can be written as

$$\tau_2^\infty = \frac{1}{\ln 2} \int_0^\infty \frac{T_{\gamma_2}(\gamma_E)}{1+\gamma_E} d\gamma_E = \frac{1}{\ln 2} \sum_{d=0}^{N_E} \sum_{a=0}^{d-1} \frac{A(d) e^{\frac{1}{\gamma_2}}}{a! \gamma_2^a} \Gamma(1+a) \Gamma\left(-a, \frac{1}{\gamma_2}\right). \tag{4.57}$$

By substituting (4.56) and (4.57) in (4.53), the asymptotic average secrecy capacity derived as

$$C^{\infty}_{MRC/MRC} = \frac{1}{\ln 2}\sum_{b=1}^{N_B} A(b)\left[\psi(b) + \log_2 \gamma_M - \frac{1}{\ln 2}\sum_{d=0}^{N_E}\sum_{a=0}^{d-1}\frac{A(d)e^{\frac{1}{\gamma_2}}}{a!\gamma_2^a}\Gamma(1+l)\Gamma\left(-a, \frac{a}{\gamma_2}\right)\right]. \tag{4.58}$$

We also examine the high SNR power offset and high SNR slope to characterize the asymptotic average SNR in a high SNR regime like a conventional non-secrecy network. The asymptotic ASC in (4.58) can be written as

$$C^{\infty}_{MRC/MRC} = \check{S}^{MRC/MRC}_{\infty}\left(\log_2 \gamma_1 - Ł^{MRC/MRC}_{\infty}\right), \tag{4.59}$$

where $\check{S}^{MRC/MRC}_{\infty}$ is the high SNR slope in bits/s/Hz (3 dB) and $Ł^{MRC/MRC}_{\infty}$ is the high SNR power offset in 3 dB units. According to [67], $\check{S}_{\infty}$ can be calculated as

$$\check{S}^{MRC/MRC}_{\infty} = \lim_{\gamma_1\to\infty}\frac{C^{\infty}_{MRC/MRC}}{\log_2 \gamma_1}. \tag{4.60}$$

Putting (4.58) into (4.60) and performing some mathematical calculations,we have

$$\check{S}^{MRC/MRC}_{\infty} = \sum_{b=1}^{N_B} A(b) = 1. \tag{4.61}$$

(4.61) exemplifies that the high SNR slope is independent of key parameters like correlation coefficients, N_B and N_E. The high SNR power offset can be expressed as

$$\begin{aligned} Ł^{MRC/MRC}_{\infty} &= \lim_{\gamma_1\to\infty}\left(\log_2 \gamma_1 - \frac{C^{\infty}_{s}}{\check{S}_{\infty}}\right) \\ &= Ł^{N_B}_{\infty} + Ł^{N_E}_{\infty}. \end{aligned} \tag{4.62}$$

It is clear that $Ł_{\infty}$ characterize the effect of main channel and Eve's channel on C_s. By substituting (4.58) and (4.61) in (4.71), we have

$$Ł^{N_B}_{\infty} = -\frac{1}{\ln 2}\sum_{b=1}^{N_B} A(b)\psi(b), \tag{4.63}$$

$$Ł^{N_E}_{\infty} = \tau^{\infty}_2. \tag{4.64}$$

From the above analysis, we conclude that critical parameters of the main channel such as N_B and ρ_B positively impact ASC, i.e., ASC improves with increasing N_B and ρ_B. On the other hand, the critical parameters of Eve's channel like N_E, ρ_E have a negative impact on C_s, i.e., secrecy performance of network decreases with increasing N_E and ρ_E.

4.3.2.2 Asymptotic Average Secrecy Capacity for SC/MRC Scheme

The asymptotic average secrecy capacity for SC/MRC can be written as

$$C_{SC/MRC}^{\infty} = \Omega_1^{\infty} - \Omega_2^{\infty}, \tag{4.65}$$

where Ω_1^{∞} and Ω_2^{∞} can be calculated as

$$\Omega_1^{\infty} = \frac{1}{\ln 2}\int_0^{\infty} \ln(\gamma_M) f_{\gamma_1}(\gamma_M) d\gamma_M = \frac{1}{\ln 2}\sum_{b=1}^{N_B-1} \frac{\Phi_B}{\xi_B}\left(\psi(1) - \ln(\xi_B)\right) + \sum_{b=1}^{N_B-1} \frac{\Phi_B}{\xi_B}\log_2 \gamma_1, \tag{4.66}$$

$$\Omega_2^{\infty} = \tau_2^{\infty}. \tag{4.67}$$

To this end, by putting (4.66) and (4.67) in (4.65), the asymptotic ASC is expressed as

$$\begin{aligned} C_{SC/MRC}^{\infty} =& \frac{1}{\ln 2}\sum_{b=1}^{N_B-1} \frac{\Phi_B}{\xi_B}\left(\psi(1) - \ln(\xi_B)\right) + \sum_{b=1}^{N_B-1} \frac{\Phi_B}{\xi_B}\log_2 \gamma_1 - \frac{1}{\ln 2}\sum_{d=1}^{N_E}\sum_{a=0}^{d-1} \frac{A(d)}{a!\gamma_2^a}\exp\left(\frac{1}{\gamma_2}\right) \\ & \Gamma(1+a)\Gamma\left(-a, \frac{1}{\gamma_2}\right), \end{aligned} \tag{4.68}$$

which can be written as

$$C_{SC/MRC}^{\infty} = \check{S}_{\infty}^{SC/MRC}\left(\log_2 \gamma_1 - Ł_{\infty}^{SC/MRC}\right). \tag{4.69}$$

where $\check{S}_{\infty}^{SC/MRC}$ is the high SNR slope in bits/s/Hz (3 dB) and $Ł_{\infty}^{SC/MRC}$ is the high SNR power offset in 3dB units. According to [192], $\check{S}_{\infty}$ can be calculated as

$$\check{S}_{\infty}^{SC/MRC} = \lim_{\gamma_1 \to \infty} \frac{C_{SC/MRC}^{\infty}}{\log_2 \gamma_1} = \sum_{b=1}^{N_B-1} \frac{\Phi_B}{\xi_B} = 1. \tag{4.70}$$

Hence, for SC/MRC high SNR slope is unity, that means it is independent of correlation coefficients and number of antenna at Bob and eavesdropper. High SNR power offset is expressed as

$$Ł_{\infty}^{SC/MRC} = \lim_{\gamma_1 \to \infty}\left(\log_2 \gamma_1 - \frac{C_{SC/MRC}^{\infty}}{\check{S}_{\infty}^{SC/MRC}}\right) = Ł_{\infty}^{N_B} + Ł_{\infty}^{N_E}, \tag{4.71}$$

where, $Ł_{\infty}^{N_B} = -\frac{1}{\ln 2}\sum_{b=1}^{N_B-1}\left(\psi(1) - \ln(\xi_B)\right)$ and $Ł_{\infty}^{N_E} = \Omega_2^{\infty}$.

From the above analysis, we find that the high power offset of the SC/MRC scheme is always more significant than the MRC/MRC scheme for a given value of N_B and ρ_B. It means that the average secrecy capacity of the MRC/MRC scheme is always greater than SC/MRC for constant parameters.

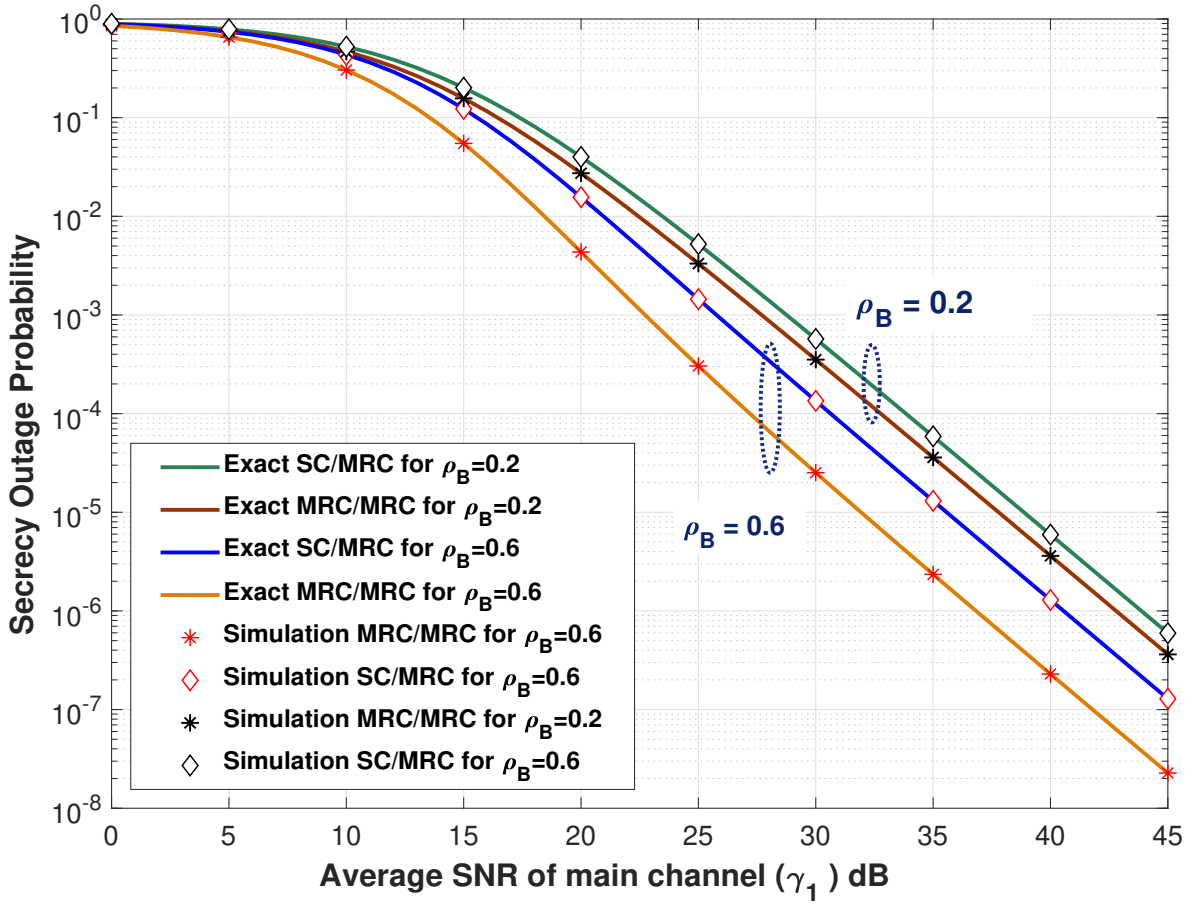

Figure 4.2: SOP versus γ_1 with $\gamma_R = 0$ dB, $\gamma_2 = 10$ dB, $\rho_E = 0.1$, $\sigma = 0.8$ and $\rho_P = 0.2$

4.4 Numerical Examples and their Interpretation

The impact of outdated CSI and different diversity combining techniques on the secrecy performance is investigated and presented by numerical results in this section. Furthermore, Monte Carlo simulation is done to check the validity of our results. The parameter R_s is set to be 1 nats/s/Hz throughout the analysis.

Figure 4.2 and Figure 4.3 plot exact SOP and intercept probability of two combining techniques (SC/MRC and MRC/MRC) for different values of ρ_B. It is apparent that SOP and intercept probability decrease as the main channel's average SNR γ_1 increases, as shown in Figure 4.2 and Figure 4.3. The increasing γ_1 increases the capacity of the main channel, which in turn reduces the SOP. Furthermore, the SOP and intercept probability decrease with increasing ρ_B. It is because the quality of main channel estimation also improves with increasing ρ_B.

Figure 4.4 plots exact and asymptotic SOP versus γ_1 for different value of ρ_R. Figure 4.4 depicts that at a high SNR regime, the parallel lines of asymptotic SOP approximate the exact SOP. These parallel lines of asymptotes authenticate that secrecy diversity order is independent of γ_E, ρ_E and N_E. Figure 4.4

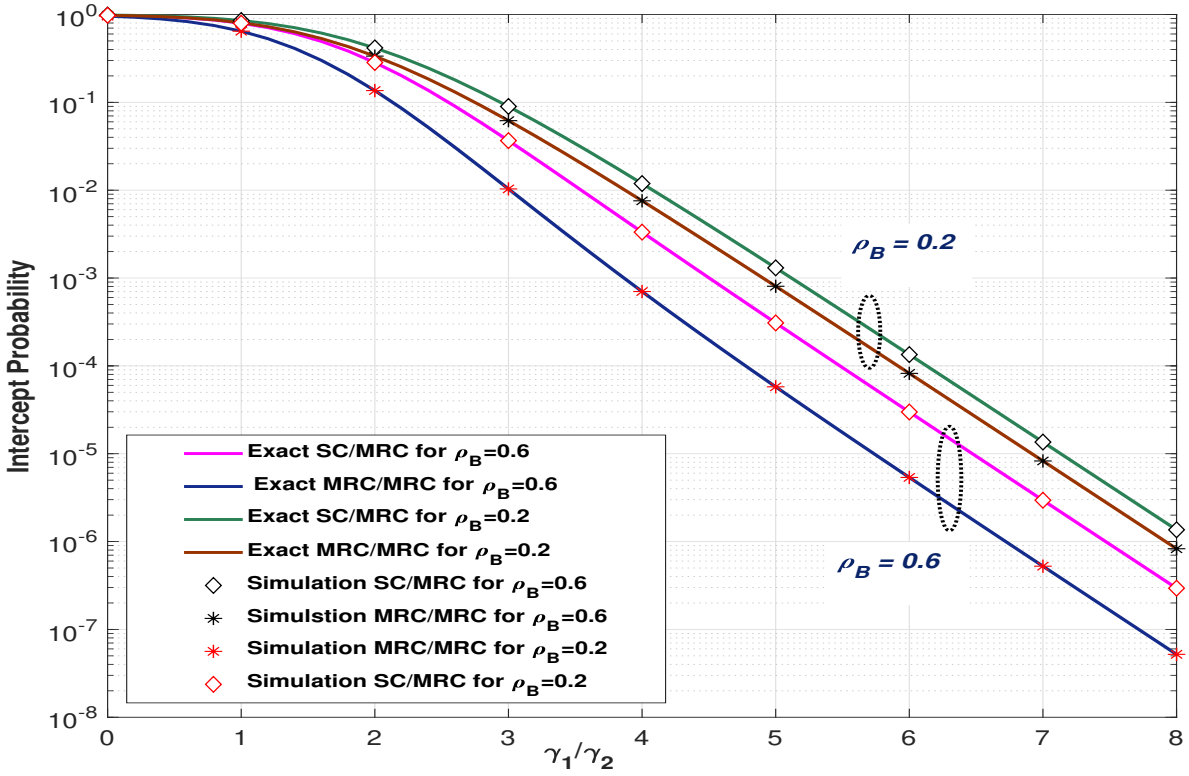

Figure 4.3: Intercept probability versus γ_1 with $\gamma_R = 0$ dB, $\gamma_2 = 10$ dB, $\rho_E = 0.1$, $\sigma = 0.8$ and $\rho_P = .01$

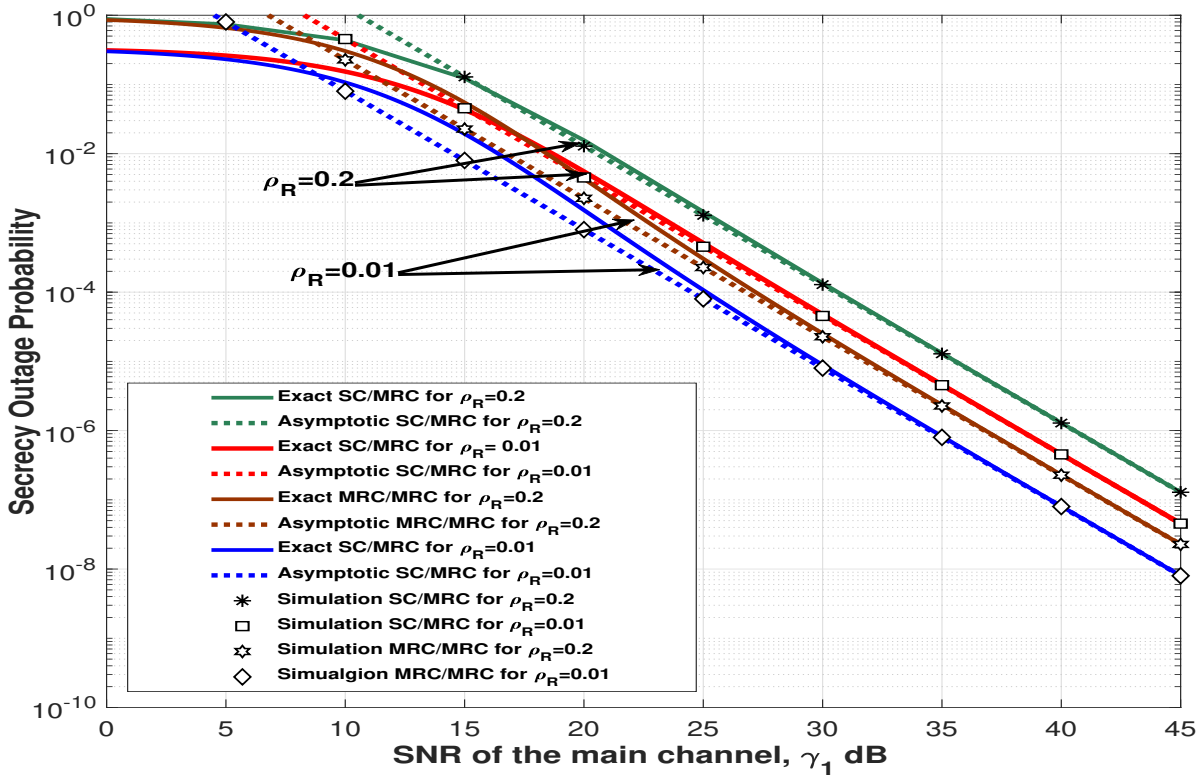

Figure 4.4: Exact and asymptotic SOP versus γ_1 dB with $R_s = 1, \gamma_R = 0$ dB, $\gamma_2 = 10$ dB, $\rho_E = 0.1$, $\sigma = 0.8$ and $\rho_B = 0.6$

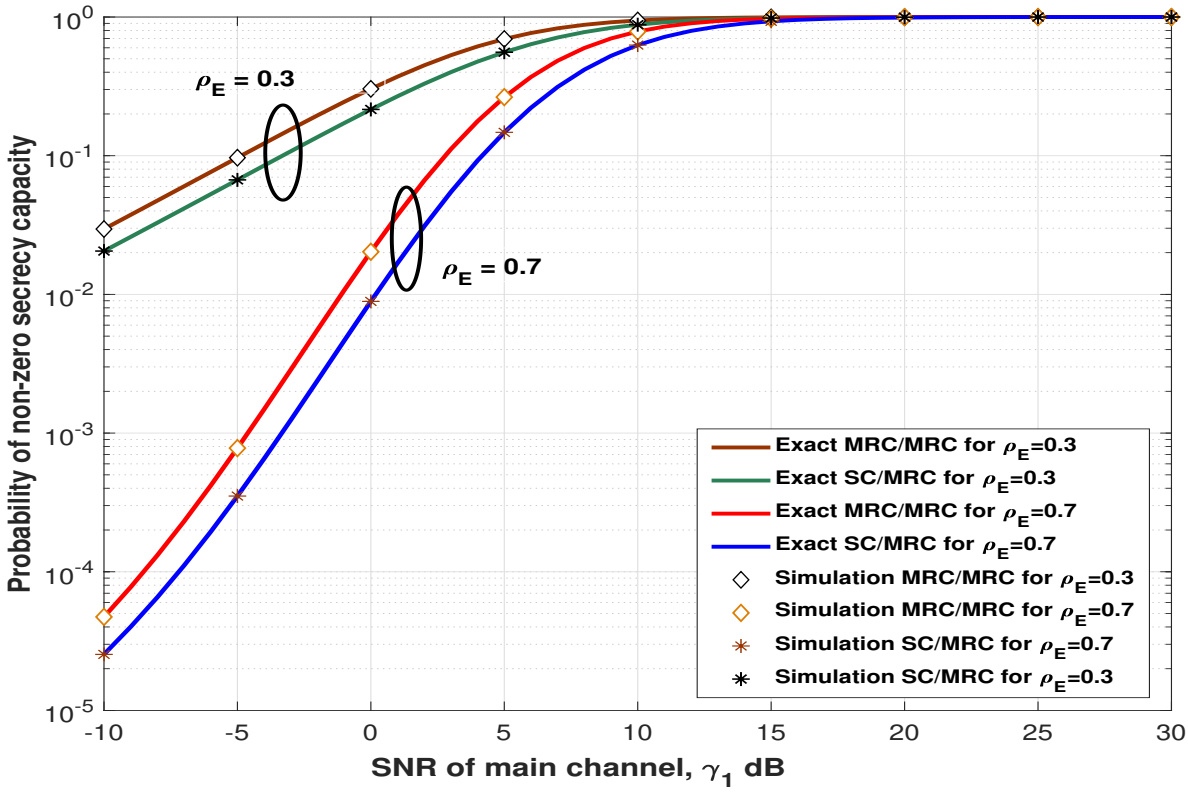

Figure 4.5: Probability of non-zero secrecy capacity as a function of γ_1 for varying ρ_B with $\rho_B = 0.3$, $\gamma_2 = 5$ dB, $N_B = 4$, $N_R = 2$ and $N_E = 5$

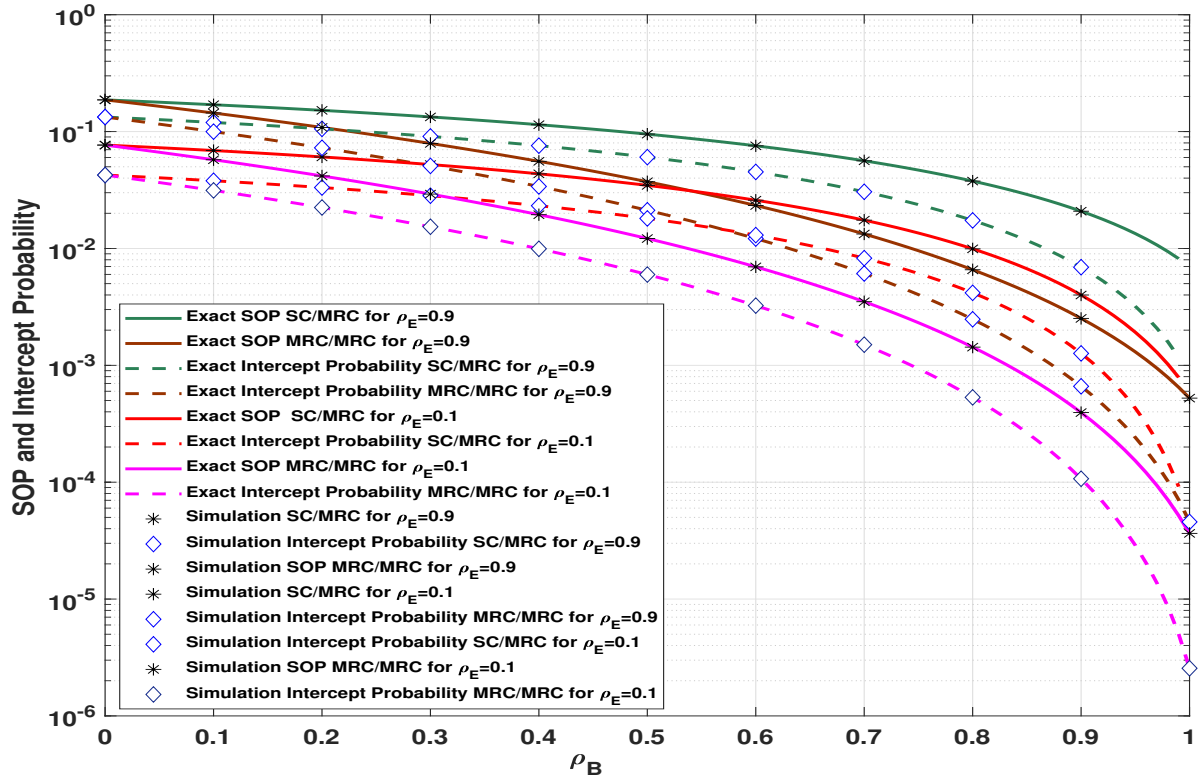

Figure 4.6: SOP and intercept probability versus ρ_B for different value of ρ_E

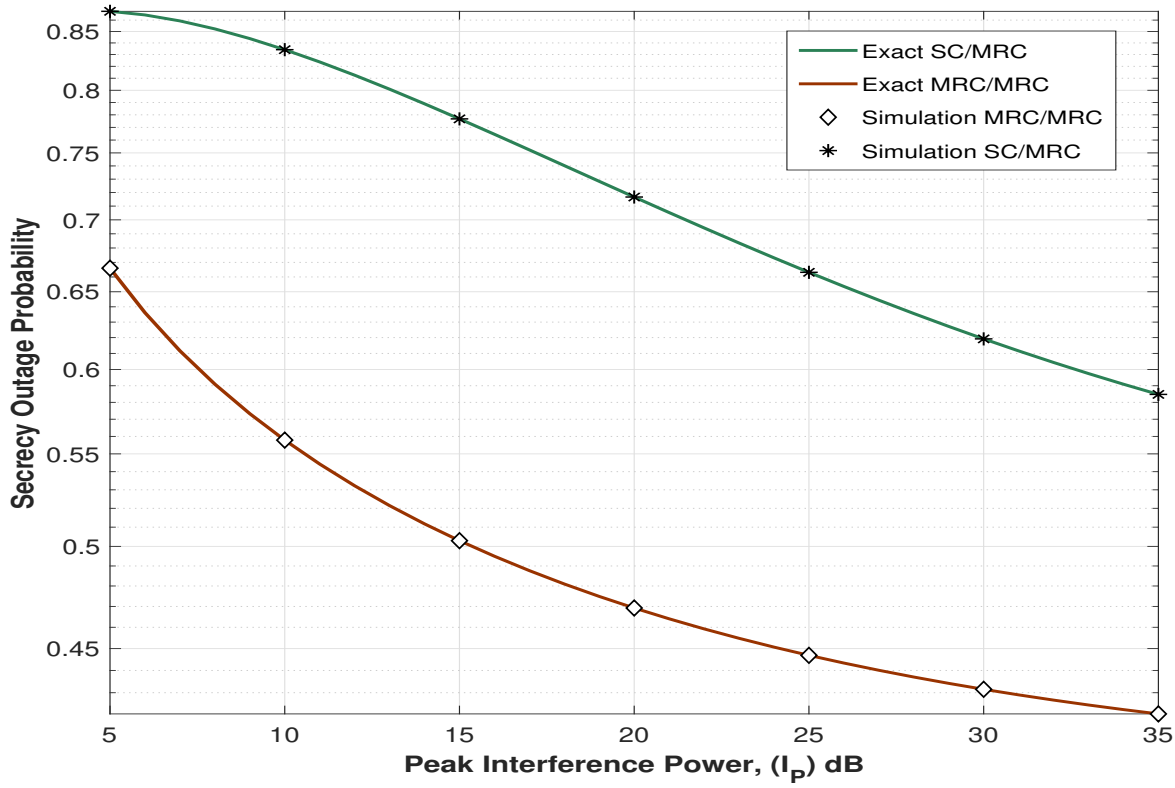

Figure 4.7: SOP versus peak interference power for $\rho_B = 0.5$, $\rho_E = 0.8$, $\rho_R = 0.1$, $\gamma_1 = 8$ dB, $\gamma_2 = \gamma_R = 0$ dB, $P_T = 15$ dB, $N_A = 2$, $N_R = 2$, $N_E = 5$ and $N_B = 2$

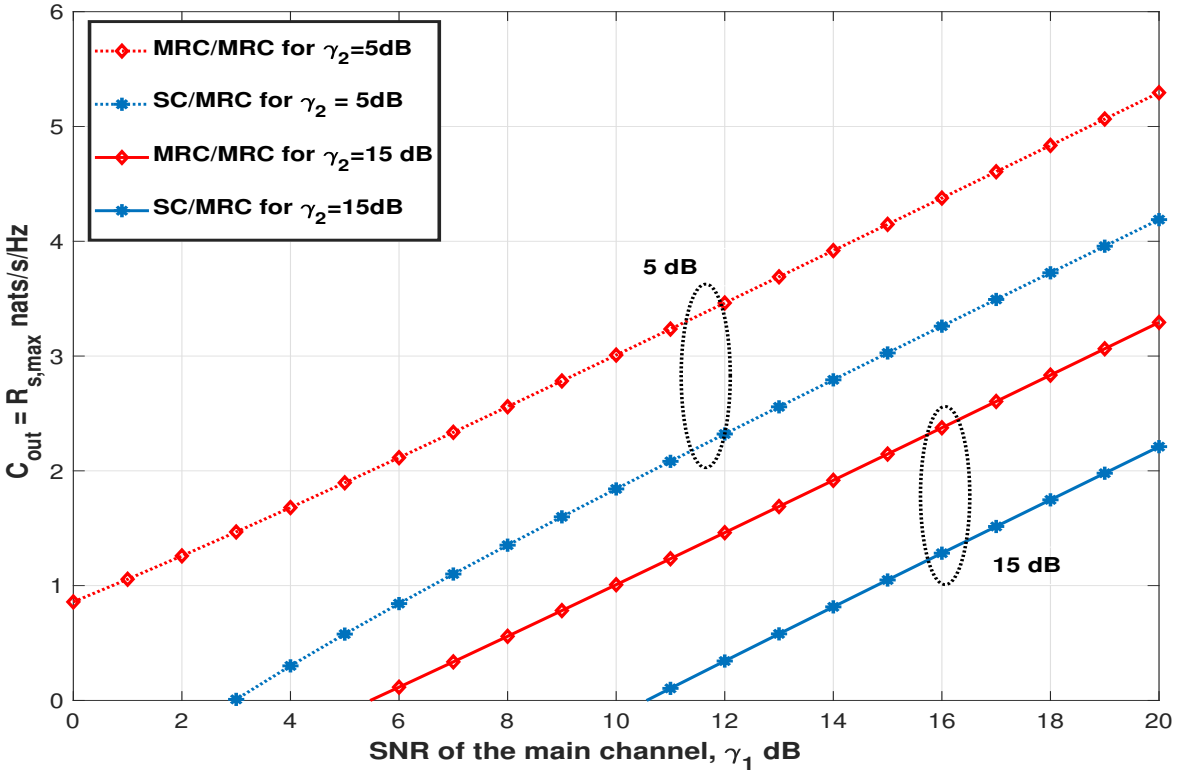

Figure 4.8: ε-Outage secrecy capacity versus SNR of main channel for $\varepsilon = 0.9$, $\rho_B = 0.9$ and $\rho_E = 0.4$

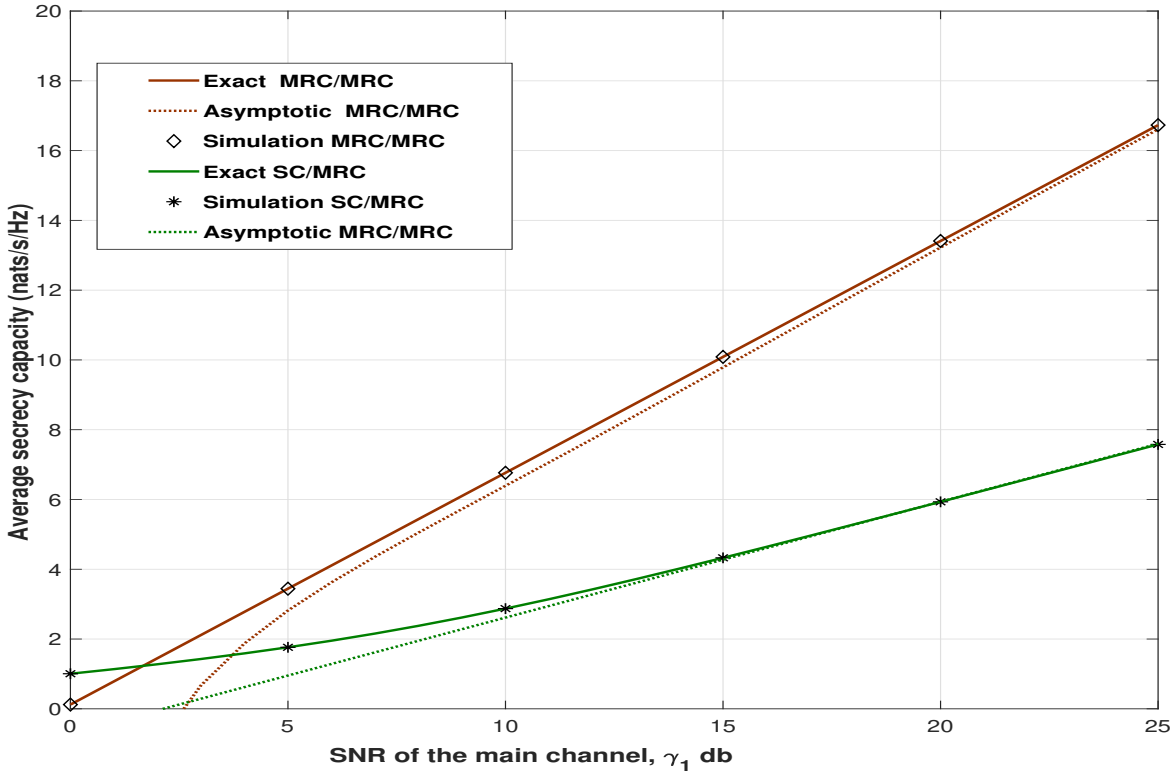

Figure 4.9: Average secrecy capacity versus γ_1 for $N_B = N_E = 2$, $\rho_B = \rho_E = 0.9$

describes that the SOP decreases with decreasing ρ_R. It is because decreasing the value of ρ_R will decrease the channel estimation at PR, resulting in more power utilization at Alice.

Figure 4.5 plots PNZC versus γ_1 for different value of ρ_B. From Figure 4.5, it is observed that PNZC exists if the SNR of the wiretap channel is greater than the SNR of the main channel. Figure 4.6 shows SOP and intercept probability versus ρ_B for various ρ_E. Figure 4.6 depicts that the secrecy performance of the system is degraded with increasing ρ_E. It is because the estimation of Eve's channel improves with increasing ρ_E. In addition, as shown in Figure 4.6, the SOP and intercept probability improve with the MRC scheme over the SC scheme as ρ_B increases.

Figure 4.7 depicts SOP versus peak interference power, $\bar{I}_P$. It is apparent from Figure 4.7 that the SOP decreases with increasing $\bar{I}_P$. It is because the peak interference power is proportional to $\bar{P}_T$, i.e., $\bar{I}_P = \sigma \bar{P}_T$, which increases the transmit power of Alice, as shown in (4.3).

Figure 4.8 plots ε-outage secrecy capacity versus γ_1 for different value of γ_2 and for $P_{out} = 0.8$ for two combining techniques. It is depicted from figure 4.8 that the ε- outage secrecy capacity is non-zero even when $\gamma_M \leq \gamma_E$ as long as $P_{out} \geq 0.5$.

Figure 4.9 plots average secrecy versus γ_1 for two combining techniques. From Figure 4.9, it is clear that the ASC increases with increasing γ_1. Since the high power offset of the SC/MRC scheme is always greater than the MRC/MRC scheme for the given value of N_B and ρ_B hence, the data security capability of the MRC/MRC scheme is higher than SC/MRC scheme.

4.5 Conclusion

In this chapter, we have examined the impact of the outdated CSI on the secrecy performance of the underlay CRN in a Rayleigh fading environment for two distinct scenarios: 1) Scenario I: passive eavesdropping, 2) Scenario II: active eavesdropping. The closed-form expressions for SOP, intercept probability, and $\varepsilon-$outage secrecy capacity has been investigated for Scenario I. These expressions reveal that the secrecy performance of the proposed network improves with increasing ρ_B from 0 to 1. As expected at $\rho_B = 1$, i.e., perfect CSI of the main channel, maximum secrecy is achieved. On the other hand, the secrecy performance of the network decreases as ρ_E increases from 0 to 1. Furthermore, the asymptotic SOP expressions reveal a special relationship between the secrecy array gain of SC/MRC and MRC/MRC combining techniques. Both SC/MRC and MRC/MRC techniques obtain the same secrecy diversity order. For Scenario II, the closed-form expressions for the exact and asymptotic ASC have been derived, which help us to describe the impact of the main and wiretap channel on a power offset. We also find that the power offset of the SC/MRC scheme is more than that of the MRC/MRC scheme for a given value of N_B and ρ_B. It means that the MRC/MRC scheme achieves more security than that of the SC/MRC scheme.

Chapter 5

Secrecy Performance with Interference Constraint

In previous chapters, we ignored the interference caused by the primary transmitter to secondary receivers. However, in a practical scenario, this interference exists when PT lies close to Bob and deteriorates the secondary network's performance. Thus, in this chapter, we have considered the interference caused by the PT as an exponentially distributed RV. This chapter analyzes the secrecy performance of CRN that consists of Alice, Bob, PR, and Eve and a dominant interferer called P.T. Alice transmits secret information on its single best antenna among N_A available antennas to Bob, and Eve tries to intercept that information. Depending upon the availability of the CSI of the main channel and wiretap channel, we analyze the secrecy performance of the underlay CRN in the Rayleigh fading environment for both passive and active eavesdropping scenarios. In this case, the quantity of interest is SINR, and we obtain analytical expressions for the SOP, intercept probability, and ε-outage secrecy capacity for the considerable value of N_A in a passive eavesdropping scenario. A thorough study of the ASC has been done, and novel expressions for the exact and asymptotic ASC have been derived for active eavesdropping. Supporting these results, we also define a high SINR power offset, which quantifies the consequence of the system's parameters on the ASC explicitly.

The analysis of PLS in the previous chapters relies on the presumption of perfect CSI of the PR-Alice link under peak interference power constraint, which is very challenging to implement in practice situations due to the time-varying properties or feedback latency from the PU [32]. This is because it cannot be guaranteed that the interference power at PR will remain below the predetermined threshold at all times. After all, the secondary user must be silent at all times to satisfy such a constraint, which makes the capacity of the secondary link zero [193]. For this reason, it makes sense to consider a constraint based on a stochastic concept; it means PR should allow a specific percentage of an outage, which is

called outage probability. The term outage probability means that the interference power at PR exceeds the predetermined threshold for a particularized percentage of the time. Therefore, we examine the consequence of outdated CSI on the secrecy performance for both cases when interference from PT to SU exits under peak interference power constraint.

5.1 System Model

We assume an underlay CRN as shown in Figure 5.1, where the primary network consists of one PT and one PR, whereas the secondary network comprises of Alice, Bob, and Eve. Since the primary network is a traditional wireless system, we suppose that both PT and PR have a single antenna [145]. On the other hand, Alice is outfitted with N_A antennas for improving the PLS of the secondary network and lessening the interference to the primary network. In contrast, Bob and Eve are equipped with a single antenna because the high hardware cost and power consumption of multiple radio frequency chains can significantly be reduced with a single antenna scheme at Bob and Eve. To achieve diversity benefits, we have used the best antenna selection scheme at Alice. This antenna selection scheme not only achieves diversity benefits but also reduces the hardware complexity. Throughout this chapter, the following assumptions are adopted.

- Similar to [109], [145], [112], and [32], we consider the environment where the interference from the PT to Bob and Eve exists.
- Similar to [69] and [62], without loss of generality, we assume that Eve does not lie in the radio path of the Bob; hence the main and eavesdropper's channel are statistically independent and undergo Rayleigh fading.

Let g denote the channel coefficient between a PT and Bob, t that between a PT and Eve, and h_{j0} that between j^{th} antenna of Alice and PR. Similarly, let h_j denote the channel coefficient between j^{th} antenna of Alice and Bob, and s_j that between j^{th} antenna of Alice and Eve. We assume that the channel coefficients of $|h_{j0}|, |g|$, $|h_j|$, $|s_j|$ and $|t|$ are i.i.d Rayleigh distributed R.Vs and channel power gains, $|h_{j0}|^2$, $|g|^2$, $|h_j|^2$, $|s_j|^2$ and $|t|^2$ have PDFs $f_{|h_{j0}|^2}(x) = \frac{e^{-\frac{x}{\Omega_0}}}{\Omega_0}$, $f_{|g|^2}(x) = \frac{e^{-\frac{x}{\lambda}}}{\lambda}$, $f_{|h_j|^2}(x) = \frac{e^{-\frac{x}{\beta_1}}}{\beta_1}$, $f_{|s_j|^2}(x) = \frac{e^{-\frac{x}{\beta_2}}}{\beta_2}$ and $f_{|t|^2}(x) = \frac{e^{-\frac{x}{\eta}}}{\eta}$ respectively [145]. We use the notations $F_{|h_{j0}|^2}, F_{|g|^2}, F_{|h_j|^2}, F_{|s_j|^2}$ and $F_{|t|^2}$ to denote the CDF of $|h_{j0}|^2$, $|g|^2$, $|h_j|^2$, $|s_j|^2$ and $|t|^2$ respectively. The link between Alice-Bob, Alice-Eve, PT-Bob and PT-PR is called the main channel, eavesdropper's channel, primary interference channel and primary channel, respectively. Similar to [109] and [112], it is assumed that Alice has perfect CSI regarding the Alice-PR channel, h_{j0}. Alice can be informed about h_{j0} through a mediate band manager between PR and Alice [17] or by considering proper signalling [194]. However, the impact of imperfect CSI of the

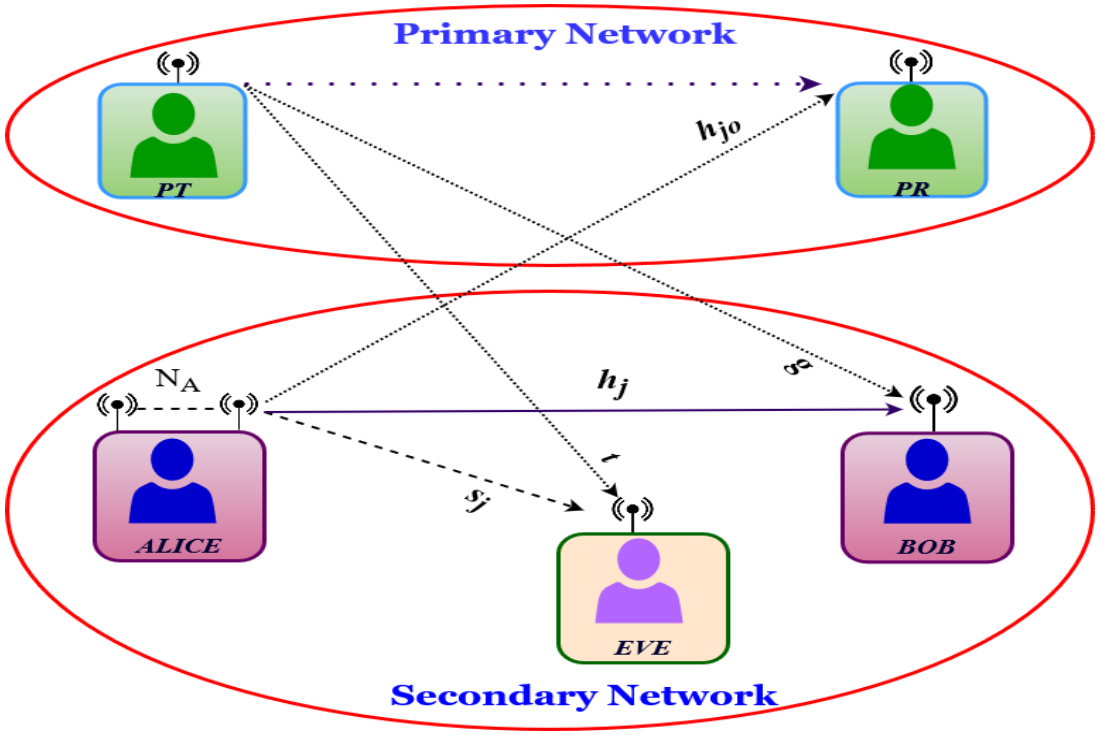

Figure 5.1: An underlay cognitive radio network with multi-antenna Alice. We assume that interference from PT to Bob and Eve exists.

Alice-PR channel on an underlay CRN's secrecy performance will be discussed later in this chapter. The SINRs at Bob and Eve due to the $j^{th}(1 \leq j \leq N_A)$ transmit antenna are, respectively, expressed as

$$\Phi_M = \frac{|h_j|^2 P_A}{1 + P_P|g|^2}, \; \Phi_E = \frac{|s_j|^2 P_A}{1 + P_P|t|^2}, \tag{5.1}$$

where P_P is the normalized transmit power of primary transmitter and Alice's normalized transmit power P_A can be expressed as

$$P_A = \frac{\bar{P}_A}{N_0} = \min\left(P_T, \frac{I_P}{|h_{j0}|^2}\right), \tag{5.2}$$

where $P_T = \frac{\bar{P}_T}{N_0}$ and $I_P = \frac{\bar{I}_P}{N_0}$. $P_P|g|^2$ and and $P_P|t|^2$ are the interference powers caused by the primary transmitter at Bob and Eve, respectively. Furthermore, we consider a continuous power adaptation scheme in which the transmit power of Alice can be adapted without any power limit, i.e., the maximum transmit power, $P_T = \infty$ [109], [113]. In such case, Alice transmit power P_A can be written as $P_A = \frac{I_P}{|h_{j0}|^2}$.

5.2 Secrecy Performance Analysis

This section shows a complete study on the secrecy performance of a proposed cognitive radio network in the presence of PT's interference.

5.2.1 Determining the CDF and PDF of Φ_M and Φ_E

Before examining the secrecy performance in detail, first, we introduce a set of statistical properties of SINRs of Φ_M and Φ_E, which will be repeatedly requested in the succeeding derivations.

Lemma 5.1. *The CDF and PDF of Φ_M are, respectively, expressed as*

$$F_{\Phi_M}(x) = 1 - \frac{\mathscr{Q}}{(x+\mathscr{Q})} e^{-\frac{x}{\beta_1 P_A}}, \tag{5.3}$$

$$f_{\Phi_M}(x) = e^{-\frac{x}{\beta_1 P_A}} \left[\frac{\mathscr{Q}}{(x+\mathscr{Q})^2} + \frac{1}{P_p \lambda} \frac{1}{(x+\mathscr{Q})} \right], \tag{5.4}$$

where $\mathscr{Q} = \frac{\beta_1 P_A}{P_p \lambda}$.

Proof: The CDF of Φ_M is calculated by conditioning on $|g|^2$ as [112]

$$F_{\Phi_M}(x) = \int_0^\infty F_{|h_j|^2}\left(\frac{x}{P_A} + \frac{P_P x y}{P_A}\right) f_{|g|^2}(y) dy, \tag{5.5}$$

where the CDF $F_{|h_j|^2}(x)$ is expressed as

$$F_{|h_j|^2}(x) = 1 - e^{-\frac{x}{\beta_1}}. \tag{5.6}$$

Substituting (5.6) and PDF of $|g|^2$ in (5.5) and performing some simple mathematical manipulation, we obtain closed-form expression of CDF of Φ_M as shown in (5.3). The PDF of Φ_M, $f_{\Phi_M(x)}$ can be calculated by differentiating the CDF of Φ_M and can be expressed in (5.4).

Lemma 5.2. *The CDF and PDF of Φ_E in the presence of dominant interferer PT are, respectively, expressed as*

$$F_{\Phi_E}(x) = 1 - \frac{\mathscr{D} e^{-\frac{x}{\beta_2 P_A}}}{(x+\mathscr{D})}, \tag{5.7}$$

$$f_{\Phi_E}(x) = \frac{\mathscr{D} e^{-\frac{x}{\beta_2 P_A}}}{(x+\mathscr{D})^2} + \frac{1}{\eta P_P} \frac{e^{-\frac{x}{\beta_2 P_A}}}{(x+\mathscr{D})}, \tag{5.8}$$

where $\mathscr{D} = \frac{\beta_2 P_A}{\eta P_p}$.

Proof: The CDF of Φ_E is calculated by conditioning on $|t|^2$ as

$$F_{\Phi_E}(x) = \int_0^\infty F_{|s_j|^2}\left(\frac{x}{P_A} + \frac{P_P x y}{P_A}\right) f_{|t|^2}(y) dy, \tag{5.9}$$

where the CDF $F_{|s_j|^2}(x)$ is expressed as

$$F_{|s_j|^2}(x) = 1 - e^{\frac{-x}{\beta_2}}. \tag{5.10}$$

By substituting (5.10) and PDF of $|t|^2$ in (5.9) and performing some simple mathematical manipulation, we obtain closed-form expression of CDF of Φ_E as shown in (5.7).

5.2.2 Secrecy Analysis for Passive Eavesdropping Scenario with PT's Interference

This section focuses on analyzing the PLS of underlay CRN with interference from PT under a passive eavesdropping scenario. Unlike the active eavesdropping scenario, the perfect secrecy cannot be assured in the passive eavesdropping scenario because Alice does not know the CSI of the wiretap channel. Inspired by this, we choose the SOP as a useful performance metric and derive novel expressions for the exact and the asymptotic SOP with continuous power adaptation. Furthermore, we investigate other essential metrics like intercept probability, the probability of non-zero secrecy capacity, and the ε-outage secrecy capacity.

5.2.2.1 Secrecy Outage Probability

In this subsection, we calculate the SOP of the proposed underlay CRN with continuous power adaptation scheme at Alice.

Proposition 5.1. *The closed-form expressions of exact SOP for single antenna based Alice in the presence of interference caused by primary transmitter PT is expressed as*

$$\begin{aligned}
P_{out}(R_s) = \Bigg[1 - \frac{\mathscr{K}\mathscr{Q}_1}{\tau} e^{-\frac{(\tau-1)}{\beta_1 P_T}} \Bigg(e^{\mathscr{A}_1} Ei(-\mathscr{A}_1) \left[\mathscr{K}\mathscr{D}_1 - \frac{1}{\eta P_P} - \mathscr{A}_1\mathscr{K}\right] - e^{\mathscr{A}_2+\mathscr{A}_3} \\
Ei(-\mathscr{A}_2-\mathscr{A}_3)\left[\mathscr{K}\mathscr{D}_1 + \frac{1}{\eta P_P}\right] - 1\Bigg)\Bigg]\left(1 - e^{-\frac{I_P}{P_T\Omega_0}}\right) + e^{-\frac{I_P}{P_T\Omega_0}} + \mathscr{E}_1 e^{\mathscr{A}_1} \\
Ei(-\mathscr{A}_1)\left[\frac{e^{-\frac{I_P\varsigma}{P_T}}}{\left(\frac{I_P}{P_T}+\mathscr{B}_1\right)} + \varsigma e^{\mathscr{B}_1\varsigma} Ei\left(-\left(\frac{I_P}{P_T}+\mathscr{B}_1\right)\varsigma\right)\right] + \mathscr{E}_1 e^{\mathscr{A}_2} E_0 \\
\left[\frac{e^{-(\varsigma-\mathscr{A}_4)\frac{I_P}{P_T}}}{\left(\frac{I_P}{P_T}+\mathscr{B}_1\right)} + (\varsigma-\mathscr{A}_4) e^{(\varsigma-\mathscr{A}_4)\mathscr{B}_1} Ei\left[-(\varsigma-\mathscr{A}_4)\left(\mathscr{B}_1+\frac{I_P}{P_T}\right)\right]\right] + \frac{\mathscr{Q}_2}{\Omega_0(\tau-1)} \\
\left[\mathscr{A}_1 e^{\mathscr{A}_1} Ei(-\mathscr{A}_1) + 1\right] e^{\varsigma\mathscr{B}_1} Ei\left(-\varsigma\left(\mathscr{B}_1+\frac{I_P}{P_T}\right)\right) + \frac{\mathscr{Q}_2}{(\tau-1)\eta P_P}\Bigg[E_0 e^{\mathscr{B}_1(\varsigma-\mathscr{A}_4)+\mathscr{A}_2} \\
Ei\left(-(\varsigma-\mathscr{A}_4)\left(\frac{I_P}{P_T}+\mathscr{B}_1\right)\right) - e^{\mathscr{A}_1} Ei(-\mathscr{A}_1) e^{\mathscr{B}_1\varsigma} Ei\left(-\varsigma\left(\frac{I_P}{P_T}+\mathscr{B}_1\right)\right)\Bigg],
\end{aligned} \tag{5.11}$$

where $Ei(x) = \int_{-\infty}^{x} \frac{e^t}{t} dt, x > 0$ *is a exponential integral function,* $E_0 = -\varphi(1) = 0.5772156649$ *is the Euler's constant and*

$$\tau = 2^{R_s}, \mathscr{Q}_1 = \frac{\beta_1 P_T}{\lambda P_P}, \mathscr{D}_1 = \frac{\beta_2 P_T}{\eta P_P}, \mathscr{A}_1 = \frac{1}{\eta P_P}\left(1 + \frac{\tau\beta_2}{\beta_1}\right), \mathscr{A}_2 = \frac{1}{\lambda P_P}\left(1 + \frac{\beta_1}{\tau\beta_2}\right),$$
$$\mathscr{A}_3 = \frac{(\tau-1)}{\tau}\left[\frac{\tau}{\beta_1 P_T} + \frac{1}{\beta_2 P_T}\right], \varsigma = \left[\frac{1}{\Omega_0} + \frac{\tau-1}{\beta_1 I_P}\right], \mathscr{Q}_2 = \frac{\beta_1 I_P}{\lambda P_P}, \mathscr{D}_2 = \frac{\beta_2 I_P}{\eta P_P}, \sigma = \frac{I_P}{P_T},$$
$$\mathscr{A}_4 = \frac{(\tau-1)}{\tau}\left[\frac{\tau}{\beta_1 I_P} + \frac{1}{\beta_2 I_P}\right], \mathscr{B}_1 = \frac{I_P}{P_P(1-\tau)}\left[\frac{\beta_2}{\eta} - \frac{\beta_1}{\lambda}\right], \mathscr{E}_1 = \frac{\tau\mathscr{Q}_2\mathscr{D}_2}{(1-\tau)^2\Omega_0}.$$

Proof: The proof of Proposition (5.1) is given in Appendix A.5.

SOP with a limited Alice power adaptation scheme, i.e., P_T and I_P limit the Alice's transmit power P_A. It should be remarked that a more simplistic expression can be obtained under the unlimited Alice power case, i.e., $P_A = \frac{I_P}{|h_{j0}|^2}$. This expression is very useful when $P_T \to \infty$ [109],[113] and it can be serve as lower bounds on SOP under the limited Alice power case. Therefore, we derive SOP with unlimited Alice power adaptation by using the Proposition 5.1 in the Corollary 5.1.

Corollary 5.1. *The SOP of an underlay CRN in the presence of primary interference with unlimited Alice power, i.e.* $P_T = \infty$ *is calculated as*

$$\begin{aligned} P_{out} =& 1 + \mathscr{E}_1 e^{\mathscr{A}_1} Ei(-\mathscr{A}_1)\left[\frac{1}{\mathscr{B}_1} + \varsigma e^{\mathscr{B}_1\varsigma} Ei(-\mathscr{B}_1\varsigma)\right] + \mathscr{E}_1 e^{\mathscr{A}_2} E_0\left[\frac{1}{\mathscr{B}_1} + (\varsigma - \mathscr{A}_4)\right. \\ & \left. e^{(\varsigma-\mathscr{A}_4)\mathscr{B}_1} Ei\left[-(\varsigma-\mathscr{A}_4)\mathscr{B}_1\right]\right] + \frac{\mathscr{Q}_2}{\Omega_0(\tau-1)}\left[\mathscr{A}_1 e^{\mathscr{A}_1} Ei(-\mathscr{A}_1) + 1\right] e^{\varsigma\mathscr{B}_1} \\ & Ei(-\varsigma\mathscr{B}_1) + \frac{\mathscr{Q}_2}{(\tau-1)\eta P_P}\left[E_0 e^{\mathscr{B}_1(\varsigma-\mathscr{A}_4)+\mathscr{A}_2} Ei(-(\varsigma-\mathscr{A}_4)\mathscr{B}_1) - e^{\mathscr{A}_1}\right. \\ & \left. Ei(-\mathscr{A}_1) e^{\mathscr{B}_1\varsigma} Ei(-\varsigma\mathscr{B}_1)\right]. \end{aligned} \tag{5.12}$$

Proof: By substituting $P_T = \infty$ in (5.11) and making some simple mathematical manipulations, we obtain a closed-form expression of the SOP with unlimited Alice power as (5.12).

We presume that Alice is outfitted with an N_A antenna, and the OAS scheme is adopted at Alice to select a single best antenna among available N_A antenna. When the global CSI is available, the OAS that maximizes the secrecy capacity can be utilized at Alice. Assuming that $|h_j|^2$ and $|s_j|^2$ are i.i.d R.Vs, then we have

$$P_{out}^{OAS} = \left(P_{out}(R_s)\right)^{N_A}, \tag{5.13}$$

where, $P_{out}(R_s)$ is the SOP of the single antenna based Alice underlay CRN calculated in (5.11).

Although, we have obtained the exact closed-form expression for SOP, it is very difficult to get insights from (5.11). Hence, we turn our attention to the asymptotic SOP in the high SINR regime, i.e., $\beta_1 \to \infty$, to get more insights. When $\beta_1 \to \infty$, $F_{\Phi_M}(x)$ and $f_{\Phi_M}(x)$ can be approximated as

$$F_{\Phi_M}(x) \approx \frac{x}{x+\mathscr{Q}}, \tag{5.14}$$

$$f_{\Phi_E}(x) \approx \frac{\mathscr{Q}}{(x+\mathscr{Q})^2}. \tag{5.15}$$

Proposition 5.2. *The asymptotic SOP for an interference-limited CRN with a single antenna based Alice is expressed as*

$$\begin{aligned} P_{out}^{\infty} =& \frac{1}{\mathscr{X}_1} U\left(1,0,\frac{1}{\eta P_P}\right) - U\left(1,1,\frac{\beta_1}{\tau\lambda P_P \beta_2}\right)\left[\frac{1}{\eta P_P \mathscr{X}_2} + \frac{\beta_1\eta}{\tau\lambda\beta_2 {\mathscr{X}_1}^2}\right] + \frac{1}{\mathscr{X}_1} \\ & U\left(1,1,\frac{1}{\eta P_P}\right)\left[\frac{\beta_1\eta}{\beta_2\tau\lambda\mathscr{X}_1} + \frac{1}{\eta P_P}\right], \end{aligned} \tag{5.16}$$

where $U(a,b,z) = \frac{1}{\Gamma(a)}\int_0^\infty e^{-zt}t^{a-1}(1+t)^{b-a-1}$ *is the confluent hypergeometric function of second kind [187, eq.(9.210.2)] and*

$$\mathscr{X}_1 = \left(1 - \frac{\eta\beta_1}{\tau\lambda\beta_2}\right),\ \mathscr{X}_2 = \left(1 - \frac{\lambda\tau\beta_2}{\eta\beta_1}\right).$$

Proof: The proof of Proposition 5.2 is given in Appendix A.6. The asymptotic SOP with optimal antenna selection scheme can be expressed as

$$P_{out}^{\infty^{OAS}} = (P_{out}^{\infty})^{N_A}, \tag{5.17}$$

where P_{out}^{∞} is the SOP with single transmit antenna. The asymptotic SOP derived in (5.17) can be written as

$$P_{out}^{\infty^{OAS}} = (G_A\beta_1)^{-G_D} + \mathscr{O}\left(\beta_1^{-G_D}\right), \tag{5.18}$$

where the secrecy diversity order, G_D is equal to N_A.

When $\beta_1 \to \infty$, $\mathscr{X}_1 \approx \frac{-\eta\beta_1}{\tau\lambda\beta_2}$ and $\mathscr{X}_2 \approx 1$. Using relation $U(a,b,x) \approx x^{-a}$ when $x \to \infty$ [195] and

neglecting the other higher power terms of β_1, secrecy array gain, G_A can be approximated as

$$G_A \approx \left[\frac{\tau\lambda\beta_2}{\eta}\left[\left(1-\frac{1}{\eta P_P}\right)U\left(1,1,\frac{1}{\eta P_P}\right)-U\left(1,0,\frac{1}{\eta P_P}\right)-1\right]\right]^{-\frac{1}{N_A}}. \tag{5.19}$$

From the asymptotic result given in (5.18), we conclude the following remarks on the network security:

- Secrecy diversity order G_D only depends on the number of transmit antenna N_A.
- Secrecy array gain G_A is inversely proportional to β_2. It means as β_2 increases, G_A reduces. Consequently, SOP increases with increasing β_2. G_A is also inversely proportional to the target rate R_s and λ. G_A decreases as R_s and λ increase which in turn increases the outage probability.
- From (5.19), for a constant value of η, as P_P increases, $U\left(1,1,\frac{1}{\eta P_P}\right)$ is also increases, which in turn reduces the secrecy array gain. It means that as P_P increases, G_A decreases, which consequently increases the outage probability.

5.2.2.2 Intercept Probability

Intercept probability is a fundamental performance metric adopted to describe the secrecy performance of an underlay CRN [196]. By setting $R_s = 0$ in (5.11) and (5.16) and performing some simple mathematical manipulation, the exact and asymptotic intercept probability for a single antenna based Alice can be calculated as

$$P_{int} = 1+\mathscr{G}_1 - e^{\frac{\mathscr{C}_1}{\eta P_P}}\Gamma\left(0,\frac{\mathscr{C}_1}{\eta P_P}\right)\left[\frac{\mathscr{G}_1\mathscr{C}_1}{\eta P_P}-\mathscr{G}_2-\frac{\mathscr{G}_1}{\eta P_P}\right]-e^{\frac{\mathscr{C}_2}{\lambda P_P}}\Gamma\left(0,\frac{\mathscr{C}_2}{\lambda P_P}\right)\left[\mathscr{G}_2+\frac{\mathscr{G}_1}{\eta P_P}\right], \tag{5.20}$$

and

$$\begin{aligned} P_{int}^{\infty} = &\frac{1}{\mathscr{Z}_1}U\left(1,0,\frac{1}{\eta P_P}\right)-U\left(1,1,\frac{\beta_1}{\lambda P_P\beta_2}\right)\left[\frac{1}{\eta P_P\mathscr{Z}_2}+\frac{\beta_1\eta}{\lambda\beta_2\mathscr{Z}_1{}^2}\right]+\frac{1}{\mathscr{Z}_1} \\ &U\left(1,1,\frac{1}{\eta P_P}\right)\left[\frac{\beta_1\eta}{\beta_2\lambda\mathscr{Z}_1}+\frac{1}{\eta P_P}\right], \end{aligned} \tag{5.21}$$

respectively, where $\mathscr{C}_1 = \left(1+\frac{\beta_2}{\beta_1}\right), \mathscr{C}_2 = \left(1+\frac{\beta_1}{\beta_2}\right), \mathscr{G}_1 = \frac{1}{\frac{\beta_2\lambda}{\eta\beta_1}-1}, \mathscr{G}_2 = \frac{\beta_1\beta_2\eta\lambda}{(\lambda\beta_2-\beta_1\eta)^2}, \mathscr{Z}_1 = \left(1-\frac{\eta\beta_1}{\lambda\beta_2}\right)$, $\mathscr{Z}_2 = \left(1-\frac{\lambda\beta_2}{\eta\beta_1}\right)$. The exact and asymptotic intercept probability with OAS scheme can be ex-

pressed as

$$P_{int}^{OAS} = (P_{int})^{N_A}, \tag{5.22}$$

$$P_{int}^{\infty,OAS} = (P_{int}^{\infty})^{N_A}, \tag{5.23}$$

respectively, where P_{int} and P_{int}^{∞} are the exact and asymptotic intercept probability defined in (5.20) and (5.21), respectively. It is found that there exists a non-zero secrecy capacity in the fading channel even when the eavesdropper channel is statistically more significant than the main channel [63, 197]. The PNZC is a probability of the SINR of the main is higher than the SINR of Eve's channel. Mathematically, we can say that $\Pr(C_s > 0) = \Pr(\Phi_M > \Phi_E)$, which is equivalent to $\Pr(C_s > 0) = 1 - P_{int}$.

From the Bob and Eve's distance point of view, noting that $\frac{\beta_1}{\beta_2} = \left(\frac{d_E}{d_M}\right)^{\alpha}$ where d_M is the distance between Alice and Bob, d_E is the distance between Alice and Eve, and α is the path loss exponent [63].

5.2.2.3 ε-Outage Secrecy Capacity

This subsection calculates the ε-Outage secrecy capacity for the proposed network in the presence of interference caused by primary transmitter,PT. The l^{th} order moment of Φ_M and Φ_E can be expressed as

$$\begin{aligned}\mathbb{E}[\Phi_M^l] &= \int_0^{\infty} \Phi_M^l f_{\Phi_M}(\Phi_M) d\Phi_M \\ &= \mathscr{Q}^l \Gamma(l+1) \left[U\left(l+1, l, \frac{1}{P_P \lambda}\right) + \frac{1}{P_P \lambda} U\left(l+1, l+1, \frac{1}{P_P \lambda}\right)\right], \end{aligned} \tag{5.24}$$

$$\begin{aligned}\mathbb{E}[\Phi_E^l] &= \int_0^{\infty} \Phi_E^l f_{\Phi_E}(\Phi_M) d\Phi_E \\ &= \mathscr{D}^l \Gamma(l+1) \times \left[U\left(l+1, l, \frac{1}{P_P \eta}\right) + \frac{1}{P_P \eta} U\left(l+1, l+1, \frac{1}{P_P \eta}\right)\right], \end{aligned} \tag{5.25}$$

respectively. The ε-secrecy outage capacity can be defined as

$$\begin{aligned} C_{\varepsilon} \approx & \log_2 e \left[\ln\left(\frac{\nu_{\Phi_M}}{\nu_{\Phi_E}}\right) - \frac{\sigma_{\Phi_M}^2}{2\nu_{\Phi_M}^2} + \frac{\sigma_{\Phi_E}^2}{2\nu_{\Phi_E}^2} \right] + \sqrt{2} \log_2 e \\ & \left[\frac{\sigma_{\Phi_M}^2}{\nu_{\Phi_M}^2} - \frac{\sigma_{\Phi_M}^2}{4\nu_{\Phi_M}^4} + \frac{\sigma_{\Phi_E}^2}{\nu_{\Phi_E}^2} - \frac{\sigma_{\Phi_E}^2}{4\nu_{\Phi_E}^4} \right]^{\frac{1}{2}} \operatorname{erfc}^{-1}(2-2\varepsilon), \end{aligned} \tag{5.26}$$

where

$$\nu_{\Phi_M} = 1+\mathbb{E}[\Phi_M], \sigma^2_{\Phi_M} = \mathbb{E}[\Phi^2_M] - E^2[\Phi_M], \nu_{\Phi_E} = 1+\mathbb{E}[\Phi_E],$$
$$\sigma^2_{\Phi_E} = \mathbb{E}[\Phi^2_E] - \mathbb{E}^2[\Phi_E]. \tag{5.27}$$

To this end by substituting (5.27) in (5.26), ε-outage secrecy capacity for a given value of P_A and $N_A = 1$ can be calculated.

5.2.3 Secrecy Performance Analysis for Active Eavesdropping Scenario with PT's interference

This section concentrates on the analysis of the secrecy performance in an active eavesdropping scenario. We obtain novel expressions for exact and asymptotic ASC.

Proposition 5.3. *The exact average secrecy capacity of the proposed CRN for the j^{th} transmit antenna in the presence of primary interference is expressed as*

$$\begin{aligned}\bar{C}_{s,j} =& \frac{\mathscr{Q}_1}{\ln(2)}\left[\frac{1}{(1-\mathscr{Q}_1)}\left[U\left(1,1,\frac{1}{\lambda P_P}\right) - U\left(1,1,\frac{1}{\beta_1 P_T}\right)\right] + \mathscr{T}_1 U(1,1,\mu_1) + \mathscr{T}_2\right.\\
& \left. U(1,1,\mu_2) + \mathscr{T}_3 U(1,1,\mu_4)\right]\left(1-e^{-\frac{I_P}{P_T\Omega_0}}\right) + \frac{\mathscr{Q}_2}{\ln(2)\Omega_0}\left[e^{-\frac{Q_2}{\Omega_0}} Ei\left(\frac{Q_2}{\Omega_0} - \frac{I_P}{\Omega_0 P_T}\right)\right.\\
& \left[-U\left(1,1,\frac{1}{\lambda P_P}\right) + \mathscr{Z}_1 U(1,1,\mu_2)\right] - E_0 e^{-\varpi_1\mathscr{Q}_2} Ei\left(\varpi_1\left(\mathscr{Q}_2 + \frac{I_P}{P_T}\right)\right) - \mathscr{Z}_1\\
& U(1,1,\mu_1) e^{-\frac{D_2}{\Omega_0}} Ei\left(\frac{D_2}{\Omega_0} - \frac{I_P}{P_T\Omega_0}\right) + \mathscr{Z}_1 E_0\left[e^{-\Omega_0\mathscr{Q}_2} Ei\left(\varpi_2\mathscr{Q}_2 - \frac{\varpi_2 I_P}{P_T}\right) - e^{-\omega_2\mathscr{D}_2}\right.\\
& \left.\left. Ei\left(\varpi_2\mathscr{D}_2 - \frac{\varpi_2 I_P}{P_T}\right)\right]\right],\end{aligned} \tag{5.28}$$

where

$$\mu_1 = \frac{\mathscr{C}_1}{\eta P_P}, \mu_2 = \frac{\mathscr{C}_2}{\lambda P_P}, \mu_3 = \left(\frac{1}{\beta_1} + \frac{1}{\beta_2}\right), \mathscr{T}_1 = \frac{\mathscr{Z}_1}{(\mathscr{D}_1 - 1)}, \mathscr{T}_2 = \frac{\mathscr{Z}_1}{(\mathscr{Q}_1 - 1)},$$
$$\mathscr{T}_3 = \frac{1}{(\mathscr{Q}_1 - 1)(\mathscr{D}_1 - 1)}, \varpi_1 = \frac{1}{\Omega_0} - \frac{1}{\beta_1 I_P}, \varpi_2 = \frac{1}{\Omega_0} - \frac{\mu_3}{I_P}.$$

Proof: See Appendix A.7.

We have analyzed the ASC under limited Alice power adaptation in Proposition 5.3. A more straightforward expression can be obtained under the unlimited Alice power case, i.e., $P_T = \infty$,

and it serves as an upper bound on ASC under a limited Alice power adaptation case. We derive the ASC with unlimited Alice power in the Corollary 5.2.

Corollary 5.2. *The exact ASC of j^{th} antenna of proposed CRN for continuous power adaption with unlimited Alice power is given by*

$$\begin{aligned}\bar{C}_{s,j} =& \frac{\mathscr{Q}_2}{\ln(2)\Omega_0}\Bigg[\left[\mathscr{Z}_1 U(1,1,\mu_2) - U\left(1,1,\frac{1}{\lambda P_P}\right)\right] e^{-\frac{Q_2}{\Omega_0}} Ei\left(\frac{Q_2}{\Omega_0}\right) - E_0 e^{-\varpi_1 \mathscr{Q}_2} \\ & Ei(\varpi_1 \mathscr{Q}_2) - \mathscr{Z}_1 U(1,1,\mu_1) e^{-\frac{D_2}{\Omega_0}} Ei\left(\frac{D_2}{\Omega_0}\right) + \mathscr{Z}_1 E_0 \big[e^{-\Omega_0 \mathscr{Q}_2} Ei(\varpi_2 \mathscr{Q}_2) \\ & - e^{-\varpi_2 \mathscr{D}_2} Ei(\varpi_2 \mathscr{D}_2)\big]\Bigg]. \end{aligned} \tag{5.29}$$

Proof: By substituting $P_T = \infty$ in (5.28) and performing simple mathematical manipulations, we obtain exact ASC for j^{th} antenna of Alice in (5.29).

Next, we analyzed the asymptotic ASC of the proposed network in the high SINR regime to get the consequences of key performance parameters on the PLS.

Proposition 5.4. *The asymptotic average secrecy capacity of an underlay CRN in the presence of interference caused by PT is given as*

$$\begin{aligned}\bar{C}_s^{\infty} =& \log_2(\beta_1) + \frac{1}{\ln(2)}\Bigg[\ln\left(\frac{P_T}{\lambda P_P}\right) - \left[\frac{\mathscr{D}_1}{(1-\mathscr{D}_1)}\left[U\left(1,1,\frac{1}{\eta P_P}\right) - U\left(1,1,\frac{1}{\beta_2 P_T}\right)\right]\right] \\ & \left(1 - e^{-\frac{I_P}{\Omega_0 P_T}}\right) - \Gamma\left(0, \frac{I_P}{P_T \Omega_0}\right) + \frac{\mathscr{D}_2}{\Omega_0} U\left(1,1,\frac{1}{\eta P_P}\right) e^{-\frac{\mathscr{D}_2}{\Omega_0}} Ei\left(\frac{\mathscr{D}_2}{\Omega_0} - \frac{I_P}{P_T \Omega_0}\right) \\ & + \frac{E_0 \mathscr{D}_2}{\Omega_0} e^{-\mathscr{D}_2\left(\frac{1}{\Omega_0} - \frac{1}{\beta_2 I_P}\right)} Ei\left[\left(\frac{\mathscr{D}_2}{\Omega_0} - \frac{\mathscr{D}_2}{\beta_2 I_P}\right) - \left(\frac{I_P}{P_T \Omega_0} - \frac{1}{\beta_2 P_T}\right)\right]\Bigg]. \end{aligned} \tag{5.30}$$

Proof: The proof of Proposition (5.4) is given in the Appendix A.8.

Based on (5.30), at high SINR, ASC can be characterized in terms of high SINR slope and the high SINR power offset [67],[68]. Hence, the asymptotic ASC in (5.30) can be rewritten as

$$\bar{C}_s^{\infty} = \bar{S}_{\infty}\left[\log_2(\beta_1) - \bar{L}_{\infty}\right], \tag{5.31}$$

where, $\bar{S}_{\infty}$ is the high SINR slope in bits/s/Hz/(3dB) and $\bar{L}_{\infty}$ is the high SINR power offset in 3 dB units. The high SINR slope $\bar{S}_{\infty}$ is calculated as

$$\bar{\mathscr{S}}_{\infty} = \lim_{\beta_1 \to \infty} \frac{\bar{C}_s^{\infty}}{\log_2(\beta_1)}. \tag{5.32}$$

By substituting (5.30) in (5.32) and doing some mathematical manipulations, $\bar{\mathscr{S}}_\infty$ can be calculated as

$$\bar{\mathscr{S}}_\infty = 1. \tag{5.33}$$

From (5.33), one can see that $\mathscr{S}_\infty$ is constant, and it is independent of parameters of main and eavesdropper's channels. Next, the high SINR power offset can be expressed as

$$\bar{\mathscr{L}}_\infty = \lim_{\beta_1 \to \infty} \left(\log_2(\beta_1) - \frac{\bar{C}_s^\infty}{\bar{\mathscr{S}}_\infty} \right). \tag{5.34}$$

It is noted that (5.34) undoubtedly marks the impact of the main and wiretap channel on ASC. Hence, substituting (5.30) and (5.33) into (5.34), the high SINR slope $\bar{S}_\infty$ is calculated as

$$\begin{aligned}\bar{\mathscr{L}}_\infty =& \frac{1}{\ln(2)} \Bigg[\frac{\mathscr{D}_1}{(1-\mathscr{D}_1)} \left[U\left(1,1,\frac{1}{\eta P_P}\right) - U\left(1,1,\frac{1}{\beta_2 P_T}\right) \right] \left(1 - e^{-\frac{I_P}{\Omega_0 P_T}}\right) \\ & - \log\left(\frac{P_T}{\Omega_0 P_P}\right) + \Gamma\left(0, \frac{I_P}{P_T \Omega_0}\right) - \frac{\mathscr{D}_2}{\Omega_0} U\left(1,1,\frac{1}{\eta P_P}\right) e^{-\frac{\mathscr{D}_2}{\Omega_0}} Ei\left(\frac{\mathscr{D}_2}{\Omega_0} - \frac{I_P}{P_T \Omega_0}\right) \\ & - \frac{E_0 \mathscr{D}_2}{\Omega_0} e^{-\left(\frac{\mathscr{D}_2}{\Omega_0} - \frac{\mathscr{D}_2}{\beta_2 I_P}\right)} Ei\left[\left(\frac{\mathscr{D}_2}{\Omega_0} - \frac{\mathscr{D}_2}{\beta_2 I_P}\right) - \left(\frac{I_P}{P_T \Omega_0} - \frac{1}{\beta_2 P_T}\right) \right] \Bigg]. \end{aligned} \tag{5.35}$$

$\bar{\mathscr{L}}_\infty$ in (5.35) highlights that β_2, λ, η and P_p has negative impact on the ASC. It is because an increase in β_2, λ, η, and P_p improve the $\bar{\mathscr{L}}_\infty$, which in turn reduces the ASC. Furthermore, $\bar{\mathscr{L}}_\infty$ is decreasing function of maximum transmit power P_T and peak interference power I_P.

Corollary 5.3. *When $\beta_1 \to \infty$ and $\beta_2 \to \infty$, ASC can be easily obtained based on Proposition 5.4. When $\beta_1 \to \infty$ and $\beta_2 \to \infty$, ASC can be easily obtained based on Proposition 4. We only need to further provide asymptotic $\xi_2 \to \infty$ when $\beta_2 \to \infty$. Observing ξ_1 in (A.57), ξ_2 can be derived as*

$$\xi_2 = \frac{\mathscr{D}\ln(\mathscr{D})}{\ln(2)(\mathscr{D}-1)}. \tag{5.36}$$

Substituting (A.57) and (5.36) in (A.54), we derive the asymptotic ASC as

$$\bar{C}_{s,j|Z}^\infty = \frac{1}{\ln(2)} \left(\frac{\mathscr{Q}\ln\left(\frac{1}{\mathscr{Q}}\right)}{(1-\mathscr{Q})} - \frac{\mathscr{D}\ln(\mathscr{D})}{(\mathscr{D}-1)} \right). \tag{5.37}$$

When $\beta_1 \to \infty$ and $\beta_2 \to \infty$, $\mathscr{Q}-1 \approx \mathscr{Q}$ and $\mathscr{D}-1 \approx \mathscr{D}$, then we have

$$\bar{C}_{s,j}^{\infty} = \log_2\left(\frac{\beta_1}{\beta_2}\right) - \log_2\left(\frac{\lambda}{\eta}\right). \tag{5.38}$$

From (5.38), we see that for a fixed ratio of β_1 and β_2, ASC is a constant value at high SINR. According to (5.32), high SINR slope, $\bar{S}_{\infty}$ is zero. (5.38) shows that when Eve is located close to Alice, increasing P_A does not effect the ASC.

The ASC with optimal antenna selection scheme is given by

$$\bar{C}_s = \mathbb{E}(C_s) = \mathbb{E}\left(\max_{j=1,2\ldots N_A} C_{s,j}\right) = \mathbb{E}\left(\prod_{j=1,2\ldots N_A} C_{s,j}\right), \tag{5.39}$$

where $C_{s,j}$ is the secrecy capacity for j^{th} transmit antenna of Alice and $\mathbb{E}(.)$ is the expectation operator. Since $C_{s,1}$, $C_{s,2}$.....C_{s,N_A} are independent, then

$$\bar{C}_s = \prod_{j=1,2\ldots N_A} \mathbb{E}\left(C_{s,j}\right) = \left[\mathbb{E}(C_{s,j})\right]^{N_A} \tag{5.40}$$

where $\left(\mathbb{E}(C_{s,j})\right) = \bar{C}_{s,j}$ is the ASC of j^{th} antenna.

5.2.4 Impact of Imperfect Channel Information

In a practical scenario, Alice has a partial CSI about the link between Alice and PR and the CSI on h_{j0} supplied to Alice is imperfect due to the time-varying nature of the wireless link. In such a scenario, the performances of both primary and secondary networks are affected. The imperfect CSI can be well explained by making use of the correlation model as [32]

$$h_{j0} = \rho\hat{h}_{j0} + \sqrt{1-\rho^2}\tilde{h}_{j0}, \tag{5.41}$$

where, $\rho\,(0 \le \rho \le 1)$ is correlation coefficient used to examine the effect of estimation errors of Alice-PR channel on CSI, $\hat{h}_{j0} \sim \mathscr{CN}(0,1)$ is the complex Gaussian R.V. and it is uncorrelated with $\tilde{h}_{j0}$. It is assumed that Alice knows the outdated channel information $\hat{h}_{j0}$ and ρ as well. In the view of $|h_{j0}|^2$ being an exponential R.V. with parameter $\frac{1}{\Omega_0}$, the estimated channel power gain $|\hat{h}_{j0}|^2$ is also an exponential R.V. with parameter $\frac{1}{\hat{\Omega}_0}$, where $\Omega_0 = \rho^2\hat{\Omega}_0 + (1-\rho^2)$ [145].

As we explained earlier, when Alice has a perfect CSI of h_{j0}, it can efficiently obtain the

radio spectrum if the peak interference power constraint can be fulfilled. On the other hand, it is tough to meet the instantaneous interference power restrictions at PR when Alice has imperfect CSI of h_{j0}. This is because it cannot be guaranteed that the interference power at the PR will remain below the predetermined threshold at all times. After all, the secondary user must be silent at all times to satisfy such a constraint, which makes the capacity of the secondary link zero [55]. Hence, instead of a strict peak power constraint, a more manageable constraint based on a pre-selected interference outage probability is utilized [32]. The term interference outage means that the interference power at the PR overpasses the pre-defined threshold for a fixed percentage of the time. Considering the impact of imperfect CSI, P_A given in (5.2) can be re-expressed as

$$P_A = \min\left(P_T, \alpha_I \frac{I_P}{|h_{j0}|^2}\right), \tag{5.42}$$

where α_I denotes the power margin factor which has to satisfy the predetermined interference outage probability. Due to the TAS scheme, before the transmission, Alice performs antenna selection using CSI received from Bob. After the antenna selection, Alice transmits its message to Bob using the selected antenna. Alice adjusts its transmit power based on the estimates $\hat{h}_{j0}$ and $\hat{h}_j$, which results in excessive interference to the PR and secrecy performance loss in the main channel. With perfect CSI, the interference power satisfies the constraint at the PR, and hence, the interference outage is zero. On the other hand, with imperfect CSI, Alice incorrectly determines the transmit power that results in excessive interference at the PR [109]. Hence, α_I can be computed numerically. However, when maximum transmit power P_T at Alice does not exist and unit variance of Alice-PR channel, α_I can be expressed as [32]

$$\alpha_I = \left(-1+2\rho^2\right) + \frac{1-\rho^2-(1-2\delta_0)\sqrt{(1-\rho^2)\left(1-(1-2\delta_0)^2\rho^2\right)}}{2\delta_0(1-\delta_0)}, \tag{5.43}$$

where δ_0 signifies the interference outage probability. As a particular case, a power margin $\alpha_I = 1$, (i.e. $\rho = 1$), specifies the perfect CSI of h_{j0} and consequently, P_A in (5.42) reduces to (5.2).

For further practical consideration, we address the imperfect CSI of the main channel and eavesdropper's channel in the secondary network, h_j and s_j respectively, for $j = 1, 2, ...N_A$. The

outdated CSI can be described as

$$h_j = \rho_B \hat{h}_j + \sqrt{1-{\rho_B}^2}\tilde{h}_j,$$
$$s_j = \rho_E \hat{s}_j + \sqrt{1-{\rho_E}^2}\tilde{s}_j, \tag{5.44}$$

where $\hat{h}_j$ and $\hat{s}_j$ are the outdated information of main and eavesdropper link, respectively and $\tilde{h}_j \sim \mathscr{CN}(0,1)$ and $\tilde{s}_j \sim \mathscr{CN}(0,1)$ are the complex Gaussian R.Vs, and uncorrelated with h_j and s_j respectively. The correlation coefficients $(0 \leq \rho_m \leq 1)$ and $(0 \leq \rho_e \leq 1)$ are constant that describe the impact of outdated CSI on main and channel, respectively. In view of $|h_j|^2$ and $|s_j|^2$ being exponential R.Vs. with parameter $\frac{1}{\beta_1}$ and $\frac{1}{\beta_2}$, the estimated channel power gains $|\hat{h}_j|^2$ and $|\hat{s}_j|^2$ are exponential distributed random variables with parameter $\frac{1}{\hat{\beta}_1}$ and $\frac{1}{\hat{\beta}_2}$ respectively, where $\beta_1 = \rho_B^2\hat{\beta}_1 + (1-\rho_B^2)$ and $\beta_2 = \rho_E^2\hat{\beta}_2 + (1-\rho_E^2)$. Futhermore, we presume that Alice knows the imperfect CSI and correlation coefficients of the primary and secondary channels [145]. Therefore, for given estimates and correlation coefficients exponential parameters of SINR distribution is calculated with parameters $\Omega_0 = \rho^2\hat{\Omega}_0 + (1-\rho^2)$, $\frac{1}{\beta_1}$, $\beta_1 = \rho_m^2\hat{\beta}_1 + (1-\rho_m^2)$, and $\beta_2 = \rho_e^2\hat{\beta}_2 + (1-\rho_e^2)$. Based on this, Alice selects an optimal transmit antenna. This selection of antenna is done with parameter β_1 and β_2. The value of β_1 is obtained using $\beta_1 = \rho_m^2\hat{\beta}_1 + (1-\rho_m^2)$. Similarly, β_2 can be found using $\beta_2 = \rho_e^2\hat{\beta}_2 + (1-\rho_e^2)$. Therefore, the expressions derived for the SOP and average secrecy capacity in the subsections (5.2.2) and (5.2.3) also hold for imperfect CSI case after replacing Ω_0 with $\rho^2\hat{\Omega}_0 + (1-\rho^2)$, I_P with $\alpha_I I_P$, replacing β_1 by $\rho_m^2\hat{\beta}_1 + (1-\rho_m^2)$ and β_2 by $\rho_e^2\hat{\beta}_2 + (1-\rho_e^2)$ [145].

5.3 Numerical Results and their Descriptions

This section presents simulation results to approve our analytical expression for both perfect and imperfect scenarios. All links are assumed to undergo Rayleigh fading. Without the loss of generality, we set $R_s = 1$ bits/sec/Hz.

5.3.1 Perfect CSI

This subsection gives the interpretation of the numerical results for perfect CSI scenario, which examine the impact of d_M, d_E, β_1, β_2, P_P, P_T, I_P and N_A on the SOP, intercept probability, PNZC, ε-outage secrecy capacity, and average secrecy capacity. We consider the following

two scenarios: 1) passive eavesdropping scenario and 2) active eavesdropping scenario. Further, Monte Carlo simulated results are numerically computed based on each figure's system parameters, confirming our analytical results' accuracy.

Figure 5.2 plots the exact SOP versus normalized maximum transmit power, $P_T = \frac{\bar{P}_T}{N_0}$, in dB for limited Alice power adaptation and unlimited Alice power adaptation, $P_T = \infty$ using (5.11) and (5.12), respectively, for varying N_A. As observed from Fig. 5.2, the analytical result agrees with the simulation one, validating the accuracy of (5.11) and (5.12). Moreover, the rise in P_T increases the information securing capability of the network. It is because P_T upper bounds Alice's power, according to (5.2). As such, the increase in P_T raises Alice's transmit power, conclusively remedying the SOP. Nevertheless, the security performance suffers the error floor at a significant value of P_T. It is because Alice's power is restricted by a minimum of I_P and P_T. Hence, when P_T is more significant than a particular value, Alice's power is limited by I_P, making the security performance unchanged despite increasing P_T. For a significant value of P_T, SOP approaches the one with unlimited Alice's power, $P_T = \infty$. We also observe that the SOP with unlimited Alice power serves as a lower bound on the SOP with limited Alice power. Furthermore, Figure 5.2 also illustrates the impact of the number of transmitting antenna N_A on secrecy performance, and it depicts that as N_A increases, SOP decreases.

Figure 5.3 plots the exact and asymptotic SOP of the CRN using (5.11) and (5.16), respectively, for varying N_A, and P_P. Our asymptotic curves precisely prognosticate the secrecy diversity gain and the array gain of the network. As expected, the SOP reduces with raising N_A and decreasing P_P. We also observe that the secrecy diversity order is found to be directly proportional to N_A, and secrecy array gain decreases with decreasing P_P, which confirms our results in (5.18) and (5.19) respectively.

Figure 5.4 draws the exact and asymptotic intercept probability versus N_A from (5.20) and (5.21), respectively, for varying P_P and β_1. By doing so, we examine the influence of P_P and N_A on the intercept probability. The special cases are characterized by setting $\beta_2 = 2$ dB, $\lambda = 8$ dB, and $\eta = -20$ dB, and it can be seen that asymptotic curves are accurate with the exact ones. We can observe that the intercept probability improves with increasing N_A. It is because the secrecy diversity order increases with increasing N_A. Furthermore, the primary interference, P_P, reduces the SINRs at both Bob and Eve but given simulation parameters, the degradation of SINR at Bob is more severe than at Eve. Therefore, the proposed CRN's security performance worsens with the increase in P_P, as shown in Figure 5.4.

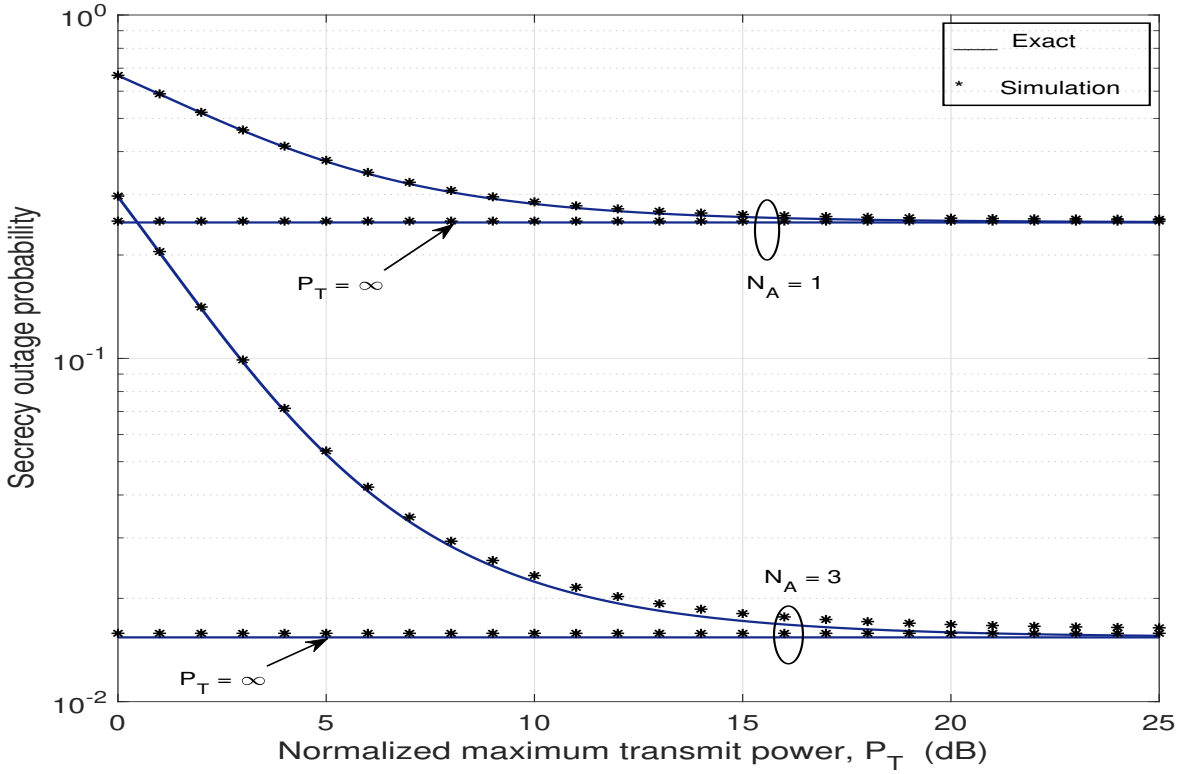

Figure 5.2: SOP against P_T for $\beta_1 = 5$ dB, $\beta_2 = 2$ dB, $I_P = 1$ dB, $\lambda = 10$ dB, $\eta = -8$ dB, and $\Omega_0 = 0$ dB

Figure 5.5 depicts the PNZC of the system against $\frac{d_E}{d_M}$ with different N_A. The path loss exponent is set to be equal to a common value of 3. From Fig. 5.5, it is clear that the PNZC increasing with increasing the $\frac{d_E}{d_M}$. Furthermore, an intuitive result is that the PNZC improves when N_A increases from 1 to 3.

Figure 5.6 plots the ε-outage secrecy capacity for varying β_1/β_2 and P_A and $\eta = 0$ dB, $\lambda = 0$ dB, $\varepsilon = 0.1$ and $P_P = 2$ dB. It can be spotted that $R_{s,\max}$ can be boosted by increasing Alice's transmit power P_A. Furthermore, the ε-outage secrecy capacity improves by increasing β_1/β_2.

Figure 5.7 and Figure 5.8 plot average secrecy capacity against d_M/d_E and interference power I_P, in dB respectively. Figure 5.7 demonstrates the impact of the maximum transmit power P_T and distance ratio d_M/d_E on average secrecy capacity. Fig. 5.7 depicts that as the distance ratio d_M/d_E increases, i.e. distance between Alice and Bob increases, average secrecy capacity decreases. On the other hand, maximum transmit power P_T has a positive impact on ASC. As P_T increases, the power at Alice increases, which in turn raises the ASC. Figure 5.8 plots average secrecy capacity for unlimited Alice power, $P_T = \infty$, and limited Alice power with $P_T = 2$ dB. We can make some interesting observations from this figure. First, for limited Alice power, $P_T = 2$ dB, average secrecy capacity is saturated. It does not improve as $I_P \geq 8$ dB. For higher values of I_P, Alice will select P_T with a higher probability. Second, the average secrecy

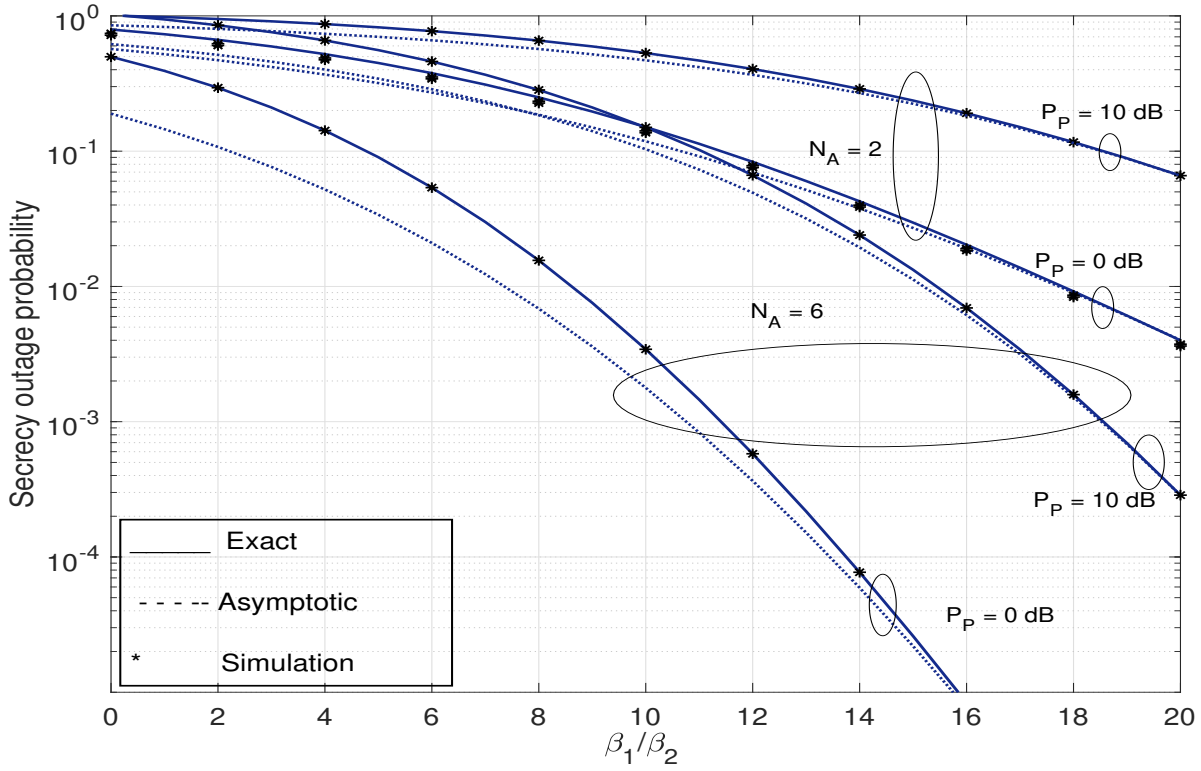

Figure 5.3: SOP against β_1/β_2 for $I_P = 2$ dB, $P_T = 0$ dB, $\eta = -2$ dB, and $\Omega_0 = 0$ dB.

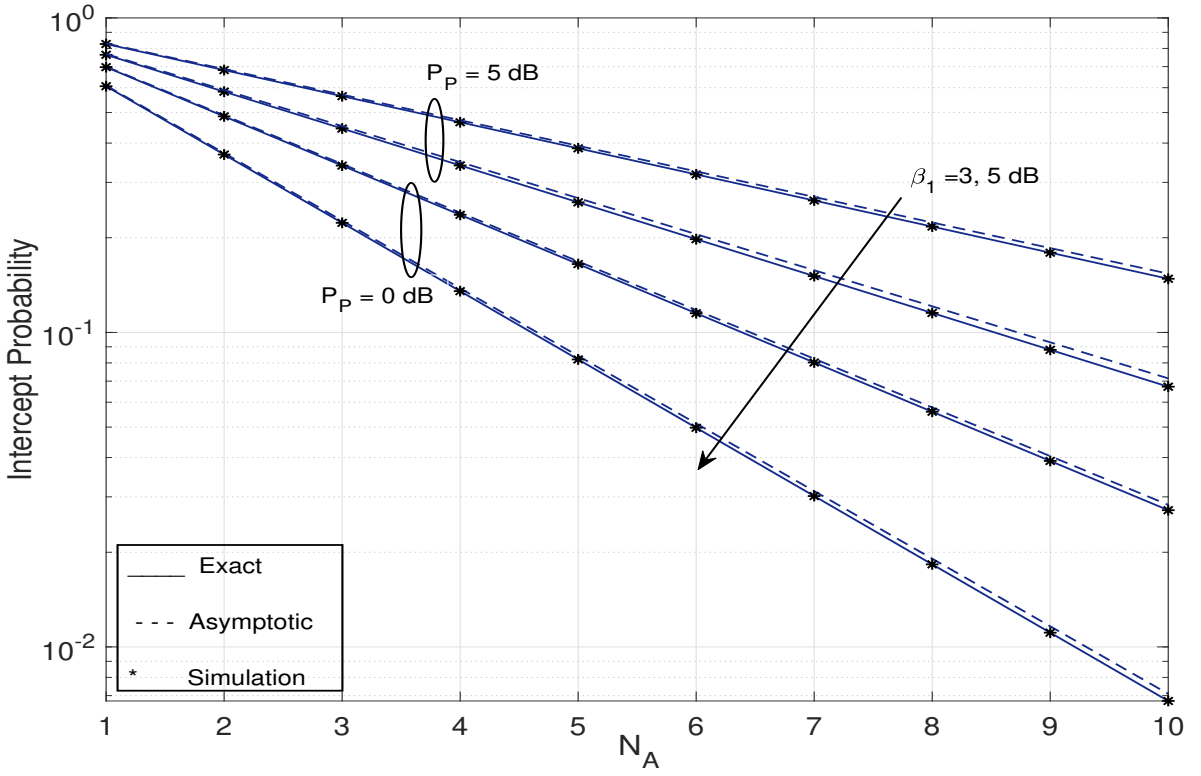

Figure 5.4: Intercept probability against N_A for $\beta_2 = 2$ dB, $\eta = -20$ dB, and $\lambda = 8$ dB.

capacity for the unlimited Alice power serves as an upper bound on the average secrecy capacity with the limited Alice power case.

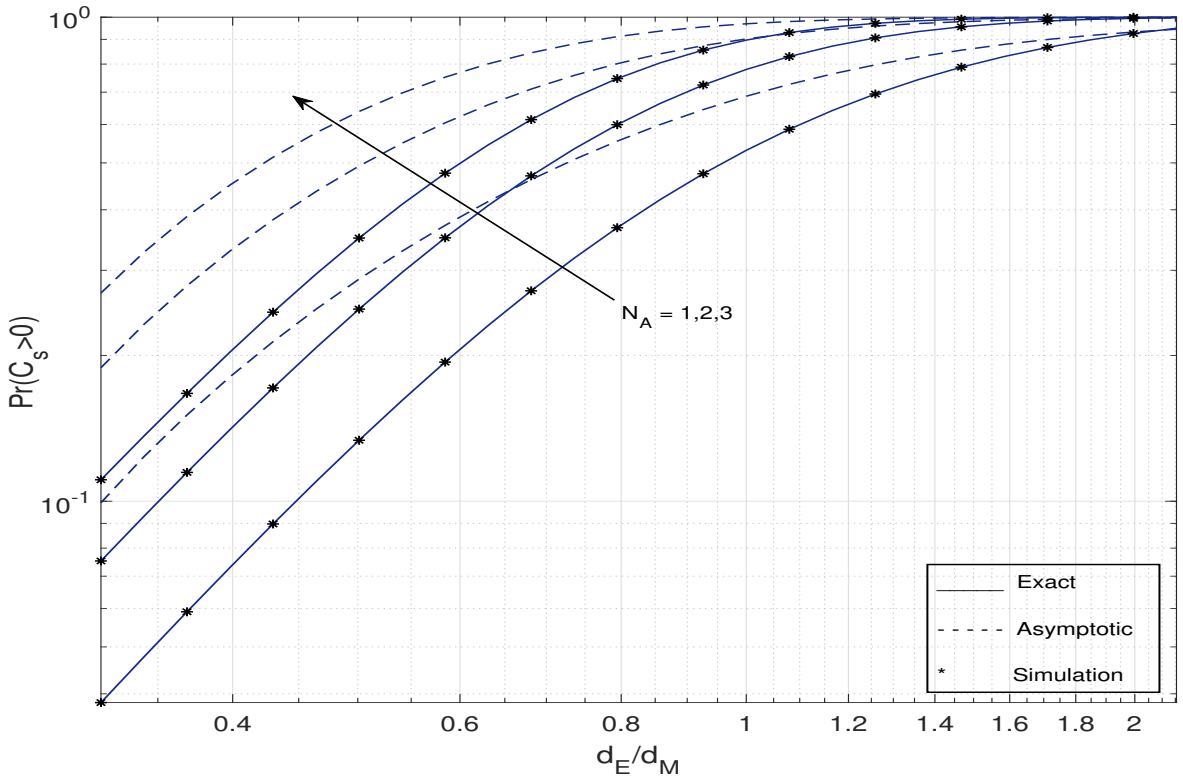

Figure 5.5: PNZC against d_E/d_M for $\lambda = 0$ dB, $\eta = 0$ dB, and $P_P = 0$ dB.

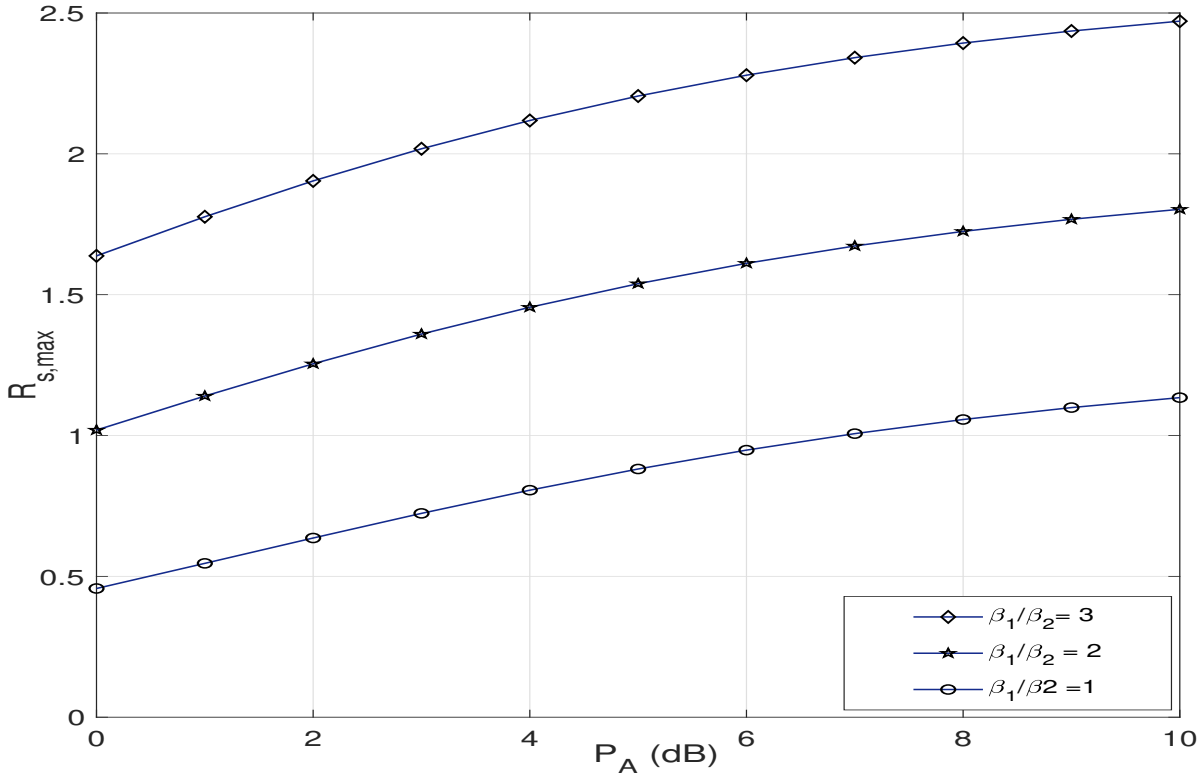

Figure 5.6: ε-Outage secrecy capacity against P_A for $\eta = 0$ dB, $\lambda = 0$ dB, $\varepsilon = 0.1$ and $P_P = 2$ dB.

Figure 5.9 shows the effect of interference power P_P on high SINR power offset with varying P_T. The high SINR power offset is obtained using (5.35). Figure 5.9 depicted that high

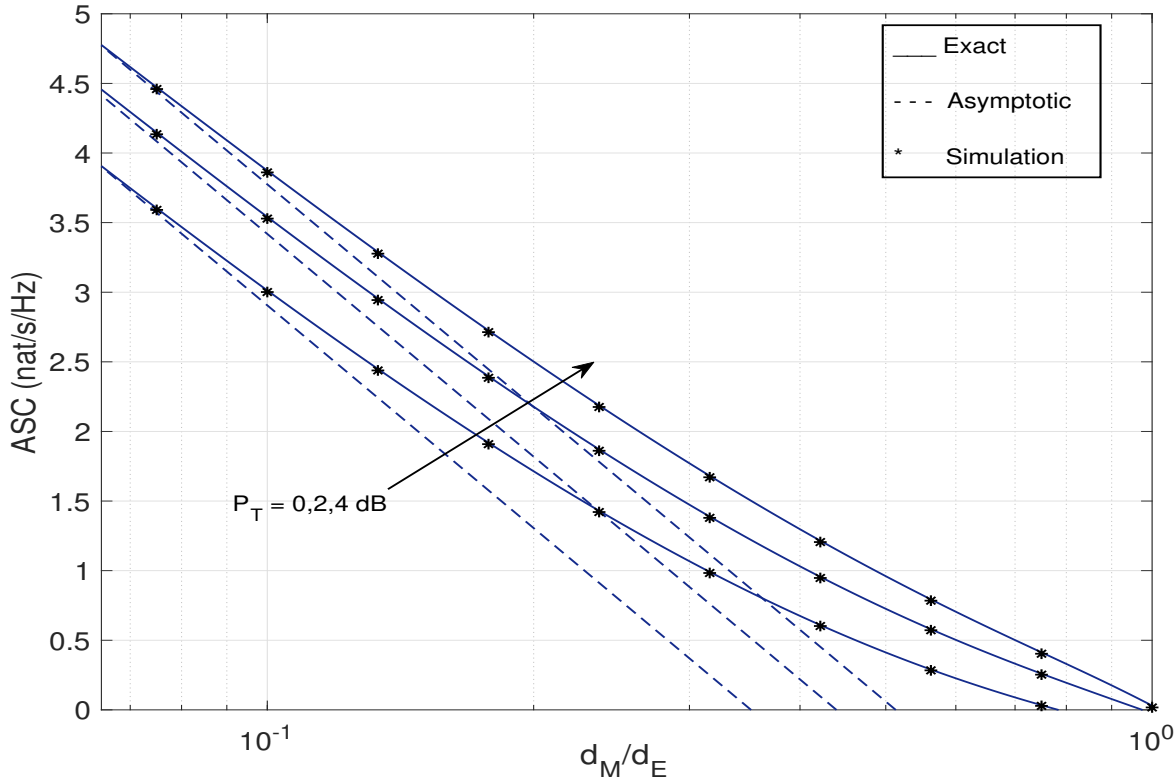

Figure 5.7: Average secrecy capacity against d_M/d_E for $I_P = 8$ dB, $\lambda = 0$ dB, and $\eta = 20$ dB.

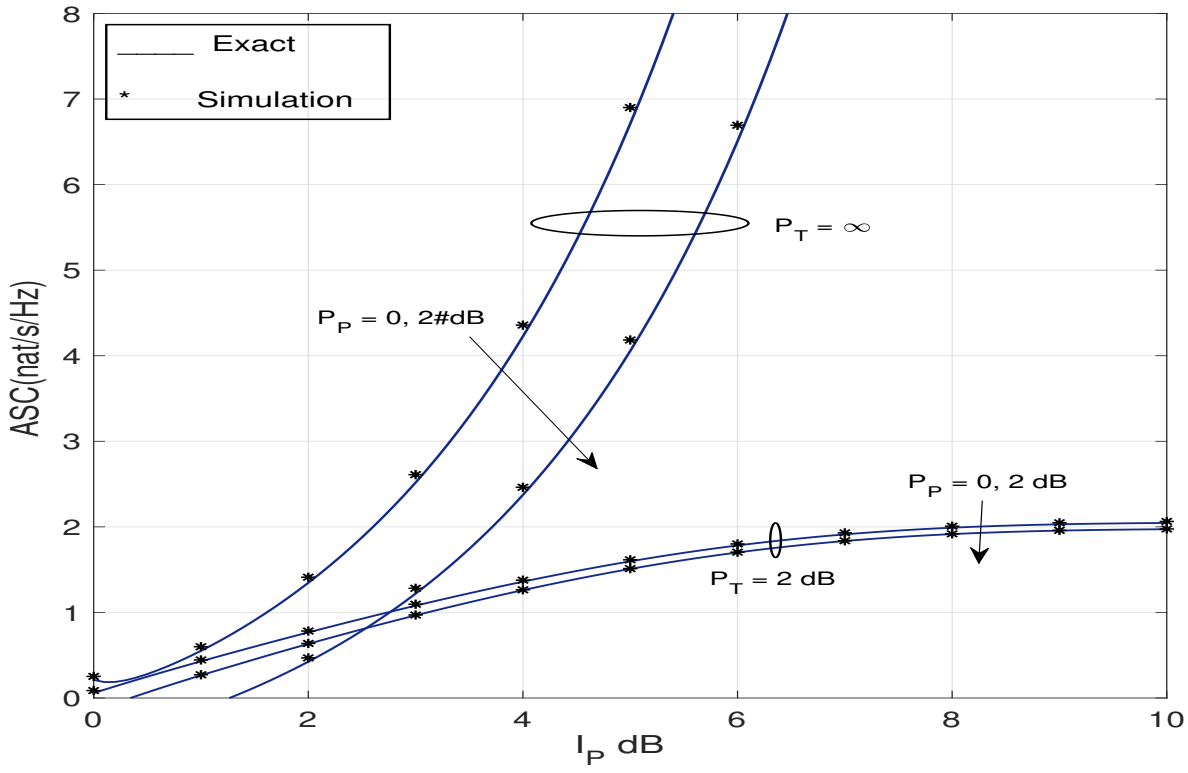

Figure 5.8: Average secrecy capacity against I_P for $\beta_1 = 5$ dB, $\beta_2 = 2$ dB, $\lambda = -10$ dB and $\eta = 20$ dB.

SINR power offset increases with increasing P_P, which in turn decreases the average secrecy capacity as shown in (5.31). Moreover, the high SINR power offset reduces with increasing P_T,

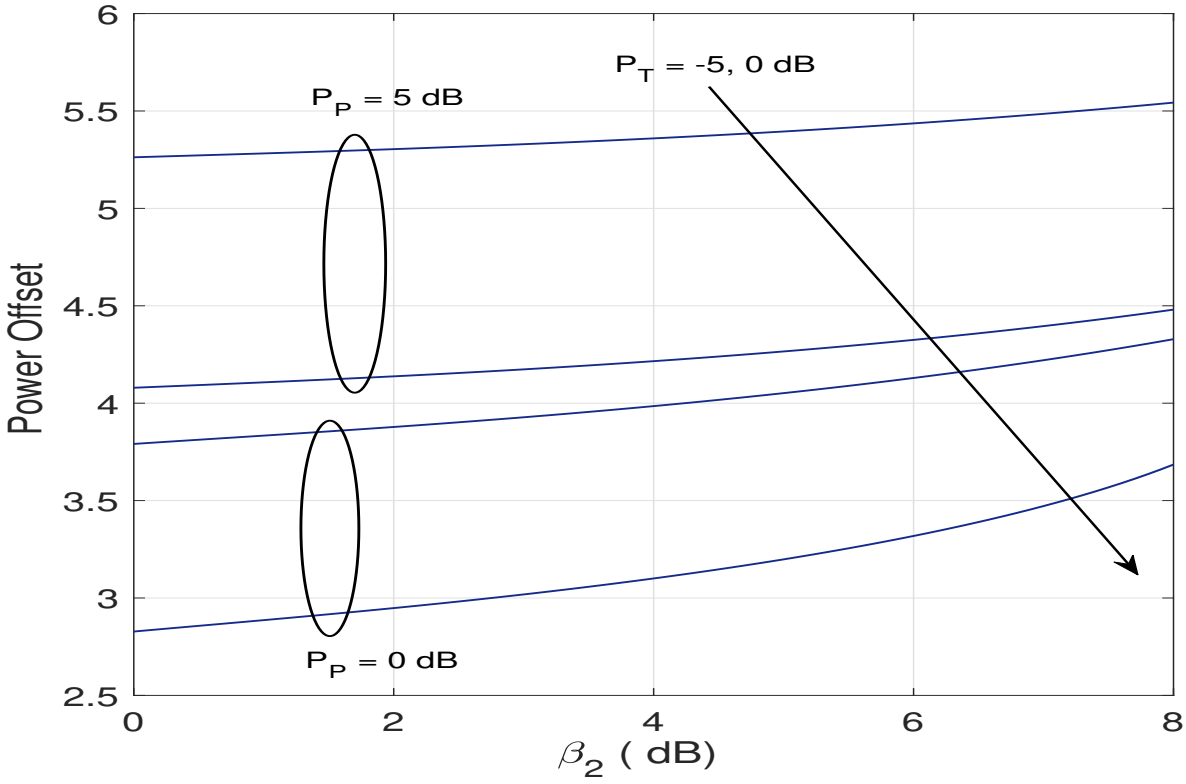

Figure 5.9: High SINR power offset against β_2 (in dB) with varying P_P and P_T.

increasing the average secrecy capacity. Moreover, as β_2 increases, high power offset increases, which decreases the PLS of the network. As β_2 increases, Eve becomes powerful in extracting information from the main channel, reducing the secrecy capacity.

5.3.2 Imperfect CSI

This subsection discusses the impact of ρ_B, ρ_E, and ρ_R as described in section 5.2.4 on secrecy outage probability and average secrecy capacity. We assume $\hat{\Omega}_0 = 0$ dB throughout our analysis.

Figure 5.10 shows the behaviour of SOP for varying ρ_B/ρ_E, $\hat{\beta}_1/\hat{\beta}_2$ and ρ for $P_T = \infty$, $N_A = 2$, $\delta_0 = 0.3$, $N_A = 3$, $I_P = 0$ dB, $\rho_E = 0.2$, $\lambda = 10$ dB, and $\eta = -20$ dB. We see that the SOP enhances as $\hat{\beta}_1/\hat{\beta}_2$ increases. It is because the quality of the main channel estimate increases compared to the quality of the wiretap channel estimate. It is observed that the SOP decreases as ρ_B/ρ_E increases from *0.5* to *5*. Since for higher values of ρ_B/ρ_E, the main channel estimates are much better than eavesdropper's channel. Further, the network security capability is improved as ρ_R increases because the Alice-PR channel estimate quality increases. The highest secrecy is obtained for $\rho = 1$, which signifies the perfect CSI of the Alice-PR channel.

Figure 5.11 illustrates the effect of ρ_m, ρ_e, and ρ on average secrecy capacity for δ_0 =

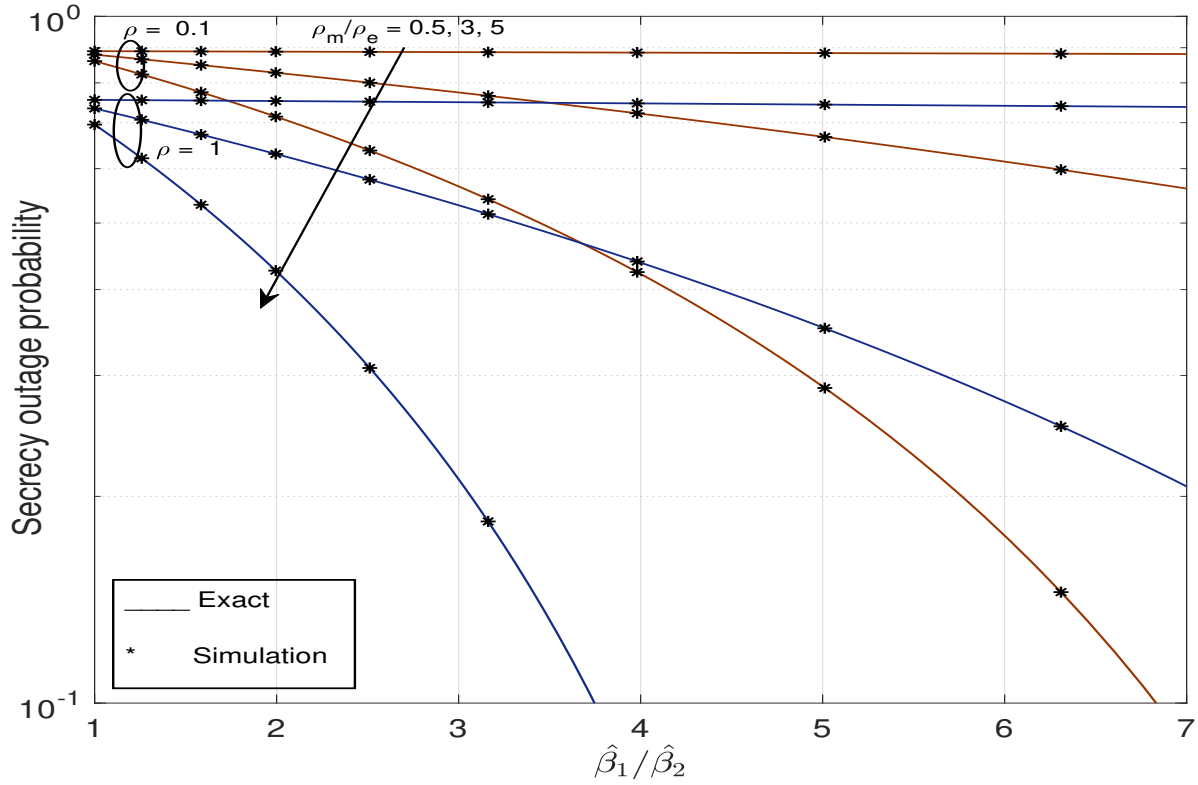

Figure 5.10: SOP versus $\hat{\beta}_1/\hat{\beta}_2$ with unlimited Alice power, $P_T = \infty$, $\delta_0 = 0.3$, $N_A = 3$, $I_P = 0$ dB, $\hat{\Omega}_0 = 0$ dB, $\rho_E = 0.2$, $\lambda = 10$ dB, and $\eta = -20$ dB.

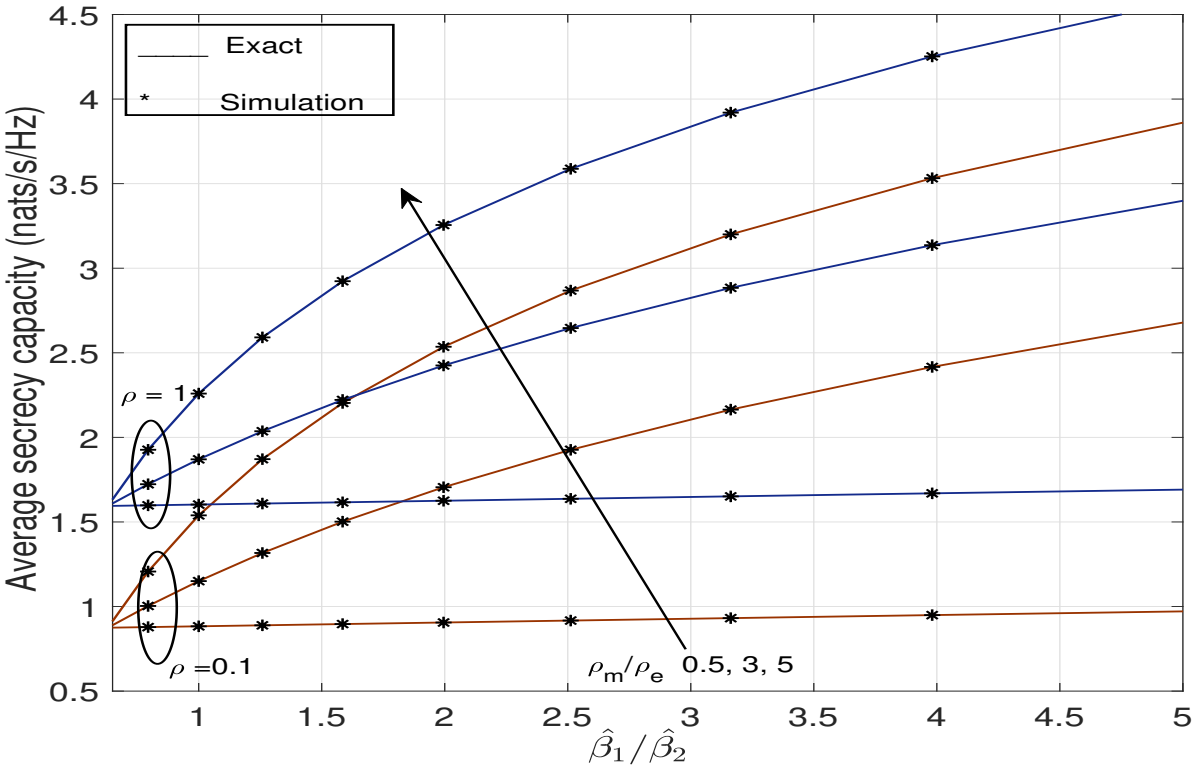

Figure 5.11: Average secrecy capacity versus $\hat{\beta}_1/\hat{\beta}_2$ with unlimited Alice power, $P_T = \infty$, $\rho_E = 0.2$, $\delta_0 = 0.1$, $N_A = 1$, $I_P = 0$ dB, $\lambda = -10$ dB, and $\eta = 15$ dB.

0.1, $N_A = 1$, $I_P = 0$ dB, $\rho_E = 0.2$ dB, $\lambda = -10$ dB, and $\eta = 15$ dB with unlimited Alice power, $P_T = \infty$. As seen in Figure 5.11, since the improvement in the quality of main channel estimates is much better than eavesdropper channel, we can find that ASC increases as $\hat{\beta}_1/\hat{\beta}_2$ increases. It can be noted that the ASC is improved for higher values of ρ_B/ρ_E. Hence, a more accurate estimate of the main channel is required to improve the secondary network's secrecy performance. Further, ASC improves with the quality of the Alice-PR channel estimate.

5.4 Conclusion

This chapter examined the consequences of interference caused by the primary transmitter on the secrecy performance of an underlay CRN in the Rayleigh fading channel with limited and unlimited Alice power adaptation schemes. We obtained the new closed-form expressions for various performance metrics like SOP, intercept probability, PNZC, ε-outage secrecy capacity, and ASC in active and passive eavesdropping scenarios. Furthermore, we examined the consequences of imperfect CSI of the Alice-PR link by considering the outage probability concept on secrecy performance analysis. It has been perceived from derived expressions that SOP and intercept probability decreases with increasing P_T, N_A and β_1, and improves with increasing primary interference power, P_P and the distance between Alice-Bob link, d_M. We also observed that the proposed CRN's data security capability increases when ρ, ρ_m, N_A and β_1 increases and decreases when ρ_e, β_2 and P_P increases.

Chapter 6

Secrecy performance of Interference-limited CRN

The performance of the secondary network is reduced by the interference produced by the primary transmitter, PT, to secondary receivers. When the interference produced by the PT is higher than the noise at the secondary receivers, the quality of interest is the signal-to-interference ratio (SIR) [145] and such CRN is called interference-limited CRN. A receive antenna selection scheme is a less complicated and less costly technique to receive the advantages of diversity combining. Hence, we examine the secrecy performance of the RAS scheme of the interference-limited underlay cognitive radio network over a general fading scenario (i.e., primary network undergoes a Rayleigh fading and a secondary network undergoes Nakagami-m fading). This chapter determines the basic requirements to guard secret information against eavesdropping in the presence of the PT's interference to secondary receivers and outdated CSI on the Alice-PR channel with a limited and unlimited Alice power adaptation scheme. Bob is outfitted with multiple antennas to improve reliable data transmission without the necessity for a secret key. Eve is also equipped with multiple antennas to intensify eavesdropping to extract more information from the main channel. This chapter aims to study the PLS of interference-limited underlay CRNs with a continuous power adaptation scheme while considering all these factors, i.e., the interference power constraints, the outdated CSI, and the interference from the PT. For this, we derive closed-form expressions of SOP, intercept probability, and average secrecy capacity. Furthermore, we use the extreme value theorem (EVT) to derive simple closed-form asymptotic expressions in the limit of a large number of antennas at Bob and Eve.

6.1 System Model

This chapter considers an interference-limited underlay CRN, where the secondary network and the primary network transmit in the same spectrum band concurrently, as long as the amount of interference inflicted on the PR is within a predetermined constraint. We consider a general model of an interference-limited underlay CRN, consisting of Alice, a Bob, a PT, a PR, and an Eve. Bob and Eve are outfitted with N_B and N_E antennas, respectively, while all other terminals are outfitted with a single antenna. Let g_i indicate the channel gain from PT to i^{th} (where $i = 1,2....N_B$) antenna of the Bob, t_j represent the channel gain between PT and j^{th} (where $j = 1,2....N_E$) antenna of Eve and h_0 represent the channel gain between Alice and PR. Therefore, the channel gains $|h_0|$, $|g_i|$ and $|t_j|$ can be presumed to follow independent Rayleigh fading implying that $|h_0|^2$, $|g_i|^2$ and $|t_j|^2$, are i.i.d exponential R.Vs with parameters $\frac{1}{\Omega_0}$, $\frac{1}{\lambda}$ and $\frac{1}{\eta}$, respectively. Let $|h_i|^2$ denote the channel gain between Alice and i^{th} antenna of Bob and $|s_j|^2$ denote the channel gain between Alice and j^{th} antenna of Eve. $|h_i|^2$ and $|s_j|^2$ are presumed to i.i.d Gamma R.Vs with PDFs

$$h_i(y) = \frac{y^{m_B-1}}{\beta_1^{m_B}\Gamma(m_B)} e^{-\frac{y}{\beta_1}}, \tag{6.1}$$

$$s_j(y) = \frac{y^{m_E-1}}{\beta_2^{m_E}\Gamma(m_E)} e^{-\frac{y}{\beta_2}}, \tag{6.2}$$

respectively, where the parameters m_B, m_E, β_1 and β_2 are positive real and $\Gamma(.)$ is the Gamma function [118]. This is because the primary network is a traditional wireless network and it is far away from the secondary network. Therefore, primary and secondary networks have different channel models. As we are interested in the secrecy performance of the secondary network, a more generalized channel fading model, i.e. Nakagami-m distribution, is considered. It includes the Rayleigh fading as a special case when $m_B = m_E = 1$. Further, the Rician distribution model is used when a line-of-sight path exists between Alice and Bob. Generally, the Nakagami-m distribution can precisely approximate the Rician distribution. Due to these reasons, the PDFs of $|h_i|^2$, and $|s_j|^2$ are assumed to be the same. On the other hand, the Rayleigh fading model is ideal for circumstances where there are large numbers of signal paths and reflections. Typical situations incorporate cellular telecommunications where there are many reflections from buildings. Similar to [112], it is believed that Alice has perfect CSI about the Alice-PR channel, h_0. Alice can be notified about h_0 by a mediate band manager between PR and Alice

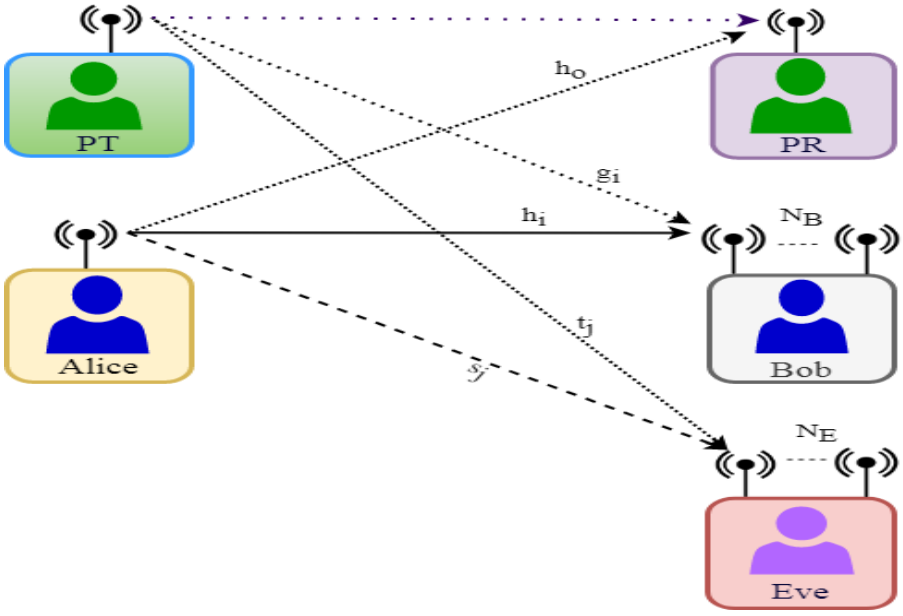

Figure 6.1: The wiretap interference-limited underlay CRN consists of single-antenna Alice, multi-antenna Bob, multi-antenna Eve, a PR and a dominant interferer, PT

or through considering proper signaling [145]. With the assumption that $|h_0|^2$ has perfectly estimated, a continuous power adaption policy is assumed at Alice to constrain its interference to the PR such that the instantaneous transmit power of the Alice can be restricted by peak interference power. We consider the RAS scheme at Bob and Eve, where Bob and Eve pick out the strongest antennas based on perfect CSI estimation via pilot signals transmitted by Alice. Assuming that the noise at the Bob and Eve is negligible compared to the interference from the PT, the instantaneous SIR of the main channel and eavesdropper's channel can be expressed as

$$\psi_M = \max_{i=1,\ldots,N_B} \frac{P_A|h_i|^2}{P_P|g_i|^2} = \max_{i=1,\ldots,N_B} \phi_i, \tag{6.3}$$

$$\psi_E = \max_{j=1,\ldots,N_E} \frac{P_A|s_j|^2}{P_P|t_j|^2} = \max_{j=1,\ldots,N_E} \phi_j, \tag{6.4}$$

respectively, where P_P is the transmit power of the primary transmitter, PT, $P_P|g_i|^2$ is PT interference power at i^{th} antenna of Bob, and $P_P|t_j|^2$ is the interference power at j^{th} antenna of Eve. The PDF of ϕ_i for given $Z = |h_0|^2$ can be calculated as

$$\begin{aligned} f_{\phi_i|Z}(x) =& \frac{P_A}{P_P}\int_0^\infty y h_i(xy) g_i\left(\frac{P_A y}{P_P}\right) dy \\ =& \frac{P_A x^{m_B-1}}{P_P \beta_1^{m_B}\Gamma(m_B)\lambda}\int_0^\infty y^{m_B} e^{-y\left(\frac{x}{\beta_1}+\frac{P_A}{P_P\lambda}\right)} dy \\ =& \frac{\mathscr{Q} m_B x^{m_B-1}}{(x+\mathscr{Q})^{m_B+1}}, \end{aligned} \tag{6.5}$$

where $\mathscr{Q} = \frac{P_A \beta_1}{\lambda P_P}$ and $g_i(x) = \frac{e^{-\frac{x}{\lambda}}}{\lambda}$. The CDF $F_{\phi_i|Z}(x)$ can be calculated by integrating $f_{\phi_i|Z}(x)$ as

$$F_{\phi_i|Z}(x) = \int_0^x f_{\phi_i|Z}(x)dx = \left(\frac{x}{x+Q}\right)^{m_B}. \tag{6.6}$$

Therefore, CDF and PDF of ϕ_M for given $|h_0|^2$ are given by

$$F_{\psi_M|Z}(x) = \max_{i=1,....,N_B} F_{\phi_i|Z}(x) = \left(\frac{x}{x+\mathscr{Q}}\right)^{m_B N_B}, \tag{6.7}$$

$$f_{\psi_M|Z}(x) = \frac{N_B m_B \mathscr{Q} x^{m_B N_B - 1}}{(x+\mathscr{Q})^{m_B N_B + 1}}, \tag{6.8}$$

respectively. Similarly, the CDF and PDF of ψ_E for given $|h_0|^2$ can be expressed as

$$F_{\psi_E|Z}(x) = \left(\frac{x}{x+\mathscr{D}}\right)^{m_E N_E}, \tag{6.9}$$

$$f_{\psi_E|Z}(x) = \frac{N_E m_E \mathscr{D} x^{m_E N_E - 1}}{(x+\mathscr{D})^{m_E N_E + 1}}, \tag{6.10}$$

where $\mathscr{D} = \frac{P_A \beta_2}{\eta P_P}$. The asymptotic distributions of ψ_M and ψ_E for large value of N_B and N_E are given in following proposition.

Proposition 6.1. *The asymptotic distributions of maximum of $\phi_i's$, ψ_M, for given $|h_0|^2$ is Fréchet distributions i.e.,*

$$\lim_{N_B \to \infty} F_{\psi_M|Z}(x) = \exp\left(-\frac{b_M}{x}\right), \tag{6.11}$$

where $b_M = \dfrac{\mathscr{Q}}{\left(\left(1-\frac{1}{N_B}\right)^{-\frac{1}{m_B}} - 1\right)}$.

Proof: It can be shown that

$$\lim_{x \to \infty} \frac{1 - F_{\phi_i|Z}(x)}{1 - F_{\phi_i|Z}(px)} = p \tag{6.12}$$

which implies that $F_{\phi_i|Z}(x)$ lies in the domain of maximum attraction of Fréchet distribution [198, Th. 10.5.2],i.e.,

$$\lim_{N_B \to \infty} F_{\psi_M|Z}(x) = \exp\left(-\frac{F^{-1}_{\phi_i|Z}\left(1-\frac{1}{N_B}\right)}{x}\right), \; x \geq 0, \tag{6.13}$$

where $F^{-1}_{\phi_i|Z}(p) = \frac{\mathscr{Q}}{\left(1-p^{-\frac{1}{m_B}}\right)}$.

Similarly, the CDF of γ_E for a large value of N_E can be approximated as

$$\lim_{N_E\to\infty} F_{\gamma_E|Z}(x) = \exp\left(-\frac{b_E}{x}\right), \tag{6.14}$$

where $b_E = \frac{\mathscr{D}}{\left(\left(1-\frac{1}{N_E}\right)^{-\frac{1}{m_E}}-1\right)}$.

6.2 Secrecy Performance Analysis for Interference-Limited CRN

This section performs a complete secrecy performance analysis of interference-limited CRN. We derive closed-form expressions for SOP intercept probability and average secrecy capacity.

6.2.1 Secrecy Outage Probability

In this subsection, we derive a novel expression for the exact SOP, as given in the Proposition 6.2.

Proposition 6.2. *The SOP of interference limited underlay CRN with receive antenna selection scheme can be expressed as*

$$\begin{aligned} P_{out} =& \mathscr{R}_1\mathscr{R}_2\left(1-e^{-\frac{I_P}{\Omega_0 P_T}}\right){}_2F_1\left(\mu_1+1, l+\mu_1; \mu_1+\mu_2+1; 1-\frac{\tau-1+\mathscr{Q}_1}{\tau\mathscr{D}_1}\right) \\ &+\left(\frac{\mathscr{R}_1\mathscr{R}_3\mathscr{W}_1\mathscr{W}_2}{\Omega_0^{l-j-h-\mu_2-1}}\right)\Gamma\left(\mu_2-l+j+h+1, \frac{I_P}{P_T\Omega_0}\right), \end{aligned} \tag{6.15}$$

where $B(m,n)$ is the Beta function and ${}_2F_1(a,b;x;y)$ is the Gauss hypergeometric function, $\Gamma(.,.)$ is the upper incomplete Gamma function, and

$$\begin{aligned} &\mu_1 = m_E N_E, \mu_2 = m_B N_B, \tau = 2^{R_s}, \mathscr{Q}_1 = \frac{P_T\beta_1}{\lambda P_P}, \mathscr{D}_1 = \frac{P_T\beta_2}{\eta P_P}, \mathscr{Q}_2 = \frac{I_P\beta_1}{\lambda P_P}, \mathscr{D}_2 = \frac{I_P\beta_2}{\eta P_P}, \\ &\mathscr{R}_1 = \frac{\mu_1}{\tau^{\mu_1}}\sum_{l=0}^{\mu_2}\binom{\mu_2}{l}(\tau-1)^{\mu_2-l}B(l+\mu_1, 1-l+\mu_2), \mathscr{R}_2 = \frac{(\tau-1+\mathscr{Q}_1)^{l+\mu_1-\mu_2}}{\mathscr{D}_1^{\mu_1}}, \\ &\mathscr{W}_1 = \frac{(\mu_1+1)_m(l+\mu_1)_m}{m!(\mu_1+\mu_2+1)_m}, \mathscr{R}_3 = \sum_{j=0}^{l+\mu_1-\mu_2}\frac{(\tau-1)^j}{(\mathscr{D}_2)^{\mu_1}}\binom{l+\mu_1-\mu_2}{j}\mathscr{Q}_2{}^{l+\mu_1-\mu_2-j}, \end{aligned}$$

$$\mathscr{W}_2 = \sum_{p=0}^{m} \binom{m}{p} (-1)^p \left(\frac{1}{\tau \mathscr{D}_2}\right)^p \sum_{h=0}^{p} \binom{p}{h} \mathscr{Q}_2^{p-h} (\tau-1)^h.$$

Proof: First, we drive the conditional SOP for given Z as

$$\begin{aligned} P_{out}(R_s|Z) &= \int_0^{\infty} F_{\psi_M|Z}(\varepsilon(\gamma_E)) f_{\psi_E|Z}(\psi_E) d\psi_E \\ &= \int_0^{\infty} F_{\psi_M|Z}(\tau(1+\psi_E)-1)) f_{\psi_E|Z}(\psi_E) d\psi_E. \end{aligned} \tag{6.16}$$

By putting (6.7) and (6.10) in (6.17) and utilizing [187], $P_{out}(R_s|Z)$ can be calculated as

$$P_{out}(R_s|Z) = \mathscr{R}_1 \mathscr{H}_{12} F_1\left(\mu_1+1, l+\mu_1; \mu_1+\mu_2+1; 1-\frac{\tau-1+\mathscr{Q}}{\tau \mathscr{D}}\right), \tag{6.17}$$

where $\mathscr{H}_1 = \frac{(\tau-1+\mathscr{Q})^{l+\mu_1-\mu_2}}{D^{\mu_1}}$. Then, unconditional SOP can be expressed as

$$P_{out}(R_s) = \int_0^{\infty} P_{out}(R_s|Z) f_Z(z) dz, \tag{6.18}$$

where $f_Z(z) = \frac{e^{-\frac{z}{\Omega_0}}}{\Omega_0}$.

To this end, the SOP can be obtained as (6.15) after utilizing [199, eq.1a], and [187, eq. 3.351.2] and carrying out some simple mathematical manipulations. In proposition 2, we concentrated on analyzing the SOP under the limited Alice power adaptation, i.e., $P_A = \min\left(P_T, \frac{I_P}{|h_0|^2}\right)$, it should be noted that simpler expression can be achieved under the unlimited Alice power case. i.e., $P_A = \frac{I_P}{|h_0|^2}$. This expression is beneficial when $P_T \to \infty$. Moreover, it serves as upper bounds on the SOP under an unlimited Alice power case. Applying the results from Proposition 2, we derive SOP for the RAS scheme with unlimited Alice power in the Corollary 6.1.

Corollary 6.1. *The SOP of interference-limited CRN for receive antenna selection scheme under continuous power adaptation with unlimited Alice power can be expressed as*

$$P_{out} = \mathscr{R}_1 \mathscr{R}_3 \mathscr{W}_1 \mathscr{W}_2 \frac{(\mu_2 - l + j + h)!}{\Omega_0^{\mu_2 - l + j + h}}. \tag{6.19}$$

Proof: By substituting $P_T = \infty$ in (6.15) and performing some mathematical manipulation, we can calculate the SOP with unlimited Alice power as mentioned in (6.19).

6.2.2 Asymptotic Secrecy Outage Probability

In order to find more insight from proposed network, we proceed to derive asymptotic SOP for two scenarios: 1) N_B is very large i.e., $N_B \to \infty$ for arbitrary N_E, and 2) N_B and N_E are very large, which is mathematically described as $N_B \to \infty$ and $N_E \to \infty$.

1. $N_B \to \infty$: In this case, we derive asymptotic SOP for a large N_B and arbitrary N_E and fixed τ. For large value of N_B, the CDF of the main channel is approximated as

$$F_{\psi_M|Z}(\varepsilon(\psi_E)) \approx \exp\left(-\frac{b_M}{\varepsilon(\psi_E)}\right) \approx \exp\left(-\frac{b_M}{\tau\psi_E}\right). \tag{6.20}$$

By utilizing (6.20), the asymptotic SOP can be derived as

$$P_{out}^{\infty}(R_s) = \mu_1 U\left(1, 1-\mu_1, \frac{\beta_1\eta}{\tau\lambda\beta_2\left(\left(1-\frac{1}{N_B}\right)^{-\frac{1}{m_B}}-1\right)}\right), \tag{6.21}$$

where $U(m,n,z) = \frac{1}{\Gamma(m)}\int_0^{\infty} e^{-tz}t^{m-1}(1+t)^{n-m-1}dt$ is Tricomi hypergeometric function. Following observations can be made from (6.21):

- From (6.21), it is clear that P_{out} is directly proportional to μ_1. It means P_{out} increases with increasing N_E. On the other hand, confluent hypergeometric function is a decreasing function of β_1, η, m_B and N_B. Therefore, one can say that secrecy performance of the interference-limited CRN improves with increasing β_1, N_B, m_B.
- Furthermore, confluent hypergeometric function is a increasing function of τ, β_2 and λ. We can obsereve from here that secrecy performance of the interference-limited CRN degrades with increasing β_2, N_E, m_E and λ.

2. $N_B \to \infty$ and $N_E \to \infty$: For a significant value of N_E, the PDF of the eavesdropper channel is approximated as

$$f_{\psi_E|Z}(\psi_E) = \frac{b_E}{\psi_E^2}\exp\left(-\frac{b_E}{\psi_E}\right). \tag{6.22}$$

By utilising (6.22), the asymptotic SOP for large value of N_B and N_E can be expressed as

$$P_{out}(R_s) \approx \left(1+\frac{b_M}{\tau b_E}\right)^{-1}. \tag{6.23}$$

From (6.23), we have drawn some insights as shown below:

- It is remarked that $P_{out}(R_s)$ expressed in (6.23) is a increasing with increasing N_E and decreasing function of N_B.
- For $m_B = m_E = 1$, (6.23) approaches to [200, eq.19] for a single Bob.
- For $N_B = N_E$ and $m_B = m_E$, $P_{out}(R_s)$ converges to a constant value i.e,

$$P_{out}(R_s) \approx \left(1 + \frac{\beta_1 \lambda}{\tau \eta \beta_2}\right)^{-1}. \tag{6.24}$$

It reveals that for large of N_B and N_E, SOP converges to a constant value that only depends on the β_1, β_2 and threshold rate R_s. It is clear from (6.24) that SOP is inversely proportional to β_1 that means SOP degrades with increasing β_1 and improves with increasing R_s and β_2.

6.2.3 Intercept Probability

This subsection calculates the novel expressions for exact and asymptotic intercept probability for receive antenna selection scheme. The exact intercept probability can be calculated by setting $R_s = 0$ in (6.15) as

$$P_{int} = \mu_1 B(\mu_1 + \mu_2, 1) \left(\frac{\beta_1 \eta}{\beta_2 \lambda}\right)^{\mu_1} {}_2F_1\left(\mu_1 + 1, \mu_1 + \mu_2; \mu_1 + \mu_2 + 1; 1 - \frac{\beta_1 \eta}{\beta_2 \lambda}\right). \tag{6.25}$$

For a large value of N_B, the asymptotic intercept probability can be calculated as

$$P_{int} \approx \mu_1 U \left(1, 1 - \mu_1, \frac{\beta_1 \eta}{\lambda \beta_2 \left(\left(1 - \frac{1}{N_B}\right)^{-\frac{1}{m_B}} - 1\right)}\right). \tag{6.26}$$

6.2.4 Average Secrecy Capacity

The ASC for an arbitrary value of N_B and N_E in closed form is defined as [68]

$$\begin{aligned} \bar{C_s} &= \frac{1}{\ln(2)} \int_0^\infty \frac{F_{\gamma_E}(\gamma_E)}{1 + \gamma_E} \left[\int_{\gamma_E}^\infty f_{\gamma_M}(\gamma_M) d\gamma_M\right] d\gamma_E \\ &= \frac{1}{\ln(2)} \int_0^\infty \frac{F_{\gamma_E}(\gamma_E)}{1 + \gamma_E} \left[1 - F_{\gamma_M}(\gamma_E)\right] d\gamma_E. \end{aligned} \tag{6.27}$$

By substituting the asymptotic approximation of $F_{\psi_M}(\psi_M)$ in (6.27), the closed form asymptotic expression for the ASC with $N_E = 1$ in derived in Proposition (6.3).

Proposition 6.3. *For large value of N_B and $N_E = m_E = 1$, the average secrecy capacity can be expressed as*

$$\bar{C}_s = \frac{1}{\ln(2)} \begin{cases} E_0 + \mathscr{D}\left(K\left(\frac{b_{N_B}}{\mathscr{D}}\right)\right) + K(b_{N_B}) & \mathscr{D} \neq 1 \\ E_0 + K(b_{N_B}) - b_{N_B} e^{b_{N_B}} Ei(-b_{N_B}) & \mathscr{D} = 1, \end{cases} \tag{6.28}$$

where, $E_0 = 0.577216$ is the Euler constant, $K(b_{N_B})$ and $K\left(\frac{b_{N_B}}{D}\right)$ are expressed in (6.35) and (6.36) respectively.

Proof: Using (6.11) and the relation $\Gamma(1,y) = 1 - \gamma(1,y)$, then we have

$$1 - F_{\gamma_M}(\gamma_E) \approx \gamma\left(1, \frac{b_{N_B}}{\gamma_E}\right), \tag{6.29}$$

where $\gamma(1,z) = \int_0^z e^{-x} dx$. By substituting (6.9) for $N_E = m_E = 1$ and (6.29) in (6.27), which yields

$$\bar{C}_s \approx \frac{1}{\ln(2)} \int_0^\infty \frac{\psi_E}{(1+\psi_E)(\psi_E + \mathscr{D})} \gamma\left(1, \frac{b_{N_B}}{\psi_E}\right) d\psi_E. \tag{6.30}$$

Put $y = \frac{b_{N_B}}{\psi_E}$ and integral representation of $\gamma\left(1, \frac{b_{N_B}}{\gamma_E}\right)$ in (6.30), we have

$$\bar{C}_s \approx \frac{1}{\ln(2)} \int_0^\infty \frac{(b_{N_B})^2}{y(y+b_{N_B})(\mathscr{D}y + b_{N_B})} \int_0^y e^{-x} dx dy. \tag{6.31}$$

Changing the order of the integration, we get

$$\bar{C}_s \approx \frac{1}{\ln(2)} \int_0^\infty e^{-x} \underbrace{\left(\int_t^\infty \frac{(b_{N_B})^2}{y(y+b_{N_B})(\mathscr{D}y + b_{N_B})} dy \right)}_{I(x)} dx, \tag{6.32}$$

where $I(x)$ can be evaluated as

$$I(x) = \begin{cases} -\ln(x) + \mathscr{D} \ln\left(x + \frac{b_{N_B}}{\mathscr{D}}\right) - \ln(x + b_{N_B}), & \mathscr{D} \neq 1 \\ -\ln(x) + \ln(x + b_{N_B}) - \frac{b_{N_B}}{(x + b_{N_B})}, & \mathscr{D} = 1. \end{cases} \tag{6.33}$$

Hence, $\bar{C}_s$ can be written as

$$\bar{C}_s = \frac{1}{\ln(2)} \int_0^\infty e^{-x} \begin{cases} -\ln(x) + \mathscr{D} \ln\left(x + \frac{b_{N_B}}{\mathscr{D}}\right) - \ln\left(x + b_{N_B}\right), & \mathscr{D} \neq 1 \\ -\ln(x) + \ln\left(x + b_{N_B}\right) - \frac{b_{N_B}}{\left(x + b_{N_B}\right)}, & \mathscr{D} = 1. \end{cases} \tag{6.34}$$

Let

$$K\left(b_{N_B}\right) = \int_0^\infty e^{-x} \ln\left(x + b_{N_B}\right) dx = \ln(b_{N_B}) - e^{b_{N_B}} Ei\left(-b_{N_B}\right), \tag{6.35}$$

$$K\left(\frac{b_{N_B}}{\mathscr{D}}\right) = \int_0^\infty e^{-x} \ln\left(x + \frac{b_{N_B}}{\mathscr{D}}\right) dx = \ln\left(\frac{b_{N_B}}{\mathscr{D}}\right) - e^{\left(\frac{b_{N_B}}{\mathscr{D}}\right)} \mathrm{Ei}\left(-\left(\frac{b_{N_B}}{\mathscr{D}}\right)\right). \tag{6.36}$$

Further the integral $\int_0^\infty e^{-x} \frac{b_{N_B}}{\left(x + b_{N_B}\right)} dx$ and $\int_0^\infty e^{-x} \ln(x) dx$ can be calculated by using [187] as

$$\begin{aligned} \int_0^\infty e^{-x} \frac{b_{N_B}}{\left(x + b_{N_B}\right)} dx &= -b_{N_B} e^{b_{N_B}} \mathrm{Ei}\left(-b_{N_B}\right) \\ \int_0^\infty e^{-x} \ln(x) dx &= -E_0. \end{aligned} \tag{6.37}$$

To this end, by using (6.35), (6.36) and (6.37) in (6.34), we obtain the closed form expression of ASC given in (6.28).

6.2.5 Secrecy Performance Analysis for Outdated CSI Scenario

In practical scenarios, only the partial information of the channel gain h_0 is available at Alice. Due to the time-varying nature of the wireless link, the CSI provided to Alice on channel gain h_0 is outdated, and it can be described as (5.41). The transmit power of Alice due to outdated CSI can be expressed as (5.42). We also consider imperfect CSI in the secondary network, i.e., CSI on h_i and s_j is imperfect for a more realistic situation. The outdated CSI for h_i and s_j can be represented as

$$\begin{aligned} h_i &= \tau \hat{h}_i + \sqrt{1 - \rho_B^2} \tilde{h}_i, \;\; i = 1, 2 \ldots\ldots N_B, \\ s_j &= \rho_E \hat{s_j} + \sqrt{1 - \rho_E^2} \tilde{s}_j, \;\; j = 1, 2 \ldots\ldots N_E, \end{aligned} \tag{6.38}$$

where, $\hat{h}_i$ and $\hat{s_j}$ are the outdated channel information on i^{th} antenna link between Bob and Alice, and j^{th} antenna link between Eve and Alice respectively. $\tilde{h}_i \sim \mathscr{CN}(0,1)$ and $\tilde{s}_j \sim \mathscr{CN}(0,1)$ are complex Gaussian R.V. with unity variance. As $|h_i|^2$ and $|s_j|^2$ are Gamma distributed R.V.

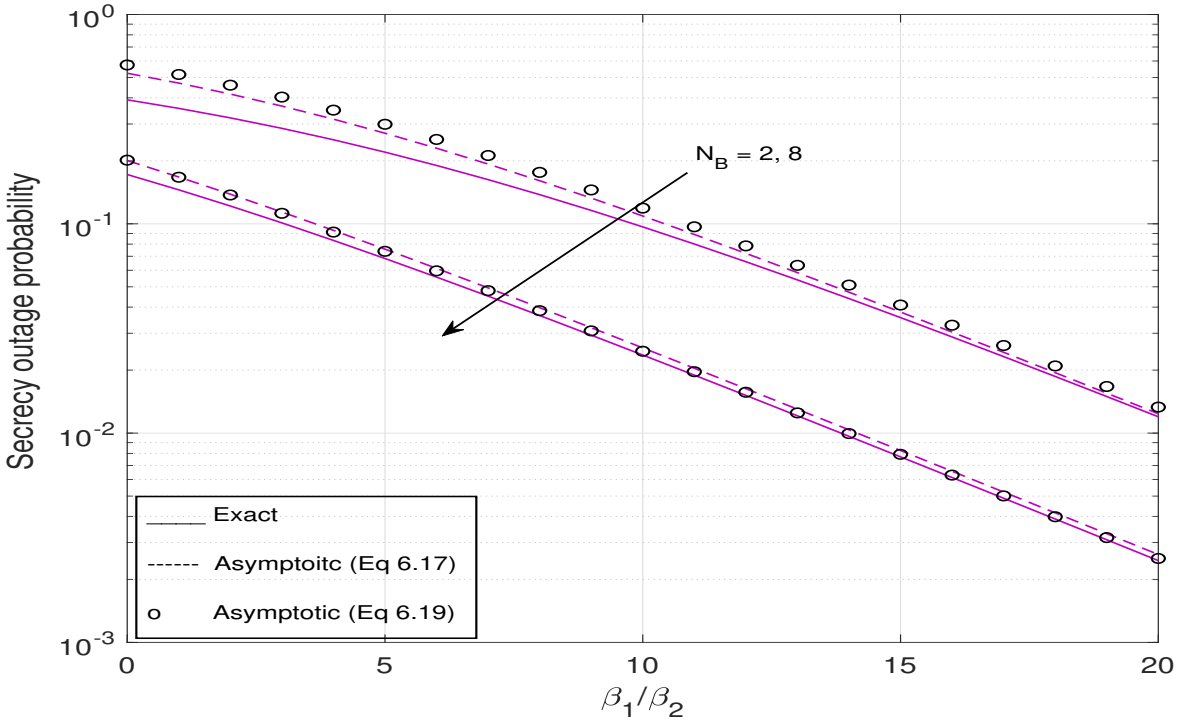

Figure 6.2: SOP versus β_1/β_2 for $\lambda = 0$ dB, $\eta = 0$ dB, $N_E = 5$, $m_E = 2$, $m_B = 2$ and $R_s = 0.1$

with parameters m_B, m_E, β_1 and β_2 respectively, similarly $|\hat{h}_i|^2$ and $|\hat{s}_j|^2$ are also are Gamma distributed R.V. with parameters m_B, m_E, $\hat{\beta}_1$ and $\hat{\beta}_2$ respectively.

This is noted that the expression for SOP with perfect CSI derived in previous subsections also hold for outdated CSI on h_0 after replacing Ω_0 with $\hat{\Omega}_0$, and I_P with $\alpha_I I_P$. Replacing b_{N_B} and b_{N_E} with $\hat{b}_{N_B}$ and $\hat{b}_{N_E}$ due to imperfect CSI on h_i and s_j respectively, where $\hat{b}_{N_B}$ and $\hat{b}_{N_E}$ are expressed as $\hat{b}_{N_B} = \dfrac{\hat{\mathscr{Q}}}{\left(\left(1-\frac{1}{N_B}\right)^{-\frac{1}{m_B}}-1\right)}$ and $\hat{b}_{N_E} = \dfrac{\hat{\mathscr{D}}}{\left(\left(1-\frac{1}{N_E}\right)^{-\frac{1}{m_E}}-1\right)}$, where $\hat{\mathscr{Q}} = \frac{P_A\hat{\beta}_1}{\lambda P_P}$ and $\hat{\mathscr{D}} = \frac{P_A\hat{\beta}_2}{\eta P_P}$.

6.3 Numerical Examples

In this section, the analytical SOP, intercept probability and average secrecy capacity expressions are validated through corresponding Monte-Carlo simulation. We clearly see from the obtained figures that the analytical results perfectly match the simulation results. We begin by showing SOP and intercept probability in perfect CSI environment. We then present SOP under peak interference power constraint in outdated CSI scenario.

Figure 6.2 plots SOP versus β_1/β_2 for different value of N_B. We validate the correctness of the asymptotic SOP expressions derived in (6.21) and (6.23) by matching them with the exact

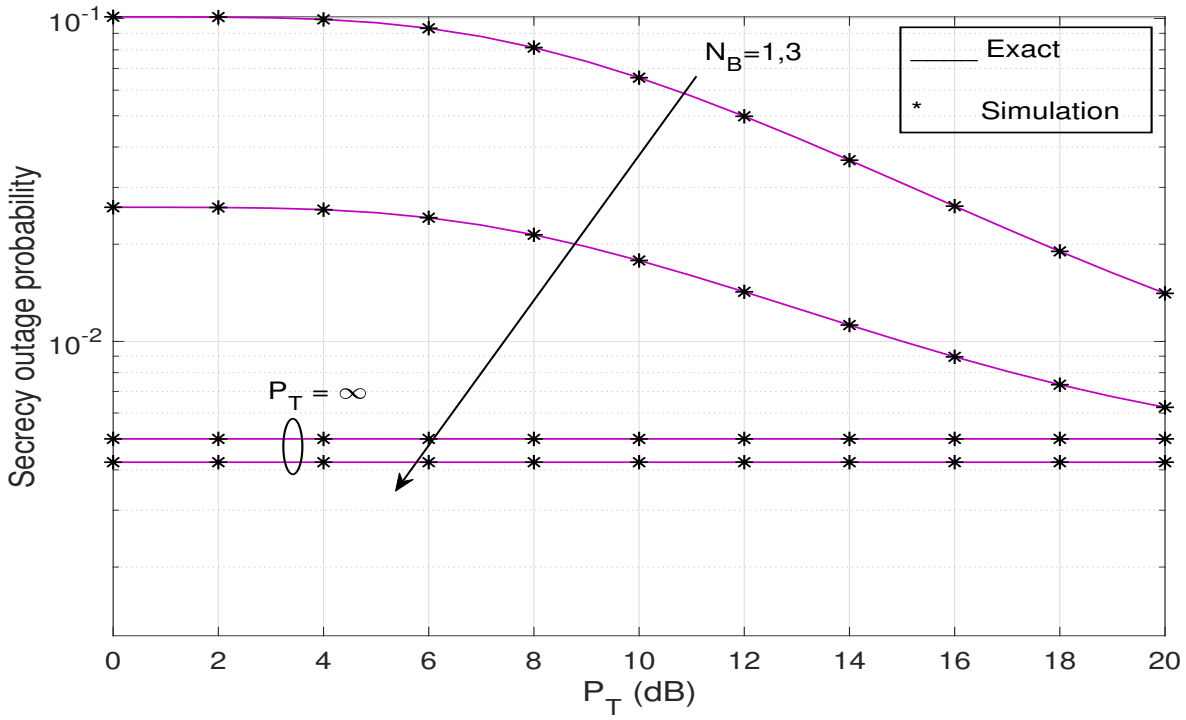

Figure 6.3: SOP versus P_T for $\lambda = 0$ dB, $\eta = 0$ dB, $\beta_1 = 10$ dB, $N_E = 5$, $R_s = 0.1$, $m_B = 2$ and $m_E = 2$

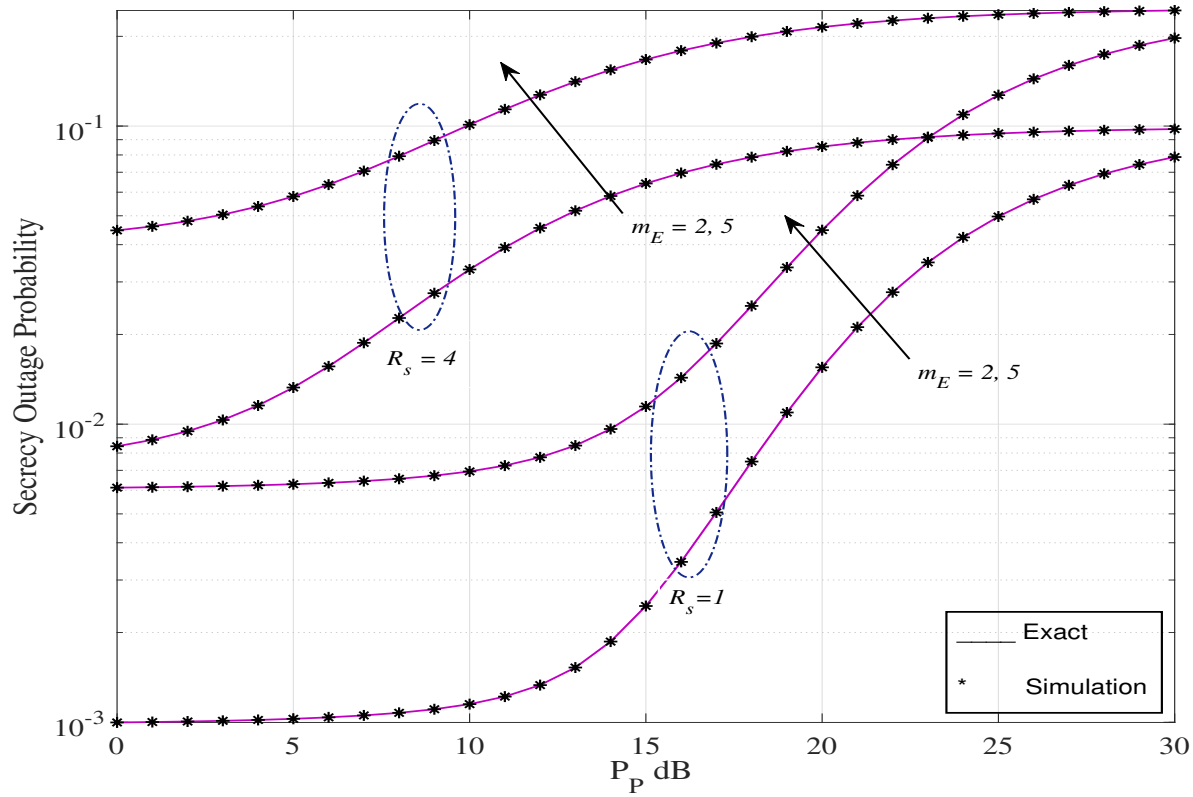

Figure 6.4: SOP versus P_P for $P_T = 10$ dB, $\beta_1 = 6$ dB, $\beta_2 = 6$ dB, $\lambda = 2$ dB, $\eta = -20$ dB, $I_P = 0$ dB, $m_B = 2$, $N_B = 3$, $N_E = 2$, and $\Omega_0 = 0$ dB

SOP result. First, we see that the SOP decreases as the antenna number at Bob, N_B progresses. Next, we observe that the asymptotic SOP expressions are less precise for small values of N_B.

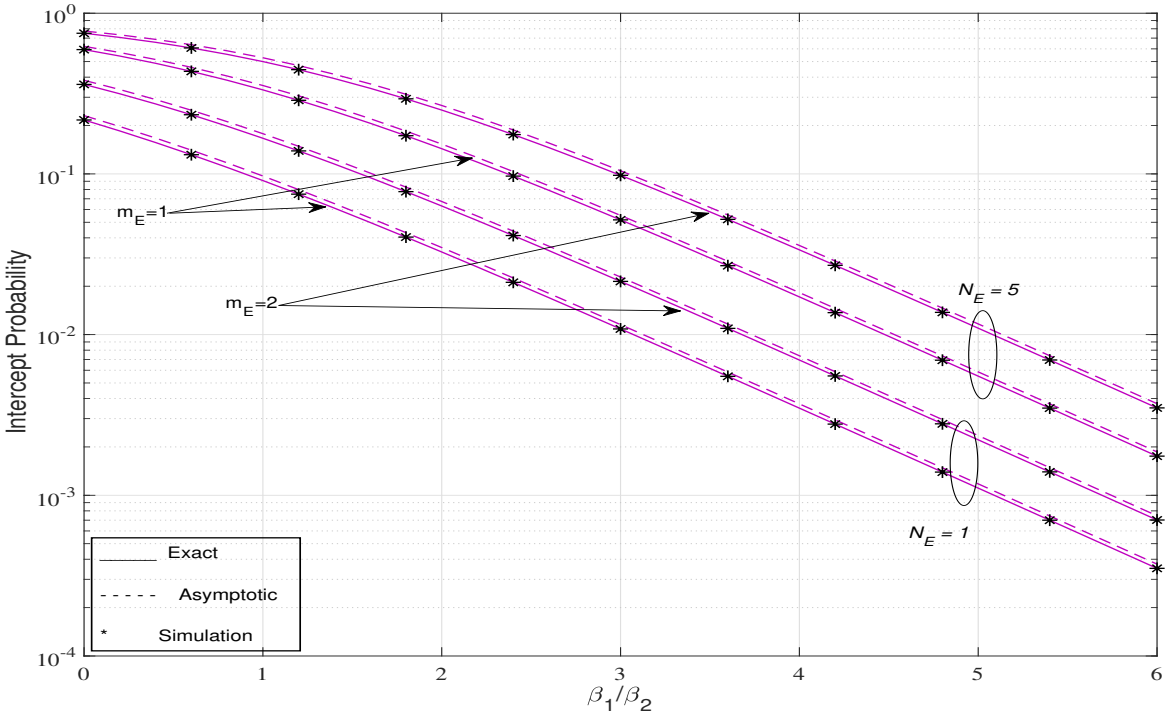

Figure 6.5: Intercept probability versus β_1/β_2 for $\lambda = 0$ dB, $\eta = 0$ dB, $N_B = 5$ and $m_B = 2$

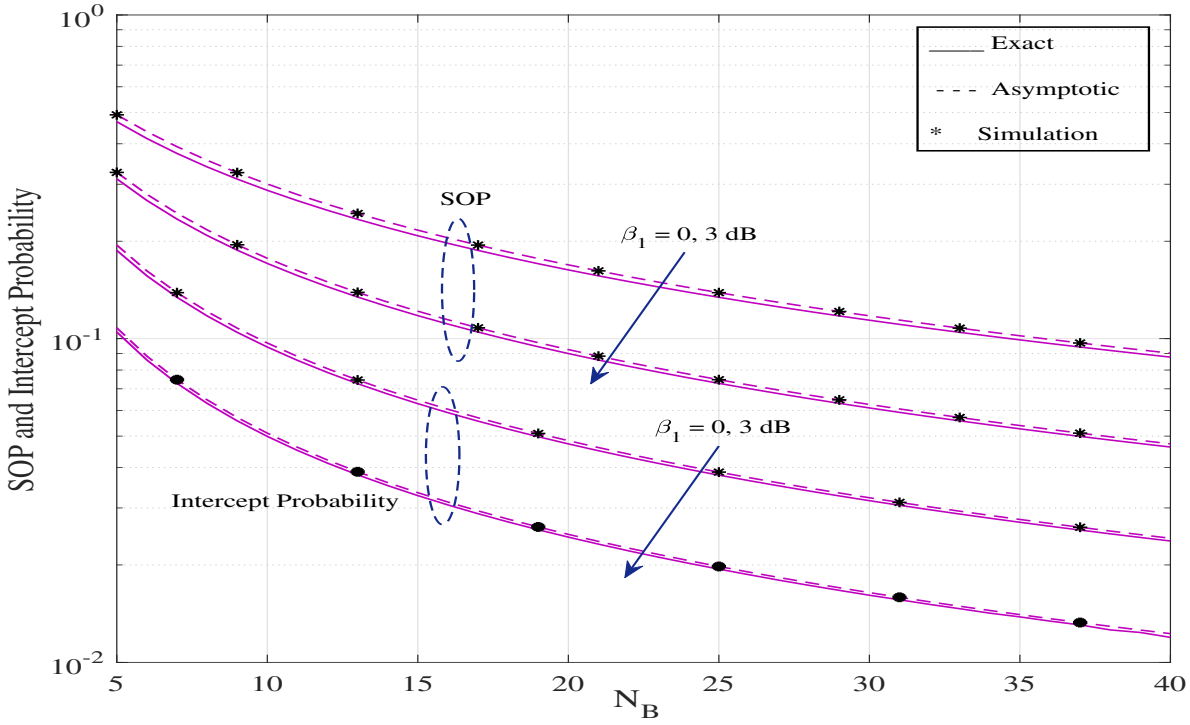

Figure 6.6: SOP and intercept probability versus N_B for $P_P = 10$ dB, $\beta_1 = 6$ dB, $\beta_2 = 6$ dB, $\lambda = 6$ dB, $\eta = -5$ dB, $I_P = 5$ dB, $m_B = 1$, $m_E = 3$, $N_E = 2$, $P_T = 15$ dB and $\Omega_0 = 0$ dB

It is because the asymptotic analysis exists with high correctness only for a large value of N_B.

In Figure 6.3, we plot the SOP versus maximum transmit power P_T, for both limited Alice power with P_T varies from 0 to 20 dB and unlimited Alice power $P_T = \infty$, for $N_B = 1, 3$. Fig. 6.3

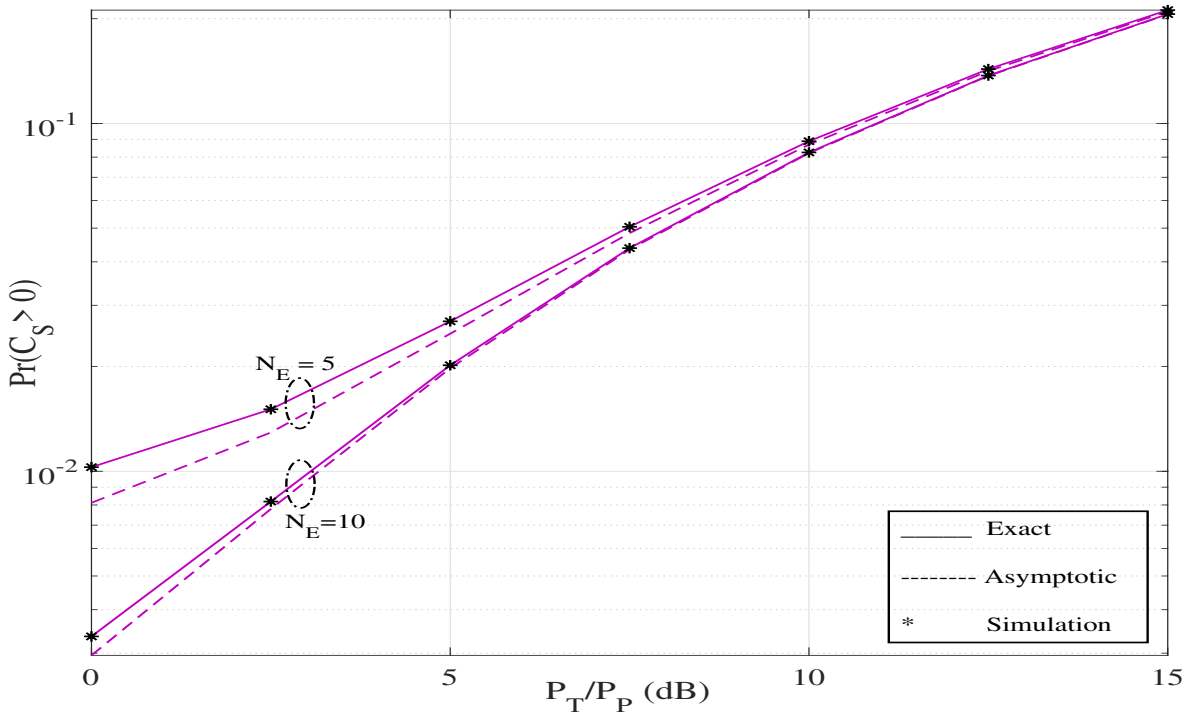

Figure 6.7: PNZC versus P_T/P_P for $P_P = 4$ dB, $\beta_1 = 6$ dB, $\beta_2 = 6$ dB, $\lambda = 10$ dB, $\eta = -10$ dB, $I_P = 5$ dB, $m_B = 2$, $m_E = 4$, and $N_B = 3$.

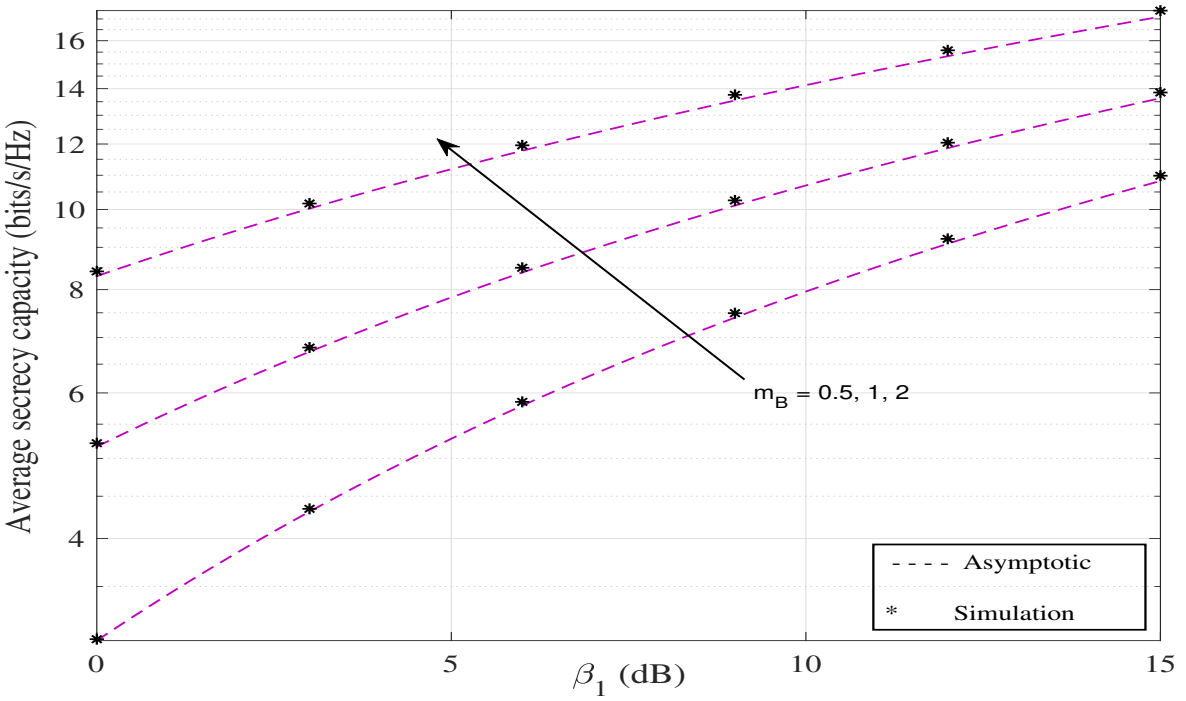

Figure 6.8: Average secrecy capacity versus β_1 for $P_T = 10$ dB, $\beta_2 = 5$ dB, $\lambda = 2$dB, and $\eta = 4$ dB

depicts that secrecy performance of interference-limited CRN improves as P_T increases. It is because P_T upper bounds Alice's power, according to $P_A = \min\left(P_T, \frac{I_P}{|h_0|^2}\right)$. As such, the increase in P_T raises Alice's transmit power, conclusively remedying the SOP. Nevertheless, the

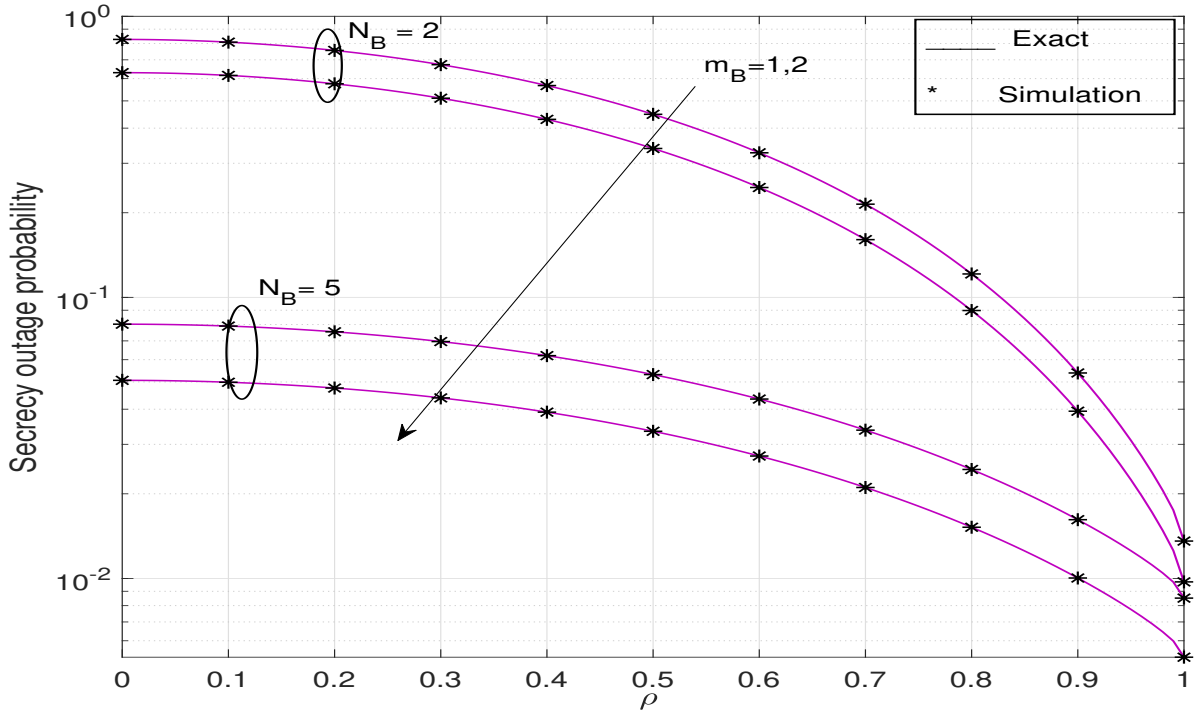

Figure 6.9: Secrecy outage probability versus correlation coefficient, ρ, with unlimited Alice power, $P_T = \infty$, $\delta_0 = 0.1$.

security performance suffers the error floor at a large value of P_T. It is because Alice's power is restricted by a minimum of I_P and P_T. Hence, when P_T is larger than a particular value, Alice's power is limited by I_P, making the security performance unchanged despite increasing P_T. For a significant value of P_T, SOP approaches the one with unlimited Alice's power, $P_T = \infty$. We also observe that the SOP with unlimited Alice power serves as a lower bound on the SOP with limited Alice power.

Figure 6.4 plots SOP versus P_P for $P_T = 10$ dB, β_1 = 6 dB, β_2 = 6 dB, λ = 2 dB, η = -20 dB, $I_P = 0$ dB, m_B = 2, N_B = 3, N_E = 2, and $\Omega_0 = 0$ dB. Figure 6.4 depicted that SOP improves with increasing primary interference P_P . It is because the interference from P_T reduces the signal to interference ratio at both Bob and Eve, which results in the enhancement in the SOP. Furthermore, SOP also improves with the increment in the fading parameter of the eavesdropper m_E.

In Figure 6.5, we plot intercept probability versus β_1/β_2 for λ = 0 dB, $\eta = 0$ dB, $N_B = 5$ and $m_B = 2$. It is also clear from Figure 6.5 that intercept probability improves with increasing β_1/β_2. Intercept probability progresses with the increase in the number of antennas at Eve, N_E and m_B.

Figure 6.6 plots SOP and intercept probability versus N_B for $P_P = 10$ dB, β_1 = 6 dB, β_2 = 6

dB , $\lambda = 6$ dB, $\eta = -5$ dB, $I_P = 5$ dB, m_B = 1, m_E = 3, N_E = 2, and P_T = 15 dB for different value of β_1. We validate the correctness of our numerical results by performing Monte Carlo simulation. It is observed from the Figure 6.6 that both SOP and intercept probability degrade with increasing the number of the antenna of the Bob. From Figure 6.6, one can concludes that intercept probability outperform the secrecy outage probability. Moreover, increasing β_1 boots up the secrecy performance of the system.

Figure 6.7 shows the variation of PNZC versus $\frac{P_T}{P_P}$ for $P_P = 4$ dB, $\beta_1 = 6$ dB, β_2 = 6 dB , λ = 10dB, $\eta = -10$ dB, $I_P = 5$ dB, m_B = 2, m_E = 4, and $N_B = 3$ for different value of N_E. It is observed from Figure 6.7 that when the P_T increases, PNZC improves and it reduces with the increasing the number of antenna of the Eve. Furthermore, from Figure 6.7, we find that non-zero secrecy capacity exists, even the SIR of the Eve link is greater than that of the Bob's link.

Figure 6.8 plots average secrecy capacity versus β_1 for $P_T = 10$ dB, β_2 = 5 dB, $\lambda = 2$ dB and $\eta = 4$ dB for different value of m_B. We validate the asymptotic ASC using Monte Carlo simulations. From Figure 6.8, it is observed that ASC improves with both β_1 and m_B.

Figure 6.9 shows the impact of outdated CSI on SOP. Figure 6.9 plots the SOP versus the correlation coefficient of Alice-PR link, ρ, for N_B = 2 & 5, $\delta_0 = 0.1$ with unlimited Alice power, $P_T = \infty$. We see that the secrecy performance increases as the channel estimate quality increases, i.e., ρ increases from 0 to 1. As expected, the highest secrecy is realized for $\rho = 1$, which signifies the perfect CSI of the Alice-PR link.

6.4 Conclusion

This chapter examined the consequences of interference caused by primary transmitter PT on the secrecy performance of an underlay CRN with limited and unlimited Alice power adaption schemes for interference-limited scenarios. We derived closed-form expressions for various performance metrics like SOP, intercept probability, and ASC over a general fading scenario. We examined the impact of imperfect CSI between the Alice-PR channel on secrecy performance. It has been observed from derived expressions that SOP and intercept probability decreases with increasing P_T, m_B, N_B, ρ_B and β_1 and increasing with increasing m_E, N_E, ρ_E and β_2. Simultaneously, SOP and intercept probability improve with increasing primary interference power, P_P. On the other hand, ASC also improves with increasing m_B, N_B, ρ_B and β_1 and degrades with

increasing with increasing m_E, N_E, ρ_E and β_2. We also observed that the proposed CRN's data security capability increases when ρ increases from 0 to 1.

Chapter 7

Conclusions and Future Scope

Information security has become a key concern in underlay CRNs because the broadcast nature of wireless channels allows eavesdroppers to intercept their transmission. Traditionally, cryptographic protocols have been designed and implemented to give security in the upper layer of the protocols stack, based upon the assumption that the physical layer link is error-free. In the wireless scenario, the distribution and management of secret keys may be challenging and vulnerable to attacks. Hence, several research efforts are have been put toward the analysis of PLS, which utilizes the properties of the wireless channel to provide secure data transmission. The different diversity techniques can be utilized to improve the PLS against eavesdropping attacks. This thesis aimed to examine the challenges to PLS in the underlay CRNs over fading channel model with different diversity combining schemes. Following are the summary and contributions of our thesis.

- In chapter 3, we investigated the PLS of an underlay CRN in a perfect CSI scenario in the presence of multiple PRs under peak interference power constraint. The GSC scheme that bridges the gap between SC and MRC scheme is adopted at Bob, and the MRC scheme (i.e., worst-case scenario) is adopted in Eve. For multi-antenna Alice, depending upon whether global CSI of main and Eve's channels is available at Alice, we have proposed OAS and SAS scheme and concluded that the OAS scheme performs better than the SAS scheme. We have derived closed-form expression for exact and asymptotic SOP and intercept probability in the Rayleigh fading environment. We have been found that the proposed network's secrecy performance degrades with increasing primary receivers, Eve's antenna, N_E, and eavesdropper channel's SNR. However, the secrecy performance increases with the increasing number of transmitting antennas, N_A, receiving antenna, N_B

at Bob, SNR of the main channel, and σ. We also compared the performance of the SOP and intercept probability and found that intercept probability outperforms the SOP.

- In chapter 4, the PLS of underlay CRN with outdated CSI has been investigated. We have considered two practical scenarios: passive eavesdropping and active eavesdropping. For the passive eavesdropping scenario, we have measured the secrecy in terms of SOP, intercept probability, and ε- outage secrecy capacity. We have taken average secrecy capacity as a leading performance metric for an active eavesdropping scenario since Alice readjusts its transmission rate based on the global CSI to attain perfect secrecy. We have studied the impact of ρ_B, ρ_E and ρ_R on network security capability and found that the PLS of the proposed network improves as ρ_B increases from 0 to 1. As expected at $\rho_B = 1$, i.e., perfect CSI of the main channel, maximum secrecy is achieved. However, the secrecy performance of the network decreases as ρ_E increases from 0 to 1. Furthermore, the secrecy performance of the network degrades with increasing ρ_R. We compared the secrecy performances of either SC or MRC schemes at the legitimate receiver, Bob, and affirmed that MRC performs better than the SC scheme.

- In chapter 5, the PLS of an underlay CRN is investigated under peak interference power constraint and PU outdated CSI constraint when the primary transmitter, PT, lies in the proximity of the secondary receivers. We have also examined the consequences of the primary interference on secrecy performance in the Rayleigh fading channel with limited and unlimited Alice power adaptation schemes. We derived closed-form expressions for different performance metrics in both active and passive eavesdropping scenarios. We have examined the impact of imperfect CSI between the Alice-PR channel on secrecy performance. From derived expressions, it has been observed that SOP and intercept probability decreases with increasing P_T, N_A, and β_1. Simultaneously, secrecy performance degrades with increasing primary interference power P_P and distance between Alice and Bob, d_M. We also observed that the proposed CRN's data security capability increases when ρ, ρ_M, N_A, and β_1 increases and decreases when ρ_E increases.

- In chapter 6, we have examined the secrecy performance of an interference-limited CRN for perfect and outdated CSI scenarios with continuous limited and unlimited power adaptation at the Alice over general fading scenario (i.e., the primary network experienced Rayleigh fading and the secondary network experienced Nakagami-m fading). We be-

gan by investigating analytical expressions for SOP, intercept probability, and average secrecy capacity for a perfect CSI scenario in the presence of interference caused by PT. It has been observed from derived expressions that SOP and intercept probability decreases with increasing P_T, m_B, N_B, ρ_B and β_1 and increasing with increasing m_E, N_E, ρ_E and β_2. Simultaneously, these improve with increasing primary interference power, P_P. We, therefore, studied the impact of outdated CSI between the Alice-PR channel on secrecy performance. We also observed that the proposed CRN's data security capability increases when ρ increases from 0 to 1. As expected, the highest secrecy is obtained for $\rho = 1$, which signifies the perfect CSI of the Alice-PR channel. The interference caused by PT has restricted the secrecy performance of CRN.

7.1 Scope of Future Work

This thesis presents the research work of applying different physical layer security techniques for underlay CRNs. However, some shortcomings of the research work in this the thesis has been identified: (1) the cooperative jamming has not been studied for secure communication in the presence of unknown Eves; (2) the correlation between channels and antennas is not considered in this thesis; (3) second-order performance metric can be introduced to analyze the secrecy performance; (4) machine learning algorithm can be introduced to handle resource allocation problems for multiple-antenna systems and 5) a combination of cognitive radio and non-orthogonal multiple access (CR-NOMA) can be considered to enhance spectral efficiency. The extensions of research work carried in this thesis are manifested in the following subsections.

7.1.1 Cooperative Jamming

Cooperative jamming can also hide secret data and decrease the SNR of unknown eavesdroppers. The critical approach of this method is to introduce a cooperative jammer to the system, which can send jamming signals to disturb the unknown eavesdroppers. Hence, the potential extension direction of the work in this thesis will be cooperative jamming-based robust designs with unknown eavesdroppers. Furthermore, a combination of artificial noise and cooperative jamming is also an exciting issue in future work.

7.1.2 Channel and Antenna Correlation

This thesis considered that all channels are independent. However, in a practical scenario, this assumption may not hold since a passive eavesdropper, or active jammer may be placed close to the legitimate receiver to overhear the information as much as possible. This eavesdropper may be the legitimate receiver for another system, but it acts as an eavesdropper for our system. This close may result in the signal received at Bob and Eve experiencing similar fading to some extent. In other words, the main channel and eavesdropper's channel may be correlated with each other with a specific correlation coefficient. In addition, this thesis also assumed that multiple antennas are independent, which is a reasonable assumption when these multiple antennas are placed spatially apart. In practice, due to space constraints, these antennas may be correlated. Thus, the extension direction of the work given in this thesis will be the channel and antenna correlation model with PU's outdated CSI.

7.1.3 Second Order Performance Metric

The performance analysis of the proposed models in the thesis focused mainly on first-order statistics, particularly the SOP and ASC, which have traditionally been the most commonly used security measures for underlay CRN. To fully understand the performance of such systems, we need second-order measures to have insights into the dynamics of such performance. For example, secrecy outage probability provides an idea about the fraction of fading realizations for which the channel can maintain a specific rate. However, it fails to give an idea of the average length for which the channel cannot carry secure communication. Mobility is another dimension where second-order statistics come to play. Hence, the work done in this thesis can be extended by considering second-order performance metrics like the amount of secrecy loss [201], average secrecy outage rate, and average secrecy outage duration [202].

7.1.4 Machine Learning for Multi-antenna System

TAS scheme is a widely employed technique in a multi-antenna system. With the rising application of ML in many different domains, the application interest in the area of TAS problems in wireless communications is also accelerating [203]. We can implement a deep neural network (DNN) scheme [204] for TAS schemes considered in Chapters 3 and 5. DNN performs better than traditional ML schemes and achieves almost the same secrecy rate as the conven-

tional scheme. If there are any dependencies in the data set, the conventional recurrent neural networks (RNNs) can be implemented for TAS. It has short-term memory and cannot handle long-term dependencies in the data set [205].

7.1.5 Cognitive Radio Assisted Non-orthogonal Multiple Access

Traditionally, CR has been marked notably in recognizing its capability to enhance spectrum utilization. The spectrum utilization efficiency of the traditional CRN can be enhanced further by exploiting the application of NOMA [206, 207]. In recent years, NOMA has been proposed and widely conducted due to its characteristics such as higher spectral efficiency, balanced user fairness, and low access latency. Therefore, a combination of CR and NOMA (CR-NOMA) will provide new expansion to our research work.

7.1.6 Physical Layer Security for Vehicle-to-Everything (V2X)

In the last few years, there has been a significant rise in the advancement of intelligent transportation systems (ITS). The primary purpose of ITS is to handle the ever-increasing number of accidents and improve traffic efficiency, road utilization, and safety [208]. Wireless communication is the main driving factor behind ITS, facilitating reliable communication between vehicles,infrastructure, pedestrians, and networks, generally referred to as vehicle-to-everything (V2X) communication. However, V2X may suffer from jamming and eavesdropping attacks due to wireless communication's broadcast nature, adversely affecting ITS [209]. The open research directions for facilitating PLS for V2X are mobility and speed challenges. Due to the high-speed mobility of vehicular equipment, channel modeling issues need to be addressed to analyze the performance of V2X in the PLS aspects. The conventional channel models (such as Rayleigh, Rician, and Nakagami) of stationary communication links do not suit well in estimating different performance metrics, including the secrecy capacity. Recently, other channel models (such as the double Rayleigh, Weibull, and $\kappa - \mu$ shadowed fading) have been theoretically and empirically investigated to give a higher precision for describing the dynamic non-line-of-sight communication links in V2X [210]. However, V2X performance yet requires more in-depth studies.

Appendix A

Mathematical Proofs

This appendix provides the proof of various propositions stated in the different chapters of this thesis.

A.1 Proof of Propositions 3.1 and 3.3

The SOP of the proposed network can be calculated as [62]

$$P_{out} = \underbrace{\int_0^{\frac{\gamma_p}{\gamma_0}} \int_0^{\infty} F_{\gamma_M|Y}(\varepsilon(\gamma_E)) f_{\gamma_E|Y}(\gamma_E) f_Y(y) d\gamma_E dy}_{J_1} + \underbrace{\int_{\frac{\gamma_p}{\gamma_0}}^{\infty} \int_0^{\infty} F_{\gamma_M|Y}(\varepsilon(\gamma_M)) f_{\gamma_E|Y}(\gamma_E) f_Y(y) d\gamma_E dy}_{J_2}. \tag{A.1}$$

The CDF of γ_M with GSC scheme can be written as [211]

$$F_{\gamma_M|Y}(\varepsilon(\gamma_E)) = \binom{N_B}{N_c} \left\{ 1 - e^{\frac{-\varepsilon(\gamma_E)}{\gamma_1}} \sum_{a=0}^{N_B-N_c-1} \frac{1}{a!} \left(\frac{\varepsilon(\gamma_E)}{\gamma_1} \right)^a + \sum_{n=1}^{N_B-N_c} \mathscr{C}_2 \times \left[\mathscr{C}_3^{-1} \left(1 - e^{-\frac{\mathscr{C}_3 \varepsilon(\gamma_E)}{\gamma_1}} \right) - \sum_{m=0}^{N_c-2} \mathscr{C}_4 \left(1 - e^{\frac{-\varepsilon(\gamma_E)}{\gamma_1}} \sum_{a=0}^{m} \frac{1}{a!} \left(\frac{\varepsilon(\gamma_E)}{\gamma_1} \right)^a \right) \right] \right\}. \tag{A.2}$$

The PDF of γ_E with MRC scheme can be written as

$$f_{\gamma_E|Y}(\gamma_E) = \frac{e^{\frac{-\gamma_E}{\gamma_2}} \gamma_E^{N_E-1}}{\gamma_2^{N_E} (N_E-1)!}. \tag{A.3}$$

Let h_{p0} is the channel coefficient of channel between Alice and $p^{\text{th}}(p = 1, 2.....N_P)$ primary receivers. The PDF of $Y = |h_{p0}|^2$ can be written as

$$f_Y(y) = \sum_{p=0}^{N_p} (-1)^{p+1} \binom{N_p}{p} \frac{p}{\Omega_0} e^{\frac{-py}{\Omega_0}}, y > 0. \tag{A.4}$$

For N_P = 1 i.e., for single PR, $f_Y(y)$ reduces to

$$f_Y(y) = \frac{e^{-\frac{y}{\Omega_0}}}{\Omega_0}, \ \ y > 0. \tag{A.5}$$

Let $\gamma_1 = \gamma_0\Omega_1 = \frac{\gamma_p\Omega_1}{\sigma}$ and $\gamma_2 = \gamma_0\Omega_2 = \frac{\gamma_p\Omega_2}{\sigma}$.

For $Y \leq \frac{\gamma_p}{\gamma_0}$, the CDF of γ_M can be expressed as

$$\begin{aligned} F_{\gamma_M|Y}(\varepsilon(\gamma_E)) = \binom{N_B}{N_c} \Bigg[1 - e^{\frac{-x_1}{\gamma_0\Omega_1}} \sum_{a=0}^{N_B-N_c-1} \frac{1}{a!} \left(\frac{\varepsilon(\gamma_E)}{\gamma_0\Omega_1} \right)^a + \sum_{n=1}^{N_B-N_c} \mathscr{C}_2 \Bigg[\mathscr{C}_3^{-1} \\ \left(1 - e^{-\frac{\mathscr{C}_3\varepsilon(\gamma_E)}{\gamma_0\Omega_1}} \right) - \sum_{m=0}^{N_c-2} \mathscr{C}_4 \left(1 - e^{\frac{-\varepsilon(\gamma_E)}{\gamma_0\Omega_1}} \sum_{a=0}^{m} \frac{1}{a!} \left(\frac{\varepsilon(\gamma_E)}{\gamma_0\Omega_1} \right)^a \right) \Bigg] \Bigg]. \end{aligned} \tag{A.6}$$

Similarly, the PDF of γ_E with MRC scheme can be written as

$$f_{\gamma_2|(X=x)}(\gamma_E) = \frac{e^{\frac{-\gamma_E}{\gamma_0\Omega_2}} \gamma_E^{N_E-1}}{(\gamma_0\Omega_2)^{N_E}(N_E-1)!} \tag{A.7}$$

By putting (A.2), (A.3) and (A.4) into (A.1), J_1 can be rewritten as

$$\begin{aligned} J_1 = \int_0^{\frac{\gamma_p}{\gamma_0}} \sum_{p=0}^{N_p-1} \binom{N_p-1}{p} \frac{N_p}{\Omega_0} (-1)^p e^{\frac{-(p+1)}{\Omega_0}} dy \Bigg(\int_0^{\infty} \binom{N_B}{N_c} \Bigg\{ 1 - e^{\frac{-\varepsilon(\gamma_E)}{\gamma_0\Omega_1}} \sum_{a=0}^{N_B-N_c-1} \frac{1}{a!} \\ \left(\frac{\varepsilon(\gamma_E)}{\gamma_0\Omega_1} \right)^a + \sum_{n=1}^{N_B-N_c} \mathscr{C}_2 \Bigg[\mathscr{C}_3^{-1} \Bigg[1 - e^{-\frac{\mathscr{C}_3\varepsilon(\gamma_E)}{\gamma_0\Omega_1}} \Bigg] - \sum_{m=0}^{N_c-2} \mathscr{C}_4 \Bigg(1 - e^{\frac{-\varepsilon(\gamma_E)}{\gamma_0\Omega_1}} \sum_{k=0}^{m} \frac{1}{a!} \\ \left(\frac{\varepsilon(\gamma_E)}{\gamma_0\Omega_1} \right)^a \Bigg) \Bigg] \Bigg\} \Bigg) \left(\frac{e^{\frac{-\gamma_E}{\gamma_0\Omega_2}} \gamma_E^{N_E-1}}{(\gamma_0\Omega_2)^{N_E}(N_E-1)!} \right) d\gamma_E. \end{aligned} \tag{A.8}$$

Using relation $\int_0^{\infty} x^m e^{-bx} dx = \frac{m!}{b^{m+1}}$, and performing some simple analytical manipulation, J_1 can be computed as

$$J_1 = \binom{N_B}{N_c} \left[\left(1 - e^{-\frac{\sigma}{\Omega_0}} \right)^{N_P} \left[1 - \mathscr{B}_1 \sum_{a=0}^{N_c-1} \alpha_1\zeta_1 + \mathscr{B}_2 - \lambda_3 \left(1 - \mathscr{B}_1 \sum_{a=0}^{m} \alpha_1\zeta_1 \right) \right] \right], \tag{A.9}$$

where $\mathscr{B}_1$, $\mathscr{B}_2$, α_1, ζ_1 and λ_3 are already defined in the Chapter 3. For $N_p = 1$, J_1 reduces to

$$J_1 = \binom{N_B}{N_c}\left[\left(1-e^{-\frac{\sigma}{\Omega_0}}\right)\left[1-\mathscr{B}_1\sum_{a=0}^{N_c-1}\alpha_1\zeta_1+\mathscr{B}_2-\lambda_3\left(1-\mathscr{B}_1\sum_{a=0}^{m}\alpha_1\zeta_1\right)\right]\right]. \tag{A.10}$$

(A.10) is corresponding to single PR and single antenna based Alice.

For $Y > \frac{\gamma_p}{\gamma_0}$, the CDF and PDF of γ_M and γ_E can be written as

$$F_{\gamma_M|Y}(\varepsilon(\gamma_E)) = \binom{N_B}{N_c}\left\{1-e^{\frac{-\varepsilon(\gamma_E)y}{\gamma_p\Omega_1}}\sum_{a=0}^{N_c-1}\frac{1}{a!}\left(\frac{\varepsilon(\gamma_E)y}{\gamma_p\Omega_1}\right)^a+\sum_{l=1}^{N_B-N_c}\mathscr{C}_2\left[\mathscr{C}_3^{-1}\left[1-e^{-\frac{y\varepsilon(\gamma_E)}{\gamma_p\Omega_1}}\right]-\sum_{m=0}^{N_c-2}\left(\mathscr{C}_4\left(1-e^{\frac{-y\varepsilon(\gamma_E)}{\gamma_p\Omega_1}}\sum_{a=0}^{m}\frac{1}{a!}\left(\frac{\varepsilon(\gamma_E)y}{\gamma_p\Omega_1}\right)^a\right)\right]\right\}, \tag{A.11}$$

$$f_{\gamma_E|(Y)}(\gamma_E) = \frac{e^{\frac{-\gamma_E y}{\gamma_p\Omega_2}}y^{N_E}(\gamma_E)^{N_E-1}}{(\gamma_p\Omega_2)^{N_E}(N_E-1)!}. \tag{A.12}$$

By substituting (A.11), (A.12) and (A.4) in (A.1) and using $\int_\rho^\infty x^m e^{-\mu x}dx = e^{-\rho\mu}\sum_{p=0}^{m}\frac{m!}{p!}\frac{\rho^p}{\mu^{m-p+1}}$, J_2 can be calculated as

$$J_2 = \binom{N_B}{N_c}\left[\tau_1\left(1-e^{-\frac{p\sigma}{\Omega_0}}\right)\left[1-\beta_1\sum_{a=0}^{N_c-1}\alpha_1\zeta_1+\beta_2-\lambda_3\left(1+\beta_1\sum_{a=0}^{m}\alpha_1\zeta_1\right)\right]+\tau_1 e^{\frac{-p\sigma}{\Omega_0}}\left(1+\lambda_5-\lambda_3\right)-\frac{1}{(N_E-1)!}\sum_{a=0}^{N_c-1}\sum_{z=0}^{a}\sum_{s=0}^{a-z}\frac{\tau_1\zeta_2\alpha_2 p}{\Omega_0}e^{-\left(\frac{(2^{Rs}-1)}{\gamma_1}+\frac{p\sigma}{\Omega_0}\right)}\frac{(\sigma)^q}{\left(\frac{(2^{Rs}-1)}{\sigma\gamma_1}+\frac{(p)}{\Omega_0}\right)^{a-z-s+1}}(1-\lambda_3)-\frac{\lambda_5\tau_1\tau_2 p}{\Omega_0}\frac{e^{-\left(\frac{\mathscr{C}_3(2^{Rs}-1)}{\gamma_1}+\frac{p\sigma}{\Omega_0}\right)}}{\left(\frac{\mathscr{C}_3(2^{Rs}-1)}{\sigma\gamma_1}+\frac{p}{\Omega_0}\right)}\right]. \tag{A.13}$$

For $N_P = 1$, J_2 becomes

$$J_2 = \binom{N_B}{N_c}\left[e^{\frac{-\sigma}{\Omega_0}}-\mathscr{H}_0\sum_{a=0}^{N_c-1}\sum_{r=0}^{a-z}\alpha_2\zeta_2\lambda_4+\lambda_5\left(e^{\frac{-\sigma}{\Omega_0}}-\frac{\lambda_2 e^{-\left(\frac{\mathscr{C}_3(2^{Rs}-1)}{\gamma_1}+\frac{\sigma}{\Omega_0}\right)}}{\left(\frac{\mathscr{C}_3 2^{Rs}}{\sigma\gamma_1}+\frac{1}{\sigma\gamma_2}\right)^{N_E}}\right)-\sum_{l=1}^{N_B-N_c}\lambda_3\left(e^{\frac{-\sigma}{\Omega_0}}-\mathscr{B}_2\sum_{a=0}^{m}\sum_{r=0}^{a-z}\alpha_2\zeta_2\lambda_4\right)\right]. \tag{A.14}$$

Hence, by substituting J_1 given as (A.9) and J_2 given as (A.13) in (A.1), the SOP for multiple primary receivers and single-antenna based Alice can be calculated. In addition, by putting J_1 given as (A.10) and J_2 given as (A.14) in (A.1), the SOP for single primary receivers i.e $N_P = 1$

and single-antenna based Alice can be calculated.

A.2 Proof of Propositions 3.2 and 3.4

For intercept probability $R_s = 0$, this implies $\varepsilon(\gamma_E) = \gamma_E$. The CDF of γ_M can be rewritten as

$$F_{\gamma_M|Y}(\gamma_E) = \frac{N_B!}{(N_B-N_c)!N_c!}\Bigg\{1-e^{\frac{-x}{\gamma_1}}\sum_{a=0}^{N_B-N_c-1}\frac{1}{a!}\left(\frac{\gamma_E}{\gamma_1}\right)^a+\sum_{l=1}^{N_B-N_c}\mathscr{C}_2\times\Bigg[\mathscr{C}_3^{-1}\left[1-e^{-\frac{\mathscr{C}_3\gamma_E}{\gamma_1}}\right]-\sum_{m=0}^{N_c-2}\mathscr{C}_4\left(1-e^{\frac{-\gamma_E}{\gamma_1}}\sum_{k=0}^{m}\frac{1}{a!}\left(\frac{\gamma_E}{\gamma_1}\right)^a\right)\Bigg]\Bigg\}. \tag{A.15}$$

Using (A.15), (A.3) and (A.4) in (A.1), the intercept probability for N_p primary users can be calculated as

$$P_{int_2} = \sum_{p=1}^{N_P}\binom{N_P}{p}(-1)^{p+1}\binom{N_B}{N_c}\Bigg[1-\frac{1}{(N_E-1)!}\sum_{a=0}^{N_c-1}\frac{(a+N_E-1)!}{k!\eta_1^{a+N_E}}+\sum_{l=1}^{N_B-N_c}\frac{\mathscr{C}_2}{\mathscr{C}_3}\left(1-\frac{1}{\eta_2^{N_E}}\right)-\sum_{l=1}^{N_B-N_c}\sum_{m=0}^{N_c-2}\mathscr{C}_2\mathscr{C}_4\left(1-\frac{1}{(N_E-1)!}\sum_{a=0}^{m}\frac{(a+N_E-1)!}{a!\eta_1^{a+N_E}}\right)\Bigg]. \tag{A.16}$$

For $N_P = 1$, (A.16) reduces to (3.16).

A.3 Proof of Propositions 3.3 and 3.6

We calculate the closed for expression for asymptotic SOP in high SNR regime $\gamma_1 \to \infty$. Using Maclaurin series expansion [187], the first order expansion of $F^{\infty}_{\gamma_M|Y}(\varepsilon(\gamma_E))$ can be written as

$$F^{\infty}_{\gamma_M|(Y=y)}(\varepsilon(\gamma_E)) = \frac{1}{(N_c)!N_c^{N_B-N_c}}\left(\frac{\varepsilon(\gamma_E)}{\gamma_1}\right)^{N_B}. \tag{A.17}$$

By utilizing binomial expansion theorem, we have

$$F^{\infty}_{\gamma_M|Y}(\varepsilon(\gamma_E)) = \frac{1}{(N_c)!N_c^{N_B-N_c}}\sum_{q=0}^{N_B}\binom{N_B}{q}\left(\frac{2^{R_s}-1}{\gamma_1}\right)^{N_B-q}\left(\frac{2^{R_s}\gamma_E}{\gamma_1}\right)^q. \tag{A.18}$$

Using (A.18), (A.3) and (A.4) into (A.1), the asymptotic SOP can be given by

$$P^{\infty}_{out} = \kappa_1(\gamma_1)^{-N_B}\tau_1\left[\left(1-e^{\frac{-p\sigma}{\Omega_0}}\right)+e^{\frac{-p\sigma}{\Omega_0}}\sum_{n=0}^{N_B-q}\frac{(N_B-q)!}{n!}\left(\frac{\Omega_0}{p\sigma}\right)^{N_B-n-q}\right]. \tag{A.19}$$

A.4 Proof of Proposition 3.7

The CDF of main channel with SAS scheme can be expressed as [114, eq.20]

$$F^{SAS}_{\gamma_M|Y}(\varepsilon(\gamma_E)) = \left[F_{\gamma_M|Y}(\varepsilon(\gamma_E))\right]^{N_A}. \tag{A.20}$$

By utilizing multinomial theorem [212], we have

$$(X_1+X_2+X_3.....X_l)^{N_A} = \sum_{m_1+m_2+m_3...m_l=N_A} \binom{N_A}{m_1,m_2.....m_l} \prod_{t=1}^{l} X_{t=1}^{m_t} \tag{A.21}$$

Hence, $F^{SAS}_{\gamma_M|Y}(\varepsilon(\gamma_E))$ can be expressed as

$$\begin{aligned} F^{SAS}_{\gamma_M|Y}(\varepsilon(\gamma_E)) = &\binom{N_B}{N_c}^{N_A} \sum_{k_1+k_2+k_3+k_4+k_5=N_A} \binom{N_A}{k_1,k_2,k_3,k_4,k_5} e^{-\frac{(2^{R_S}-1)A}{\gamma_1}} \sum_{j=0}^{N_c-1} \sum_{l=1}^{N_B-1} \sum_{c=0}^{k_3} \\ &\sum_{v=1}^{N_B-N_c} \sum_{m=0}^{N_c-2} \sum_{k=0}^{m} Z_1 Z_2 Z_3 Z_4 x^{b+d} e^{-\frac{2^{R_S}Ax}{\gamma_1}}. \end{aligned} \tag{A.22}$$

By putting (A.22), (A.3) and (A.4) into (A.1), $P^{SAS}_{out_6}$ can be expressed as (3.29).

A.5 Proof of Proposition 5.1

Based on (1), we note that when $Z \leq \left(\frac{I_P}{P_T}\right)$, $\Phi_M = \frac{|h_j|^2 P_T}{N_0+P_P|g_b|^2}$,$\Phi_E = \frac{|s_j|^2 P_T}{N_0+P_P|t|^2}$, and when $Z > \left(\frac{I_P}{P_T}\right)$, $\Phi_M = \frac{|h_j|^2 I_P}{Z\left(N_0+P_P|g_b|^2\right)}$,$\Phi_E = \frac{|s_j|^2 I_P}{Z\left(N_0+P_P|t|^2\right)}$. Hence, the SOP in (11) can be written as [62]

$$\begin{aligned} P_{out} = &\underbrace{\int_0^{\frac{I_p}{P_T}} \int_0^{\infty} F_{\Phi_M|\{Z=z\}}(\varepsilon(y)) f_{\Phi_E|\{Z=z\}}(y) f_Z(z) dy dz}_{\mathscr{J}_1} \\ &+ \underbrace{\int_{\frac{I_p}{P_T}}^{\infty} \int_0^{\infty} F_{\Phi_M|\{Z=z\}}(\varepsilon(y)) f_{\Phi_E|\{Z=z\}}(y) f_Z(z) dy dz}_{\mathscr{J}_2}. \end{aligned} \tag{A.23}$$

Let $\Phi_1 = P_T\beta_1 = \frac{I_P\beta_1}{\sigma}$ and $\Phi_2 = P_T\beta_2 = \frac{I_P\beta_2}{\sigma}$. For $Z \leq \left(\frac{I_P}{P_T}\right)$, the CDF of Φ_M can be written as

$$F_{\Phi_M}(x) = 1 - \frac{\mathscr{Q}_1}{(\varepsilon(y)+\mathscr{Q}_1)} e^{-\frac{\varepsilon(y)}{\Phi_1}}. \tag{A.24}$$

where $\mathscr{Q}_1 = \frac{\beta_1 P_T}{P_p \lambda}$ and $\varepsilon(y) = \tau - 1 + \tau y$. The PDF of Φ_E can be expressed as

$$f_{\Phi_E}(x) = \mathscr{D}_1 \frac{e^{-\frac{y}{\Phi_2}}}{(y+\mathscr{D}_1)^2} + \frac{1}{\eta P_P} \frac{e^{-\frac{y}{\Phi_2}}}{(y+D_1)}. \tag{A.25}$$

where $D_1 = \frac{\beta_2 P_T}{\eta P_p}$. Substituting (A.24), (A.25) and $f_Z(z) = \frac{1}{\Omega_0} e^{-\frac{z}{\Omega_0}}$ into J_1 of (A.23), J_1 can be expressed as

$$\begin{aligned}\mathscr{J}_1 &= \int_0^{\sigma} \int_0^{\infty} \left(1 - \frac{\mathscr{Q}_1}{(\varepsilon(y)+\mathscr{Q}_1)} e^{-\frac{\varepsilon(y)}{\Phi_1}}\right) \left(\frac{\mathscr{D}_1 e^{-\frac{y}{\Phi_2}}}{(y+\mathscr{D}_1)^2} + \frac{1}{\eta P_P} \frac{e^{-\frac{y}{\Phi_2}}}{(y+\mathscr{D}_1)}\right) \frac{1}{\Omega_0} e^{-\frac{z}{\Omega_0}} dy dz \\ &= \int_0^{\sigma} [I_1 + I_2 - I_3 - I_4] \frac{1}{\Omega_0} e^{-\frac{z}{\Omega_0}} dz, \end{aligned} \tag{A.26}$$

where

$$\mathscr{I}_1 = \int_0^{\infty} \mathscr{D}_1 \frac{e^{-\frac{y}{\Phi_2}}}{(y+\mathscr{D}_1)^2} dy, \tag{A.27}$$

$$\mathscr{I}_2 = \int_0^{\infty} \frac{1}{\eta P_P} \frac{e^{-\frac{y}{\Phi_2}}}{(y+\mathscr{D}_1)} dy, \tag{A.28}$$

$$\mathscr{I}_3 = \int_0^{\infty} \frac{\mathscr{Q}_1 e^{-\frac{\varepsilon(y)}{\Phi_1}}}{(\varepsilon(y)+\mathscr{Q}_1)} \mathscr{D}_1 \frac{e^{-\frac{y}{\Phi_2}}}{(y+\mathscr{D}_1)^2} dy, \tag{A.29}$$

$$\mathscr{I}_4 = \int_0^{\infty} \frac{\mathscr{Q}_1 e^{-\frac{\varepsilon(y)}{\Phi_1}}}{(\varepsilon(y)+\mathscr{Q}_1)} \frac{1}{\eta P_P} \frac{e^{-\frac{y}{\Phi_2}}}{(y+\mathscr{D}_1)} dy. \tag{A.30}$$

By utilizing [187, eq. 3.352.4], $\mathscr{I}_1$ and $\mathscr{I}_2$ are further simplified as

$$\mathscr{I}_1 = \frac{1}{\eta P_P} e^{\frac{1}{\eta P_P}} Ei\left(-\frac{1}{\eta P_P}\right) + 1, \tag{A.31}$$

$$\mathscr{I}_2 = -\frac{1}{\eta P_P} e^{\frac{1}{\eta P_P}} Ei\left(-\frac{1}{\eta P_P}\right). \tag{A.32}$$

$\mathscr{I}_3$ can be further simplified as

$$\mathscr{I}_3 = \frac{\mathscr{D}_1 \mathscr{Q}_1 e^{-\frac{(\tau-1)}{\Phi_1}}}{\tau} \int_0^{\infty} \frac{e^{-\alpha_1 y}}{(y+\Theta_1)(y+\mathscr{D}_1)^2} dy, \tag{A.33}$$

where $\alpha_1 = \frac{\tau}{\Phi_1} + \frac{1}{\Phi_2}$ and $\Theta_1 = \frac{\mathscr{Q}_1+\tau-1}{\tau}$.

Applying Partial fraction expansion to decompose (A.33), we have

$$\mathscr{I}_3 = \frac{\mathscr{D}_1\mathscr{Q}_1 e^{-\frac{(\tau-1)}{\Phi_1}}}{\tau}\int_0^\infty \left[\frac{-\mathscr{K}^2 e^{-\alpha_1 y}}{(y+\mathscr{D}_1)} + \frac{\mathscr{K}^2 e^{-\alpha_1 y}}{(y+\Theta_1)} - \frac{\mathscr{K} e^{-\alpha_1 y}}{(y+\mathscr{D}_1)^2}\right] dy, \tag{A.34}$$

where $\mathscr{K} = \frac{1}{(\mathscr{D}_1-\Theta_1)}$. By utilizing [187, eq. 3.3524 , 3.353.4], $\mathscr{I}_3$ can be written as

$$\begin{aligned}\mathscr{I}_3 =& \frac{\mathscr{D}_1\mathscr{Q}_1 e^{-\frac{(\tau-1)}{\Phi_1}}}{\tau}\Bigg[\mathscr{K}^2 e^{\mathscr{D}_1\alpha_1} Ei(-\alpha_1\mathscr{D}_1) - \mathscr{K}^2 e^{\Theta_1\alpha_1} \\ & Ei(-\Theta_1\alpha_1) - \mathscr{K}\left(\alpha_1 e^{\alpha_1 D_1} Ei(-\alpha_1\mathscr{D}_1) + \frac{1}{\mathscr{D}_1}\right)\Bigg].\end{aligned} \tag{A.35}$$

Similarly, $\mathscr{I}_4$ can be calculated as

$$\begin{aligned}\mathscr{I}_4 &= \frac{\mathscr{Q}_1 e^{-\frac{(\tau-1)}{\Phi_1}}}{\eta\tau P_P}\left(\int_0^\infty \frac{K e^{-\alpha_1 y}}{(y+\Theta_1)} - \frac{\mathscr{K} e^{-\alpha_1 y}}{(y+\mathscr{D}_1)}\right) dy \\ &= \frac{\mathscr{Q}_1 e^{-\frac{(\tau-1)}{\Phi_1}}\mathscr{K}}{\eta\tau P_P}\left[-e^{\alpha_1\Theta_1} Ei(-\alpha_1\Theta_1) + e^{\alpha_1\mathscr{D}_1} Ei(-\alpha_1\mathscr{D}_1)\right].\end{aligned} \tag{A.36}$$

For $Z > \left(\frac{I_P}{P_T}\right)$, we have

$$F_{X|\{Z=z\}}(x) = 1 - \frac{\mathscr{Q}_2}{z}\frac{e^{-\frac{\varepsilon(y)z}{\sigma\Phi_1}}}{\left(\varepsilon(y)+\frac{\mathscr{Q}_2}{z}\right)} \tag{A.37}$$

$$f_{Y|\{Z=z\}}(y) = \frac{\mathscr{D}_2}{z}\frac{e^{-\frac{yz}{\sigma\Phi_2}}}{\left(y+\frac{\mathscr{D}_2}{z}\right)^2} + \frac{1}{\eta P_P}\frac{e^{-\frac{yz}{\sigma\Phi_2}}}{\left(y+\frac{\mathscr{D}_2}{z}\right)}, \tag{A.38}$$

where $\mathscr{Q}_2 = \frac{\sigma\Phi_1}{\lambda P_P}$ and $\mathscr{D}_2 = \frac{\sigma\Phi_1}{\eta P_P}$. Substituting (A.37),(A.38) into J_2 of (A.23), $\mathscr{J}_2$ can be expressed as

$$\begin{aligned}\mathscr{J}_2 &= \int_\sigma^\infty\int_0^\infty \left(1 - \frac{\mathscr{Q}_2}{z}\frac{e^{-\frac{\varepsilon(y)z}{\sigma\Phi_1}}}{\left(\varepsilon(y)+\frac{\mathscr{Q}_2}{z}\right)}\right)\left[\frac{\mathscr{D}_2}{z}\frac{e^{-\frac{yz}{\sigma\Phi_2}}}{\left(y+\frac{\mathscr{D}_2}{z}\right)^2} + \frac{1}{\eta P_P}\frac{e^{-\frac{yz}{\sigma\Phi_2}}}{\left(y+\frac{\mathscr{D}_2}{z}\right)}\right]\frac{1}{\Omega_0}e^{-\frac{z}{\Omega_0}} dy dz \\ &= I_5 + I_6 - I_7 - I_8,\end{aligned} \tag{A.39}$$

where

$$\mathscr{I}_5 = \int_\sigma^\infty \int_0^\infty \frac{\mathscr{D}_2}{z\Omega_0} \frac{e^{-\frac{yz}{\sigma\Phi_2}}}{\left(y+\frac{\mathscr{D}_2}{z}\right)^2} e^{-\frac{z}{\Omega_0}} dydz = \left[\frac{1}{\eta P_P} e^{\frac{1}{\eta P_P}} Ei\left(-\frac{1}{\eta P_P}\right)+1\right] e^{-\frac{\sigma}{\Omega_0}} \tag{A.40}$$

$$\mathscr{I}_6 = \int_\sigma^\infty \int_0^\infty \frac{1}{\eta P_P} \frac{e^{-\frac{yz}{\sigma\Phi_2}}}{\left(y+\frac{\mathscr{D}_2}{z}\right)} \frac{1}{\Omega_0} e^{-\frac{z}{\Omega_0}} dydz = -\left[\frac{1}{\eta P_P} e^{\frac{1}{\eta P_P}} Ei\left(-\frac{1}{\eta P_P}\right)\right] e^{-\frac{\sigma}{\Omega_0}}. \tag{A.41}$$

$\mathscr{I}_7$ can be expressed as

$$\begin{aligned}\mathscr{I}_7 &= \int_\sigma^\infty \int_0^\infty \frac{\mathscr{Q}_2 \mathscr{D}_2 e^{-\frac{\varepsilon(y)z}{\sigma\Phi_1}}}{\Omega_0 z\left(\varepsilon(y)+\frac{\mathscr{Q}_2}{z}\right)} \frac{e^{-\frac{yz}{\sigma\Phi_2}}}{\left(y+\frac{\mathscr{D}_2}{z}\right)^2} e^{-\frac{z}{\Omega_0}} dydz \\ &= \iota_1+\iota_2+\iota_3,\end{aligned} \tag{A.42}$$

where ι_1 can be calculated as

$$\begin{aligned}\iota_1 &= \mathscr{E}_1 e^{\mathscr{A}_1} Ei(-\mathscr{A}_1) \int_\sigma^\infty \frac{e^{-\varsigma z}}{(z+\mathscr{B}_1)^2} dz \\ &= \mathscr{E}_1 e^{\mathscr{A}_1} Ei(-\mathscr{A}_1)\left[\frac{e^{-\varsigma\sigma}}{(\sigma+\mathscr{B}_1)} + \varsigma e^{\mathscr{B}_1\varsigma} Ei\left(-\left(\sigma+\mathscr{B}_1\right)\varsigma\right)\right].\end{aligned} \tag{A.43}$$

ι_2 can be expressed as

$$\iota_2 = -\int_\sigma^\infty \frac{\mathscr{E}_1 e^{-\frac{(\tau-1)}{\sigma\phi_1}} e^{(\mathscr{A}_2+z\mathscr{A}_4)} Ei\left(-\mathscr{A}_2-z\mathscr{A}_4\right) e^{-\frac{z}{\Omega_0}}}{\Omega_0(z+\mathscr{B}_1)^2} dz. \tag{A.44}$$

Using Puiseux series for the exponential integral function, we have

$$\begin{aligned}\iota_2 &\approx -\mathscr{E}_1 e^{\mathscr{A}_2} E_0 \int_\sigma^\infty \frac{e^{-(\varsigma-\mathscr{A}_4)z}}{(z+\mathscr{B}_1)^2} dz \\ &= \mathscr{E}_1 e^{\mathscr{A}_2} E_0\left[\frac{e^{-(\varsigma-\mathscr{A}_4)\sigma}}{(\sigma+\mathscr{B}_1} + (\varsigma-\mathscr{A}_4) e^{(\varsigma-\mathscr{A}_4)\mathscr{B}_1} Ei\left[-\left(\varsigma-\mathscr{A}_4\right)\left(\mathscr{B}_1+\sigma\right)\right]\right].\end{aligned} \tag{A.45}$$

By utilizing [187, eq. 3.352], ι_3 can be computed as

$$\begin{aligned}\iota_3 &= -\frac{\mathscr{Q}_2}{\Omega_0(\tau-1)}\left[\mathscr{A}_1 e^{\mathscr{A}_1} Ei(-\mathscr{A}_1)+1\right] \int_\sigma^\infty \frac{e^{-\varsigma z}}{z+\mathscr{B}_1} dz \\ &= -\frac{\mathscr{Q}_2}{\Omega_0(\tau-1)}\left[\mathscr{A}_1 e^{\mathscr{A}_1} Ei(-\mathscr{A}_1)+1\right] e^{\mathscr{B}_1\varsigma} Ei\left(-\varsigma\left(\sigma+\mathscr{B}_1\right)\right).\end{aligned} \tag{A.46}$$

I_8 can be written as

$$I_8 = \int_{\sigma}^{\infty}\int_{0}^{\infty}\left(\frac{\mathscr{K}e^{-\frac{\alpha_1}{\sigma}yz}}{\left(y+\frac{\mathscr{Q}_2+z(1-\tau)}{\tau z}\right)}-\frac{\mathscr{K}e^{-\frac{\alpha_1}{\sigma}yz}}{(y+\frac{\mathscr{D}_2}{z})}\right)\frac{\mathscr{Q}_2 e^{-\frac{(\tau-1)z}{\sigma\Phi_1}}}{z\eta\tau P_P}dydz$$
$$= \frac{\mathscr{Q}_2}{(\tau-1)\eta P_P}\left[E_0 e^{\mathscr{B}_1(\varsigma-\mathscr{A}_4)+\mathscr{A}_2}Ei\left(-(\varsigma-\mathscr{A}_4)\left(\frac{I_P}{P_T}+\mathscr{B}_1\right)\right)-e^{\mathscr{A}_1}Ei(-\mathscr{A}_1)e^{\mathscr{B}_1\varsigma}\right.$$
$$\left.Ei\left(-\varsigma\left(\frac{I_P}{P_T}+\mathscr{B}_1\right)\right)\right] \tag{A.47}$$

To this end, substituting (A.26) and (A.39) into (A.23) and performing some mathematical manipulation, we obtain secrecy outage probability as in (5.11).

A.6 Proof of Proposition 5.2

The asymptotic SOP can be written as

$$P_{out}^{\infty} = \int_0^{\infty} Pr\left(\Phi_M \leq \tau - 1 + \tau\Phi_E\right) f_Z(z)dz$$
$$\approx \int_0^{\infty} Pr\left(\Phi_M \leq \tau\Phi_E\right) f_Z(z)dz \tag{A.48}$$

By substituting (5.14), (A.25) and $f_Z(z)$ in (A.48), and utilising [213, eq.39], the asymptotic SOP of an underlay CRNs with primary interference for single antenna based Alice can be calculated in (5.16).

A.7 Proof of Proposition 5.3

By recalling the definition of the achievable secrecy rate defined in (6.17), we have

$$\bar{C}_{s|Z} = \int_0^{\infty}\int_y^{\infty}\left[\log_2(1+x)-\log_2(1+y)\right] f_{\phi_E|Z}(y)F_{\phi_M|Z}(x)dydx. \tag{A.49}$$

To evaluate the above integral, we adopt the same steps developed in [67]. Applying some mathematical manipulations, the conditional ASC can be represented as follows :

$$\bar{C}_{s|Z} = \frac{1}{\ln(2)}\int_0^{\infty}\frac{F_{\phi_E|Z}(y)}{1+y}\int_y^{\infty}\left[f_{\phi_M|Z}(x)dx\right]dy$$
$$= \frac{1}{\ln(2)}\int_0^{\infty}\frac{F_{\Phi_E|Z}(y)}{1+y}\left[1-F_{\Phi_M|Z}(y)\right]dy. \tag{A.50}$$

By substituting (5.3) and (5.7) in (A.50), we have

$$= \frac{1}{\ln(2)} \int_0^{\infty} \frac{\mathscr{Q} e^{-\frac{y}{\beta_1 P_A}}}{(y+\mathscr{Q})(1+y)} \left[1 - \frac{\mathscr{D} e^{-\frac{y}{\beta_2 P_A}}}{(y+\mathscr{D})}\right] dy. \tag{A.51}$$

Applying partial fraction expansion and utilising [213, eq.39], (A.51) can be written as

$$\bar{C}_{s|Z} = \frac{\mathscr{Q}}{\ln(2)} \left[\frac{1}{1-\mathscr{Q}} \left[U\left(1,1,\frac{1}{\lambda P_P}\right) - U\left(1,1,\frac{1}{\beta_1 P_A}\right)\right] - \mathscr{D}\left[\mathscr{M}_1 U\left(1,1,\mu_1\right) + \mathscr{M}_2 U\left(1,1,\mu_2\right) + \mathscr{M}_3 U\left(1,1,\frac{\mu_3}{P_A}\right)\right]\right], \tag{A.52}$$

where $\mathscr{M}_1 = \frac{1}{(\mathscr{D}-1)(\mathscr{D}-\mathscr{Q})}$, $\mathscr{M}_2 = \frac{1}{(\mathscr{Q}-1)(\mathscr{Q}-\mathscr{D})}$ and $\mathscr{M}_3 = \frac{1}{(\mathscr{Q}-1)(\mathscr{D}-1)}$. Then, the unconditional ASC can be represented as

$$\begin{aligned}
\bar{C}_s &= \int_0^{\infty} C_{s|Z} f_Z(z) dz \\
&= \frac{\mathscr{Q}_1}{\ln(2)} \int_0^{\frac{I_P}{P_T}} \left[\left(\frac{1}{(1-\mathscr{Q}_1)} \left[U\left(1,1,\frac{1}{\lambda P_P}\right) - U\left(1,1,\frac{1}{\beta_1 P_T}\right)\right] - \left[\mathscr{T}_1 U(1,1,\mu_1) + \mathscr{T}_2 U(1,1,\mu_2) + \mathscr{T}_3 U\left(1,1,\frac{\mu_3}{P_A}\right)\right]\right) f_Z(z) dz + \int_{\frac{I_P}{P_T}}^{\infty} \left[\frac{1}{(z-Q_2)} \left[U\left(1,1,\frac{1}{\lambda P_P}\right) - U\left(1,1,\frac{z}{\beta_1 I_P}\right)\right] - \left[\frac{\mathscr{Z}_1 U(1,1,\mu_1)}{(D_2-z)} - \frac{\mathscr{Z}_1 U(1,1,\mu_2)}{(Q_2-z)} + \frac{1}{(Q_2-z)(D_2-z)} U\left(1,1,z\frac{\mu_3}{I_P}\right)\right]\right] f_Z(z) dz \right].
\end{aligned} \tag{A.53}$$

To this end, substituting the PDF of Z into (A.53) and utilizing [187], the desired in (5.28) can be derived after some algebraic manipulations.

A.8 Proof of Proposition 5.4

Before going into the detail analysis of the asymptotic ASC, we first rewrite the conditional CDF of Φ_E as $F_{\Phi_{E||Z}}(y)$=1- $\Delta(y)$, where $\Delta(y) = \frac{\mathscr{D}}{y+\mathscr{D}} e^{-\frac{y}{\beta_2 P_A}}$. Taking this into consideration, the conditional ASC in (A.50) can be re-expressed as

$$\bar{C}_{s|Z}^{\infty} = \frac{1}{ln(2)} \int_0^{\infty} \left[\int_0^x \frac{1-\Delta(y)}{1+y} dy \right] f_{\Phi_M|Z}(x) dx = \xi_1 - \xi_2, \tag{A.54}$$

where

$$\xi_1 = \frac{1}{\ln(2)} \int_0^{\infty} \ln(1+x) f_{\Phi_M|Z}(x) dx \tag{A.55}$$

$$\xi_2 = \frac{1}{\ln(2)} \int_0^{\infty} \int_0^{x} \frac{\Delta(y)}{1+y} f_{\Phi_M|Z}(x) dy dx. \tag{A.56}$$

Next, we drive ξ_1 and ξ_2 in the high SINR region respectively. When $x \to \infty$, we have $\ln(1+x) \approx \ln(x)$[67]. Hence, by substituting PDF of Φ_M and utilizing [187, eq.4.231.5],we have

$$\xi_1 = \frac{\mathscr{Q}}{\ln(2)} \int_0^{\infty} \frac{\ln(x)}{(x+\mathscr{Q})^2} dx = \frac{\ln(\mathscr{Q})}{\ln(2)}. \tag{A.57}$$

Similarly, according to [68, eq.67], ξ_2 can be expressed as

$$\begin{aligned}
\xi_2 &= \frac{\mathscr{D}}{\ln(2)} \int_0^{\infty} \frac{e^{-\frac{x}{\beta P_A}}}{(1+x)(x+\mathscr{D})} dx \\
&= \frac{\mathscr{D}}{(1-\mathscr{D}) ln(2)} \int_0^{\infty} \left(\frac{e^{-\frac{x}{\beta_2 P_A}}}{x+D} - \frac{e^{-\frac{x}{\beta_2 P_A}}}{x+1} \right) dx \\
&= \frac{\mathscr{D}}{(1-\mathscr{D})\ln(2)} \left[U\left(1,1,\frac{1}{\eta P_P}\right) - U\left(1,1,\frac{1}{\beta_2 P_A}\right) \right].
\end{aligned} \tag{A.58}$$

By substituting (A.57) and (A.58) into (A.54), conditional ASC can be written as

$$\bar{C}^{\infty}_{s|Z} = \frac{1}{\ln(2)} \left[\ln(\mathscr{Q}) - \frac{\mathscr{D}}{(1-\mathscr{D})} \left(U\left(1,1,\frac{1}{\eta P_P}\right) - U\left(1,1,\frac{1}{\beta_2 P_A}\right) \right) \right]. \tag{A.59}$$

Then, the unconditional asymptotic ASC can be written as

$$\begin{aligned}
\bar{C}^{\infty}_{s} &= \int_0^{\infty} C^{\infty}_{s|Z} f_Z(z) dz \\
&= \frac{1}{\ln(2)} \left[\int_0^{\frac{I_P}{P_T}} \left[\ln(\mathscr{Q}_1) - \frac{\mathscr{D}_1}{(1-\mathscr{D}_1)} \left(U\left(1,1,\frac{1}{\eta P_P}\right) - U\left(1,1,\frac{1}{\beta_2 P_T}\right) \right) \right] f_Z(z) dz \right. \\
&\left. + \int_{\frac{I_P}{P_T}}^{\infty} \left[\log_2\left(\frac{Q_2}{z}\right) - \frac{D_2}{(z-D_2)} \left(U\left(1,1,\frac{1}{\eta P_P}\right) - U\left(1,1,\frac{z}{\beta_2 I_P}\right) \right) \right] f_Z(z) dz \right].
\end{aligned} \tag{A.60}$$

By using [187] and performing some simple mathematical manipulations, the closed-form expression for asymptotic ASC can be derived as (5.30).

References

[1] J. Mitola, "Cognitive radio. an integrated agent architecture for software defined radio.," 2002.

[2] D. Cabric, S. M. Mishra, and R. W. Brodersen, "Implementation issues in spectrum sensing for cognitive radios," in *Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers, 2004.*, vol. 1, pp. 772–776, Ieee, 2004.

[3] P. Kolodzy and I. Avoidance, "Spectrum policy task force," *Federal Commun. Comm., Washington, DC, Rep. ET Docket*, vol. 40, no. 4, pp. 147–158, 2002.

[4] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE journal on selected areas in communications*, vol. 23, no. 2, pp. 201–220, 2005.

[5] J. Mitola and G. Q. Maguire, "Cognitive radio: making software radios more personal," *IEEE personal communications*, vol. 6, no. 4, pp. 13–18, 1999.

[6] T. A. Weiss and F. K. Jondral, "Spectrum pooling: an innovative strategy for the enhancement of spectrum efficiency," *IEEE communications Magazine*, vol. 42, no. 3, pp. S8–14, 2004.

[7] H. Hui, A. L. Swindlehurst, G. Li, and J. Liang, "Secure relay and jammer selection for physical layer security," *IEEE Signal Processing Letters*, vol. 22, no. 8, pp. 1147–1151, 2015.

[8] X. Zhou, L. Song, and Y. Zhang, *Physical layer security in wireless communications*. Crc Press, 2013.

[9] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "A survey on spectrum management in cognitive radio networks," *IEEE Communications magazine*, vol. 46, no. 4, pp. 40–48, 2008.

[10] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Physical communication*, vol. 4, no. 1, pp. 40–62, 2011.

[11] J. Mitola, "Cognitive radio architecture," in *Cooperation in wireless networks: Principles and applications*, pp. 243–311, Springer, 2006.

[12] B. Wang and K. R. Liu, "Advances in cognitive radio networks: A survey," *IEEE Journal of selected topics in signal processing*, vol. 5, no. 1, pp. 5–23, 2010.

[13] F. K. Jondral, "Software-defined radio−basics and evolution to cognitive radio," *EURASIP journal on wireless communications and networking*, vol. 2005, no. 3, pp. 1–9, 2005.

[14] Q. Zaho and B. Sadler, "A survey of dynamic spectrum access: Signal processing, networking and regulatory policy," *IEEE Signal Processing Magazine*, vol. 55, no. 5, pp. 2294–2309, 2007.

[15] L. Sibomana, *Performance analysis of cognitive radio networks under spectrum sharing and security constraints*. Blekinge Tekniska Högskola, 2016.

[16] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrum gridlock with cognitive radios: An information theoretic perspective," *Proceedings of the IEEE*, vol. 97, no. 5, pp. 894–914, 2009.

[17] J. M. Peha, "Approaches to spectrum sharing," *IEEE Communications magazine*, vol. 43, no. 2, pp. 10–12, 2005.

[18] M. Matinmikko, H. Okkonen, M. Palola, S. Yrjola, P. Ahokangas, and M. Mustonen, "Spectrum sharing using licensed shared access: the concept and its workflow for lte-advanced networks," *IEEE Wireless Communications*, vol. 21, no. 2, pp. 72–79, 2014.

[19] J. Wang, M. Ghosh, and K. Challapali, "Emerging cognitive radio applications: A survey," *IEEE Communications Magazine*, vol. 49, no. 3, pp. 74–81, 2011.

[20] M. Mishra and D. Vidyarthi, "Spectrum handoff in cognitive radio cellular network: A review," in *2019 8th International Conference System Modeling and Advancement in Research Trends (SMART)*, pp. 210–215, 2019.

[21] L. Huang, G. Zhu, and X. Du, "Cognitive femtocell networks: an opportunistic spectrum access for future indoor wireless coverage," *IEEE wireless communications*, vol. 20, no. 2, pp. 44–51, 2013.

[22] N. Bouabdallah, B. Ishibashi, and R. Boutaba, "Performance of cognitive radio-based wireless mesh networks," *IEEE Transactions on Mobile Computing*, vol. 10, no. 1, pp. 122–135, 2011.

[23] H. Tang and S. Watson, "Cognitive radio networks for tactical wireless communications," tech. rep., Defence Research and Development Canada-Ottawa Research Centre Ottawa . . . , 2014.

[24] T. J. Willink, "Sdr and cognitive radio for military applications," *Emerging Wireless Technologies, Educational Notes RTO-EN-IST-070*, pp. 8–1, 2007.

[25] A. Gorcin and H. Arslan, "Public safety and emergency case communications: Opportunities from the aspect of cognitive radio," in *2008 3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks*, pp. 1–10, 2008.

[26] S. K. Jayaweera, G. Vazquez-Vilar, and C. Mosquera, "Dynamic spectrum leasing: A new paradigm for spectrum sharing in cognitive radio networks," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 5, pp. 2328–2339, 2010.

[27] A. Ghasemi and E. S. Sousa, "Fundamental limits of spectrum-sharing in fading environments," *IEEE Transactions on Wireless Communications*, vol. 6, no. 2, pp. 649–658, 2007.

[28] R. Zhang, "On peak versus average interference power constraints for protecting primary users in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 4, pp. 2112–2120, 2009.

[29] M. Gastpar, "On capacity under receive and spatial spectrum-sharing constraints," *IEEE Transactions on Information Theory*, vol. 53, no. 2, pp. 471–487, 2007.

[30] X. Kang, R. Zhang, Y.-C. Liang, and H. K. Garg, "Optimal power allocation strategies for fading cognitive radio channels with primary user outage constraint," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 2, pp. 374–383, 2011.

[31] L. Sibomana and H.-J. Zepernick, "Ergodic capacity of multiuser scheduling in cognitive radio networks: analysis and comparison," *Wireless Communications and Mobile Computing*, vol. 16, no. 16, pp. 2759–2774, 2016.

[32] H. Kim, H. Wang, S. Lim, and D. Hong, "On the impact of outdated channel information on the capacity of secondary user in spectrum sharing environments," *IEEE Transactions on Wireless Communications*, vol. 11, no. 1, pp. 284–295, 2011.

[33] P. J. Smith, P. A. Dmochowski, H. A. Suraweera, and M. Shafi, "The effects of limited channel knowledge on cognitive radio system capacity," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 2, pp. 927–933, 2012.

[34] S. A. Jafar and A. Goldsmith, "On optimality of beamforming for multiple antenna systems with imperfect feedback," in *Proceedings. 2001 IEEE International Symposium on Information Theory (IEEE Cat. No. 01CH37252)*, p. 321, IEEE, 2001.

[35] Y.-W. P. Hong, W.-J. Huang, and C.-C. J. Kuo, *Cooperative communications and networking: technologies and system design*. Springer Science & Business Media, 2010.

[36] S. Sanayei and A. Nosratinia, "Antenna selection in mimo systems," *IEEE Communications magazine*, vol. 42, no. 10, pp. 68–73, 2004.

[37] S. Sanayei and A. Nosratinia, "Asymptotic capacity analysis of transmit antenna selection," in *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.*, p. 241, IEEE, 2004.

[38] D. G. Brennan, "Linear diversity combining techniques," *Proceedings of the IRE*, vol. 47, no. 6, pp. 1075–1102, 1959.

[39] M. K. Simon and M.-S. Alouini, *Digital communication over fading channels*, vol. 95. John Wiley & Sons, 2005.

[40] D. Brennan, "Linear diversity combining techniques," *Proceedings of the IEEE*, vol. 91, no. 2, pp. 331–356, 2003.

[41] M.-S. Alouini and M. K. Simon, "An mgf-based performance analysis of generalized selection combining over rayleigh fading channels," *IEEE Transactions on Communications*, vol. 48, no. 3, pp. 401–415, 2000.

[42] R. F. Schaefer and H. Boche, "Physical layer service integration in wireless networks: Signal processing challenges," *IEEE Signal Processing Magazine*, vol. 31, no. 3, pp. 147–156, 2014.

[43] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE wireless Communications*, vol. 18, no. 2, pp. 66–74, 2011.

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

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

[46] R. Liu and W. Trappe, *Securing wireless communications at the physical layer*, vol. 7. Springer, 2010.

[47] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE transactions on information theory*, vol. 24, no. 4, pp. 451–456, 1978.

[48] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4687–4698, 2008.

[49] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE transactions on information theory*, vol. 24, no. 3, pp. 339–348, 1978.

[50] X. He and A. Yener, "Strong secrecy and reliable byzantine detection in the presence of an untrusted relay," *IEEE transactions on information theory*, vol. 59, no. 1, pp. 177–192, 2012.

[51] A. Yener and S. Ulukus, "Wireless physical-layer security: Lessons learned from information theory," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1814–1825, 2015.

[52] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2470–2492, 2008.

[53] J. Zhu, "Performance of physical layer security under correlated fading wire-tap channel," 2014.

[54] M. N. Wegman and J. L. Carter, "New hash functions and their use in authentication and set equality," *Journal of computer and system sciences*, vol. 22, no. 3, pp. 265–279, 1981.

[55] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 351–368, Springer, 2000.

[56] H.-P. Shiang and M. van der Schaar, "Distributed resource management in multihop cognitive radio networks for delay-sensitive transmission," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 2, pp. 941–953, 2009.

[57] M. Shokair, W. Saad, and S. M. Ibraheem, "Statistical analysis of a class of secure relay assisted cognitive radio networks," *China Communications*, vol. 15, no. 12, pp. 174–189, 2018.

[58] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, *Physical Layer Security*, pp. 117–141. 2017.

[59] M. Bloch and J. Barros, *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.

[60] D. W. K. Ng, T. Q. Duong, C. Zhong, and R. Schober, *Physical Layer Security in SWIPT Systems with Nonlinear Energy Harvesting Circuits*, pp. 197–216. 2019.

[61] F. Oggier and B. Hassibi, "The secrecy capacity of the mimo wiretap channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961–4972, 2011.

[62] M. Elkashlan, L. Wang, T. Q. Duong, G. K. Karagiannidis, and A. Nallanathan, "On the security of cognitive radio networks," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 8, pp. 3790–3795, 2014.

[63] J. Barros and M. R. Rodrigues, "Secrecy capacity of wireless channels," in *2006 IEEE international symposium on information theory*, pp. 356–360, IEEE, 2006.

[64] Y. O. Basciftci, O. Gungor, C. E. Koksal, and F. Ozguner, "On the secrecy capacity of block fading channels with a hybrid adversary," *IEEE Transactions on Information Theory*, vol. 61, no. 3, pp. 1325–1343, 2014.

[65] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1027–1053, 2016.

[66] B. Wang, P. Mu, and Z. Li, "Secrecy rate maximization with artificial-noise-aided beamforming for miso wiretap channels under secrecy outage constraint," *IEEE Communications Letters*, vol. 19, no. 1, pp. 18–21, 2014.

[67] Y. Huang, F. S. Al-Qahtani, T. Q. Duong, and J. Wang, "Secure transmission in mimo wiretap channels using general-order transmit antenna selection with outdated csi," *IEEE Transactions on Communications*, vol. 63, no. 8, pp. 2959–2971, 2015.

[68] L. Wang, M. Elkashlan, J. Huang, R. Schober, and R. K. Mallik, "Secure transmission with antenna selection in mimo nakagami-*m* fading channels," *IEEE Transactions on Wireless Communications*, vol. 13, no. 11, pp. 6054–6067, 2014.

[69] A. Singh, M. R. Bhatnagar, and R. K. Mallik, "Physical layer security of a multiantenna-based cr network with single and multiple primary users," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 12, pp. 11011–11022, 2017.

[70] S.-I. Chu, "Secrecy performance analysis of af relaying with relay selection scheme over nakagami-m fading channels," *International Journal of Communication Systems*, vol. 31, no. 14, p. e3738, 2018.

[71] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober, and I. B. Collings, "Transmit antenna selection for security enhancement in mimo wiretap channels," *IEEE transactions on communications*, vol. 61, no. 1, pp. 144–154, 2012.

[72] V. U. Prabhu and M. R. Rodrigues, "On wireless channels with *m*-antenna eavesdroppers: Characterization of the outage probability and ε-outage secrecy capacity," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 853–860, 2011.

[73] P. Wang, G. Yu, and Z. Zhang, "On the secrecy capacity of fading wireless channel with multiple eavesdroppers," in *2007 IEEE International Symposium on Information Theory*, pp. 1301–1305, IEEE, 2007.

[74] W. Trappe, "The challenges facing physical layer security," *IEEE communications magazine*, vol. 53, no. 6, pp. 16–20, 2015.

[75] M. Ghamari Adian and H. Aghaeinia, "Joint transmit beamforming and antenna selection in cognitive radio networks," in *2010 5th International Symposium on Telecommunications*, pp. 33–37, 2010.

[76] S.-H. Lai, P.-H. Lin, S.-C. Lin, and H.-J. Su, "On optimal artificial-noise assisted secure beamforming for the fading eavesdropper channel," in *2011 IEEE 22nd International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 1167–1171, IEEE, 2011.

[77] C. Jeong, I.-M. Kim, and D. I. Kim, "Joint secure beamforming design at the source and the relay for an amplify-and-forward mimo untrusted relay system," *IEEE Transactions on Signal Processing*, vol. 60, no. 1, pp. 310–325, 2011.

[78] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Communications Surveys Tutorials*, vol. 19, no. 2, pp. 1027–1053, 2017.

[79] J. Mo, M. Tao, Y. Liu, B. Xia, and X. Ma, "Secure beamforming for mimo two-way transmission with an untrusted relay," in *2013 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 4180–4185, IEEE, 2013.

[80] Y. Yang, Q. Li, W.-K. Ma, J. Ge, and P. Ching, "Cooperative secure beamforming for af relay networks with multiple eavesdroppers," *IEEE Signal Processing Letters*, vol. 20, no. 1, pp. 35–38, 2012.

[81] J. Huang and A. L. Swindlehurst, "Secure communications via cooperative jamming in two-hop relay systems," in *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, pp. 1–5, IEEE, 2010.

[82] M. Sharif and B. Hassibi, "On the capacity of mimo broadcast channels with partial side information," *IEEE Transactions on information Theory*, vol. 51, no. 2, pp. 506–522, 2005.

[83] B. He, X. Zhou, and T. D. Abhayapala, "Wireless physical layer security with imperfect channel state information: A survey," *arXiv preprint arXiv:1307.4146*, 2013.

[84] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas?part ii: The mimome wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, 2010.

[85] S. A. A. Fakoorian and A. L. Swindlehurst, "Full rank solutions for the mimo gaussian wiretap channel with an average power constraint," *IEEE Transactions on Signal Processing*, vol. 61, no. 10, pp. 2620–2631, 2013.

[86] Q. Li, M. Hong, H.-T. Wai, Y.-F. Liu, W.-K. Ma, and Z.-Q. Luo, "Transmit solutions for mimo wiretap channels using alternating optimization," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1714–1727, 2013.

[87] K. Cumanan, Z. Ding, B. Sharif, G. Y. Tian, and K. K. Leung, "Secrecy rate optimizations for a mimo secrecy channel with a multiple-antenna eavesdropper," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 4, pp. 1678–1690, 2013.

[88] Y. Wu, C. Xiao, Z. Ding, X. Gao, and S. Jin, "Linear precoding for finite-alphabet signaling over mimome wiretap channels," *IEEE transactions on vehicular technology*, vol. 61, no. 6, pp. 2599–2612, 2012.

[89] Z. Rezki and M.-S. Alouini, "Secure diversity-multiplexing tradeoff of zero-forcing transmit scheme at finite-snr," *IEEE transactions on communications*, vol. 60, no. 4, pp. 1138–1147, 2012.

[90] Z. Chu, K. Cumanan, Z. Ding, M. Johnston, and S. Le Goff, "Robust outage secrecy rate optimizations for a mimo secrecy channel," *IEEE Wireless Communications Letters*, vol. 4, no. 1, pp. 86–89, 2014.

[91] Q. Li and W.-K. Ma, "Optimal and robust transmit designs for miso channel secrecy by semidefinite programming," *IEEE Transactions on Signal Processing*, vol. 59, no. 8, pp. 3799–3812, 2011.

[92] S. Bashar, Z. Ding, and G. Y. Li, "On secrecy of codebook-based transmission beamforming under receiver limited feedback," *IEEE transactions on wireless communications*, vol. 10, no. 4, pp. 1212–1223, 2011.

[93] X. Zhou and M. R. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 8, pp. 3831–3842, 2010.

[94] X. Zhang, X. Zhou, M. R. McKay, and R. W. Heath, "Artificial-noise-aided secure multi-antenna transmission in slow fading channels with limited feedback," in *2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 3968–3972, IEEE, 2014.

[95] Y. Yang, W. Wang, H. Zhao, and L. Zhao, "Transmitter beamforming and artificial noise with delayed feedback: Secrecy rate and power allocation," *Journal of Communications and Networks*, vol. 14, no. 4, pp. 374–384, 2012.

[96] D. J. Love, R. W. Heath, V. K. Lau, D. Gesbert, B. D. Rao, and M. Andrews, "An overview of limited feedback in wireless communication systems," *IEEE Journal on selected areas in Communications*, vol. 26, no. 8, pp. 1341–1365, 2008.

[97] P. Xia and G. B. Giannakis, "Design and analysis of transmit-beamforming based on limited-rate feedback," *IEEE Transactions on Signal Processing*, vol. 54, no. 5, pp. 1853–1863, 2006.

[98] U. Salim and D. Slock, "How much feedback is required for tdd multi-antenna broadcast channels with user selection?," *EURASIP Journal on Advances in Signal Processing*, vol. 2010, pp. 1–14, 2010.

[99] T. T. Kim and H. V. Poor, "Secure communications with insecure feedback: Breaking the high-snr ceiling," *IEEE Transactions on Information Theory*, vol. 56, no. 8, pp. 3700–3711, 2010.

[100] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE transactions on wireless communications*, vol. 7, no. 6, pp. 2180–2189, 2008.

[101] Q. Li and W.-K. Ma, "Spatially selective artificial-noise aided transmit optimization for miso multi-eves secrecy rate maximization," *IEEE Transactions on Signal Processing*, vol. 61, no. 10, pp. 2704–2717, 2013.

[102] N. Yang, S. Yan, J. Yuan, R. Malaney, R. Subramanian, and I. Land, "Artificial noise: Transmission optimization in multi-input single-output wiretap channels," *IEEE Transactions on Communications*, vol. 63, no. 5, pp. 1771–1783, 2015.

[103] Y. Tang, J. Xiong, D. Ma, and X. Zhang, "Robust artificial noise aided transmit design for miso wiretap channels with channel uncertainty," *IEEE communications letters*, vol. 17, no. 11, pp. 2096–2099, 2013.

[104] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Communications Letters*, vol. 16, no. 10, pp. 1628–1631, 2012.

[105] T. Gucluoglu and T. M. Duman, "Performance analysis of transmit and receive antenna selection over flat fading channels," *IEEE Transactions on Wireless Communications*, vol. 7, no. 8, pp. 3056–3065, 2008.

[106] H. Alves, R. D. Souza, M. Debbah, and M. Bennis, "Performance of transmit antenna selection physical layer security schemes," *IEEE Signal Processing Letters*, vol. 19, no. 6, pp. 372–375, 2012.

[107] N. Yang, H. A. Suraweera, I. B. Collings, and C. Yuen, "Physical layer security of tas/mrc with antenna correlation," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 254–259, 2012.

[108] N. S. Ferdinand, D. B. da Costa, A. L. de Almeida, and M. Latva-aho, "Physical layer secrecy performance of tas wiretap channels with correlated main and eavesdropper channels," *IEEE Wireless Communications Letters*, vol. 3, no. 1, pp. 86–89, 2013.

[109] M. Hanif, H.-C. Yang, and M.-S. Alouini, "Transmit antenna selection for power adaptive underlay cognitive radio with instantaneous interference constraint," *IEEE Transactions on Communications*, vol. 65, no. 6, pp. 2357–2367, 2017.

[110] J. Zhu, Y. Zou, G. Wang, Y.-D. Yao, and G. K. Karagiannidis, "On secrecy performance of antenna-selection-aided mimo systems against eavesdropping," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 1, pp. 214–225, 2015.

[111] J. Xiong, Y. Tang, D. Ma, P. Xiao, and K.-K. Wong, "Secrecy performance analysis for tas-mrc system with imperfect feedback," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 8, pp. 1617–1629, 2015.

[112] M. Hanif, H.-C. Yang, and M.-S. Alouini, "Transmit antenna selection for underlay cognitive radio with instantaneous interference constraint," in *2015 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–5, IEEE, 2015.

[113] V. Blagojevic and P. Ivanis, "Ergodic capacity for tas/mrc spectrum sharing cognitive radio," *IEEE Communications Letters*, vol. 16, no. 3, pp. 321–323, 2012.

[114] H. Lei, C. Gao, I. S. Ansari, Y. Guo, Y. Zou, G. Pan, and K. A. Qaraqe, "Secrecy outage performance of transmit antenna selection for mimo underlay cognitive radio systems over nakagami-*m* channels," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2237–2250, 2016.

[115] N. Sadeque, I. Land, and R. Subramanian, "Average secrecy rate under transmit antenna selection for the multiple-antenna wiretap channel," in *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 238–242, IEEE, 2013.

[116] H. Zhang, A. F. Molisch, and J. Zhang, "Applying antenna selection in wlans for achieving broadband multimedia communications," *IEEE Transactions on Broadcasting*, vol. 52, no. 4, pp. 475–482, 2006.

[117] Q. Li, X. E. Lin, J. Zhang, and W. Roh, "Advancement of mimo technology in wimax: from ieee 802.16 d/e/j to 802.16 m," *IEEE Communications Magazine*, vol. 47, no. 6, pp. 100–107, 2009.

[118] M. Hanif, H.-C. Yang, and M.-S. Alouini, "Receive antenna selection for underlay cognitive radio with instantaneous interference constraint," *IEEE Signal Processing Letters*, vol. 22, no. 6, pp. 738–742, 2014.

[119] F. He, H. Man, and W. Wang, "Maximal ratio diversity combining enhanced security," *IEEE Communications Letters*, vol. 15, no. 5, pp. 509–511, 2011.

[120] J. Si, Z. Li, J. Cheng, and C. Zhong, "Secrecy performance of multi-antenna wiretap channels with diversity combining over correlated rayleigh fading channels," *IEEE Transactions on Wireless Communications*, vol. 18, no. 1, pp. 444–458, 2018.

[121] J. Si, Z. Li, J. Cheng, and C. Zhong, "Asymptotic secrecy outage performance for tas/mrc over correlated nakagami-*m* fading channels," *IEEE Transactions on Communications*, vol. 67, no. 11, pp. 7700–7714, 2019.

[122] M. Z. I. Sarkar and T. Ratnarajah, "Enhancing security in correlated channel with maximal ratio combining diversity," *IEEE transactions on signal processing*, vol. 60, no. 12, pp. 6745–6751, 2012.

[123] K. Chopra, R. Bose, and A. Joshi, "Secrecy outage performance of cognitive radio network with selection combining at eavesdropper," *Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science)*, vol. 13, no. 5, pp. 987–998, 2020.

[124] L. Chen, Y. Yang, and G. Wei, "Physical layer security enhancement with generalized selection diversity combining," in *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp. 518–521, IEEE, 2013.

[125] Y. Deng, L. Wang, M. Elkashlan, K. J. Kim, and T. Q. Duong, "Generalized selection combining for cognitive relay networks over nakagami-*m* fading," *IEEE Transactions on Signal Processing*, vol. 63, no. 8, pp. 1993–2006, 2015.

[126] K. R. Liu, A. K. Sadek, W. Su, and A. Kwasinski, *Cooperative communications and networking*. Cambridge university press, 2009.

[127] J. N. Laneman, D. N. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Transactions on Information theory*, vol. 50, no. 12, pp. 3062–3080, 2004.

[128] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "On the application of cooperative transmission to secrecy communications," *IEEE journal on selected areas in communications*, vol. 30, no. 2, pp. 359–368, 2012.

[129] S. Jin, M. R. McKay, C. Zhong, and K.-K. Wong, "Ergodic capacity analysis of amplify-and-forward mimo dual-hop systems," *IEEE Transactions on Information Theory*, vol. 56, no. 5, pp. 2204–2224, 2010.

[130] S. Jin, X. Liang, K.-K. Wong, X. Gao, and Q. Zhu, "Ergodic rate analysis for multipair massive mimo two-way relay networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 3, pp. 1480–1491, 2014.

[131] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE transactions on signal processing*, vol. 58, no. 3, pp. 1875–1888, 2009.

[132] Z. Ding, K. K. Leung, D. L. Goeckel, and D. Towsley, "Opportunistic relaying for secrecy communications: Cooperative jamming vs. relay chatting," *IEEE Transactions on Wireless Communications*, vol. 10, no. 6, pp. 1725–1729, 2011.

[133] J. Chen, R. Zhang, L. Song, Z. Han, and B. Jiao, "Joint relay and jammer selection for secure two-way relay networks," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 310–320, 2011.

[134] Q. Liu, Z. Zhou, C. Yang, and Y. Ye, "The coverage analysis of cognitive radio network," in *2008 4th International Conference on Wireless Communications, Networking and Mobile Computing*, pp. 1–4, IEEE, 2008.

[135] Y. Zou, B. Champagne, W.-P. Zhu, and L. Hanzo, "Relay-selection improves the security-reliability trade-off in cognitive radio systems," *IEEE Transactions on Communications*, vol. 63, no. 1, pp. 215–228, 2014.

[136] L. Fan, X. Lei, R. Q. Hu, and W. Seah, "Outdated relay selection in two-way relay network," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 8, pp. 4051–4057, 2013.

[137] L. Fan, R. Zhao, F.-K. Gong, N. Yang, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying over correlated fading channels," *IEEE Transactions on Communications*, vol. 65, no. 7, pp. 2811–2820, 2017.

[138] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical-layer security in cooperative wireless networks," *IEEE journal on selected areas in communications*, vol. 31, no. 10, pp. 2099–2111, 2013.

[139] L. Wu, L. Yang, J. Chen, and M.-S. Alouini, "Physical layer security for cooperative relaying over generalized-*k* fading channels," *IEEE Wireless Communications Letters*, vol. 7, no. 4, pp. 606–609, 2018.

[140] H. A. Shah and I. Koo, "Improving physical layer security via cooperative diversity in energy-constrained cognitive radio networks with multiple eavesdroppers," *International Journal of Communication Systems*, vol. 32, no. 14, p. e4008, 2019.

[141] T. W. Ban, W. Choi, B. C. Jung, and D. K. Sung, "Multi-user diversity in a spectrum sharing system," *IEEE Transactions on Wireless Communications*, vol. 8, no. 1, pp. 102–106, 2009.

[142] B. Aghazadeh and M. Torabi, "Performance analysis of a multi-user diversity in a simo spectrum sharing system," in *2016 8th International Symposium on Telecommunications (IST)*, pp. 331–336, IEEE, 2016.

[143] R. Zhang and Y.-C. Liang, "Investigation on multiuser diversity in spectrum sharing based cognitive radio networks," *IEEE Communications Letters*, vol. 14, no. 2, pp. 133–135, 2010.

[144] L. Fan, N. Yang, T. Q. Duong, M. Elkashlan, and G. K. Karagiannidis, "Exploiting direct links for physical layer security in multiuser multirelay networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 3856–3867, 2016.

[145] Y. H. Al-Badarneh, C. N. Georghiades, and M.-S. Alouini, "Asymptotic performance analysis of generalized user selection for interference-limited multiuser secondary networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 5, no. 1, pp. 82–92, 2019.

[146] P. Bender, P. Black, M. Grob, R. Padovani, N. Sindhushyana, and A. Viterbi, "Cdma/hdr: a bandwidth efficient high speed wireless data service for nomadic users," *IEEE Communications magazine*, vol. 38, no. 7, pp. 70–77, 2000.

[147] E. G. Larsson, "On the combination of spatial diversity and multiuser diversity," *IEEE Communications Letters*, vol. 8, no. 8, pp. 517–519, 2004.

[148] F. Capozzi, G. Piro, L. A. Grieco, G. Boggia, and P. Camarda, "Downlink packet scheduling in lte cellular networks: Key design issues and a survey," *IEEE communications surveys & tutorials*, vol. 15, no. 2, pp. 678–700, 2012.

[149] F. A. Khan, T. Ratnarajah, and M. Sellathurai, "Multiuser diversity analysis in spectrum sharing cognitive radio networks," in *2010 Proceedings of the Fifth International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, pp. 1–5, IEEE, 2010.

[150] S. Ekin, F. Yilmaz, H. Celebi, K. A. Qaraqe, M.-S. Alouini, and E. Serpedin, "Capacity limits of spectrum-sharing systems over hyper-fading channels," *Wireless Communications and Mobile Computing*, vol. 12, no. 16, pp. 1471–1480, 2012.

[151] D. Li, "On the capacity of cognitive broadcast channels with opportunistic scheduling," *Wireless Communications and Mobile Computing*, vol. 13, no. 2, pp. 198–203, 2013.

[152] D. Fudenberg and J. Tirole, "Game theory cambridge ma," *MIT press Grossman S. and O. Hart [1983]:?An Analysis of the Principal-Agent Problem? Econometrica*, vol. 51, pp. 7–45, 1991.

[153] T. Basar, "The gaussian test channel with an intelligent jammer," *IEEE Transactions on Information Theory*, vol. 29, no. 1, pp. 152–157, 1983.

[154] A. Mukherjee and A. L. Swindlehurst, "Equilibrium outcomes of dynamic games in mimo channels with active eavesdroppers," in *2010 IEEE International Conference on Communications*, pp. 1–5, IEEE, 2010.

[155] A. Mukherjee and A. L. Swindlehurst, "Optimal strategies for countering dual-threat jamming/eavesdropping-capable adversaries in mimo channels," in *2010-MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE*, pp. 1695–1700, IEEE, 2010.

[156] Z. Han, N. Marina, M. Debbah, and A. Hjorungnes, "Improved wireless secrecy rate using distributed auction theory," in *2009 Fifth International Conference on Mobile Ad-hoc and Sensor Networks*, pp. 442–447, IEEE, 2009.

[157] W. Saad, Z. Han, M. Debbah, and A. Hjorungnes, "A distributed coalition formation framework for fair user cooperation in wireless networks," *IEEE Transactions on wireless communications*, vol. 8, no. 9, pp. 4580–4593, 2009.

[158] A. Houjeij, W. Saad, T. Bas, *et al.*, "A game-theoretic view on the physical layer security of cognitive radio networks," in *2013 IEEE International Conference on Communications (ICC)*, pp. 2095–2099, IEEE, 2013.

[159] D. D. Nguyen, H. X. Nguyen, and L. B. White, "Reinforcement learning with network-assisted feedback for heterogeneous rat selection," *IEEE Transactions on Wireless Communications*, vol. 16, no. 9, pp. 6062–6076, 2017.

[160] F. Zhou, X. Zhang, R. Q. Hu, A. Papathanassiou, and W. Meng, "Resource allocation based on deep neural networks for cognitive radio networks," in *2018 IEEE/CIC International Conference on Communications in China (ICCC)*, pp. 40–45, IEEE, 2018.

[161] H. Ye, G. Y. Li, and B.-H. Juang, "Power of deep learning for channel estimation and signal detection in ofdm systems," *IEEE Wireless Communications Letters*, vol. 7, no. 1, pp. 114–117, 2017.

[162] C. Jiang, H. Zhang, Y. Ren, Z. Han, K.-C. Chen, and L. Hanzo, "Machine learning paradigms for next-generation wireless networks," *IEEE Wireless Communications*, vol. 24, no. 2, pp. 98–105, 2016.

[163] I. Goodfellow, Y. Bengio, and A. Courville, *Deep learning*. MIT press, 2016.

[164] F. Sebastiani, "Machine learning in automated text categorization," *ACM computing surveys (CSUR)*, vol. 34, no. 1, pp. 1–47, 2002.

[165] Y. Anzai, *Pattern recognition and machine learning*. Elsevier, 2012.

[166] C. Andrieu, N. De Freitas, A. Doucet, and M. I. Jordan, "An introduction to mcmc for machine learning," *Machine learning*, vol. 50, no. 1, pp. 5–43, 2003.

[167] M. Chen, U. Challita, W. Saad, C. Yin, and M. Debbah, "Machine learning for wireless networks with artificial intelligence: A tutorial on neural networks," *arXiv preprint arXiv:1710.02913*, vol. 9, 2017.

[168] M. T. Hagan, H. B. Demuth, and M. Beale, *Neural network design*. PWS Publishing Co., 1997.

[169] T. Lin and Y. Zhu, "Beamforming design for large-scale antenna arrays using deep learning," *IEEE Wireless Communications Letters*, vol. 9, no. 1, pp. 103–107, 2019.

[170] H. Huang, Y. Song, J. Yang, G. Gui, and F. Adachi, "Deep-learning-based millimeter-wave massive mimo for hybrid precoding," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 3027–3032, 2019.

[171] C. Huang, G. C. Alexandropoulos, A. Zappone, C. Yuen, and M. Debbah, "Deep learning for ul/dl channel calibration in generic massive mimo systems," in *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, 2019.

[172] M. Zhang, K. Cumanan, L. Ni, H. Hu, A. G. Burr, and Z. Ding, "Robust beamforming for an aided miso swipt system with unknown eavesdroppers and non-linear eh model," in *2018 IEEE Globecom Workshops (GC Wkshps)*, pp. 1–7, IEEE, 2018.

[173] M. Zeng, N.-P. Nguyen, O. A. Dobre, and H. V. Poor, "Securing downlink massive mimo-noma networks with artificial noise," *IEEE Journal of Selected Topics in Signal Processing*, vol. 13, no. 3, pp. 685–699, 2019.

[174] K. Cumanan, H. Xing, P. Xu, G. Zheng, X. Dai, A. Nallanathan, Z. Ding, and G. K. Karagiannidis, "Physical layer security jamming: Theoretical limits and practical designs in wireless networks," *IEEE Access*, vol. 5, pp. 3603–3611, 2016.

[175] K. Cumanan, Z. Ding, M. Xu, and H. V. Poor, "Secrecy rate optimization for secure multicast communications," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 8, pp. 1417–1432, 2016.

[176] H. Sun, X. Chen, Q. Shi, M. Hong, X. Fu, and N. D. Sidiropoulos, "Learning to optimize: Training deep neural networks for wireless resource management," in *2017 IEEE 18th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, pp. 1–6, IEEE, 2017.

[177] C. Huang, G. C. Alexandropoulos, C. Yuen, and M. Debbah, "Indoor signal focusing with deep learning designed reconfigurable intelligent surfaces," in *2019 IEEE 20th interna-*

tional workshop on signal processing advances in wireless communications (SPAWC), pp. 1–5, IEEE, 2019.

[178] C. Huang, R. Mo, and C. Yuen, "Reconfigurable intelligent surface assisted multiuser miso systems exploiting deep reinforcement learning," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 8, pp. 1839–1850, 2020.

[179] H. Sun, X. Chen, Q. Shi, M. Hong, X. Fu, and N. D. Sidiropoulos, "Learning to optimize: Training deep neural networks for interference management," *IEEE Transactions on Signal Processing*, vol. 66, no. 20, pp. 5438–5453, 2018.

[180] H. Ye and G. Y. Li, "Deep reinforcement learning for resource allocation in v2v communications," in *2018 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, 2018.

[181] M. Zhang, K. Cumanan, J. Thiyagalingam, Y. Tang, W. Wang, Z. Ding, and O. A. Dobre, "Exploiting deep learning for secure transmission in an underlay cognitive radio network," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 1, pp. 726–741, 2021.

[182] Y. Chen, Y. Wu, J. Zhang, and N. Chen, "New estimators for primary channel gain in cognitive radio networks," *IEEE Communications Letters*, vol. 22, no. 12, pp. 2435–2438, 2018.

[183] J. Yao, M. Jin, Q. Guo, and Y. Li, "Simultaneous estimation of primary and cross-channel gains for underlay cognitive radios," *IEEE Access*, vol. 6, pp. 29190–29199, 2018.

[184] L. Zhang, G. Zhao, W. Zhou, L. Li, G. Wu, Y.-C. Liang, and S. Li, "Primary channel gain estimation for spectrum sharing in cognitive radio networks," *IEEE transactions on communications*, vol. 65, no. 10, pp. 4152–4162, 2017.

[185] Y. Zou, J. Zhu, X. Wang, and V. C. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Network*, vol. 29, no. 1, pp. 42–48, 2015.

[186] M. Bloch, J. Barros, M. R. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Transactions on Information Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[187] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*. Academic press, 2014.

[188] X. Cai and G. B. Giannakis, "Performance analysis of combined transmit selection diversity and receive generalized selection combining in rayleigh fading channels," *IEEE Transactions on Wireless Communications*, vol. 3, no. 6, pp. 1980–1983, 2004.

[189] Y. Hu and X. Tao, "Secrecy outage on transmit antenna selection with weighting errors at maximal-ratio combiners," *IEEE Communications Letters*, vol. 19, no. 4, pp. 597–600, 2015.

[190] A. P. Shrestha and K. S. Kwak, "On maximal ratio diversity with weighting errors for physical layer security," *IEEE communications letters*, vol. 18, no. 4, pp. 580–583, 2014.

[191] J. Pérez, J. Ibánez, L. Vielva, and I. Santamaria, "Closed-form approximation for the outage capacity of orthogonal stbc," *IEEE Communications Letters*, vol. 9, no. 11, pp. 961–963, 2005.

[192] Y.-c. Yu, L. Hu, H.-t. Li, Y.-m. Zhang, F.-m. Wu, and J.-f. Chu, "The security of physical layer in cognitive radio networks," *J Commun*, vol. 9, no. 12, pp. 28–33, 2014.

[193] L. Musavian and S. Aissa, "Fundamental capacity limits of cognitive radio in fading environments with imperfect channel information," *IEEE Transactions on Communications*, vol. 57, no. 11, pp. 3472–3480, 2009.

[194] X. Kang, H. K. Garg, Y.-C. Liang, and R. Zhang, "Optimal power allocation for ofdm-based cognitive radio with new primary transmission protection criteria," *IEEE Transactions on Wireless Communications*, vol. 9, no. 6, pp. 2066–2075, 2010.

[195] A. B. O. Daalhuis, "Confluent hypergeometric functions.," 2010.

[196] Y. Zou, X. Wang, and W. Shen, "Intercept probability analysis of cooperative wireless networks with best relay selection in the presence of eavesdropping attack," in *2013 IEEE international conference on communications (ICC)*, pp. 2183–2187, IEEE, 2013.

[197] C. Tang, G. Pan, and T. Li, "Secrecy outage analysis of underlay cognitive radio unit over nakagami-*m* fading channels," *IEEE Wireless Communications Letters*, vol. 3, no. 6, pp. 609–612, 2014.

[198] H. A. David and H. N. Nagaraja, *Order statistics*. John Wiley & Sons, 2004.

[199] H. Buchholz, *The confluent hypergeometric function: with special emphasis on its applications*, vol. 15. Springer Science & Business Media, 2013.

[200] Y. H. Al-Badarneh, C. N. Georghiades, R. M. Radaydeh, and M.-S. Alouini, "On the secrecy performance of generalized user selection for interference-limited multiuser wireless networks," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 12, pp. 12442–12446, 2018.

[201] S. Li, L. Yang, M. O. Hasna, M.-S. Alouini, and J. Zhang, "Amount of secrecy loss: A novel metric for physical layer security analysis," *IEEE Communications Letters*, vol. 24, no. 8, pp. 1626–1630, 2020.

[202] A. Omri and M. O. Hasna, "Average secrecy outage rate and average secrecy outage duration of wireless communication systems with diversity over nakagami-m fading channels," *IEEE Transactions on Wireless Communications*, vol. 17, no. 6, pp. 3822–3833, 2018.

[203] R. Yao, Y. Zhang, N. Qi, T. A. Tsiftsis, and Y. Liu, "Machine learning-based antenna selection in untrusted relay networks," in *2019 2nd International Conference on Artificial Intelligence and Big Data (ICAIBD)*, pp. 323–328, IEEE, 2019.

[204] R. Yao, Y. Zhang, S. Wang, N. Qi, N. I. Miridakis, and T. A. Tsiftsis, "Deep neural network assisted approach for antenna selection in untrusted relay networks," *IEEE Wireless Communications Letters*, vol. 8, no. 6, pp. 1644–1647, 2019.

[205] S. Tripathi, C. Kundu, O. A. Dobre, A. Bansal, and M. F. Flanagan, "Recurrent neural network assisted transmitter selection for secrecy in cognitive radio network," in *GLOBECOM 2020-2020 IEEE Global Communications Conference*, pp. 1–6, IEEE, 2020.

[206] M. Zhu, Z. Yang, and Y. Feng, "Physical layer security of noma with decode-and-forward relaying in underlay cr network," in *2020 International Conference on Wireless Communications and Signal Processing (WCSP)*, pp. 783–788, IEEE, 2020.

[207] N.-L. Nguyen, H.-N. Nguyen, N.-T. Nguyen, D.-T. Do, A.-T. Le, M. Voznak, and J. Zdralek, "On secure cognitive radio networks with noma: Design of multiple-antenna

and performance analysis," in *2020 IEEE Microwave Theory and Techniques in Wireless Communications (MTTW)*, vol. 1, pp. 1–6, IEEE, 2020.

[208] H. M. Furqan, M. S. J. Solaija, J. M. Hamamreh, and H. Arslan, "Intelligent physical layer security approach for v2x communication," *arXiv preprint arXiv:1905.05075*, 2019.

[209] X. Luo, Y. Liu, H.-H. Chen, and Q. Guo, "Physical layer security in intelligently connected vehicle networks," *IEEE Network*, vol. 34, no. 5, pp. 232–239, 2020.

[210] B. M. ElHalawany, A. A. A. El-Banna, and K. Wu, "Physical-layer security and privacy for vehicle-to-everything," *IEEE Communications Magazine*, vol. 57, no. 10, pp. 84–90, 2019.

[211] H.-C. Yang, "New results on ordered statistics and analysis of minimum-selection generalized selection combining (gsc)," *IEEE Transactions on Wireless Communications*, vol. 5, no. 7, pp. 1876–1885, 2006.

[212] C. Morris, "Central limit theorems for multinomial sums," *The Annals of Statistics*, pp. 165–188, 1975.

[213] M. Kang and M.-S. Alouini, "Capacity of mimo rician channels," *IEEE Transactions on Wireless Communications*, vol. 5, no. 1, pp. 112–122, 2006.

List of publications

Journals

Published/Accepted

- S. Thakur and A. Singh,"Underlay Cognitive Radio With Instantaneous Interference Constraint: A Secrecy Performance," IEEE Transactions on Vehicular Technology, volume 70, number 08, pages 7839-7844, August 2021.
- S. Thakur and A. Singh,"Secure Transmission Using Optimal Antenna Selection for MIMO Underlay CRN With Multiple Primary Users," IET Communications, volume 14, issue 7, pages 1090-1101, April 2020.
- S. Thakur and A. Singh," Secure transmission in Underlay Cognitive Radio Network with Outdated Channel State Information," Elsevier Journal on Physical Communications, volume 37, pages 1-10, December 2019.

Under Review

- S. Thakur and A. Singh, ,"Secure Transmission in Underlay Cognitive Radio Networks With Primary Interference," IEEE Transactions on Network Science and Engineering.

Conferences

- S. Thakur and A. Singh,"Secrecy performance Analysis for Underlay Cognitive Radio Network with Optimal Antenna Selection and Generalized Receiver Selection," In Proc. IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Goa, India, pages 1-5, December 2019.

- S. Thakur and A. Singh,"Ergodic Secrecy Capacity in Nakagami-m Fading Channels," In Proc. for IEEE International Carnahan Conference on Security Technology (ICCST 2019), Chennai, India, pages 1-3, October 2019.
- S. Thakur and A. Singh," Secrecy Performance of Cognitive Radio Networks using Arbitrary Transmit Antenna Selection and Threshold- Based MRC," In Proc. for IEEE Vehicular Technology Conference (VTC-Fall), Honolulu, Hawaii, U.S.A., pages 1-5, September 2019.

Funding Details

This work was supported in part by Science and Engineering Research Board (SERB), Department of Science and Technology (DST), Government of India, for the Project ”Physical Layer Security of Cognitive Radio Networks ” (Project Ref. no. YSS/2015/001738).