On Achieving Covertness and Secrecy in Wireless Communications

by

Huihui Wu

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Graduate School of Systems Information Science)
in Future University Hakodate
September 2021

To my family

ACKNOWLEDGEMENTS

First and foremost, I would like to thank my advisor Professor Xiaohong Jiang, not only for his warm encouragement and thoughtful guidance in my research but also for his financial support that makes me able to fully concentrate on my research. He has been teaching me, both consciously and unconsciously, the important skills required to be a good researcher and the great personality traits that make a better person. It is a great honor for me to be one of his Ph.D. students and the Ph.D. experience under his supervision is definitely life-changing for me. I would also like to thank Professor Jiang's wife, Mrs Li, for her meticulous care and support for my life. I could not have imagined how hard my life in Hakodate would be without her help. I believe the time we spent together would be the greatest and fantastic memory that I will treasure forever.

Besides my advisor, I would like to thank the rest of my thesis committee: Professor Yuichi Fujino, Professor Hiroshi Inamura and Professor Masaaki Wada for their encouragement and insightful comments that not only help me to greatly improve this thesis but also inspire me to widen the area of my future research.

I would also like to give my sincere gratitude to Professor Yulong Shen from Xidian University, China, who gave me the opportunity to work together with Professor Xiaohong Jiang and other members in the laboratory when I was a Master student.

My sincere thanks also go to other members of our laboratory: Yuanyu Zhang, Lisheng Ma, Xuening Liao, Xiaolan Liu, Pinchang Zhang, Xiaochen Li, Ji He, Chan Gao, Ahmed, Guozhu Zhao, Wenhao Zhang, Yan Liu, He Zhu and Xinzhe Pi, for

their contributions in some way to this thesis. I also want to thank my Japanese teachers Katsuko Takahashi and Keiko Ishikawa; the university staffs Mr. Igi, Mr. Yoshida, Ms. Kawagishi, Ms. Arashida and Ms. Mitobe; teachers and students in the Japanese Salon who made my life in Hakodate colorful and memorable.

Last but not the least, I would like to thank my family, especially my parents. Words cannot express how grateful I am to them for all of the sacrifices they have made for me.

ABSTRACT

On Achieving Covertness and Secrecy in Wireless Communications

by

Huihui Wu

Due to the rapid development of information and communication technologies and widespread proliferation of wireless user equipment, an enormous amount of sensitive and confidential information is transmitted via wireless channels, so wireless communications have become the most fundamental communication technology indispensable in our daily life. The broadcast nature of wireless medium makes the exchange of confidential information in such communication vulnerable to various security attacks, which brings security vulnerabilities and threats in wireless information transmission. Therefore, the fundamental research of wireless communication security is of great importance for the development of secure network communication, information security and communication privacy. It is notable that in modern secure wireless communication applications, covertness and secrecy serve as two typical properties. Covertness concerns with the protection of wireless communication from detection attacks that attempt to detect the existence of the communication, while secrecy deals with the protection of wireless communication from eavesdropping attacks which manage to intercept the information conveyed by the communication.

With the wide applications of secure wireless communication, how to ensure both the covertness and secrecy of such communication has become an increasingly urgent demand. Thanks to the rapid progress of information and communication technologies, physical layer security (PLS) technique is now regarded as a highly promising approach to counteract the detection and eavesdropping attacks and thus to ensure the covertness and secrecy properties of wireless communications. This thesis therefore focuses on exploring a new secure wireless communication paradigm where the PLS technology is applied to counteract both the detection and eavesdropping attacks, such that the critical covertness and secrecy properties of the communication are jointly guaranteed.

We first investigate the covertness guarantee for a two-way two-hop wireless communication system, where two sources wish to covertly exchange information through a relay against the detection from a detector, i.e., a malicious node that attempts to detect the existence of communication between the two sources. We consider various scenarios regarding the detector's prior knowledge about the relay, the sources/relay's prior knowledge about the detector, as well as different relaying patterns, and then propose the covertness strategy to resist the detector's detection for each scenario. To depict the performance limit of the system, we derive the scaling law result for the covert throughput of the system for each scenario, i.e., the maximum number of bits that the two sources can exchange subject to a constraint on the detection probability of the detector. Our results indicate that the covert throughput of the concerned system follows the well-known square root scaling law, which is independent of the relaying patterns, detection schemes, covertness strategies, and prior knowledges of the sources/relay and detector.

We next consider the covertness and secrecy guarantees in wireless communications, and explore a new secure wireless communication paradigm where the critical covertness and secrecy properties are jointly guaranteed under the passive detec-

tion/eavesdropping attacks by applying the PLS technique. We first provide theoretical modeling for covertness outage probability (COP), secrecy outage probability (SOP) and transmission probability (TP) to depict the covertness, secrecy and transmission performances of the paradigm. To understand the fundamental security performance under the new paradigm, we then define a new metric - covert secrecy rate (CSR), which characterizes the maximum transmission rate subject to the constraints of COP, SOP and TP. We further conduct detailed theoretical analysis to identify the CSR under various scenarios determined by the detector-eavesdropper relationships and the secure transmission schemes adopted by transmitters. We also provide numerical results to illustrate the achievable performances under the new secure communication paradigm.

Finally, we extend the secure wireless communication paradigm to the active attacker scenario where attackers can perform jamming and detection/eavesdropping simultaneously. To understand the covertness, secrecy and transmission performances in the active attacker scenario, we first provide theoretical modeling for covertness outage probability, secrecy outage probability and transmission probability, respectively. Based on the theoretical model, we further conduct detailed theoretical analysis to identify the CSR in this scenario under power control (PC)-based and artificial noise (AN)-based transmission schemes adopted at transmitters. Extensive numerical results are then presented to validate the theoretical analysis, reveal the impact of active attackers on the CSR under each transmission scheme and illustrate the achievable performances in the secure wireless communication paradigm under the active attacker scenario.

TABLE OF CONTENTS

LIST OF FIGURES

Figure

LIST OF TABLES

Table

CHAPTER I

Introduction

In this chapter, we first introduce the background of wireless communications security and physical layer security, and then we present the objective and main works of this thesis. Finally, we give the outline and main notations of this thesis.

1.1 Security in Wireless Communications

With the rapid development of information and communication technologies and widespread proliferation of wireless user equipment, an enormous amount of sensitive and confidential information is transmitted via wireless channels, so wireless communications have become the most fundamental communication technology indispensable in our daily life [1, 2]. However, due to the broadcast nature of wireless medium, wireless communications suffer from various security attacks, which brings security vulnerabilities and threats in wireless information transmission. The fundamental research of wireless communication security, therefore, is of great importance for the development of secure network communication, information security and communication privacy [1, 3]. It is notable that in modern secure wireless communication applications, covertness and secrecy serve as two typical properties. Covertness concerns with the protection of wireless communication from detection attacks that attempt to detect the existence of the communication [4, 5], while secrecy deals with the pro-

tection of wireless communication from eavesdropping attacks[6, 7] which manage to intercept the information conveyed by the communication. With the wide application of secure wireless communication, how to ensure the covertness and secrecy of such communication has become an increasingly urgent demand.

Classical technologies for protecting the covertness property of wireless communications from the detection attacks are mainly based on steganography [8], which conceals messages in covertext objects (e.g., image, voice and video files) to achieve covertness [9]. However, the finite covertext objects limit the amount of concealed messages, and the messages remain in the covertext objects permanently and will be eventually recovered by adversaries with high probability. Besides, the messages cannot be transmitted without the covertext objects, which poses a significant challenge to the covert messages delivery when the transmissions of covertext objects are prohibited. In addition, spread spectrum [10] is also a representative technology for ensuring the covertness of wireless communications. The basic idea of spread spectrum is to spread signals over a much wider frequency band, such that the signal power spectral density (PSD) is much lower than the noise PSD and, consequently, malicious users are unable to determine whether the signals exist or not [10]. Although spread spectrum architecture for covertness guarantee in wireless communications has been well developed, the fundamental proof that how many covert messages can be reliably transmitted has not been established.

Traditional solution of secrecy guarantee in wireless communications against eavesdropping attacks mostly depends on the cryptography technology, which achieves secrecy by using secret keys and complex encryption algorithms to convert plaintext messages into ciphertexts based on some computationally difficult mathematical problems such as integer factorization [11]. Secret keys are accessible to only the transmitter-receiver pair and any other user without the secret keys cannot recover the messages from the ciphertexts. The management of the secret keys and execution

of the encryption algorithms usually require a large amount of resources (e.g., bandwidth and computation power), making the cryptography technology too expensive for resource-limited wireless networks, such as sensor networks and the Internet of Things [12, 13]. More importantly, cryptographic methods are based on the premise that it is computationally infeasible for them to be deciphered without the secret key, which has not been proven in mathematics. However, ciphers that were considered virtually unbreakable in the past are continually surmounted due to the potential growth in computational power, e.g., quantum computing [14]. Recently, the research trend on achieving covertness and secrecy of wireless communications has been shifted to the physical layer security technology.

1.2 Physical Layer Security

Thanks to the rapid progress of information and communication technologies, physical layer security (PLS) technique is now regarded as a highly promising approach to counteract the detection and eavesdropping attacks and thus to ensure the covertness and secrecy properties of wireless communications. The basic principle behind the PLS technology is to exploit the inherent physical layer randomness of wireless channels (e.g., noise and fading) to implement the secure and covert communications [15]. For example, transmitters can intentionally inject artificial noise (AN) into their channels to hide their signals from detectors or to add uncertainty to the information intercepted by eavesdroppers. The PLS technology realizes secure wireless communications from the information-theoretic perspective and thus provides stronger form of covertness and secrecy guarantees than traditional security technologies like the cryptography and spread spectrum [10, 16, 17]. Actually, the PLS technology serves as an effective supplement for the traditional security technologies to significantly improve the covertness and secrecy of wireless communications [5, 18].

By now, extensive research efforts have been devoted to study of covertness or

secrecy guarantees for wireless communications based on the PLS technology. In [19–24], the AN technique or cooperative jamming technique was adopted for covert wireless communication in the typical three-node scenario with a transmitter, a receiver and a malicious detector. In these works, the AN may be initiated by the transmitter [19, 20], by the (full-duplex) receiver [21, 22], or by some external helper nodes [23, 24] to avoid the communication signal from being detected by the detector. The works in [20, 25–27] showed that the covert wireless communication can be implemented by exploiting the detector's uncertainty about its channel state information, like the instantaneous channel coefficient [25], statistical channel coefficient [20] or background noise [26, 27]. Such uncertainty makes it difficult for the detector to determine the received signal power or the background noise power, and thus unable to distinguish between the scenarios with or without wireless communication by examining the power difference in these scenarios. Some recent works also explored the possibility of ensuring covertness based on other PLS technologies, such as multi-antenna technique [28, 29], coding scheme [30, 31], relay selection [32, 33] and resource (i.e., channel use) allocation [34].

The PLS technology has also been widely adopted for achieving secrecy in various wireless communication scenarios, such as ad-hoc networks [35, 36], device-to-device (D2D) communications [37, 38], cellular networks [39, 40] and the Internet of Things (IoT) [41, 42]. These works mainly exploited the application of AN technique to create a relatively better channel to the receiver than that to the eavesdropper with the aim of achieving a positive secrecy rate. In [43, 44], the beamforming technique was explored for secure wireless communication in multi-antenna scenarios, where the transmit power of signals was concentrated toward the direction of intended receiver such that a much better signal quality at the receiver can be created than that at the eavesdropper. The work in [45] further combined the beamforming and AN techniques to achieve a significant signal advantage at the receiver, while the works in [46, 47]

considered the multi-user scenarios and applied relay selection technique to create a transmitter-receiver channel advantage over the transmitter-eavesdropper channel. Some other works in [48–50] also studied the secure wireless communication based on the technique of resource allocation (e.g., power allocation, time slot allocation, energy allocation).

1.3 Objective and Main Works

This thesis focuses on the fundamental research of wireless communication security, which is of great importance for the development of secure network communication, information security and communication privacy. Our objective is to apply the physical layer security technology to counteract both the detection and eavesdropping attacks, such that the critical covertness and secrecy properties of the wireless communication are jointly guaranteed. Towards this end, we first study the covertness guarantee for a two-way two-hop wireless communication system, and derive the scaling law result for the covert throughput of the system. We then explore a new secure wireless communication paradigm where the critical covertness and secrecy properties of communication are jointly guaranteed under the passive detection/eavesdropping attacks, and conduct detailed theoretical analysis to study the covert secrecy rate (C-SR) under various scenarios determined by the detector-eavesdropper relationships and the secure transmission schemes adopted by transmitters. Finally, we extend the secure wireless communication paradigm to the active attacker scenario where attackers perform detection/eavesdropping and jamming simultaneously. We also provide extensive numerical results to demonstrate the achievable performances under the new secure wireless communication paradigm. The main works and contributions of this thesis are summarized in the following subsections.

1.3.1 Covertness Guarantee in Two-Way Relay Wireless Communication

This work focuses on ensuring the covertness in two-way two-hop relay wireless communications. Two-hop wireless networks have been a class of fundamental and important network models, which serve as the building blocks for more complex networks like the mobile ad hoc networks and sensor networks [51, 52]. Moreover, it has been commonly recognized that the performance analysis in two-hop wireless networks will lay a solid foundation for that in more complex networks, and also provide guidelines for the long-distance transmission scheme design [53]. Two-way two-hop wireless networks are one representative class of two-hop wireless networks, so they enjoy the benefits of two-hop wireless networks and, at the same time, support a variety of transmissions, like four-slot, three-slot and two-slot transmissions [54].

While the previous works represent a significant progress in the study of covert wireless communication, they mainly focus on one-way single-hop communication scenarios. However, due to the low transmit power feature of covert wireless communication, single-hop transmissions may not be able to meet the requirement for long-distance covert information delivery in practical wireless networks [55]. Moreover, two-way communication has been a common scenario in practice, where two nodes exchange information simultaneously, so it attracted considerable research attentions [56]. Thus, investigating the performance of two-way multi-hop covert wireless communication is significantly important for the development of practical covert wireless communication schemes.

As the first step towards this research direction, this work investigates the performance of a two-way two-hop wireless system with two sources, one relay and one malicious detector. We consider three relaying patterns used by the transmitters, where the two-way communication is completed in four, three and two time slots, respectively. We also consider three cases for the prior knowledge of the detector about the relay information, i.e., Unknown Relay Information (URI), Partial Relay

Information (PRI), and Full Relay Information (FRI) cases, where the detector does not know the existence of the relay, knows the existence of the relay but is not sure about whether the relay is involved in the communication, and exactly knows the involvement of the relay in the communication, respectively. We assume that the detector switches between two detection schemes, i.e., a *blind* detection scheme and a *cautious* detection scheme, according to his prior knowledge. In the blind (resp. cautious) scheme, the detector judges that the detection is successful if it detects the existence of the communication in either hop (resp. in both hops). In addition, we also assume two cases regarding the prior knowledge of the legitimate nodes about the detector (i.e., detection scheme and prior knowledge of the relay), i.e., *smart* and *ignorant* legitimate node cases, where such knowledge is known or unknown, respectively. Thus, to resist the detector's detection, legitimate nodes employ an adaptive covertness mechanism (described in the first contribution) proposed in this work. The main contributions of this work are summarized as follows.

- This work proposes an adaptive covertness mechanism that switches among a *complete* covertness strategy guaranteeing the covertness of the communication in every hop, a *partial* covertness strategy, and a *selective* covertness strategy according to different scenarios of the prior knowledges. More specifically, the partial (resp. selective) covertness strategy is utilized to hide the transmissions in either hop instead of both hops (resp. in the hops where the sources transmit) under the scenario where the legitimate nodes are smart and the detector has PRI (resp. URI) and uses the cautious (resp. blind) detection scheme, while the complete covertness strategy is employed in other scenarios.

- For each relaying pattern (i.e., four-slot, three-slot and two-slot) under the above scenarios, we derive the scaling law results for the covert throughput that the two sources can covertly exchange information, while satisfying a detection

probability constraint at the detector. The results in this work reveal that the performance of the considered two-way two-hop wireless system also follow the well-known square root scaling law (i.e., $\mathcal{O}(\sqrt{n})$), which is independent of the relaying patterns, detection schemes, covertness strategies, and prior knowledges of the legitimate nodes and detector.

1.3.2 Covertness and Secrecy Guarantees in Wireless Communications with Passive Attackers

The existing works help us understand the great potentials of the PLS technology in ensuring the covertness or secrecy of wireless communication. It is notable that these works mainly focus on the traditional paradigms of secure wireless communication where only one type of attack may exist, be it detection or eavesdropping, and concern with either the covertness guarantee or secrecy guarantee for wireless communications. In practice, however, both detection or eavesdropping attacks may coexist, especially in some critical communication scenarios consisting of multiple groups with common or conflicting interests, like military communications and coastal surveillance. Therefore, in this work we are motivated to explore a new secure wireless communication paradigm, where the PLS technology is applied to counteract both the detection and eavesdropping attacks in which both the detector and eavesdropper are passive attackers. To the best of our knowledge, this is the first work that studies the joint guarantee for the critical covertness and secrecy properties of wireless communications at the physical layer. The main contributions of this work are summarized as follows.

- *A new secure wireless communication paradigm*: In this paradigm, the PLS technology is applied to counteract both the detection and eavesdropping attacks and thus to jointly guarantee the covertness and secrecy properties of wireless communications. To demonstrate the new paradigm, we consider four

representative communication scenarios of the paradigm, which are categorized by the detector-eavesdropper relationships (i.e., *independence* and *friend*) and the secure transmission schemes adopted by the transmitters (i.e., a *power control (PC)-based* scheme and an *AN-based* scheme). In the friend relationship case, the detector group and eavesdropper group share their signals received from the target transmitters in the hope of enhancing the attack performance of both sides, while in the independence relationship case, the two groups independently conduct their own attack without such signal sharing.

- *Theoretical modeling for the new paradigm*: To depict the covertness, secrecy and transmission performances of the new paradigm, for each concerned communication scenario we provide the corresponding theoretical modeling of covertness outage probability (COP) (i.e., the probability that detectors can detect the transmitted signals), the secrecy outage probability (SOP) (i.e., the probability that eavesdroppers can recover the conveyed information) and the transmission probability (TP) (i.e., the probability of successfully conducting a transmission), respectively.

- *A novel security metric characterizing the covertness, secrecy and transmission performances*: This work defines a novel security metric-*covert secrecy rate* (CSR), which characterizes the maximum transmission rate subject to the constraints of COP, SOP and TP, and thus can serve as the fundamental security criterion for this new communication paradigm. We further conduct detailed theoretical analysis to identify the CSR for each of the four communication scenarios. Finally, extensive numerical results are provided to illustrate the CSR performances under the new secure communication paradigm.

1.3.3 Covertness and Secrecy Guarantees in Wireless Communications with Active Attackers

In this work, we study the secure wireless communication paradigm that jointly ensures the covertness and secrecy in wireless communications under a active attacker scenario where attackers perform detection/eavesdropping and jamming simultaneously. The active attackers, i.e., detector and eavesdropper, send the artificial noises that can not only impair the covertness, secrecy and transmission performances of wireless communication between transmitter and receiver but also reduce the covert secrecy rate in this scenario. Thus, based on the PLS technology, the transmitter and receiver adopt two secure transmission schemes to counteract both detection and eavesdropping attacks for achieving the secure wireless communication paradigm in the active attacker scenario. The main contributions of this work are summarized as follows.

- For the theoretical modeling in the secure wireless communication paradigm scenario with active attackers, we derive the covertness outage probability (COP) (i.e., the probability that detectors can detect the transmitted signals), the secrecy outage probability (SOP) (i.e., the probability that eavesdroppers can recover the conveyed information), and the transmission probability (TP) (i.e., the probability of successfully conducting a transmission) to illustrate the covertness, secrecy and transmission performances in this scenario, respectively.

- To guarantee the covertness and secrecy properties of wireless communications resisting both the detection and eavesdropping attacks, we consider the on-off transmission model to determine whether the transmission takes place or not as well as the secure transmission schemes adopted by the transmitters (i.e., either power control (PC)-based scheme or AN-based scheme).

- We formulate the optimization problems of the covert secrecy rate (CSR) that

represents the maximum transmission rate subject to the requirements of COP, SOP and TP in this scenario under two secure transmission schemes, respectively. Finally, extensive numerical results are provided to reveal the impact of the active attackers on the CSR under each transmission scheme, and illustrate the achievable performances under the active attacker scenario in the secure wireless communication paradigm.

1.4 Thesis Outline

The remainder of this thesis is outlined as follows. Chapter II introduces the related works of this thesis. In Chapter III, we introduce our work regarding covertness guarantee in two-way relay wireless communications. Chapter IV presents the work on covertness and secrecy guarantees in wireless communications with passive attackers and Chapter V introduces the work regarding covertness and secrecy guarantees in wireless communications with active attackers. Finally, we conclude this thesis in Chapter VI.

1.5 Notations

The main notations of this thesis are summarized in Table 1.1.

Table 1.1: Main notations

Symbol	Definition
$\mathcal{O}(\cdot)$	Asymptotic upper bound
$o(\cdot)$	Upper bound that is not asymptotically tight
n	Number of channel uses
ρ	Power allocation factors
$\mathbf{x}$	Transmitted signal vector

$\mathbf{v}$	Artificial noise signal vector
$\mathbf{y}$	Received signal vector
$Z^{(i)}$	Background noise at i-th sampling location
σ^2	Power of noise
$\mathcal{N}(\mu, \sigma^2)$	Gaussian distribution with mean μ and variance σ^2
P	Probability distribution
M	Maximum number of bits
$\bar{P}$	Average power
$\mathcal{H}$	Hypothesis
S	Transmitted message signal
ξ	The sum of detection error probabilities
$\|\cdot\|_1$	$\mathcal{L}_1$ norm
$V_T(\cdot)$	The function of total variance distance
$D(\cdot)$	Relative entropy
$\mathbf{E}_X[\cdot]$	The expectation operator over random variable X
$\mathbb{P}(\cdot)$	Probability operator
θ	Detection threshold
$\|h_{ij}\|^2$	Coefficient of the channel from i to j
R_{cs}	Covert secrecy rate (CSR)
ϵ_c	Covertness requirement
ϵ_s	Secrecy requirement
ϵ_t	Transmission requirement
p_{co}	Covertness outage probability (COP)
p_{so}	Secrecy outage probability (SOP)
p_{tx}	Transmission probability (TP)
p_{FA}	False alarm probability

p_{MD}	Missed detection probability
υ	Arbitrarily small value
$\mathrm{W}_0(\cdot)$	Principal branch of Lambert's W function
$\mathrm{W}_{-1}(\cdot)$	Non-principle branch of Lambert's W function
$\boldsymbol{e}$	Euler's number
γ	Signal to interference plus noise ratio (SINR)
μ	SINR threshold
χ^2_{2n}	Chi-squared random variable with $2n$ degrees of freedom

CHAPTER II

Related Works

This chapter introduces the existing works related to our study in this thesis, including the works on achieving the secure wireless communication, covert wireless communication, and other classical technologies, respectively.

2.1 Secure Wireless Communication

Compared to our work, available works focused on traditional paradigms, where only the detection or eavesdropping attack is counteracted. However, none of them jointly considered protecting transmissions from both attacks as in our new secure communication paradigm. This significantly distinguishes our work from the available ones. In what follows, we introduce the available works related to this thesis with a particular focus on the three-node scenario consisting of one transmitter, one receiver, and one attacker (i.e., detector or eavesdropper) in secure/covert wireless communication.

The study of secure wireless communications against eavesdropping attacks at the physical layer was pioneered by [57], where the classic wiretap channel model and the notion of secrecy rate were introduced. The results in [57] reveal that positive secrecy rates can be achieved when the transmitter-eavesdropper channel is a degraded version of the transmitter-receiver channel. This work was later extended to other channel

models, like the Gaussian wiretap channel [58], the BSC [59], and the type-II wiretap channel [60]. Recent studies in this filed of three-node scenarios mainly focused on the fading channel model and adopted the SOP [61] as one of the main performance metrics and the artificial noise (AN)-based scheme as one of the fundamental PLS techniques.

The authors in [62] adopted an AN-based scheme, where the transmitter splits its power between message transmission and AN transmission. Different from our AN-based scheme, the receiver in [62] is assumed to be able to cancel the AN out from the received signals. The optimal power allocation parameters were determined to minimize the SOP and maximize the secrecy rate respectively. A similar AN-based scheme was adopted in [63] for a scenario with an active full-duplex eavesdropper, which also transmits AN while intercepting messages. Same to our AN-based scheme, the cancellation of the AN from the transmitter is not available at the receiver side. The SOP and secrecy rate performances were also optimized over the power allocation parameter respectively. Helper nodes can also be added to the three-node scenario to take over the job of AN generation from the transmitter [64, 65]. The secrecy performance analysis in the three-node scenario can also be extended to other large-scale scenarios, e.g., ad hoc networks [66, 67], device-to-device (D2D) communications [37, 68], cellular networks [69, 70], and Internet of Things (IoT) [41].

2.2 Covert Wireless Communication

To achieve covert wireless communication against detection attacks in the three-node scenario, Bash *et al.* [71] proposed a power control (PC)-based scheme to make the detector unable to distinguish between message signals and background noise. In this scheme, Alice sends message signals at power much lower than that of the background noise as if hiding the signals in the noise, so that Willie can hardly detect the existence of the message signals. In addition, the authors in [71] explored

the fundamental performance limits of covert wireless communication, which are the scaling-law results of the covert rate. The $\mathcal{O}$ here represents the asymptotic notation, which has been widely used in order-sense performance analysis in not only the research field of covert communications but also other fields, like in the physical layer security [72–74]. The results in this work showed that Alice can send at most $\mathcal{O}(\sqrt{n})$ number of bits to Bob in n channel uses, while guaranteeing a negligible detection probability at Willie. This result was originally obtained for additive Gaussian white noise (AGWN) channels with a static detector, and was later extended to the scenario with a mobile detector [75] and other channel models such as binary symmetric channels (BSCs) [76] and discrete memoryless channels (DMCs) [77, 78].

The research of Bash *et al.* in [71] is the first work which considers information-theoretical bound on covert wireless communication. The research efforts have also been devoted to improving the square root limit $\mathcal{O}(\sqrt{n})$ by considering more powerful covertness schemes. In [79], Bash *et al.* showed that a performance limit of $\mathcal{O}(\min\{\sqrt{n \log T(n)}, n\})$ can be achieved under a "time-hopping" scheme, where Alice selects one out of $T(n)$ time slots to send messages while keeping the selected slot unknown to Willie. Under the same "time-hopping" scheme, the limit was further improved to $\mathcal{O}(n)$ if Willie has no knowledge about his noise statistics [26]. The authors in [23] showed that the $\mathcal{O}(n)$ limit can also be achieved when a friendly jammer is introduced to confuse the detection of Willie by generating artificial noise. For a scenario with multiple friendly jammers, an improved limit of $\mathcal{O}(\min\{n, m^{\frac{\gamma}{2}}\sqrt{n}\})$ was shown achievable even if Willie knows his noise statistics [80]. These scaling-law results show how the covert rate scales up as the number of channel uses tends to infinity, while they fail to reflect the exact covertness performances of more practical scenarios under finite channel uses.

Thus, researchers began to devote their efforts to the exact covertness analysis. A variant three-node scenario was considered in [19], where a greedy relay wishes to

transmit its own covert messages to the receiver while forwarding the transmitter's messages. To avoid being detected by the transmitter, the relay adopts the PC-based scheme to control its transmit power. For the covertness modeling, the authors derived the detection error probability of the transmitter and the covert rate. The authors in [21] considered a full-duplex receiver, which generates AN while receiving signals from the transmitter in a Rayleigh fading channel, and obtained the maximum detection error probability of the detector under a given constraint of the minimum required covert rate. For scenarios with a half-duplex receiver, the covert rate performances were analyzed under the PC-based scheme and various assumptions. For example, the detector was assumed to have no knowledge about the time slots in which the transmitter sends messages to the receiver [81, 82], about the instantaneous channel coefficient or statistical characteristic of its channel [20, 25], and about the exact background noise power [26, 27, 83]. The results in these three-node scenarios can also be extended to other scenarios, like the multiple access channels (MACs) [84], broadcast channels [85, 86], relay channels [1, 4, 87], and multi-detector scenarios [90].

2.3 Classical Technologies for Secure/Covert Communications

The classical technologies for achieving secure or covert communications are not only for the physical layer as mentioned above but also for other upper network layers, and we briefly introduce some representative technologies here. For example, digital steganography [8] conceals messages in covertext objects which encompass image, voice, or video files. The digital steganography can be achieved at the application layers due to the widespread applications (e.g., Voice over IP (VoIP), video streaming, and online games) of the Internet traffic around the world. Miao *et al.* in [91] investigated the least significant bit (LSB) embedding scheme for VoIP, which ad-

dressed the speech quality degradation and high detectability issues by factoring the smoothness of sample blocks. Zhao *et al.* proposed a technique used over streaming networks, which stores a steganogram into B frames of Group of Picture (GOP) and deliberately place it on the receiver side to indicate that there is a steganogram [92]. For digital steganography, however, the given size of covertext objects limit the extent of information that can be hidden, and the messages remain in the covertext objects permanently and may be eventually recovered by adversaries with high probability. Besides, the messages cannot be transmitted without the covertext objects, which poses a significant challenge to the covert message delivery when the transmissions of covertext objects are prohibited. The above issues can be mitigated or even eliminated in the network steganography. For network steganography, the TCP/IP layers are popular as covert channels because steganograms can be easily embedded and effortlessly retained over multiple hops. Abdullaziz *et al.* proposed a storage-based technique by using the length of the User Datagram Protocol (UDP) payload, where an even length is denoted as 0 and an odd length is denoted as 1 [93]. The available fields are transparently identified (i.e. header fields of Protocol Data Unit (PDU)), and thus unless the hiding mechanism is exceptionally exquisite, the header fields cannot hide messages when steganograms are not allowed to be detected.

CHAPTER III

Covertness Guarantee in Two-Way Relay Wireless Communications

This chapter focuses on the performance limit of covert throughput and the covertness guarantee in important two-way relay covert wireless communications. As the most significant contribution, this work investigates such performance limit in a system where two sources wish to covertly exchange information through a relay against the detection from a detector, i.e., a malicious node that attempts to detect the existence of communication between the two sources. As the second contribution, this work considers various scenarios regarding the detector's prior knowledge about the relay, the sources/relay's prior knowledge about the detector, as well as different relaying patterns, and then proposes a covertness strategy to resist the detector's detection for each scenario. As the last contribution, we derive the scaling law result for the covert throughput of the system for each scenario, i.e., the maximum number of bits that the two sources can exchange subject to a constraint on the detection probability of the detector. The results in this work indicate that the covert throughput of the concerned system follows the well-known square root scaling law, which is independent of the relaying patterns, detection schemes, covertness strategies, and prior knowledges of the sources/relay and detector.

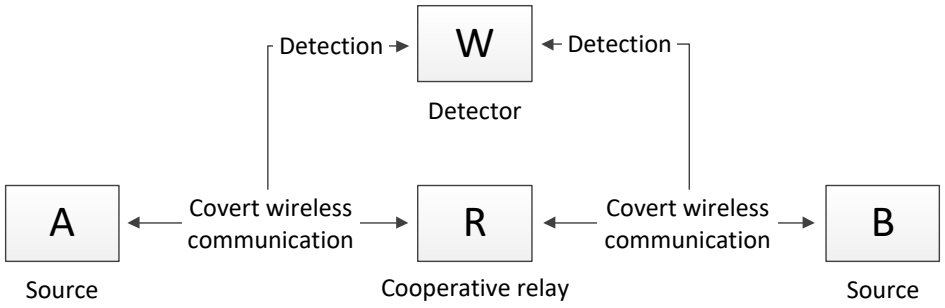


Figure 3.1: Illustration of system model.

3.1 System Model and Transmission Schemes

In this section, we introduce the system model and the transmission schemes between two sources.

3.1.1 System Model

As depicted in Fig. 3.1, we consider a two-way two-hop relay wireless network consisting of two source nodes A and B who wish to exchange information through a Decode-and-Forward (DF) relay R without being detected by an adversarial detector W. We assume that each node has a single omnidirectional antenna and operates in the half-duplex mode such that it cannot transmit and receive signals simultaneously. We also assume that there is no direct link between A and B, so that they can only exchange information with the assistance of the relay R. Time is assumed to be divided into successive slots with equal duration, and one and only one single-hop transmission can be conducted during each time slot. We assume that each single-hop transmission contains n symbols. We consider a discrete-time AWGN channel model, where the noise is modeled by a zero-mean complex Gaussian random variable with variance σ^2. The noises at all nodes are assumed to be independent and identically distributed (i.i.d.).

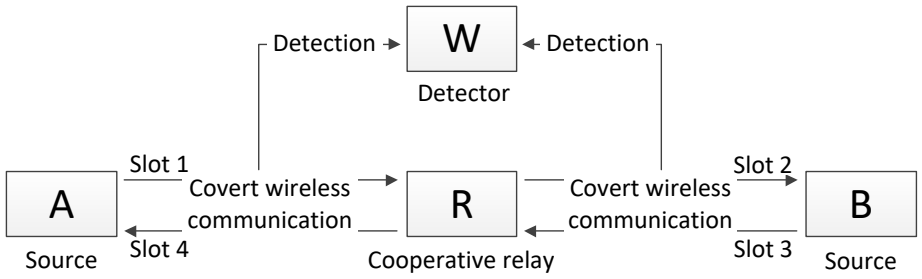
To covertly deliver the message in each transmission, legitimate nodes can use a

prior shared secret of sufficient length as the encoder, while the secret is unknown to W, which is consistent with the common assumption in [71, 75]. As to W, without knowing the codebook of the secret, he cannot detect the existence of transmission with a low detection error probability. Thus, in each transmission, the legitimate node who intends to covertly deliver the message will select a codebook randomly from an ensemble of codebooks and then encode the message into the transmitted symbols. After transmission through the covert channel, the symbols will be received and decoded by the other legitimate node(s) using the shared secret.

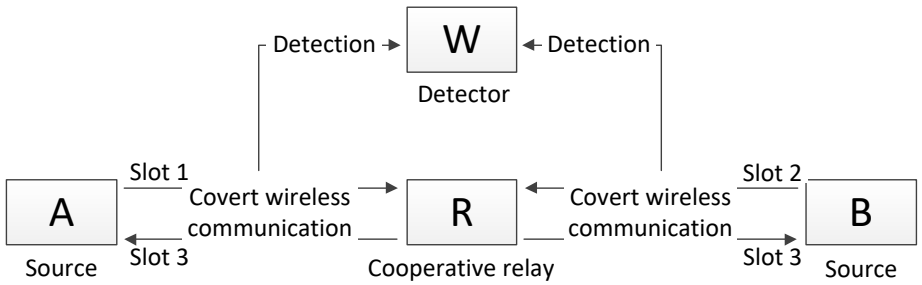
We consider three cases for the prior knowledge of the detector about the relay information, i.e., the Unknown Relay Information (URI), Partial Relay Information (PRI), and Full Relay Information (FRI) cases. In the URI case, we assume that the detector does not know the existence of the relay and cannot receive signals from R. In the PRI case, the detector knows the existence of the relay but is not sure about whether the relay is involved in the communication. In the FRI case, the detector exactly knows the involvement of the relay in the communication. In addition, we also assume two cases regarding the prior knowledge of the legitimate nodes (i.e., A, B and R) about the detector (i.e., detection scheme and prior knowledge of the relay), i.e., *smart* and *ignorant* legitimate node cases, where such knowledge is known or unknown, respectively.

3.1.2 Transmission Schemes between Two Sources

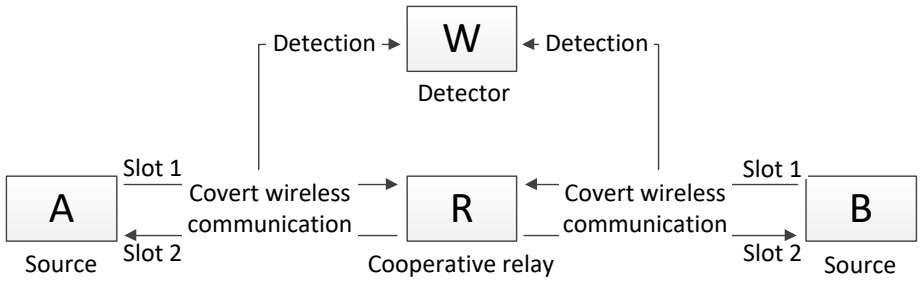
The two-way two-hop covert wireless communication is illustrated in Fig. 3.2, where the communication can be completed in four, three or two time slots, respectively [54]. In the four-slot scenario, A sends messages to B in the first two time slots, while B sends messages to A in the remaining two time slots. More specifically, in the first time slot, A randomly chooses an M-bit message $w \in \{1, 2, \cdots, 2^M\}$ and encodes it into a random vector of n real-valued symbols $\mathbf{x}_A = [X_A^{(1)}, X_A^{(2)}, \cdots, X_A^{(n)}]$, where



(a) Four-slot Transmission Scheme



(b) Three-slot Transmission Scheme



(c) Two-slot Transmission Scheme

Figure 3.2: Transmission schemes of four, three and two time slots.

$X_A^{(i)} \in \mathbb{R}$ $(i = 1, 2, \cdots, n)$ are independent and identically distributed according to a Gaussian distribution $\mathcal{N}(0, S_A)$ with variance S_A. A then sends W to R in n channel uses. Thus, R receives a signal vector

$$\mathbf{y}_{A,R} = [Y_{A,R}^{(1)}, Y_{A,R}^{(2)}, \cdots, Y_{A,R}^{(n)}], \tag{3.1}$$

where $Y_{A,R}^{(i)} = X_A^{(i)} + Z_R^{(i)}$ and $Z_R^{(i)} \sim \mathcal{N}(0, \sigma_R^2)$ $(i = 1, 2, \cdots, n)$ is the AWGN at R. Meanwhile, W receives a signal vector

$$\mathbf{y}_{A,W} = [Y_{A,W}^{(1)}, Y_{A,W}^{(2)}, \cdots, Y_{A,W}^{(n)}], \tag{3.2}$$

where $Y_{A,W}^{(i)} = X_A^{(i)} + Z_W^{(i)}$ and $Z_W^{(i)} \sim \mathcal{N}(0, \sigma_W^2)$ is the AWGN at W. After receiving the signals, R decodes them by employing a maximum-likelihood (ML) decoder and then transmits the decoded signals to B in the second time slot. Thus, B receives a signal vector $\mathbf{y}_B = [Y_B^{(1)}, Y_B^{(2)}, \cdots, Y_B^{(n)}]$ and W receives $\mathbf{y}_{R(A),W} = [Y_{R(A),W}^{(1)}, Y_{R(A),W}^{(2)}, \cdots, Y_{R(A),W}^{(n)}]$ from R. Here, $Y_B^{(i)} = X_A^{(i)} + Z_B^{(i)}$ with $Z_B^{(i)} \sim \mathcal{N}(0, \sigma_B^2)$ being the AWGN at B, and $Y_{R(A),W}^{(i)} = \mathbf{1}_{\neq \mathrm{URI}} \cdot X_A^{(i)} + Z_W^{(i)}$ where $\mathbf{1}_{\neq \mathrm{URI}} = 1$ for the PRI and FRI cases and 0 for the URI case. Similarly, in the remaining two time slots, B transmits a vector of symbols $\mathbf{x}_B = [X_B^{(1)}, X_B^{(2)}, \cdots, X_B^{(n)}]$ to A through R, and the received signals at R and A are

$$\mathbf{y}_{B,R} = [Y_{B,R}^{(1)}, Y_{B,R}^{(2)}, \cdots, Y_{B,R}^{(n)}] \tag{3.3}$$

and $\mathbf{y}_A = [Y_A^{(1)}, Y_A^{(2)}, \cdots, Y_A^{(n)}]$ respectively, where $Y_{B,R}^{(i)} = X_B^{(i)} + Z_R^{(i)}$, $Y_A^{(i)} = X_B^{(i)} + Z_A^{(i)}$ with $Z_A^{(i)} \sim \mathcal{N}(0, \sigma_A^2)$ being the AWGN at A. The received signals at W from B and R are

$$\mathbf{y}_{B,W} = [Y_{B,W}^{(1)}, Y_{B,W}^{(2)}, \cdots, Y_{B,W}^{(n)}] \tag{3.4}$$

and $\mathbf{y}_{R(B),W} = [Y_{R(B),W}^{(1)}, Y_{R(B),W}^{(2)}, \cdots, Y_{R(B),W}^{(n)}]$ respectively, where $Y_{B,W}^{(i)} = X_B^{(i)} + Z_W^{(i)}$ and $Y_{R(B),W}^{(i)} = \mathbf{1}_{\neq \mathrm{URI}} \cdot X_B^{(i)} + Z_W^{(i)}$.

In the three-slot scenario, A and B transmit to R in the first two time slots respectively and the received signal vectors at R and W are given by (3.1), (3.3) and (3.2), (3.4), respectively. In the third time slot, R combines the received signals from

A and B into a signal vector $\mathbf{x}_R = [X_R^{(1)}, X_R^{(2)}, \cdots, X_R^{(n)}]$ and broadcasts it to A and B simultaneously. Here, $X_R^{(i)} = \rho_A X_A^{(i)} + \rho_B X_B^{(i)}$, and $\rho_A \in [0,1]$ and $\rho_B = 1 - \rho_A$ denote the power allocation factors for transmitting $X_A^{(i)}$ and $X_B^{(i)}$, respectively. Thus, A and B receive signal vectors $\tilde{\mathbf{y}}_A = [\tilde{Y}_A^{(1)}, \tilde{Y}_A^{(2)}, \cdots, \tilde{Y}_A^{(n)}]$ and $\tilde{\mathbf{y}}_B = [\tilde{Y}_B^{(1)}, \tilde{Y}_B^{(2)}, \cdots, \tilde{Y}_B^{(n)}]$, where $\tilde{Y}_A^{(i)} = X_R^{(i)} + Z_A^{(i)}$ and $\tilde{Y}_B^{(i)} = X_R^{(i)} + Z_B^{(i)}$, respectively. Meanwhile, W receives a signal vector $\tilde{\mathbf{y}}_{R,W} = [\tilde{Y}_{R,W}^{(1)}, \tilde{Y}_{R,W}^{(2)}, \cdots, \tilde{Y}_{R,W}^{(n)}]$, where $\tilde{Y}_{R,W}^{(i)} = \mathbf{1}_{\neq \mathrm{URI}} \cdot X_R^{(i)} + Z_W^{(i)}$. Since each source node knows its transmitted signals, it has the capability to cancel the self-interference and recover the original messages from the received signals by employing a ML decoder.

Finally, in the two-slot transmission scenario, regarding the first time slot, A transmits $\mathbf{x}_A$ to R and at the same time B transmits $\mathbf{x}_B$ to R, such that the received signal vectors at R and W are given by $\mathbf{y}_{(A,B),R} = [Y_{(A,B),R}^{(1)}, Y_{(A,B),R}^{(2)}, \cdots, Y_{(A,B),R}^{(n)}]$ and $\mathbf{y}_{(A,B),W} = [Y_{(A,B),W}^{(1)}, Y_{(A,B),W}^{(2)}, \cdots, Y_{(A,B),W}^{(n)}]$, where $Y_{(A,B),R}^{(i)} = X_A^{(i)} + X_B^{(i)} + Z_R^{(i)}$ and $Y_{(A,B),W}^{(i)} = X_A^{(i)} + X_B^{(i)} + Z_W^{(i)}$. The relay R decodes the received signal vectors and broadcasts a combined vector $\mathbf{x}_A + \mathbf{x}_B$ to both sources in the second time slot. The received signals at A and B from R are $\hat{\mathbf{y}}_A = [\hat{Y}_A^{(1)}, \hat{Y}_A^{(2)}, \cdots, \hat{Y}_A^{(n)}]$ and $\hat{\mathbf{y}}_B = [\hat{Y}_B^{(1)}, \hat{Y}_B^{(2)}, \cdots, \hat{Y}_B^{(n)}]$, where $\hat{Y}_A^{(i)} = X_A^{(i)} + X_B^{(i)} + Z_A^{(i)}$ and $\hat{Y}_B^{(i)} = X_A^{(i)} + X_B^{(i)} + Z_B^{(i)}$, respectively. Meanwhile, W receives a vector of signals $\hat{\mathbf{y}}_{R,W} = [\hat{Y}_{R,W}^{(1)}, \hat{Y}_{R,W}^{(2)}, \cdots, \hat{Y}_{R,W}^{(n)}]$, where $\hat{Y}_{R,W}^{(i)} = \mathbf{1}_{\neq \mathrm{URI}} \cdot (X_A^{(i)} + X_B^{(i)}) + Z_W^{(i)}$. Similar to the three-slot transmission scenario, A and B can cancel the self-interference and recover their intended messages from the received signals.

3.2 Detection Schemes and Covertness Strategies

In this section, we first detail two detection schemes of the detector, and then illustrate how the legitimate nodes choose their most suitable covertness strategy.

Table 3.1: Detection schemes and covertness strategies.

Prior Knowledge of Detector	Detection Scheme of Detector	Covertness Strategy of Legitimate Nodes	
		Ignorant Legitimate Nodes case	Smart Legitimate Nodes case
URI case	blind detection	complete covertness strategy	selective covertness strategy
PRI case	blind detection	complete covertness strategy	complete covertness strategy
	cautious detection	complete covertness strategy	partial covertness strategy
FRI case	blind detection	complete covertness strategy	complete covertness strategy

3.2.1 Detection Schemes of the Detector

We assume that the detection of the detector W is independent in each hop, which means that he will not combine the signals received from all hops to perform the detection. The detector adopts the method of hypothesis test for detection, where he proposes two hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$, which represent that the transmission does not exist and exists, respectively. W asserts that if $\mathcal{H}_0$ is true, the received signal should contain only the background noise, i.e., the distribution of the received signal is very close to that of his background noise. On the other hand, if $\mathcal{H}_1$ is true, the distribution of the received signal differs significantly from that of his background noise. We take a single hop as an example to show how the detection works. Using the hypothesis test, W randomly chooses one sample from the received signal vector and compares the distribution of the sample with $\mathcal{N}(0, \sigma_W^2)$. If the difference of the distributions exceeds a predefined threshold, W asserts that transmission exists; otherwise, W asserts that the transmission does not exist. The hypothesis test introduces two types of detection

errors. One is called *false alarm* where W reports a detected transmission while the transmission does not exist in fact, and the other is called *missed detection* where W reports no detected transmissions while the transmission exists indeed. We use p_{FA} and p_{MD} to denote the probabilities of false alarm and missed detection, respectively, and use the sum $\xi = p_{FA} + p_{MD}$ to characterize the detection performance of W. Obviously, the smaller the ξ is, the better detection performance W will have.

In this work, we consider two detection schemes for W, i.e., the blind scheme and the cautious scheme. In the blind (resp. cautious) scheme, W asserts that he detects the existence of the transmission between A and B if he does so in either hop (resp. in both hops). We denote $\mathcal{D}_i$ ($i \in \{1, 2\}$) as the event that W detects the existence of transmission in the i-th hop. Thus, the blind (resp. cautious) scheme corresponds to $\mathcal{D}_1 \cup \mathcal{D}_2$ (resp. $\mathcal{D}_1 \cap \mathcal{D}_2$). The blind scheme is proper for a blind detector, who prefers to detecting the existence of transmissions as much as possible without caring about making wrong detections. On the other hand, the cautious scheme is more appropriate for a cautious detector, who also cares about making wrong decisions, since some punishment may be imposed for wrong detections. As shown in Table 3.1, we assume that W uses the blind scheme in all cases (i.e., the URI, PRI and FRI cases) about his prior knowledge of the relay information, while he uses the cautious detection scheme in the PRI case only. Notice that when W uses the blind scheme in the URI case, he performs detection only when A and B transmits, since he does not know the existence of the relay.

3.2.2 Covertness Strategies of the Legitimate Nodes

To resist the detector's detection, the legitimate nodes will adopt different covertness strategies based on their prior knowledge about the detector's prior knowledge and detection schemes. We assume that the legitimate nodes can be ignorant or smart, which means that they do not know or know the detector's prior knowledge

and detection schemes. For ignorant legitimate nodes, they use the complete covertness strategy as shown in Table 3.1, where they try to hide the transmissions in each hop against the detector. For smart legitimate nodes, the choice of covertness strategies depends on the detector's prior knowledge and detection schemes. In the URI case, the legitimate nodes employ the selective covertness strategy, where they hide the transmissions only when A and B transmit. In the PRI case, when the detector W uses the blind scheme, the legitimate nodes adopt the complete covertness strategy, whereas when W uses the cautious scheme, the legitimate nodes adopt the partial covertness strategy to hide the transmission in either hop. In the FRI case, the legitimate nodes apply the complete covertness strategy, as W is interested in all hops.

To illustrate the overall scheme for the covert communication of legitimate nodes, we take the four-slot transmission scenario as an example case. In the four-slot scenario, the legitimate nodes will employ the complete covertness strategy if they are ignorant or they are smart and the detector uses the blind detection scheme in the PRI and FRI case. This means that A needs to hide its transmission to the relay R in the first slot and R needs to hide its transmission to B in the second slot as well. Similarly, during the transmission from B to A in the remaining two slots, both B and R needs to hide their transmissions. If the legitimate nodes are smart and the detector is in the URI case, they will employ the selective covertness strategy. Based on the strategy, A needs to hide its transmission to R in the first slot, while R does not need to hide its transmission to B in the second slot. Similarly, B needs to hide its transmission to R in the third slot while R does not need to do so in the last slot. If the legitimate nodes are smart and know that the detector uses the cautious detection scheme, they will apply the partial covertness strategy in two ways. The first way is that A and R hide their transmissions in the first and fourth slots respectively, leaving the transmissions in other slots unhidden. The second is that R

and B hide their transmissions in the second and third slots respectively, leaving the other transmissions unhidden.

3.3 Covert Throughput Performance Analysis in Four-Slot Scenario

In this section, we theoretically analyze the covert throughput of the considered system in four-slot scenario for the cases of ignorant and smart legitimate nodes, respectively.

3.3.1 Ignorant Legitimate Nodes Case

For the ignorant legitimate nodes case, the prior knowledge and the detection schemes of detector are not available at the legitimate nodes. To reduce the detection probability of detector and ensure the covert wireless communication between the two sources, A, B and R will adopt the complete covertness strategy to hide the transmission in every hop, as can be seen in Table 3.1. The detector W, however, will employ the blind detection scheme to detect the existence of transmissions as much as possible. As assumed in Section 3.2.1, the detector independently detects the transmission in each time slot. Thus, it is sufficient to ensure covert transmission in each time slot so as to guarantee the covertness of the overall communication. Here, we take the transmission in the first time slot as an example to show how the covert throughput can be theoretically analyzed.

Using the blind scheme, W will observe the signal vector $\mathbf{y}_{A,W}$ in the first time slot, as introduced in Section 3.1.2. After receiving the vector $\mathbf{y}_{A,W}$, W will randomly select a sample with index $i = 1, 2, \cdots, n$ from $\mathbf{y}_{A,W}$ to detect whether the transmission in this time slot occurs by applying the hypothesis test. Thus, the signals correspond

to the hypothesis $\mathcal{H}_1$ and $\mathcal{H}_0$ are

$$\begin{cases} \mathcal{H}_1 : Y_{A,W}^{(i)} = X_A^{(i)} + Z_W^{(i)} \\ \mathcal{H}_0 : Y_{A,W}^{(i)} = Z_W^{(i)}, \end{cases} \tag{3.5}$$

where $X_A^{(i)} \sim \mathcal{N}(0, S_A)$ is the transmitted message signal and $Z_W^{(i)} \sim \mathcal{N}(0, \sigma_W^2)$ is AWGN at W. We use P_0 and P_1 to denote the probability distributions of the sampled signals $Y_{A,W}^{(i)}$ in $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively. Thus, we have $P_0 = \mathcal{N}(0, \sigma_W^2)$ and $P_1 = \mathcal{N}(0, \sigma_W^2 + S_A)$.

To ensure covert wireless communication, two conditions must be satisfied: 1) the detection probability of detector must be lower than an arbitrarily small constraint; 2) the transmitted symbols must be recovered successfully at the receiver. To satisfy Condition 1), the detection error probability at the detector ξ should follow [71]

$$\xi = p_{FA} + p_{MD} \geq 1 - \epsilon, \text{ for any } \epsilon > 0, \tag{3.6}$$

where p_{FA} and p_{MD} are probabilities of false alarm and missed detection, respectively. It's notable that in (3.6) a larger $1 - \epsilon$ means a stricter constraint on the detection performance at detector, what is more difficult to satisfy. Given P_0 and P_1, we can determine the detection probability regarding the vector of n real-valued symbols at W in the first time slot as [94]

$$\xi = p_{FA} + p_{MD} = 1 - V_T(P_0^n, P_1^n), \tag{3.7}$$

where $V_T(P_0^n, P_1^n) = \frac{1}{2} \left\| P_0^n - P_1^n \right\|_1$ is the function of total variance distance between two probability measures, P_0^n and P_1^n denote the probability measures related to the vector $\mathbf{y}_{A,W}$, and $\|\cdot\|_1$ is the $\mathcal{L}_1$ norm. As mentioned in Section 3.2.1, a smaller ξ means a better detection performance at W. Therefore, to improve the detection

performance, W will attempt to reduce the value of ξ, while the legitimate nodes will try to increase the detection probability of W.

To determine the total variation metric, we adopt in this work the relative entropy by Pinsker's inequality as in [95] and calculate the total variance distance as

$$V_T(P_0^n, P_1^n) \leq \sqrt{\frac{1}{2} D(P_0^n \| P_1^n)}, \tag{3.8}$$

where $D(P_0^n \| P_1^n)$ denotes the relative entropy (also known as Kullback-Leibler (KL) divergence [95]) to measure how probability distribution P_1^n is different from P_0^n, and thus

$$D(P_0^n \| P_1^n) = \frac{n}{2} \left[\ln \left(\frac{S_A + \sigma_W^2}{\sigma_W^2} \right) - \frac{S_A}{S_A + \sigma_W^2} \right]. \tag{3.9}$$

To calculate the approximate value in (3.9), based on the Taylor's Theorem [96] and the Lagrange Remainder [97], if $S_A \leq \frac{2\sqrt{2}\epsilon f(n)}{\sqrt{n}}$ for any $\epsilon > 0$ and function $f(n) = \mathcal{O}(1)$, the $V_T(P_0^n, P_1^n)$ in the first time slot can be given as

$$V_T(P_0^n, P_1^n) \leq \sqrt{\frac{n}{2} \cdot \frac{(S_A)^2}{4\sigma_W^4}} \leq \frac{\epsilon f(n)}{\sigma_W^2}. \tag{3.10}$$

From (3.10) we can observe that, if A knows σ_W^2, he can set $f(n) = \hat{\sigma}_W^2$ ($\hat{\sigma}_W^2 \leq \sigma_W^2$) such that

$$V_T(P_0^n, P_1^n) \leq \epsilon. \tag{3.11}$$

In fact, however, the constant σ_W^2 is not available at A. In this case, A can set $f(n) = o(1)$ [98], and the same result can be obtained. By doing this limitation, the detection performance of W is limited and the transmission between A and R is unperceivable, which satisfies the requirement of covert wireless communication in (3.6).

To satisfy Condition 2), the average decoding error probability $\mathbf{P}^{(e)}$ at the receiver

should follow

$$\mathbf{P}^{(e)} \to 0. \tag{3.12}$$

With help of the theoretical analysis in [71, 99], we can obtain that the $\mathbf{P}^{(e)}$ at R over all 2^M possible codewords is $\mathbf{P}^{(e)} = \mathbf{E}_{c_k}\left[P(\cup_{i=1,i\neq k}^{2^M} E_i(c_k))\right]$, where $\mathbf{E}_X[\cdot]$ is the expectation operator over random variable X, and $P(\cdot)$ denotes the probability function. It's notable that the decoding error probabilities are represented as the sum of the error probabilities of every decoding event. As for one error event, $E_i(c_k)$ represents the error event when the received codeword c_k at W is similar to another codeword c_i $(i \neq k)$. Moreover, it has been proved in [71, 99] that, if the variable S_A equals $\frac{2\sqrt{2}\epsilon f(n)}{\sqrt{n}}$, i.e., the upper bound of the power of the transmitted signal, a decoding error probability approaching 0, as in (3.12), can be guaranteed.

Following the theoretical analysis in [4, 71] , the maximum number of bits in the first time slot is obtained as $M_1 = \frac{2\sqrt{2n}\theta\epsilon f(n)}{4\sigma_R^2 \ln 2}$ when the channel uses n is large enough [4, 71], which ensuring constraints on the detection probability and decoding error probability in (3.6) and (3.12), respectively. With the help of result in the first time slot, we can similarly derive the maximum number of bits in the second time slot as $M_2 = \frac{2\sqrt{2n}\theta\epsilon f(n)}{4\sigma_B^2 \ln 2}$, and in last two time slots as $M_3 = M_1$ and $M_4 = \frac{2\sqrt{2n}\theta\epsilon f(n)}{4\sigma_A^2 \ln 2}$ by replacing $X_A^{(i)}$ with $X_B^{(i)}$ in (3.5) and replacing S_A with S_B in (3.9) and (3.10), respectively.

Based on the analysis above we can see that if complete covertness strategy is employed at A, B and R, the covert throughput for the four-slot relaying system is [100]

$$M_{A,B} = \min\left(M_1, M_2, M_3, M_4\right). \tag{3.13}$$

Applying the covert throughput $M_{A,B}$, A and B can covertly communicate to each other when the total detection error at W satisfies $\xi \geq 1-\epsilon$ and the detection probability is thus less than ϵ. Moreover, when the constant $\epsilon > 0$, $M_{A,B} = o(\sqrt{n})$ as

$n \to \infty$. If $f(n) = \hat{\sigma}_W^2$, $M_{A,B}$ can be improved to $\mathcal{O}(\sqrt{n})$ as $n \to \infty$ [101].

3.3.2 Smart Legitimate Nodes Case

For smart legitimate nodes case, the legitimate nodes know the prior knowledge of the detector W. As assumed in Section 3.1.1, the prior knowledge of W includes both its detection schemes (i.e., blind detection or cautious detection) and his prior knowledge about the relay node R (i.e., unknown relay information (URI), partial relay information (PRI) and full relay information (FRI)).

3.3.2.1 URI Case

In URI case, the detector W does not know the existence of the relay R due to that W cannot receive signals from R. To improve the detection probability, W will adopt the blind detection scheme to detect the existence of transmission at either A or B as much as possible without caring about making wrong detections. Based on the prior knowledge of W, the legitimate nodes, however, will employ the selective covertness strategy to hide the transmission when A and B transmit, making it difficult for W to detect the transmission in either hop.

By applying the blind detection scheme, W will receive signal vectors $\mathbf{y}_{A,W}$, $\mathbf{y}_{R(A),W}$, $\mathbf{y}_{B,W}$ and $\mathbf{y}_{R(B),W}$ in four time slots, respectively. According to the assumptions of four-slot transmission scheme (as described in Section 3.1.2) and the URI case, W observes the symbols from A or B and his background noise when A and B transmit, while receiving only his background noise when R transmits as W is not within the transmission range of R. With all these information, in the first and third time slots, the received signals at W when two hypotheses are true are given similar as in (3.5). However, in the second time slot, the received signals corresponding to

W's two hypotheses are

$$\begin{cases} \mathcal{H}_1 : Y_{R(A),W}^{(i)} = Z_W^{(i)} \\ \mathcal{H}_0 : Y_{R(A),W}^{(i)} = Z_W^{(i)}. \end{cases} \tag{3.14}$$

The received signals $Y_{R(B),W}^{(i)}$ in the fourth time slot is same as (3.14). Thus, legitimate nodes only need to ensure that the transmission in the first and third time slots are hidden.

Based on the hypothesis $\mathcal{H}_0$ and $\mathcal{H}_1$ of W in the first (resp. third) time slot, we can then give the probability distributions P_0 and P_1 as $P_0 = \mathcal{N}(0, \sigma_W^2)$ and $P_1 = \mathcal{N}(0, \sigma_W^2 + S_A)$ (resp. $P_1 = \mathcal{N}(0, \sigma_W^2 + S_B)$). Combining the assumptions of the four-slot transmission scheme and the similar theoretical analysis in Section 3.3.1, A and B can covertly transmit information as the transmission bits in the first and third time slots are limited as $M_1 = M_3 = \frac{2\sqrt{2n}\theta\epsilon f(n)}{4\sigma_R^2 \ln 2}$. Thus, we can finally conclude that, when legitimate nodes employ the selective covertness strategy over four-slot transmission scheme for a blind detector, the covert wireless communication can be achieved as the covert throughput between the legitimate nodes is

$$M_{A,B} = \min\left(M_1, M_3\right), \tag{3.15}$$

which meets the scaling law of $\mathcal{O}(\sqrt{n})$.

3.3.2.2 PRI Case

Different from URI case where selective covertness strategy is always selected by legitimate nodes, legitimate nodes in PRI case can choose the complete covertness strategy or partial covertness strategy when the blind detection or cautious detection is employed at the detector W, respectively. For blind detection at W, legitimate nodes employ complete covertness strategy against the detection of W to achieve the covert wireless communication, and the covert throughput in this case is the same as

that in ignorant legitimate nodes case as in (3.13).

If cautions detection scheme is selected by W who knows the existence of relay R but is not sure whether R is involved in the communication or not, legitimate nodes employ the partial covertness strategy to hide transmission in either link A-R or link R-B. Thus, the number of bits transmitted over the A-R or R-B link should satisfy the requirement of covert wireless communication. Moreover, the detector W observes the signal in each time slot and detects existence of transmission between A and B. W will observe signals $\mathbf{y}_{A,W}$, $\mathbf{y}_{R(A),W}$, $\mathbf{y}_{B,W}$ and $\mathbf{y}_{R(B),W}$ in four time slots, respectively. Applying the partial covertness strategy, legitimate nodes will hide the transmission in either the first and fourth or the second and third time slots to achieve covert wireless communication between A and B. Thus, the received signals in the first two time slots at W when hypothesis $\mathcal{H}_0$ and $\mathcal{H}_1$ are true are similar as in (3.5), while replacing $X_A^{(i)}$ in (3.5) with $X_B^{(i)}$ in the last two time slots.

The probability distribution metrics P_0 and P_1 as above are denoted as $P_0 = \mathcal{N}(0, \sigma_W^2)$ and $P_1 = \mathcal{N}(0, \sigma_W^2 + S_A)$ in the first two time slots, while replacing S_A with S_B in the last two time slots. Applying the partial covertness strategy, legitimate nodes will limit the maximum number of bits either in the first and fourth time slots or in the second and third time slots to decrease the detection probability of W. In each time slot, the analysis of maximum number of bits is same as that for ignorant legitimate nodes case in this section. Therefore, A and B can covertly transmit information with $V_T(P_0^n, P_1^n) \leq \epsilon$ as either the first and fourth time slots or the second and third time slots are subject to the maximum number of bits limitation, which is $M_\tau = \frac{2\sqrt{2n}\theta\epsilon f(n)}{4\nu \ln 2}$ (denoted $\tau = 1, 2, 3, 4$ as the sequence of time slots), where $\nu = \sigma_R^2$, σ_B^2, σ_R^2 and σ_A^2 for M_1, M_2, M_3 and M_4, respectively. Finally, we can conclude that, if the partial covertness strategy is employed at legitimate nodes over four-slot transmission scheme, the legitimate nodes only need to hide the transmission either

in link A-R or R-B, and the covert throughput is

$$M_{A,B} = \max\left(\min\left(M_1, M_4\right), \min\left(M_2, M_3\right)\right). \tag{3.16}$$

Similarly, by using asymptotically notation, covert wireless communication over four-slot transmission scheme for the partial covertness strategy can be achieved between legitimate nodes as the scaling law of the covert throughput is $\mathcal{O}(\sqrt{n})$.

3.3.2.3 FRI Case

Since the detector W knows the involvement of relay R in FRI case exactly, legitimate nodes will employ complete covertness strategy to hide their transmission. Based on the complete covertness strategy in FRI case, the analysis of the maximum number of bits for FRI case is same as that for ignorant legitimate nodes case (Section 3.3.1). According to the similar result of the covert throughput in (3.13), the total detection error at W will satisfy $\xi \geq 1 - \epsilon$, and the detection probability of W is less than ϵ. With this result, an arbitrarily small detection probability at detector means that he detects the existence of transmission with a low probability, and thus covert wireless communication over four-slot transmission can be achieved.

3.4 Covert Throughput Performance Analysis in Three-Slot Scenario

In this section, we will investigate the covert throughput of two-hop two-way covert wireless communication with three-slot relaying for both ignorant and smart legitimate nodes.

3.4.1 Ignorant Legitimate Nodes Case

Same as the assumptions for network with four-slot transmission in Section 3.3, ignorant legitimate nodes in network with three-slot transmission scheme do not have the prior knowledge about the detector W, and they employ complete covertness strategy to hide the transmission as much as possible. From Fig. 3.2 (b) we can observe that, the transmission processes of three-slot transmission scheme in the first two time slots are the same as that in the first and third time slots of the four-slot transmission scheme but differs in the third time slot. For wireless network adopting the three-slot transmission scheme, the relay R combines the received signals and broadcasts them to A and B simultaneously instead of transmitting them separately to A and B.

The detector W will receive signal vectors $\mathbf{y}_{A,W}$, $\mathbf{y}_{B,W}$ and $\tilde{\mathbf{y}}_{R,W}$ in three time slots, respectively. According to the observed signals and his background noise, W will distinguish and find out the existence of the transmission between A and B by applying the hypothesis test. Noting that the analysis for the first two slots are the same as that in four-slot transmission scenario, thus, the received signals at W corresponding to two hypotheses in the first two slots of three-slot transmission are similar as (3.5). Moreover, the received signals of W in the third time slot regarding his two hypotheses are

$$\begin{cases} \mathcal{H}_1 : \tilde{Y}_{R,W}^{(i)} = X_R^{(i)} + Z_W^{(i)} \\ \mathcal{H}_0 : \tilde{Y}_{R,W}^{(i)} = Z_W^{(i)}, \end{cases} \tag{3.17}$$

where $X_R^{(i)} = \rho_A X_A^{(i)} + \rho_B X_B^{(i)}$ denotes symbols transmitted from the relay R, and $Z_W^{(i)}$ denotes the background noise at W. Based on the results of $\mathcal{H}_0$ and $\mathcal{H}_1$ in (3.17), the probability distributions P_0 and P_1 can be given as $P_0 = \mathcal{N}(0, \sigma_W^2)$ and $P_1 = \mathcal{N}(0, \sigma_W^2 + \rho_A S_A + \rho_B S_B)$, respectively.

To decrease the sum of detection errors ξ, legitimate nodes limit the upper-bound

of transmission bits in each time slot to weaken the detection probability of W, such that covert wireless communication can be achieved between A and B. From (3.6) we can know that, A and B can covertly transmit as $V_T(P_0^n, P_1^n) \leq \epsilon$, which can be achieved by the maximum number of bits at A and B as

$$M_1 = M_2 = \frac{2\sqrt{2n}\theta\epsilon f(n)}{4\sigma_R^2 \ln 2}, \tag{3.18}$$

and at the relay R as

$$M_3 = \frac{2\sqrt{2n}\theta\epsilon f(n)}{4\ln 2(\rho_A\sigma_A^2 + \rho_B\sigma_B^2)}. \tag{3.19}$$

Thus, the covert throughput in the three-slot scenario to ensure covert wireless communication between A and B is

$$M_{A,B} = \min\left(M_1, M_2, M_3\right). \tag{3.20}$$

Based on the covert throughput in (3.20), legitimate nodes can hide the existence of transmission where total detection errors of W is $\xi \geq 1-\epsilon$, and detection probability of W less than ϵ. Similar to the results in Section 3.3.1, the covert throughput can also be asymptotically obtained as a scaling law of $\mathcal{O}(\sqrt{n})$.

3.4.2 Smart Legitimate Nodes Case

Same as the assumptions in Section 3.1.1, smart legitimate nodes know the prior knowledge of the detector, including his detection scheme and his prior knowledge of the relay (i.e., URI, PRI and FRI cases).

3.4.2.1 URI Case

Since blind detection scheme is adopted by the detector W in URI case and legitimate nodes employ the selective covertness strategy, the signals from the relay

R will not been considered because W is without the transmission range of R. Thus, the transmission bits are only limited in the first and second time slots. Noting that the theoretical analysis for the selective covertness strategy in the first and second time slots are the same as that in the four-slot scenario, the transmission bits for A and B are M_1 and M_2 respectively, where M_1 and M_2 are same as (3.18). Therefore, legitimate nodes can covertly communicate with each other as the covert throughput is given as

$$M_{A,B} = \min\left(M_1, M_2\right), \tag{3.21}$$

which meets the scaling law of $\mathcal{O}(\sqrt{n})$.

3.4.2.2 PRI Case

In PRI case, the detector W can choose between blind detection scheme and cautious detection scheme. If blind detection scheme is adopted by W, legitimate nodes will employ the complete covertness strategy as in PRI case for four-slot transmission scheme. In this case, the theoretical analysis and result of the covert throughput follow the same result as that in Section 3.3.

If cautious detection scheme is applied at W, the legitimate nodes will employ partial covertness strategy as they know the detection scheme of W in advance. To achieve covert wireless communication between A and B, the transmission need to be hidden either in link A-R and B-R or R-A,B. By applying the cautious detection scheme, W will receive signal vectors $\mathbf{y}_{A,W}$, $\mathbf{y}_{B,W}$ and $\tilde{\mathbf{y}}_{R,W}$ in three time slots, respectively. The received signals corresponding to the null hypothesis $\mathcal{H}_0$ and alternative $\mathcal{H}_1$ hypothesis in the first two time slots as (3.5) where replace $X_A^{(i)}$ with $X_B^{(i)}$ in the second time slot, while in the third time slot as (3.17).

Based on the similar theoretical analysis in Section 3.3.1, A and B can achieve covert wireless communication as $V_T(P_0^n, P_1^n) \leq \epsilon$ in either the first and second time slots or the third time slot. Therefore, legitimate nodes can covertly communicate

with each other if the covert throughput is

$$M_{A,B} = \max\left(\min\left(M_1, M_2\right), M_3\right), \tag{3.22}$$

where M_1 and M_2 are given in (3.18), as well as M_3 is given in (3.19). Similar to the results in Section 3.3, the covert throughput in PRI case is asymptotically given as the scaling law of $\mathcal{O}(\sqrt{n})$.

3.4.2.3 FRI Case

In FRI case, legitimate nodes employ complete covertness strategy as they know that the blind detection is used by detector. The covert throughput $M_{A,B}$ for FRI case is the same as that for the ignorant legitimate nodes case in this section as (3.20). The same as the asymptotically notation, we can finally find that the covert throughput of the considered two-way two-hop system with three-slot transmission scheme also follows the well-known square root scaling law as $\mathcal{O}(\sqrt{n})$.

3.5 Covert Throughput Performance Analysis in Two-Slot Scenario

In this section, we aim to conduct performance analysis for two-hop two-way covert wireless communication with two-slot relaying and derive the covert throughput for different legitimate nodes cases (i.e., ignorant legitimate node case and smart legitimate node case).

3.5.1 Ignorant Legitimate Nodes Case

For ignorant legitimate nodes, they do not know the prior knowledge about the detector W. To ensure covert wireless communication achieved between A and B, they choose complete covertness strategy to hide the transmission in the wireless

network. Different from the transmission in four-slot and three-slot scenarios, the two sources A and B transmit information to the relay R simultaneously in the first time slot. After receiving the signals, R decodes and broadcasts a combined vector of the signals from A and B to both sources in the second time slot.

W will receive signal vectors $\mathbf{y}_{(A,B),W}$ and $\hat{\mathbf{y}}_{R,W}$ in two time slots, respectively. The received signals at W corresponding to the null hypothesis $\mathcal{H}_0$ and alternative hypothesis $\mathcal{H}_1$ in the first time slot are

$$\begin{cases} \mathcal{H}_1 : Y_{(A,B),W}^{(i)} = X_A^{(i)} + X_B^{(i)} + Z_W^{(i)} \\ \mathcal{H}_0 : Y_{(A,B),W}^{(i)} = Z_W^{(i)}, \end{cases} \tag{3.23}$$

where the received signal $\hat{Y}_{R,W}^{(i)}$ in the second time slot is same as (3.23). $X_A^{(i)}$ and $X_B^{(i)}$ are transmitted symbols from A and B respectively, and $Z_W^{(i)}$ denotes the background noise at W. Based on the definition of hypothesis test, we can give the probability distributions P_0 and P_1 in each time slot as $P_0 = \mathcal{N}(0, \sigma_W^2)$ and $P_1 = \mathcal{N}(0, \sigma_W^2 + S_A + S_B)$, respectively.

According to the theoretical analysis in Section 3.3.1, two sources A and B can covertly transmit as $V_T(P_0^n, P_1^n) \leq \epsilon$, and the maximum number of bits for each time slot can be obtained, where M_1 in the first time slot is same as (3.18) and the second time slot M_2 is given by

$$M_2 = \frac{2\sqrt{2n}\theta\epsilon f(n)}{4 \ln 2(\sigma_A^2 + \sigma_B^2)}. \tag{3.24}$$

Therefore, the covert throughput for covert wireless communication with two-slot relaying is

$$M_{A,B} = \min\left(M_1, M_2\right), \tag{3.25}$$

which is asymptotically equal to the scaling law of $\mathcal{O}(\sqrt{n})$.

3.5.2 Smart Legitimate Nodes Case

3.5.2.1 URI Case

As selective covertness strategy is adopted by legitimate nodes in URI case, the transmission is hidden only in the first time slot when the sources A and B transmit information to the relay R. Therefore, the detector W can receive signals either his background noise (when A and B does not transmit) or his background noise and symbols from both A and B (when A and B transmit). During two time slots, W will receive the signal vectors $\mathbf{y}_{(A,B),W}$ and $\hat{\mathbf{y}}_{R,W}$, and the received signals corresponding to two hypotheses in the first time slot are same as (3.23), while in the second time slot are given by

$$\begin{cases} \mathcal{H}_1 : \hat{Y}_{R,W}^{(i)} = Z_W^{(i)} \\ \mathcal{H}_0 : \hat{Y}_{R,W}^{(i)} = Z_W^{(i)}, \end{cases} \tag{3.26}$$

where $Z_W^{(i)}$ is the background noise at W.

Because W cannot receive the signals from R in the second time slot, legitimate nodes just need to ensure that the transmission is hidden in the first time slot. Therefore, we can give the probability distributions P_0 and P_1 as $P_0 = \mathcal{N}(0, \sigma_W^2)$ and $P_1 = \mathcal{N}(0, \sigma_W^2 + S_A + S_B)$, respectively. Then, based on the requirements of covert wireless communication, A and B can covertly transmit information as $V_T(P_0^n, P_1^n) \leq \epsilon$, and the maximum number of bits M_1 in the first time slot as (3.18). Thus, the covert wireless communication between A and B can be achieved as the covert throughput is

$$M_{A,B} = M_1, \tag{3.27}$$

which meets the well-known scaling law as $\mathcal{O}(\sqrt{n})$.

3.5.2.2 PRI Case

As illustrated in Table 3.1, the detector W knows the existence of the relay R but is not sure whether it is involved in the communication or not in PRI case. To increase the detection performance, W may employ the blind detection scheme to observe signals from all possible transmitter. The legitimate nodes will choose the complete covertness strategy to hide every transmission to ensure covert wireless communication between two sources A and B. The analysis of the covert throughput in this case is the same as that in ignorant legitimate nodes case in this section.

Notice that the blind detection may increase the probability of making wrong detections at W as he asserts the existence of the transmission if he does in either hop of the transmission, W may employ cautious detection scheme to assert the existence of the transmission if he does in both hops of the transmission. To ensure covert wireless communication in this case, legitimate nodes will adopt partial covertness strategy to hide their transmissions either in link A-R and B-R or R-A and R-B. By employing the blind detection scheme, W will receive the signal vectors $\mathbf{y}_{(A,B),W}$ and $\hat{\mathbf{y}}_{R,W}$ respectively, and the received signals regarding two hypotheses in each time slot are same as (3.23). Based on the definition of hypothesis test, we can give the probability distributions P_0 and P_1 in each time slot as $P_0 = \mathcal{N}(0, \sigma_W^2)$ and $P_1 = \mathcal{N}(0, \sigma_W^2 + S_A + S_B)$.

According to the same theoretical analysis in Section 3.3.1, A and B can covertly transmit information as $V_T(P_0^n, P_1^n) \leq \epsilon$ in each time slot, which can be satisfied as the transmission bits for the first and second time slots are set as M_1 and M_2 respectively, where M_1 is given in (3.18) and M_2 is given in (3.24). Therefore, when considering the cautious detection scheme of W and the partial covertness strategy of legitimate nodes, covert wireless communication between two sources A and B can

be achieved as the covert throughput between legitimate nodes is

$$M_{A,B} = \max\left(M_1, M_2\right), \tag{3.28}$$

which can be asymptotically given as the scaling law of $\mathcal{O}(\sqrt{n})$.

3.5.2.3 FRI Case

In FRI case, legitimate nodes employ complete covertness strategy as they know that blind detection is used by detector. The theoretical analysis and result for FRI case are the same as that in ignorant legitimate nodes case in this section. Thus, we can obtain a similar covert throughput $M_{A,B}$ as the scaling law of $\mathcal{O}(\sqrt{n})$, with which covert wireless communication between two sources A and B can be achieved.

3.6 Discussion

In this chapter, our work mainly focuses on analyzing the asymptotic performance limits when the number of channel uses n tends to infinity. However, the results cannot be used to quantitatively evaluate the system performances via simulations. Thus, as one of our future works, we will consider some other system scenarios with parameters of finite values, like the background noise power of detector in [27], and derive exact closed-form results to enable the quantitative evaluation of system performances via simulations.

Regarding the comparison with previous methods, please notice that this is the first work that proposes covertness schemes for two-way two-hop relay systems. Thus, there are few previous methods in this regard. Due to this reason, the goal of this work is to investigate the performance limits for the two-way two-hop relay systems rather than compare our scheme with others or improve the performances of existing methods. Although there exist previous methods for other systems, like adding an

uninformed jammer node in a single-hop wireless network and employing a full-duplex receiver over fading channels, comparing them with our method may tell us little about which outperforms the others. We have shown that our schemes can achieve the result of $\mathcal{O}(\sqrt{n})$, which is the same as the well-known limit of the square root law in the literature. This shows that our schemes work as well as most existing methods. Of course, we can introduce some new ideas (e.g., increasing the uncertainty of detector about background noise and transmission time) into our schemes to improve this limit, but this requires a new and dedicated work, which is regarded as one of the future works.

3.7 Summary

This chapter investigated the performance of covert communication in a two-way two-hop wireless system. Covertness strategies were proposed and scaling law results for the covert throughput were derived for various scenarios with different relaying patterns (i.e., four-slot, three-slot and two-slot), and prior knowledge of the legitimate nodes and detector. The results in this work showed that the covert throughput of the concerned two-way two-hop wireless system follows the $\mathcal{O}(\sqrt{n})$ scaling law and is independent of the relaying patterns, detection schemes, covertness strategies, and prior knowledge of the sources and detector. In addition, most related works mainly focus on assuming static detectors, while an active detector can dynamically adjust his location to detect better [75]. Thus, a possible future research is to consider two-way two-hop wireless systems with the active detector.

CHAPTER IV

Covertness and Secrecy Guarantees in Wireless Communications with Passive Attackers

This chapter explores a new secure wireless communication paradigm where the physical layer security technology is applied to counteract both the detection and eavesdropping attacks, such that the critical covertness and secrecy properties of the communication are jointly guaranteed. We first provide theoretical modeling for covertness outage probability (COP), secrecy outage probability (SOP) and transmission probability (TP) to depict the covertness, secrecy and transmission performances of the paradigm. To understand the fundamental security performance under the new paradigm, we then define a new metric - covert secrecy rate (CSR), which characterizes the maximum transmission rate subject to the constraints of COP, SOP and TP. We further conduct detailed theoretical analysis to identify the CSR under various scenarios determined by the detector-eavesdropper relationships and the secure transmission schemes adopted by transmitters. Finally, numerical results are provided to illustrate the achievable performances under the new secure communication paradigm.

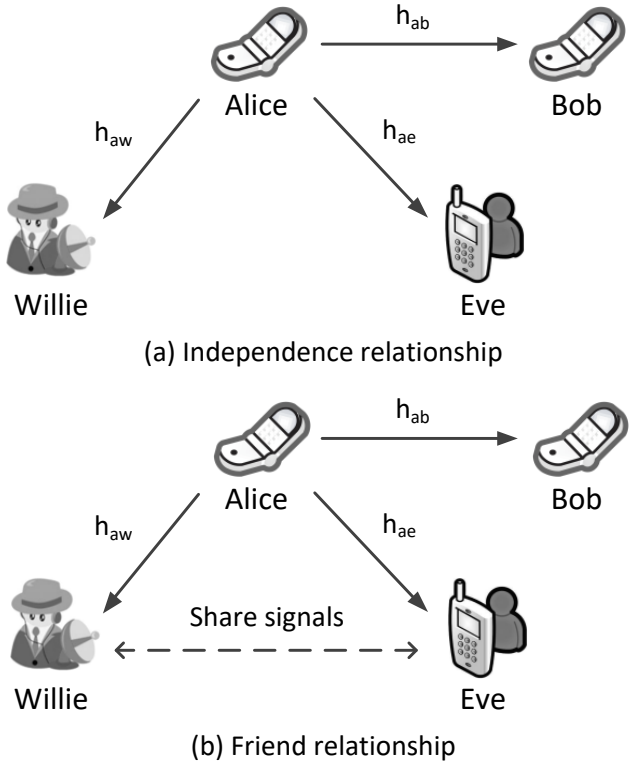


Figure 4.1: Two relationships between Willie and Eve.

4.1 New Paradigm and Security Metric

In this section, we first introduce the system model, the secure transmission schemes and the attacking model of the new secure wireless communication paradigm, and then define the covert secrecy rate as a novel metric in the proposed paradigm.

4.1.1 System Model

To demonstrate the new secure wireless communication paradigm, we consider a system (as illustrated in Fig. 4.1) where a transmitter Alice sends messages to a receiver Bob in the presence of a detector Willie and an eavesdropper Eve. Willie attempts to detect the existence of the signals transmitted from Alice, while Eve targets the messages contained in the signals. Alice and Bob operate in the half-duplex mode, while Willie and Eve can operate in the full-duplex mode. All nodes

are assumed to be equipped with a single omnidirectional antenna. For notation simplicity, we use a, b, e and w to represent Alice, Bob, Eve and Willie, respectively, throughout this chapter.

Time is divided into successive slots with the same duration that is long enough for Alice to transmit multiple symbols. To characterize the channels, we adopt the quasi-static Rayleigh fading channel model, where the channel coefficients remain constant in one slot and change independently from one slot to another at random. We use h_{ij} to denote the coefficient of the channel from i to j, where $i \in \{a, b, e, w\}$ and $j \in \{a, b, e, w\}$. As assumed in [19], the corresponding channel gain $|h_{ij}|^2$ follows the exponential distribution with unit mean. We assume that Alice and Bob know the *instantaneous* and *statistical* channel coefficient h_{ab} but only the *statistical* coefficients of other channels including those to Eve and Willie, such that the analysis of the covert secrecy rate provides meaningful theoretical performance results. We also assume that Eve knows the *instantaneous* channel coefficient h_{ae}, while Willie knows only the *statistical* channel coefficient of h_{aw} and h_{ew}. These assumptions are widely used in previous research related to physical layer security (PLS) and covert communication.

4.1.2 Secure Transmission Schemes

Alice employs two transmission schemes based on power control (PC) and artificial noise (AN), respectively. In the *PC-based scheme*, Alice controls her transmit power P_a in order to hide the message signals into the background noise to achieve covertness and secrecy. In the *AN-based scheme*, Alice intentionally injects AN into the message signals to confuse Willie and Eve so as to reduce their attack effects. Different from the PC-based scheme, in the AN-based scheme, Alice uses a constant transmit power (also denoted by P_a) and splits the power between message and noise transmissions. We use $\rho \in (0, 1]$ to denote the fraction of transmit power used for the message transmission. In addition to the strategies of transmit power, Alice also adopts the Wyner encoding

scheme [57] to resist the eavesdropping of Eve. To transmit a message, Alice chooses a target secrecy rate R_s for this message and another rate R_t for the whole transmitted symbol. The difference $R_t - R_s$ represents the rate sacrificed to confuse Eve.

The goal of Alice is to ensure a positive and *constant* secrecy rate R_s. Thus, Alice will send messages to Bob only when the instantaneous capacity C_b of the Alice-Bob channel can support the secrecy rate R_s (i.e., $C_b \geq R_s$). In this situation, Alice will set R_t arbitrarily close to C_b to cause as much confusion to Eve as possible, while ensuring reliable message transmission to Bob. Thus, the probability of Alice transmitting messages in a certain time slot can be defined as

$$p_{tx} = \mathbb{P}(C_b \geq R_s). \tag{4.1}$$

Note that the ***transmission probability*** **(TP)** p_{tx} can be interpreted as a metric to measure the transmission performance.

4.1.3 Attacking Model

In practice, Willie and Eve can belong to different organizations with unrelated or common goals, resulting in various relationships between them. In this work, we consider two representative relationships, i.e., *independence* and *friend*. As shown in Fig. 4.1, in the independence relationship, Eve and Willie care only about their own attack without helping or hindering the other. In the friend relationship, Willie and Eve will share their signals received from Alice to help improve the attack power of the other.

To detect the existence of signals transmitted from Alice in each slot, Willie adopts the commonly-used likelihood ratio test [23], in which he first determines a threshold θ and then measures the average power $\bar{P}_w$ of the symbols received from Alice in this slot. If $\bar{P}_w \geq \theta$, Willie accepts a hypothesis $\mathcal{H}_1$ that Alice transmitted messages to

Bob in this slot. If $\bar{P}_w \leq \theta$, Willie accepts a hypothesis $\mathcal{H}_0$ that Alice did not transmit messages. Formally, the likelihood ratio test can be given by

$$\bar{P}_w \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \theta. \tag{4.2}$$

In general, the likelihood test introduces two types of detection errors. One is called *false alarm*, which means that Willie reports a detected transmission whilst the transmission does not exist in fact. The other is called *missed detection*, which means that Willie reports no detected transmission whilst the transmission exists indeed. We use p_{FA} and p_{MD} to denote the probabilities of false alarm and missed detection, respectively. If neither false alarm nor missed detection occurs, the transmission from Alice to Bob is said to suffer from covertness outage. Thus, the ***covertness outage probability*** **(COP)** is given by

$$p_{co} = 1 - (p_{FA} + p_{MD}). \tag{4.3}$$

The smaller the COP is, the higher the covertness of the transmission is. Note that $1 - p_{co}$ can be interpreted as the detection error probability of Willie.

Compared with the detection of Willie, the eavesdropping attack of Eve is relatively simpler. To intercept the transmitted messages, Eve tries to decode the signals received from Alice. If Eve is able to recover the messages (i.e., the instantaneous secrecy capacity C_s [95] of the Alice-Bob channel falls below the target secrecy rate R_s), the transmission from Alice to Bob is said to suffer from secrecy outage. Note that secrecy outage occurs only when Alice actually transmits a message (i.e., $C_b \geq R_s$). Thus, we can define the ***secrecy outage probability*** **(SOP)** as the following conditional probability:

$$p_{so} = \mathbb{P}(C_s < R_s \mid C_b \geq R_s). \tag{4.4}$$

Similarly, the smaller the SOP is, the stronger the secrecy of the transmission is.

4.1.4 Covert Secrecy Rate

To understand the fundamental security performance under the new paradigm, we propose a novel metric, called ***covert secrecy rate*** **(CSR)**, by jointly considering the covertness, secrecy and transmission performances. The CSR is defined as the maximum transmission rate under which the constraints of COP, SOP and TP can be ensured. To obtain the CSR, we formulate two optimization problems for the PC-based and AN-based transmission schemes, respectively, which are given by

$$\textbf{P1 (PC-based):} \quad R_{cs} = \max_{P_a, R_s} R_s p_{tx}(P_a, R_s), \tag{4.5a}$$

$$\text{s.t.} \quad p_{co}(P_a) \leq \epsilon_c, \tag{4.5b}$$

$$p_{so}(R_s) \leq \epsilon_s, \tag{4.5c}$$

$$p_{tx}(P_a, R_s) \geq 1 - \epsilon_t, \tag{4.5d}$$

and

$$\textbf{P2 (AN-based):} \quad R_{cs} = \max_{\rho \in [0,1], R_s} R_s p_{tx}(\rho, R_s), \tag{4.6a}$$

$$\text{s.t.} \ p_{co}(\rho) \leq \epsilon_c, \tag{4.6b}$$

$$p_{so}(\rho, R_s) \leq \epsilon_s, \tag{4.6c}$$

$$p_{tx}(\rho, R_s) \geq 1 - \epsilon_t, \tag{4.6d}$$

where R_{cs} denotes the CSR, ϵ_c, ϵ_s and ϵ_t denote the constraints of COP, SOP and TP. Note that Problem P1 optimizes the transmission rate over the transmit power P_a and the secrecy rate R_s, while Problem P2 conducts the optimization over the power allocation parameter ρ and the secrecy rate R_s.

4.2 CSR Analysis: Independence Relationship Case

In this section, we investigate the CSR performance under the independence relationship case, for which we focus on the PC-based and AN-based transmission schemes in Subsections 4.2.1 and 4.2.2, respectively.

4.2.1 PC-Based Transmission Scheme

As mentioned in Section 4.1.2, Alice decides to transmit in a certain time slot only when the instantaneous capacity C_b of Alice-Bob channel can support the secrecy rate R_s. To do this, Alice measures the instantaneous channel coefficient $|h_{ab}|^2$ and determines the Alice-Bob channel capacity C_b based on the well-known Shannon Capacity formula [95], i.e.,

$$C_b = \log\left(1 + \frac{P_a|h_{ab}|^2}{\sigma_b^2}\right), \tag{4.7}$$

where log is to the base of 2. Since $|h_{ab}|^2$ is exponentially distributed, the transmission probability p_{tx} of Alice under the PC-based transmission scheme is

$$p_{tx}^{\mathrm{IP}}(P_a, R_s) = \mathbb{P}\left(C_b \geq R_s\right) = \exp\left(-\frac{(2^{R_s}-1)\sigma_b^2}{P_a}\right). \tag{4.8}$$

When Alice chooses to transmit, she sends n symbols to Bob, represented by a complex vector $\mathbf{x}$, where each symbol $\mathbf{x}[i]$ $(i = 1, 2, \cdots, n)$ is subject to the unit power constraint, i.e., $\mathbb{E}[|\mathbf{x}[i]|^2] = 1$. Thus, the signal vectors received at Bob, Willie and Eve are given by

$$\mathbf{y}_\kappa = \sqrt{P_a} h_{a\kappa}\mathbf{x} + \mathbf{n}_\kappa, \tag{4.9}$$

where the subscript $\kappa \in \{b, w, e\}$ stands for Bob, Willie or Eve, a represents Alice, and $\mathbf{n}_\kappa$ denotes the noise at κ with the i-th element $\mathbf{n}_\kappa[i]$ being the complex additive Gaussian noise with zero mean and variance σ_κ^2, i.e., $\mathbf{n}_\kappa[i] \sim \mathcal{CN}(0, \sigma_\kappa^2)$.

According to the detection scheme in Subsection 4.1.3, Willie makes a decision on the existence of transmitted signals based on the average power $\bar{P}_w$ of the received symbols $\mathbf{y}_w$. In this case, $\bar{P}_w$ is given by

$$\bar{P}_w = \frac{\sum_{i=1}^{n} |\mathbf{y}_w[i]|^2}{n} = \lim_{n\to\infty} (P_a|h_{aw}|^2 + \sigma_w^2)\chi_{2n}^2/n = P_a|h_{aw}|^2 + \sigma_w^2, \tag{4.10}$$

where χ_{2n}^2 is a chi-squared random variable with $2n$ degrees of freedom. By the Strong Law of Large Numbers [102], $\frac{\chi_{2n}^2}{n}$ converges in probability to 1 as n tends to infinity. If $\bar{P}_w \leq \theta$, Willie accepts the hypothesis $\mathcal{H}_0$ that Alice did not transmit messages, leading to a missed detection. Thus, the probability of missed detection p_{MD} can be given by

$$p_{MD} = \mathbb{P}\left(P_a|h_{aw}|^2 + \sigma_w^2 \leq \theta\right) = \begin{cases} 1 - \exp\left(-\frac{\theta - \sigma_w^2}{P_a}\right), & \theta > \sigma_w^2, \\ 0, & \theta \leq \sigma_w^2. \end{cases} \tag{4.11}$$

The eavesdropping result of Eve depends on the instantaneous secrecy capacity C_s of the Alice-Bob channel, which is the difference between the channel capacity of the Alice-Bob channel and that of the Alice-Eve channel [95]. Thus, C_s is formulated as

$$C_s = \log\left(1 + \frac{P_a|h_{ab}|^2}{\sigma_b^2}\right) - \log\left(1 + \frac{P_a|h_{ae}|^2}{\sigma_e^2}\right). \tag{4.12}$$

Note that $|h_{ab}|^2$ and $|h_{ae}|^2$ are random variables here. Based on the definition of the SOP in Subsection 4.1.3, the SOP under the PC-based scheme can be given by

$$\begin{aligned} p_{so}^{\mathrm{IP}}(R_s) &= \frac{\mathbb{P}\left(R_s < C_b < C_e + R_s\right)}{\mathbb{P}\left(C_b > R_s\right)} = 1 - \frac{\mathbb{P}\left(C_s > R_s\right)}{\mathbb{P}\left(C_b > R_s\right)} \\ &= 1 - e^{\frac{(2^{R_s}-1)\sigma_b^2}{P_a}} \mathbb{P}\left(\frac{P_a|h_{ab}|^2}{\sigma_b^2} - \frac{2^{R_s}P_a|h_{ae}|^2}{\sigma_e^2} > 2^{R_s} - 1\right) \\ &= \frac{2^{R_s}\sigma_b^2}{2^{R_s}\sigma_b^2 + \sigma_e^2}. \end{aligned} \tag{4.13}$$

When Alice does not transmit, security performance is not a concern and thus we only focus on the covertness performance. In this case, Willie receives only noise, i.e., $\mathbf{y}_w = \mathbf{n}_w$ and thus the average power $\bar{P}_w$ of the received symbols $\mathbf{y}_w$ is $\bar{P}_w = \sigma_w^2$. If $\bar{P}_w \geq \theta$, Willie accepts the hypothesis $\mathcal{H}_1$ that Alice transmitted messages, leading to a false alarm. Thus, the probability of false alarm p_{FA} is given by

$$p_{FA} = \mathbb{P}\left(\sigma_w^2 \geq \theta\right) = \begin{cases} 0, & \theta > \sigma_w^2, \\ 1, & \theta \leq \sigma_w^2. \end{cases} \tag{4.14}$$

Combining the p_{MD} in (4.11) and the p_{FA} in (4.14), we obtain the COP under the PC-based scheme as

$$p_{co}^{\mathrm{IP}}(P_a, \theta) = \begin{cases} \exp\left(-\frac{\theta - \sigma_w^2}{P_a}\right), & \theta > \sigma_w^2, \\ 0, & \theta \leq \sigma_w^2. \end{cases} \tag{4.15}$$

Note that the COP is identical for Alice and Willie, since they have the same knowledge about $|h_{aw}|^2$, i.e., the statistical $|h_{aw}|^2$. To maximize the COP p_{co}^{IP}, Willie will choose the optimal detection threshold θ, denoted by θ_{IP}^*. We can see from (4.15) that p_{co}^{IP} is a decreasing function of θ and is larger than or equal to 0 for $\theta > \sigma_w^2$. Thus, the optimal θ_{IP}^* exists in (σ_w^2, ∞) and is thus given by $\theta_{\mathrm{IP}}^* = \upsilon + \sigma_w^2$, where $\upsilon > 0$ is an arbitrarily small value.

Under the condition that Willie chooses the optimal detection threshold θ_{IP}^*, Alice solves the optimization problem in (4.5) to obtain the CSR. The main result is summarized in the following theorem.

Theorem IV.1 *Under the scenario where Willie and Eve are in the independence relationship and Alice adopts the PC-based secure transmission scheme, the CSR of*

the system can be given by

$$R_{cs}^{\mathrm{IP}}=\begin{cases}\frac{1}{\ln 2}\mathrm{W}_0\left(-\frac{\upsilon}{\sigma_b^2\ln\epsilon_c}\right)\exp\left(-\frac{1}{\mathrm{W}_0\left(-\frac{\upsilon}{\sigma_b^2\ln\epsilon_c}\right)}-\frac{\sigma_b^2\ln\epsilon_c}{\upsilon}\right), & R_{s,\mathrm{IP}}^{*}=R_{s,\mathrm{IP}}^{0}\leq\min\left\{R_{s,\mathrm{IP}}^{SOP},R_{s,\mathrm{IP}}^{TP}\right\},\\ \log\left(\frac{\sigma_e^2\epsilon_s}{(1-\epsilon_s)\sigma_b^2}\right)\exp\left(\frac{\left(\sigma_e^2\epsilon_s-(1-\epsilon_s)\sigma_b^2\right)\ln\epsilon_c}{(1-\epsilon_s)\upsilon}\right), & R_{s,\mathrm{IP}}^{*}=R_{s,\mathrm{IP}}^{SOP}\leq\min\left\{R_{s,\mathrm{IP}}^{0},R_{s,\mathrm{IP}}^{TP}\right\},\\ (1-\epsilon_t)\log\left(1+\frac{\upsilon\ln(1-\epsilon_t)}{\sigma_b^2\ln\epsilon_c}\right), & R_{s,\mathrm{IP}}^{*}=R_{s,\mathrm{IP}}^{TP}\leq\min\left\{R_{s,\mathrm{IP}}^{0},R_{s,\mathrm{IP}}^{SOP}\right\},\end{cases}\tag{4.16}$$

where

$$R_{s,\mathrm{IP}}^{SOP}=\log\left(\frac{\sigma_e^2\epsilon_s}{(1-\epsilon_s)\sigma_b^2}\right),\tag{4.17}$$

$$R_{s,\mathrm{IP}}^{TP}=\log\left(1-\frac{P_{a,\mathrm{IP}}^{*}\ln(1-\epsilon_t)}{\sigma_b^2}\right),\tag{4.18}$$

$$R_{s,\mathrm{IP}}^{0}=\frac{1}{\ln 2}\mathrm{W}_0\left(\frac{P_{a,\mathrm{IP}}^{*}}{\sigma_b^2}\right),\tag{4.19}$$

$\mathrm{W}_0(\cdot)$ *is the principal branch of Lambert's W function, and* $P_{a,\mathrm{IP}}^{*}=-\frac{\upsilon}{\ln\epsilon_c}$ *is the optimal transmit power.*

Proof 1 *As can be seen from* (4.5a)*, the optimal transmit power* P_a *and optimal target secrecy rate* R_s *are required to solve the optimization problem P1. We first derive the optimal* P_a*. It is easy to see from* (4.8) *and* (4.15) *that both* p_{tx}^{IP} *and* p_{co}^{IP} *monotonically increase as* P_a *increases. Thus, the covertness constraint in* (4.5b) *results in an upper bound on* P_a*, which is*

$$P_{a,\mathrm{IP}}^{\max}=-\frac{\upsilon}{\ln\epsilon_c},\tag{4.20}$$

and the TP constraint in (4.5d) *leads to a lower bound on* P_a*, which is*

$$P_{a,\mathrm{IP}}^{\min}=-\frac{(2^{R_s}-1)\sigma_b^2}{\ln(1-\epsilon_t)}.\tag{4.21}$$

Note that the inequality $P_{a,\mathrm{IP}}^{\min} \leq P_{a,\mathrm{IP}}^{\max}$ *must hold, which gives the following condition on* R_s*:*

$$R_s \leq \log\left(1 + \frac{\upsilon \ln(1-\epsilon_t)}{\sigma_b^2 \ln \epsilon_c}\right). \tag{4.22}$$

Since the objective function in (4.5a) *is an increasing function of* P_a*, the optimal* P_a *is the upper bound, i.e.,* $P_{a,\mathrm{IP}}^{*} = P_{a,\mathrm{IP}}^{\max}$*.*

Next, we derive the optimal R_s *by analyzing the feasible region of* R_s *and the monotonicity of the objective function with respect to* R_s*. We can see that as* R_s *increases,* p_{tx}^{IP} *in* (4.8) *monotonically decreases while* p_{so}^{IP} *in* (4.13) *monotonically increases. Thus, based on the constraints* (4.5c) *and* (4.5d)*, the regions of* R_s *for ensuring secrecy and transmission performances are* $[0, R_{s,\mathrm{IP}}^{SOP}]$ *and* $[0, R_{s,\mathrm{IP}}^{TP}]$ *with* $R_{s,\mathrm{IP}}^{SOP}$ *and* $R_{s,\mathrm{IP}}^{TP}$ *given by* (4.17) *and* (4.18)*, respectively. Note that* $R_{s,\mathrm{IP}}^{TP}$ *is obtained at* $P_a = P_{a,\mathrm{IP}}^{*} = -\frac{\upsilon}{\ln \epsilon_c}$ *and thus the region* $[0, R_{s,\mathrm{IP}}^{TP}]$ *is equivalent to* (4.22)*. Hence, the feasible region of* R_s *is* $[0, \min\{R_{s,\mathrm{IP}}^{SOP}, R_{s,\mathrm{IP}}^{TP}\}]$*. Taking the first derivative of the objective function in* (4.5a) *in terms of* R_s *gives*

$$\frac{\partial R_{cs}}{\partial R_s} = \left(1 - \frac{R_s 2^{R_s} \sigma_b^2 \ln 2}{P_a}\right) \exp\left(-\frac{(2^{R_s}-1)\sigma_b^2}{P_a}\right). \tag{4.23}$$

Solving $\frac{\partial R_{cs}}{\partial R_s} = 0$*, we can obtain the stationary point* $R_{s,\mathrm{IP}}^{0}$ *in* (4.19)*. We can see that the objective function is increasing over* $[0, R_{s,\mathrm{IP}}^{0})$ *and decreasing over* $[R_{s,\mathrm{IP}}^{0}, \infty)$*. This implies that if* $R_{s,\mathrm{IP}}^{0}$ *falls inside the feasible region of* R_s*, i.e.,* $R_{s,\mathrm{IP}}^{0} \leq \min\{R_{s,\mathrm{IP}}^{SOP}, R_{s,\mathrm{IP}}^{TP}\}$*, the optimal* R_s *is* $R_{s,\mathrm{IP}}^{*} = R_{s,\mathrm{IP}}^{0}$*. Otherwise, the optimal* R_s *is* $R_{s,\mathrm{IP}}^{*} = \min\{R_{s,\mathrm{IP}}^{SOP}, R_{s,\mathrm{IP}}^{TP}\}$*. Finally, substituting the optimal* P_a *and* R_s *into the objective function in* (4.5a) *completes the proof.*

4.2.2 AN-Based Transmission Scheme

Suppose Alice transmits, in addition to the message symbols, she will also inject AN, represented by a complex vector $\mathbf{z}$, where each symbol $\mathbf{z}[i]$ $(i = 1, 2, \cdots, n)$ is

subject to the unit power constraint, i.e., $\mathbb{E}[|\mathbf{z}[i]|^2] = 1$. Alice will use a fraction ρ of her transmit power P_a for message transmission and the remaining power for AN radiation. Thus, the signal vectors received at Bob will be given by

$$\mathbf{y}_b = \sqrt{\rho P_a} h_{ab} \mathbf{x} + \sqrt{(1-\rho) P_a} h_{ab} \mathbf{z} + \mathbf{n}_b. \tag{4.24}$$

Based on (4.24), Alice measures the instantaneous Alice-Bob channel capacity C_b as

$$C_b = \log \left(1 + \frac{\rho P_a |h_{ab}|^2}{(1-\rho) P_a |h_{ab}|^2 + \sigma_b^2} \right), \tag{4.25}$$

and decides to transmit when $C_b \geq R_s$. Thus, the transmission probability under the AN-based scheme can be given by

$$\begin{aligned} p_{tx}^{\mathrm{IA}}(\rho, R_s) &= \mathbb{P}\left(C_b \geq R_s\right) = \mathbb{P}\left(\frac{\rho P_a |h_{ab}|^2}{(1-\rho) P_a |h_{ab}|^2 + \sigma_b^2} \geq 2^{R_s} - 1 \right) \\ &= \exp\left(- \frac{(2^{R_s} - 1)\sigma_b^2}{\rho P_a - (2^{R_s} - 1)(1-\rho) P_a} \right). \end{aligned} \tag{4.26}$$

Next, we analyze the secrecy and covertness performances when Alice transmits messages. In this situation, the signal vectors received at Willie and Eve have the same form of that received at Bob, which are given by

$$\mathbf{y}_\kappa = \sqrt{\rho P_a} h_{a\kappa} \mathbf{x} + \sqrt{(1-\rho) P_a} h_{a\kappa} \mathbf{z} + \mathbf{n}_\kappa, \tag{4.27}$$

where the subscript $\kappa \in \{w, e\}$ stands for Willie or Eve. From (4.27), we can see that the average power $\bar{P}_w$ of the received symbols $\mathbf{y}_\kappa$ at Willie is the same as that given in (4.10). Thus, the probability of missed detection p_{MD} under the AN-based scheme can also be given by (4.11).

According to (4.27), the secrecy capacity C_s under the AN-based scheme can be

formulated as

$$C_s = \log\left(1 + \frac{\rho P_a |h_{ab}|^2}{(1-\rho)P_a|h_{ab}|^2 + \sigma_b^2}\right) - \log\left(1 + \frac{\rho P_a |h_{ae}|^2}{(1-\rho)P_a|h_{ae}|^2 + \sigma_e^2}\right). \tag{4.28}$$

Thus, following the definition of SOP in (4.4), we derive the SOP under the AN-based scheme as

$$\begin{aligned} p_{so}^{\mathrm{IA}}(\rho, R_s) &= 1 - \exp\left(\frac{(2^{R_s}-1)\sigma_b^2}{\rho P_a - (2^{R_s}-1)(1-\rho)P_a}\right) \\ &\quad \times \mathbb{P}\left(\frac{\rho P_a |h_{ab}|^2}{(1-\rho)P_a|h_{ab}|^2 + \sigma_b^2} - \frac{2^{R_s}\rho P_a |h_{ae}|^2}{(1-\rho)P_a|h_{ae}|^2 + \sigma_e^2} > 2^{R_s} - 1\right) \\ &= 1 - \exp\left(\frac{(2^{R_s}-1)\sigma_b^2}{\rho P_a - (2^{R_s}-1)(1-\rho)P_a} - \frac{(2^{R_s}+\rho-1)\sigma_b^2}{(1-2^{R_s})(1-\rho)P_a}\right) \\ &\quad \times \int_0^{\phi} \exp\left(\frac{\frac{(2^{R_s}+\rho-1)(1-(1-\rho)2^{R_s})\sigma_b^2\sigma_e^2}{(1-2^{R_s})(1-\rho)} - (2^{R_s}-1)\sigma_b^2\sigma_e^2}{(1-2^{R_s})(1-\rho)P_a^2 y + (1-(1-\rho)2^{R_s})P_a\sigma_e^2} - y\right) \mathrm{d}y, \end{aligned} \tag{4.29}$$

where $\phi = \frac{(1-2^{R_s}(1-\rho))\sigma_e^2}{(2^{R_s}-1)(1-\rho)P_a}$.

Finally, we analyze the covertness performance when Alice does not transmit messages. In this situation, Alice still generates AN to confuse Willie, which is different from the PC-based scheme. Thus, the signal vector $\mathbf{y}_w$ received by Willie consists of both the AN $\mathbf{z}$ and background noise, i.e.,

$$\mathbf{y}_w = \sqrt{(1-\rho)P_a} h_{aw}\mathbf{z} + \mathbf{n}_w. \tag{4.30}$$

In this case, the average power of the received symbols of Willie is $\bar{P}_w = (1-\rho)P_a|h_{aw}|^2 + \sigma_w^2$, and thus the probability of false alarm is given by

$$p_{FA} = \mathbb{P}\left((1-\rho)P_a|h_{aw}|^2 + \sigma_w^2 \geq \theta\right) = \begin{cases} \exp\left(-\frac{(\theta-\sigma_w^2)}{(1-\rho)P_a}\right), & \theta > \sigma_w^2, \\ 1, & \theta \leq \sigma_w^2. \end{cases} \tag{4.31}$$

Combining the p_{FA} in (4.31) and the p_{MD} in (4.11), we obtain the COP p_{co}^{IA} under

the AN-based scheme as

$$p_{co}^{\mathrm{IA}}(\rho,\theta)=\begin{cases}\exp\left(-\frac{(\theta-\sigma_w^2)}{P_a}\right)-\exp\left(-\frac{(\theta-\sigma_w^2)}{(1-\rho)P_a}\right), & \theta>\sigma_w^2,\\ 0, & \theta\leq\sigma_w^2.\end{cases} \tag{4.32}$$

We can see from (4.32) that the optimal detection threshold θ_{IA}^* for Willie exists when $\theta>\sigma_w^2$ and can be obtained by solving $\frac{\partial p_{co}^{\mathrm{IA}}}{\partial\theta}=0$. Thus, θ_{IA}^* is given by

$$\theta_{\mathrm{IA}}^*=\sigma_w^2+\frac{(\rho-1)P_a}{\rho}\ln(1-\rho). \tag{4.33}$$

By solving the optimization problem in (4.6) with $\theta=\theta_{\mathrm{IA}}^*$, we can obtain the CSR, which is given in the following theorem.

Theorem IV.2 *Under the scenario where Willie and Eve are in the independence relationship and Alice adopts the AN-based secure transmission scheme, the CSR of the system is*

$$R_{cs}^{\mathrm{IA}}=R_{s,\mathrm{IA}}^*(\rho_{\mathrm{IA}}^*)\exp\left(-\frac{(2^{R_{s,\mathrm{IA}}^*(\rho_{\mathrm{IA}}^*)}-1)\sigma_b^2}{\rho_{\mathrm{IA}}^*P_a-(2^{R_{s,\mathrm{IA}}^*(\rho_{\mathrm{IA}}^*)}-1)(1-\rho_{\mathrm{IA}}^*)P_a}\right), \tag{4.34}$$

where ρ_{IA}^* is the optimal power allocation parameter and $R_{s,\mathrm{IA}}^*$ is the optimal secrecy rate. Here, ρ_{IA}^* can be obtained by solving $p_{co}^{\mathrm{IA}}(\rho,\theta_{\mathrm{IA}}^*)=\epsilon_c$ with θ_{IA}^* given by (4.33). $R_{s,\mathrm{IA}}^*$ is given by

$$R_{s,\mathrm{IA}}^*(\rho_{\mathrm{IA}}^*)=\begin{cases}R_{s,\mathrm{IA}}^0(\rho_{\mathrm{IA}}^*), & R_{s,\mathrm{IA}}^*=R_{s,\mathrm{IA}}^0\leq\min\left\{R_{s,\mathrm{IA}}^{SOP},R_{s,\mathrm{IA}}^{TP}\right\},\\ R_{s,\mathrm{IA}}^{SOP}(\rho_{\mathrm{IA}}^*), & R_{s,\mathrm{IA}}^*=R_{s,\mathrm{IA}}^{SOP}\leq\min\left\{R_{s,\mathrm{IA}}^0,R_{s,\mathrm{IA}}^{TP}\right\},\\ R_{s,\mathrm{IA}}^{TP}(\rho_{\mathrm{IA}}^*), & R_{s,\mathrm{IA}}^*=R_{s,\mathrm{IA}}^{TP}\leq\min\left\{R_{s,\mathrm{IA}}^0,R_{s,\mathrm{IA}}^{SOP}\right\},\end{cases} \tag{4.35}$$

where the stationary point $R_{s,\mathrm{IA}}^0$ can be obtained by solving $\frac{\partial R_{cs}}{\partial R_s}=0$, $R_{s,\mathrm{IA}}^{SOP}$ is the

solution of $p_{so}^{\mathrm{IA}}(R_s) = \epsilon_s$ *and* $R_{s,\mathrm{IA}}^{TP}$ *is given by*

$$R_{s,\mathrm{IA}}^{TP}(\rho_{\mathrm{IA}}^*) = \log\left(\frac{P_a \ln(1-\epsilon_t) - \sigma_b^2}{(1-\rho_{\mathrm{IA}}^*)P_a \ln(1-\epsilon_t) - \sigma_b^2}\right). \tag{4.36}$$

Proof 2 *The proof follows the same idea as the one for Theorem IV.1. The only difference is to derive the optimal power allocation parameter* ρ *instead of optimal transmit power* P_a*. Here, we focus on the derivation of the optimal* ρ *and omit the analysis of the optimal* R_s*. We can see that the objective function in* (4.6a) *is an increasing function of* ρ*, implying that the upper bound on* ρ *is needed. Substituting* $\theta = \theta_{\mathrm{IA}}^*$ *into* (4.32) *yields*

$$p_{co}^{\mathrm{IA}} = \rho(1-\rho)^{\frac{1-\rho}{\rho}}. \tag{4.37}$$

Taking the first derivative of (4.37) *in terms of* ρ*, we have*

$$\frac{\partial p_{co}^{\mathrm{IA}}}{\partial \rho} = \frac{-\ln(1-\rho)}{\rho}(1-\rho)^{\frac{1-\rho}{\rho}} > 0, \tag{4.38}$$

which shows that p_{co}^{IA} *is an increasing function of* ρ*. We can see from* (4.26) *and* (4.29) *that* p_{tx}^{IA} *is also an increasing function of* ρ*, while* ρ_{IA}^{SOP} *is a decreasing function. Thus, only the covertness constraint* (4.6b) *gives an upper bound* $\rho_{\mathrm{IA}}^{\max}$ *on* ρ*, while the TP and SOP constraints in* (4.6d) *and* (4.6c) *give two lower bounds* ρ_{IA}^{TP} *and* ρ_{IA}^{SOP} *respectively. Hence, the optimal* ρ *is* $\rho_{\mathrm{IA}}^* = \rho_{\mathrm{IA}}^{\max}$*. Note that* $\rho_{\mathrm{IA}}^{\max} \geq \max\left\{\rho_{\mathrm{IA}}^{TP}, \rho_{\mathrm{IA}}^{SOP}\right\}$ *must hold, which imposes a constraint (or region) on* R_s*. However, this region is equivalent to the one obtained from the TP and SOP constraints in* (4.6d) *and* (4.6c)*, and thus can be neglected in the analysis of optimal* R_s*.*

4.3 CSR Analysis: Friend Relationship Case

The CSR performance of the friend relationship case is investigated in this section, for which the CSR analyses for the PC-based and AN-based transmission schemes are

provided in Subsections 4.3.1 and 4.3.2, respectively. To depict the friend relationship, we interpret Willie and Eve as two antennas of a super attacker. This model is widely used to characterize the collusion among eavesdroppers [103].

4.3.1 PC-Based Transmission Scheme

Alice follows the same decision process as introduced in Section 4.2.1 to decide whether to transmit messages or not. Note that the instantaneous Alice-Bob channel capacity C_b in this case is identical to that in (4.7), which means that the transmission probability is also the same. Thus, the transmission probability p_{tx}^{FP} in the friend relationship scenario under the PC-based scheme is given by (4.8).

Next, we analyze the covertness and secrecy performances when Alice transmits messages. When Alice chooses to transmit a signal vector $\mathbf{x}$, Willie and Eve receive the same signal vectors $\mathbf{y}_w$ and $\mathbf{y}_e$ as that given in (4.9). Since Willie and Eve share their received signals in this case, the signal vectors received at Willie and Eve contain the one from the other side. Thus, based on the signal vector $\mathbf{y}_\kappa$ in (4.9), the average power of the received symbols at Willie can be given by $\bar{P}_w = \sum_{\kappa\in\{w,e\}} |\mathbf{y}_\kappa|^2 = P_a|h_{aw}|^2 + P_a|h_{ae}|^2 + \sigma_e^2 + \sigma_w^2$. Note that $|h_{aw}|^2$ and $|h_{ae}|^2$ are random variables for Willie. Thus, the probability of missed detection p_{MD} is given by

$$\begin{aligned} p_{MD} &= \mathbb{P}\left(P_a|h_{aw}|^2 + P_a|h_{ae}|^2 + \sigma_e^2 + \sigma_w^2 \le \theta\right) \\ &= \begin{cases} 1 - \frac{P_a+\theta-\sigma_e^2-\sigma_w^2}{P_a} \exp\left(-\frac{\theta-\sigma_e^2-\sigma_w^2}{P_a}\right), & \theta > \sigma_e^2 + \sigma_w^2, \\ 0, & \theta \le \sigma_e^2 + \sigma_w^2. \end{cases} \end{aligned} \tag{4.39}$$

According to [41], the signal sharing results in an improved Signal-to-Noise Ratio (SNR) for Eve, which is $\frac{P_a|h_{ae}|^2+P_a|h_{aw}|^2}{\sigma_e^2+\sigma_w^2}$. Thus, the secrecy capacity C_s is

$$C_s = \log\left(1 + \frac{P_a|h_{ab}|^2}{\sigma_b^2}\right) - \log\left(1 + \frac{P_a|h_{ae}|^2 + P_a|h_{aw}|^2}{\sigma_e^2 + \sigma_w^2}\right). \tag{4.40}$$

Since $|h_{ab}|^2$, $|h_{ae}|^2$ and $|h_{aw}|^2$ are independent, the SOP under the PC-based scheme is given by

$$\begin{aligned} p_{so}^{\mathrm{FP}}(R_s) &= 1 - \exp\left(\frac{(2^{R_s}-1)\sigma_b^2}{P_a}\right)\mathbb{P}\left(\frac{P_a|h_{ab}|^2}{\sigma_b^2} - 2^{R_s}\frac{P_a|h_{aw}|^2 + P_a|h_{ae}|^2}{\sigma_w^2+\sigma_e^2} > 2^{R_s}-1\right) \\ &= \frac{2^{R_s}\sigma_b^2(2^{R_s}\sigma_b^2 + 2\sigma_w^2 + 2\sigma_e^2)}{(2^{R_s}\sigma_b^2 + \sigma_w^2 + \sigma_e^2)^2}. \end{aligned} \tag{4.41}$$

Finally, we focus on the covertness performance when Alice suspends her transmission. Since the decision of suspending transmission is *unknown* to Willie and Eve, they still share their signals, which contain only background noises. Thus, the received signal at Willie is given by $\mathbf{y}_w = \mathbf{n}_e + \mathbf{n}_w$ and the average received power is $\bar{P}_w = \sigma_e^2 + \sigma_w^2$. Hence, the probability of false alarm p_{FA} can be given by

$$p_{FA} = \mathbb{P}\left(\sigma_e^2 + \sigma_w^2 \geq \theta\right) = \begin{cases} 0, & \theta > \sigma_e^2 + \sigma_w^2, \\ 1, & \theta \leq \sigma_e^2 + \sigma_w^2. \end{cases} \tag{4.42}$$

Combining the p_{FA} in (4.42) and the p_{MD} in (4.39), we obtain the COP as

$$p_{co}^{\mathrm{FP}}(P_a, \theta) = \begin{cases} \frac{P_a+\theta-\sigma_e^2-\sigma_w^2}{P_a}\exp\left(-\frac{\theta-\sigma_e^2-\sigma_w^2}{P_a}\right), & \theta > \sigma_e^2 + \sigma_w^2, \\ 0, & \theta \leq \sigma_e^2 + \sigma_w^2. \end{cases} \tag{4.43}$$

Taking the derivative of the p_{co}^{FP} in (4.43) gives

$$\frac{\partial p_{co}^{\mathrm{FP}}}{\partial \theta} = -\frac{\theta - \sigma_e^2 - \sigma_w^2}{P_a^2}\exp\left(-\frac{\theta-\sigma_e^2-\sigma_w^2}{P_a}\right). \tag{4.44}$$

This shows that p_{co}^{FP} is a decreasing function of θ when $\theta > \sigma_e^2 + \sigma_w^2$. Thus, the optimal detection threshold is

$$\theta_{\mathrm{FP}}^* = \upsilon + \sigma_e^2 + \sigma_w^2, \tag{4.45}$$

where $\upsilon > 0$ is an arbitrarily small value.

Given the θ^*_{FP}, the p_{tx} in (4.8), the SOP in (4.41) and the COP in (4.43), the problem in (4.5) can now be solved to obtain the CSR. The result is given in the following theorem.

Theorem IV.3 *Under the scenario where Willie and Eve are in the friend relationship and Alice adopts the PC-based secure transmission scheme, the CSR of the system is given by*

$$R_{cs}^{\mathrm{FP}} = \begin{cases} \frac{1}{\ln 2}\mathrm{W}_0\left(-\frac{\upsilon}{\left(1+\mathrm{W}_{-1}(-\frac{\epsilon_c}{\boldsymbol{e}})\right)\sigma_b^2}\right)\exp\left(-\frac{1}{\mathrm{W}_0\left(-\frac{\upsilon}{(1+\mathrm{W}_{-1}(-\frac{\epsilon_c}{\boldsymbol{e}}))\sigma_b^2}\right)}-\frac{\left(1+\mathrm{W}_{-1}(-\frac{\epsilon_c}{\boldsymbol{e}})\right)\sigma_b^2}{\upsilon}\right), \\ \qquad\qquad \textbf{if} \quad R^*_{s,\mathrm{FP}} = R^0_{s,\mathrm{FP}} \le \min\left\{R^{SOP}_{s,\mathrm{FP}}, R^{TP}_{s,\mathrm{FP}}\right\}, \\ \log\left(\frac{(1-\sqrt{1-\epsilon_s})(\sigma_w^2+\sigma_e^2)}{\sigma_b^2\sqrt{1-\epsilon_s}}\right)\exp\left(\frac{\left((1-\sqrt{1-\epsilon_s})(\sigma_w^2+\sigma_e^2)-\sqrt{1-\epsilon_s}\sigma_b^2\right)\left(1+\mathrm{W}_{-1}(-\frac{\epsilon_c}{\boldsymbol{e}})\right)}{\upsilon\sqrt{1-\epsilon_s}}\right), \\ \qquad\qquad \textbf{if} \quad R^*_{s,\mathrm{FP}} = R^{SOP}_{s,\mathrm{FP}} \le \min\left\{R^0_{s,\mathrm{FP}}, R^{TP}_{s,\mathrm{FP}}\right\}, \\ (1-\epsilon_t)\log\left(1+\frac{\upsilon\ln(1-\epsilon_t)}{\sigma_b^2\left(1+\mathrm{W}_{-1}\left(-\frac{\epsilon_c}{\boldsymbol{e}}\right)\right)}\right), \\ \qquad\qquad \textbf{if} \quad R^*_{s,\mathrm{FP}} = R^{TP}_{s,\mathrm{FP}} \le \min\left\{R^0_{s,\mathrm{FP}}, R^{SOP}_{s,\mathrm{FP}}\right\}. \end{cases} \tag{4.46}$$

Here,

$$R^{SOP}_{s,\mathrm{FP}} = \log\left(\frac{(1-\sqrt{1-\epsilon_s})(\sigma_w^2+\sigma_e^2)}{\sigma_b^2\sqrt{1-\epsilon_s}}\right), \tag{4.47}$$

$R^{TP}_{s,\mathrm{FP}}$ *and* $R^0_{s,\mathrm{FP}}$ *are the same as those given in* (4.18) *and* (4.19)*, respectively, with the optimal transmit power* $P^*_{a,\mathrm{FP}}$ *given by*

$$P^*_{a,\mathrm{FP}} = -\frac{\upsilon}{1+\mathrm{W}_{-1}(-\frac{\epsilon_c}{\boldsymbol{e}})}. \tag{4.48}$$

$\mathrm{W}_0(\cdot)$ *and* $\mathrm{W}_{-1}(\cdot)$ *are the principal branch and the non-principle branch of Lambert's W function, respectively, and* $\boldsymbol{e}$ *is Euler's number.*

Proof 3 *The proof is similar to that of Theorem IV.1 and thus omitted here.*

4.3.2 AN-Based Transmission Scheme

We first derive the transmission probability to characterize the transmission performance of the transmission. Suppose Alice transmits under the AN-based scheme, Bob will receive the same signal as that given in (4.27), yielding the same instantaneous Alice-Bob channel capacity C_b as that given in (4.25). This means that the transmission probability p_{tx}^{FA} under the AN-based scheme in the friend relationship scenario is identical to that in the independence scenario, which is given in (4.26).

We proceed to analyze the miss detection probability and SOP when Alice transmits messages. When Alice transmits a signal vector $\mathbf{x}$, the signal vectors at Willie and Eve are the same as that given in (4.27). After receiving the shared signals from Eve, the average power $\bar{P}_w$ of the received symbols at Willie is given by $\bar{P}_w = \sum_{\kappa\in\{w,e\}} |\mathbf{y}_\kappa|^2 = P_a|h_{ae}|^2 + P_a|h_{aw}|^2 + \sigma_e^2 + \sigma_w^2$, which is identical to (4.10), i.e., the average power in the independence case. Thus, the probability of missed detection p_{MD} can be given by (4.39).

After Eve receives the signals from Willie, the Signal-to-Noise-plus-Interference Ratio (SINR) is

$$\frac{\rho P_a|h_{ae}|^2 + \rho P_a|h_{aw}|^2}{(1-\rho)P_a|h_{ae}|^2 + (1-\rho)P_a|h_{aw}|^2 + \sigma_e^2 + \sigma_w^2}. \tag{4.49}$$

Thus, the secrecy capacity C_s under the AN-based scheme is

$$\begin{aligned} C_s = &\log\left(1 + \frac{\rho P_a|h_{ab}|^2}{(1-\rho)P_a|h_{ab}|^2 + \sigma_b^2}\right) \\ &- \log\left(1 + \frac{\rho P_a|h_{ae}|^2 + \rho P_a|h_{aw}|^2}{(1-\rho)P_a|h_{ae}|^2 + (1-\rho)P_a|h_{aw}|^2 + \sigma_e^2 + \sigma_w^2}\right). \end{aligned} \tag{4.50}$$

According to the definition in (4.4), the SOP is given by

$$
\begin{aligned}
p_{so}^{\mathrm{FA}}(\rho, R_s) &= 1 - \exp\left(\frac{(2^{R_s}-1)\sigma_b^2}{\rho_a - (2^{R_s}-1)(1-\rho)P_a}\right)\mathbb{P}\left(\frac{\rho P_a|h_{ab}|^2}{(1-\rho)P_a|h_{ab}|^2+\sigma_b^2}\right. \\
&\quad \left. -\frac{2^{R_s}(\rho P_a|h_{ae}|^2+\rho P_a|h_{aw}|^2)}{(1-\rho)P_a|h_{ae}|^2+(1-\rho)P_a|h_{aw}|^2+\sigma_e^2+\sigma_w^2} > 2^{R_s}-1\right) \\
&= 1 - \exp\left(\frac{(2^{R_s}-1)\sigma_b^2}{\rho P_a - (2^{R_s}-1)(1-\rho)P_a} - \frac{(2^{R_s}+\rho-1)\sigma_b^2}{(1-2^{R_s})(1-\rho)P_a}\right) \\
&\quad \times \int_0^{\frac{(1-2^{R_s}(1-\rho))(\sigma_w^2+\sigma_e^2)}{(2^{R_s}-1)(1-\rho)P_a}} \int_0^{\frac{(1-2^{R_s}(1-\rho))(\sigma_w^2+\sigma_e^2)}{(2^{R_s}-1)(1-\rho)P_a}-z} \exp\Bigg(- y - z \\
&\quad -\frac{(2^{R_s}-1)\sigma_b^2(\sigma_w^2+\sigma_e^2) - \frac{(2^{R_s}+\rho-1)(1-(1-\rho)2^{R_s})\sigma_b^2(\sigma_w^2+\sigma_e^2)}{(1-2^{R_s})(1-\rho)}}{(1-2^{R_s})(1-\rho)P_a^2(y+z)+(1-(1-\rho)2^{R_s})P_a(\sigma_w^2+\sigma_e^2)}\Bigg)\,\mathrm{d}y\,\mathrm{d}z.
\end{aligned} \tag{4.51}
$$

When Alice does not transmit messages, we consider only the covertness of the transmission by analyzing the probability of false alarm. In this case, Alice still sends AN to confuse Willie. Thus, based on (4.30), the signal vector $\mathbf{y}_w$ contains both the signals (i.e., AN and background noise) shared by Eve, AN and background noise. In this case, the average power of the received symbols at Willie is $\bar{P}_w = (1-\rho)P_a|h_{aw}|^2 + (1-\rho)P_a|h_{ae}|^2 + \sigma_e^2 + \sigma_w^2$. Thus, the probability of false alarm p_{FA} is given by

$$
\begin{aligned}
p_{FA} &= \mathbb{P}\left((1-\rho)P_a|h_{aw}|^2 + (1-\rho)P_a|h_{ae}|^2 + \sigma_e^2 + \sigma_w^2 \geq \theta\right) \\
&= \begin{cases} \left(1+\frac{\theta-\sigma_e^2-\sigma_w^2}{(1-\rho)P_a}\right)\exp\left(-\frac{\theta-\sigma_e^2-\sigma_w^2}{(1-\rho)P_a}\right), & \theta > \sigma_e^2+\sigma_w^2, \\ 1, & \theta \leq \sigma_e^2+\sigma_w^2. \end{cases}
\end{aligned} \tag{4.52}
$$

Combining the p_{FA} in (4.52) and the p_{MD} in (4.39), the COP can be given by

$$
p_{co}^{\mathrm{FA}}(\rho,\theta) = \begin{cases} \left(1+\frac{\theta-\sigma_e^2-\sigma_w^2}{P_a}\right)\exp\left(-\frac{\theta-\sigma_e^2-\sigma_w^2}{P_a}\right) \\ \quad -\left(1+\frac{\theta-\sigma_e^2-\sigma_w^2}{(1-\rho)P_a}\right)\exp\left(-\frac{\theta-\sigma_e^2-\sigma_w^2}{(1-\rho)P_a}\right), & \theta > \sigma_e^2+\sigma_w^2, \\ 0, & \theta \leq \sigma_e^2+\sigma_w^2. \end{cases} \tag{4.53}
$$

We can see from (4.53) that the optimal detection threshold $\theta_{\rm FA}^*$ can be obtained by solving $\frac{\partial p_{co}^{\rm FA}}{\partial \theta} = 0$, which is

$$\theta_{\rm FA}^* = \sigma_e^2 + \sigma_w^2 + \frac{2(\rho-1)P_a}{\rho}\ln(1-\rho). \tag{4.54}$$

Given the $\theta_{\rm FA}^*$ in (4.54), we solve the optimization problem in (4.6) to obtain the CSR, which is given in the following theorem.

Theorem IV.4 *Under the scenario where Willie and Eve are in the friend relationship and Alice adopts the AN-based secure transmission scheme, the CSR of the system is*

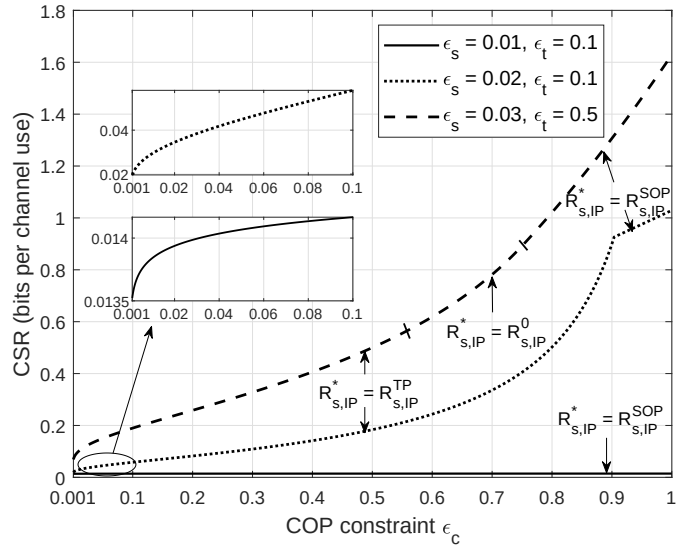
$$R_{cs}^{\rm FA} = R_{s,{\rm FA}}^*(\rho_{\rm FA}^*)\ \exp\left(-\frac{(2^{R_{s,{\rm FA}}^*(\rho_{\rm FA}^*)}-1)\sigma_b^2}{\rho_{\rm FA}^* P_a - (2^{R_{s,{\rm FA}}^*(\rho_{\rm FA}^*)}-1)(1-\rho_{\rm FA}^*)P_a}\right). \tag{4.55}$$

Here, the optimal power allocation parameter $\rho_{\rm FA}^*$ solves $p_{co}^{\rm FA}(\rho,\theta_{\rm FA}^*) = \epsilon_c$ with $\theta_{\rm FA}^*$ given by (4.54)*. The optimal secrecy rate $R_{s,{\rm FA}}^*$ is given in* (4.35)*, where $R_{s,{\rm FA}}^0$ can be obtained by solving $\frac{\partial R_{cs}}{\partial R_s} = 0$, $R_{s,{\rm FA}}^{SOP}$ is the solution of $p_{so}^{\rm FA}(R_s) = \epsilon_s$ and $R_{s,{\rm FA}}^{TP}$ is given in* (4.36)*.*

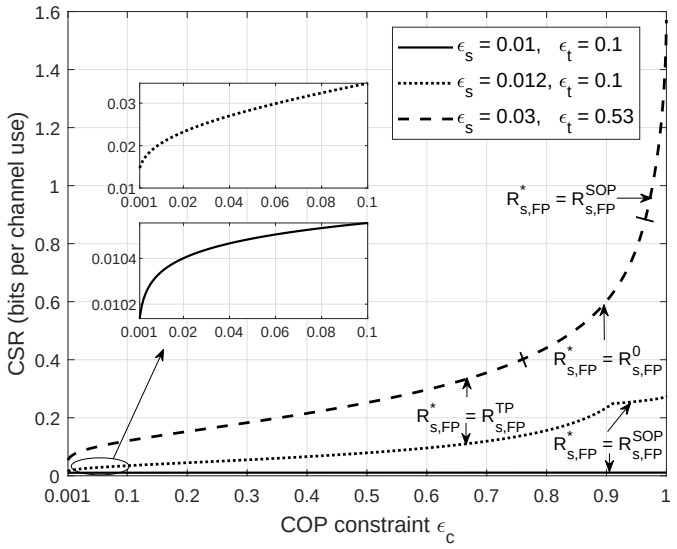
Proof 4 *The proof is similar to that of Theorem IV.2 and thus omitted here.*

4.4 Numerical Results

In this section, we provide extensive numerical results to illustrate the CSR performances of the four representative scenarios under the new secure communication paradigm. We also show the impacts of various system parameters (e.g., COP constraint ϵ_c, SOP constraint ϵ_s, TP constraint ϵ_t and transmit power P_a) on the CSR performance. Unless otherwise stated, we set the parameter υ to $\upsilon = 0.01$ and the noise powers at Bob, Willie and Eve to $\sigma_b^2 = -20$ dB and $\sigma_w^2 = \sigma_e^2 = 0$ dB.



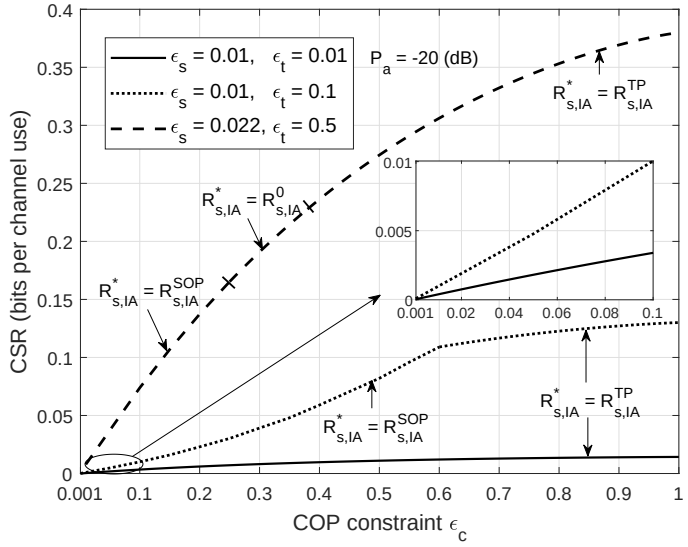
(a) Independence relationship scenario.



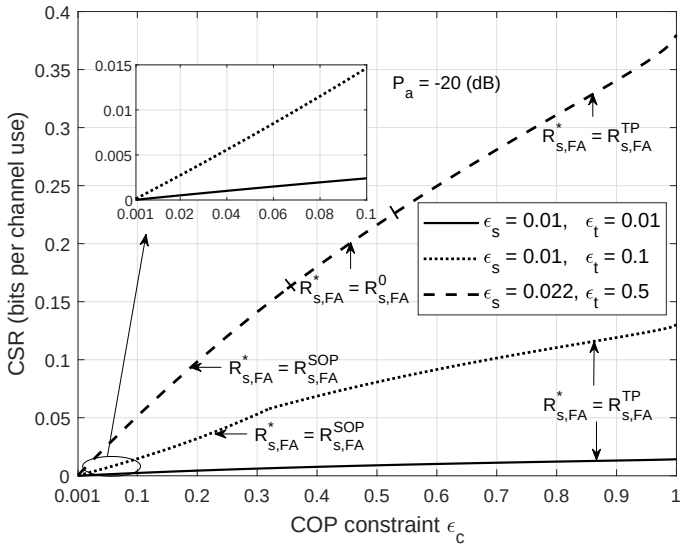
(b) Friend relationship scenario.

Figure 4.2: CSR R_{cs} vs. COP constraint ϵ_c (PC-based transmission scheme).

To explore the impact of the COP constraint ϵ_c on the CSR performance, we show in Fig. 4.2 R_{cs} vs. ϵ_c in the independence relationship case under the PC-based and AN-based transmission schemes, respectively. The results for the friend relationship case under both transmission schemes are presented in Fig. 4.3. We set the transmit power of Alice to $P_a = -20$ dB in Fig. 4.3. In each subfigure of Fig. 4.2 and Fig.



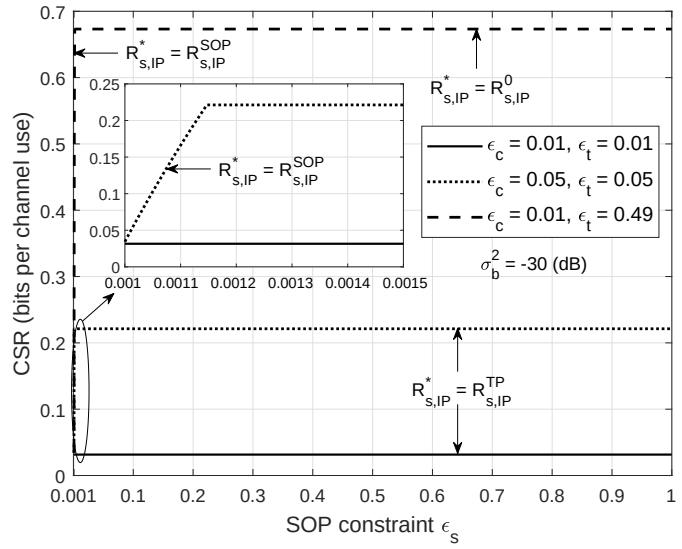
(a) Independence relationship scenario.



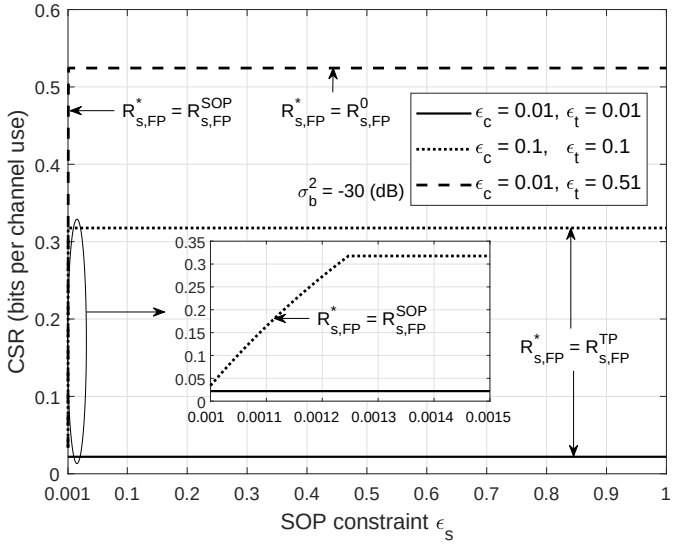
(b) Friend relationship scenario.

Figure 4.3: CSR R_{cs} vs. COP constraint ϵ_c (AN-based transmission scheme).

4.3, we also plot the CSR curves under different settings of SOP constraint ϵ_s and TP constraint ϵ_t. We can see from Fig. 4.2 and Fig. 4.3 that the CSRs achieved under different SOP and TP constraints always increase as ϵ_c increases. This is because a looser COP constraint results in a larger optimal transmit power in the PC-based scheme (resp. a larger optimal power allocation parameter in the AN-based scheme)



(a) Independence relationship scenario.

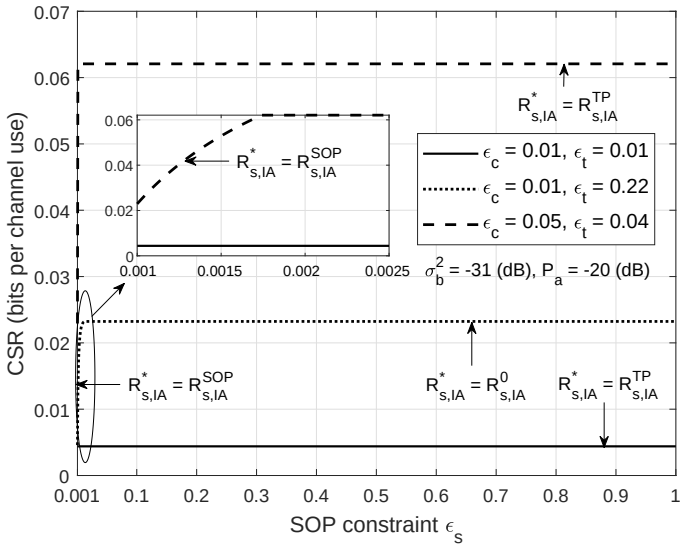


(b) Friend relationship scenario.

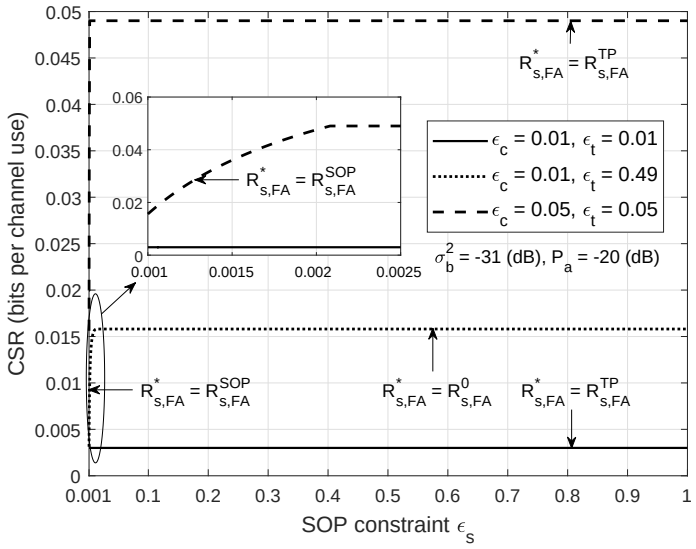
Figure 4.4: CSR R_{cs} vs. SOP constraint ϵ_s (PC-based transmission scheme).

and thus a larger CSR.

We can also observe from Fig. 4.2 and Fig. 4.3 that the shape of the CSR curve varies as the values of the SOP constraint ϵ_s and TP constraint ϵ_t change. For example, the CSR curve under the setting of $\epsilon_s = 0.03$ and $\epsilon_t = 0.5$ (dashed line) in Fig. 4.2 exhibits an exponential growth and that under the setting of $\epsilon_s = 0.02$ and



(a) Independence relationship scenario.



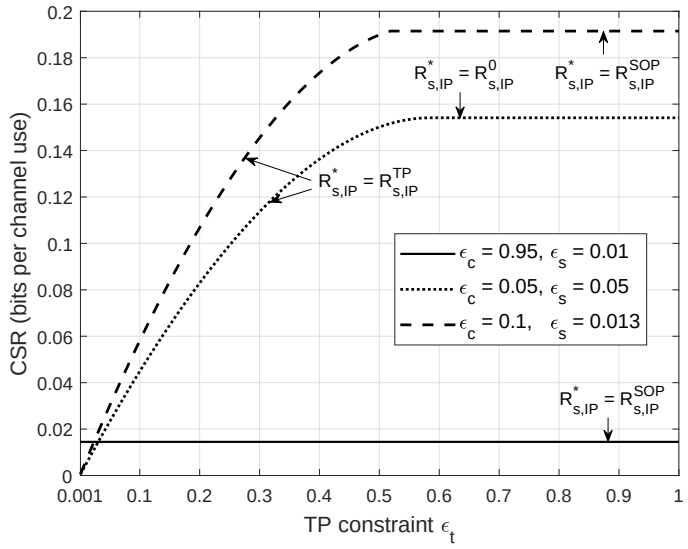
(b) Friend relationship scenario.

Figure 4.5: CSR R_{cs} vs. SOP constraint ϵ_s (AN-based transmission scheme).

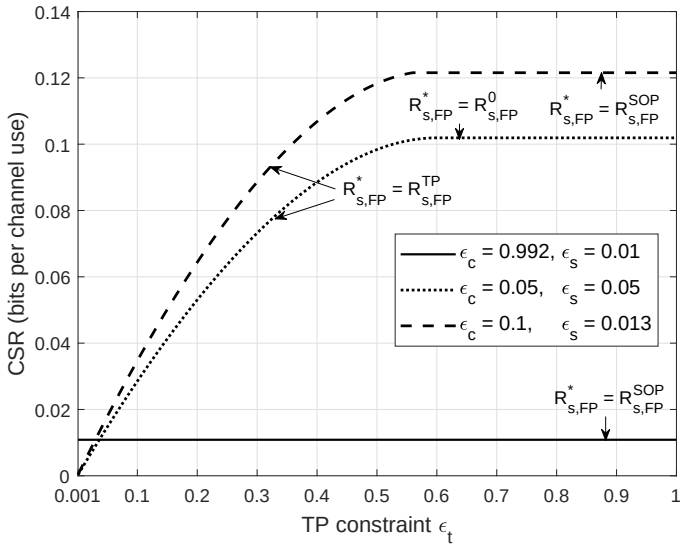
$\epsilon_t = 0.1$ (dotted line) grows in a piecewise fashion. This is because different values of ϵ_s, ϵ_t and the COP constraint ϵ_c result in different $R^{\rm SOP}_{s,\rm IP}$, $R^{\rm TP}_{s,\rm IP}$ and $R^0_{s,\rm IP}$ in (4.17-4.19) (resp. $R^{\rm SOP}_{s,\rm FP}$, $R^{\rm TP}_{s,\rm FP}$, $R^0_{s,\rm FP}$ in (4.47,4.18,4.19), $R^{\rm SOP}_{s,\rm IA}$, $R^{\rm TP}_{s,\rm IA}$, $R^0_{s,\rm IA}$ in (4.35) and $R^{\rm SOP}_{s,\rm FA}$, $R^{\rm TP}_{s,\rm FA}$, $R^0_{s,\rm FA}$ in (4.35)), which further lead to different optimal target secrecy rates (as labeled in Fig. 4.2 and Fig. 4.3) and thus different CSR curves.

Next, we investigate the impact of the SOP constraint ϵ_s on the CSR performance, for which we show R_{cs} vs. ϵ_s in the independence and friend relationship cases under the PC-based transmission scheme in Fig. 4.4 and those under the AN-based transmission scheme in Fig. 4.5. We set the noise power at Bob to $\sigma_b^2 = -30$ dB in Fig. 4.4 and that to $\sigma_b^2 = -31$ dB in Fig. 4.5. We set the transmit power of Alice to $P_a = -20$ dB in Fig. 4.5. For both figures, we consider three different settings of COP constraint ϵ_c and TP constraint ϵ_t, respectively. We can see from Fig. 4.4 and Fig. 4.5 that, when both ϵ_c and ϵ_t are relatively small (e.g., $\epsilon_c = 0.01$ and $\epsilon_t = 0.01$ in Fig. 4.4(a)), the CSR stays unchanged as the SOP constraint ϵ_s increases, which implies that the SOP constraint ϵ_s has no impacts on the CSR performance. This is because, in this situation, the CSR is achieved at only the optimal target secrecy rate $R_{s,\mathrm{IP}}^* = R_{s,\mathrm{IP}}^{\mathrm{TP}}$ (as labeled in Fig. 4.4(a)), which is independent of ϵ_s as can be seen from (4.18). On the other hand, when either ϵ_c or ϵ_t is large, the CSR first increases sharply and then remains constant as the SOP constraint ϵ_s increases. This is because the optimal target secrecy rate is $R_{s,\mathrm{IP}}^* = R_{s,\mathrm{IP}}^{\mathrm{SoP}}$ for small ϵ_s, which increases as ϵ_s increases, and then changes to $R_{s,\mathrm{IP}}^* = R_{s,\mathrm{IP}}^0$ or $R_{s,\mathrm{IP}}^* = R_{s,\mathrm{IP}}^{\mathrm{TP}}$ for large ϵ_s, which is independent of ϵ_s. Such phenomenon indicates that, when either ϵ_c or ϵ_t is large, the CSR is sensitive to the change of the SOP constraint ϵ_s in an extremely small region, e.g., from 0 to about 0.00115 in Fig. 4.4(a). Similar phenomena can be observed from Fig. 4.4(b), Fig. 4.5(a) and Fig. 4.5(b).

We now show the impact of the TP constraint ϵ_t on the CSR performance in Fig. 4.6 and Fig. 4.7, where we plot R_{cs} vs. ϵ_t for the two relationship cases under the PC-based and AN-based transmission schemes, respectively. Three different settings of COP constraint ϵ_c and SOP constraint ϵ_s are adopted for each subfigure in Fig. 4.6 and Fig. 4.7. We set the transmit power of Alice to $P_a = -20$ dB in Fig. 4.7. We can see from Fig. 4.6(a) that, if the COP constraint ϵ_c is much larger than the SOP constraint ϵ_s, the CSR stays constant as the constraint ϵ_t increases, i.e., the



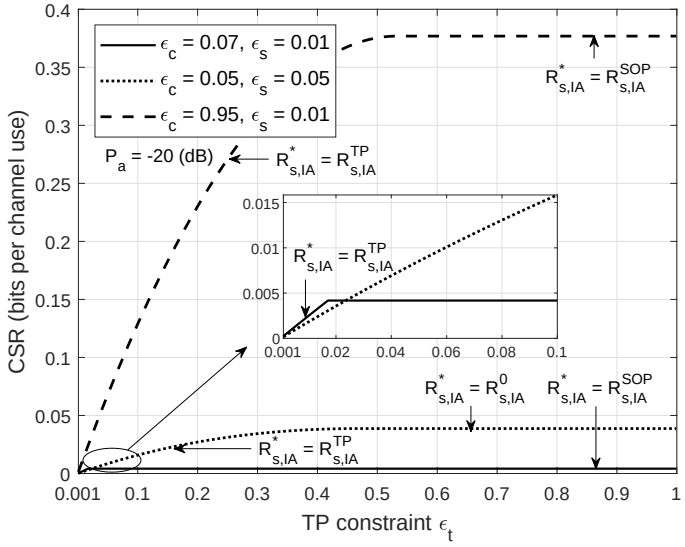
(a) Independence relationship scenario.



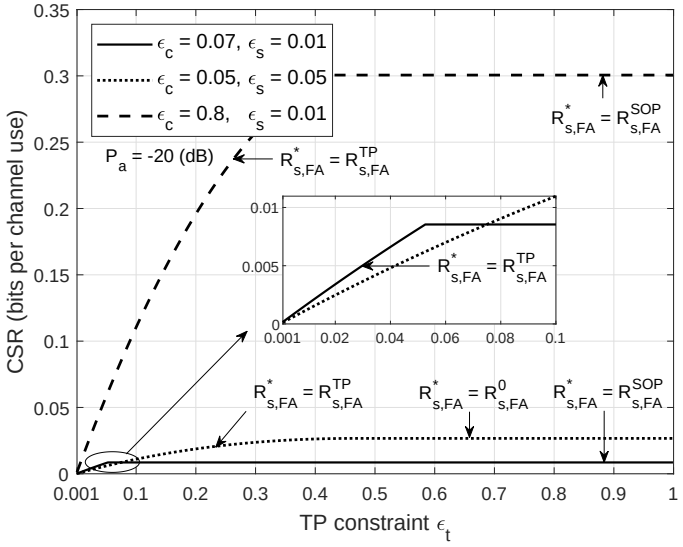
(b) Friend relationship scenario.

Figure 4.6: CSR R_{cs} vs. TP constraint ϵ_t (PC-based transmission scheme).

CSR is independent of ϵ_t. Otherwise, the CSR first increases and then stays constant as ϵ_t increases. This is because, for the former case, the CSR is achieved at only the optimal target secrecy rate $R^*_{s,\mathrm{IP}} = R^{\mathrm{SOP}}_{s,\mathrm{IP}}$ (as labeled in Fig. 4.6(a)), which is independent of ϵ_t as can be seen from (4.17). For the latter case, the optimal target secrecy rate is $R^*_{s,\mathrm{IP}} = R^{\mathrm{TP}}_{s,\mathrm{IP}}$ for small ϵ_t, which increases as ϵ_t increases, and then



(a) Independence relationship scenario.

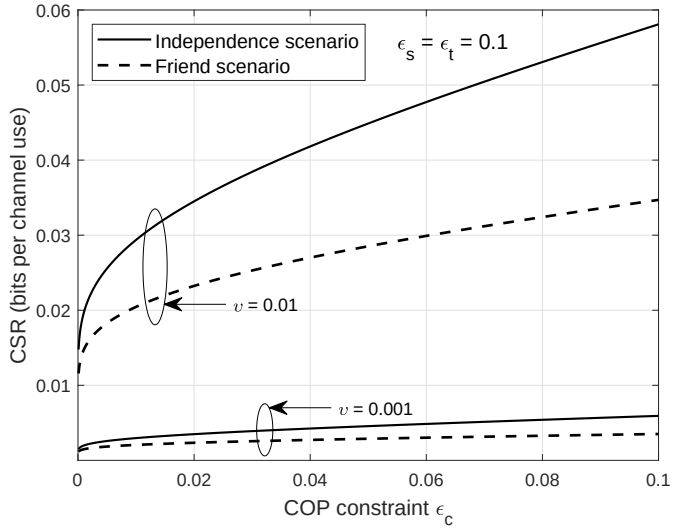


(b) Friend relationship scenario.

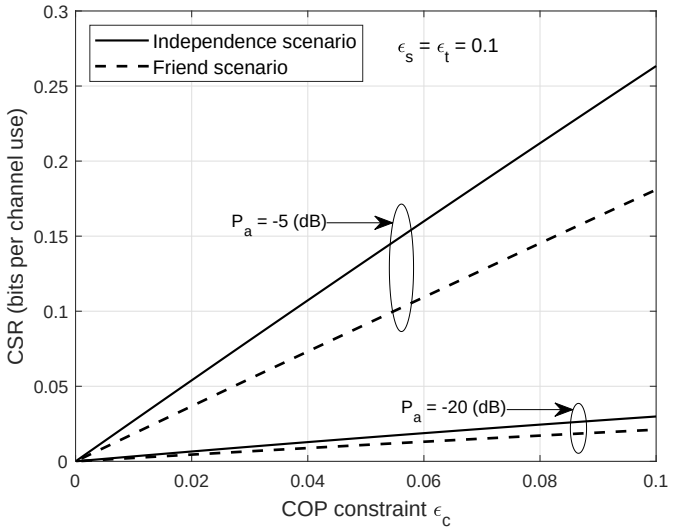
Figure 4.7: CSR R_{cs} vs. TP constraint ϵ_t (AN-based transmission scheme).

changes to $R^*_{s,\mathrm{IP}} = R^0_{s,\mathrm{IP}}$ or $R^*_{s,\mathrm{IP}} = R^{\mathrm{SOP}}_{s,\mathrm{IP}}$ for large ϵ_t, which is independent of ϵ_t. We can observe similar phenomena from Fig. 4.6(b), Fig. 4.7(a) and Fig. 4.7(b).

We proceed to compare the CSR performance achieved in the independence relationship scenario and that achieved in the friend relationship scenario, for which we show R_{cs} vs. ϵ_c for both relationship scenarios under the PC-based transmission



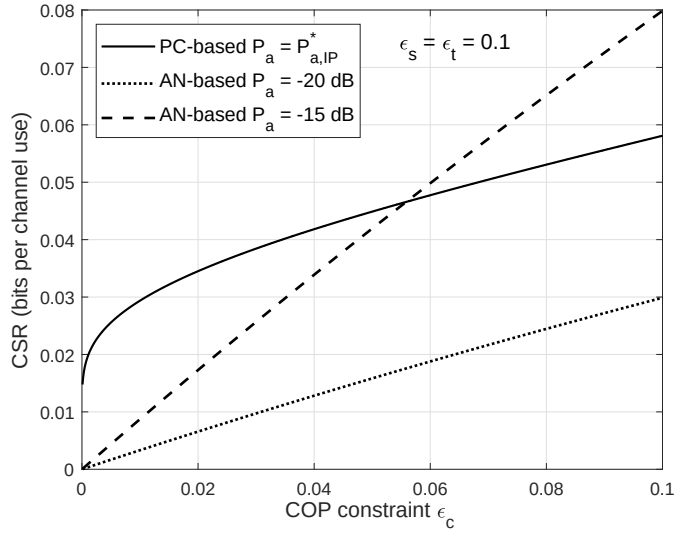
(a) PC-based transmission scheme.



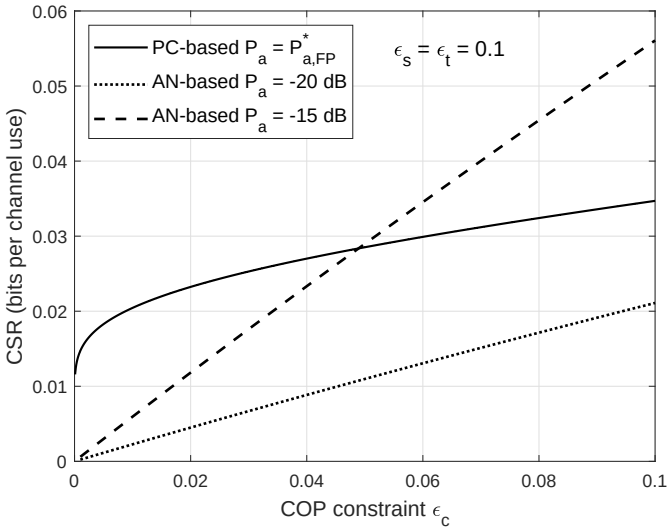
(b) AN-based transmission scheme.

Figure 4.8: Comparisons of the CSR performances in two relationship cases.

scheme in Fig. 4.8(a) and those under the AN-based transmission scheme in Fig. 4.8(b), respectively. We set the SOP constraint and TP constraint to $\epsilon_s = \epsilon_t = 0.1$ in both figures. In addition, we set the parameter υ to $\upsilon = 0.01$ and 0.001 in Fig. 4.8(a) and the transmit power of Alice P_a to $P_a = -5$ dB and -20 dB in Fig. 4.8(b). We can observe from both subfigures that the CSRs in the independence relationship case are always larger than those in the friend relationship case under all the



(a) Independence relationship scenario.

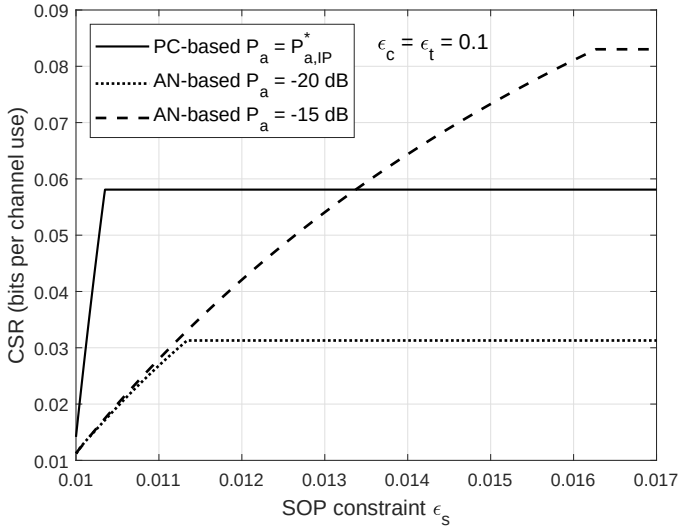


(b) Friend relationship scenario.

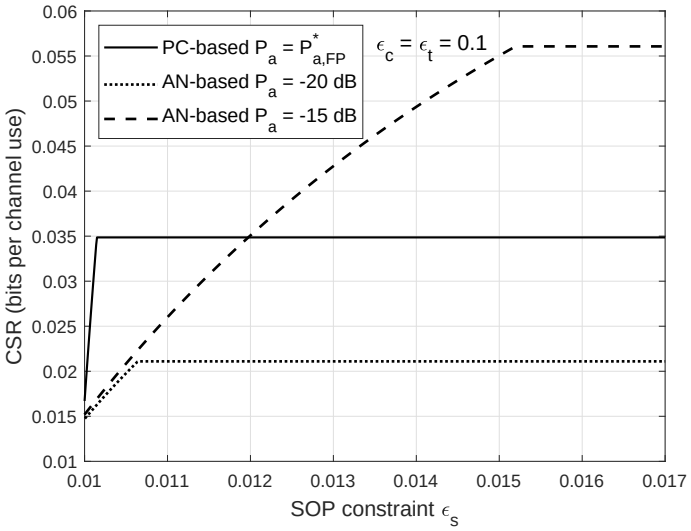
Figure 4.9: Comparisons of the CSR performances in the PC-based and AN-based transmission schemes (R_{cs} vs. ϵ_c).

parameter settings and both transmission schemes. This is intuitive since Willie and Eve can improve their attacking abilities by sharing their signals. The above observations indicate that being friends is the better choice than being independent for the eavesdropper group and detector group.

Finally, we compare the PC-based transmission scheme and the AN-based trans-



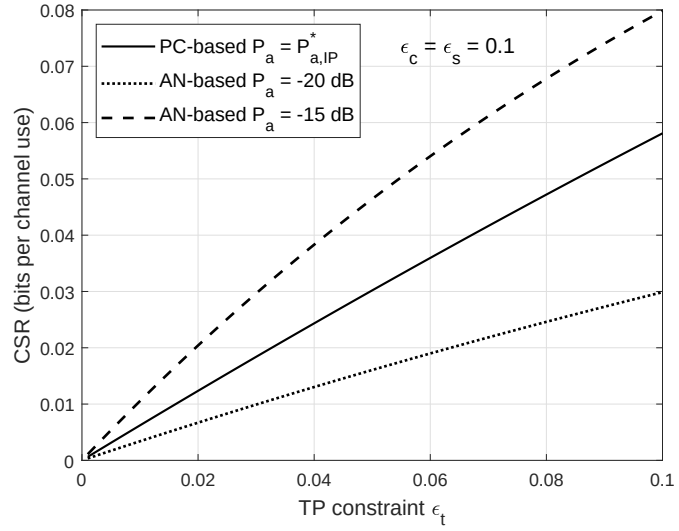
(a) Independence relationship scenario.



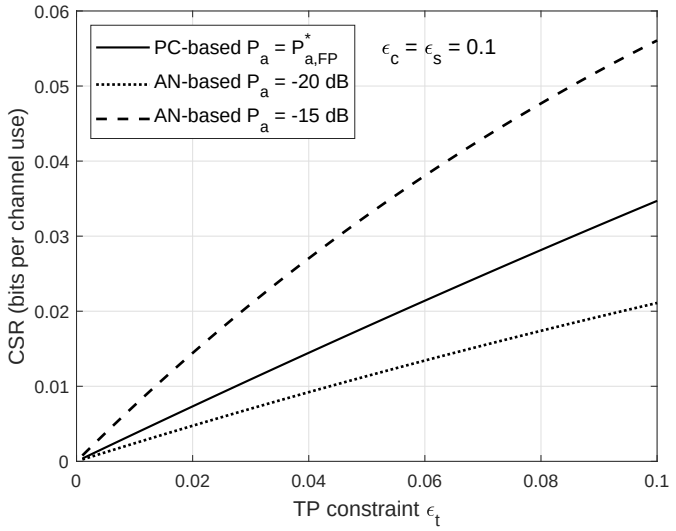
(b) Friend relationship scenario.

Figure 4.10: Comparisons of the CSR performances in the PC-based and AN-based transmission schemes (R_{cs} vs. ϵ_s).

mission scheme in terms of the CSR performance. To do so, we show R_{cs} vs. ϵ_c in Fig. 4.9 (resp. R_{cs} vs. ϵ_s in Fig. 4.10 and R_{cs} vs. ϵ_t in Fig. 4.11) under both transmission schemes in the independence and friend relationship scenarios, respectively. We set $\epsilon_s = \epsilon_t = 0.1$ in Fig. 4.9, $\epsilon_c = \epsilon_t = 0.1$ in Fig. 4.10 and $\epsilon_c = \epsilon_s = 0.1$ in Fig. 4.11. For each figure, we consider two different settings of the transmit power of Alice P_a



(a) Independence relationship scenario.



(b) Friend relationship scenario.

Figure 4.11: Comparisons of the CSR performances in the PC-based and AN-based transmission schemes (R_{cs} vs. ϵ_t).

for the AN-based scheme. We can observe from Fig. 4.9 that, in both relationship scenarios, the PC-based scheme achieves better CSR performance than the AN-based scheme, when a small transmit power (e.g., $P_a = -20$ dB) is adopted in the AN-based scheme. However, when the transmit power of AN-based scheme is relatively larger (e.g., $P_a = -15$ dB), the PC-based scheme achieves better CSR performance than

the AN-based scheme under stringent COP constraints (e.g., less than about 0.055 in Fig. 4.9(a)), while the AN-based scheme achieves better CSR performance than the PC-based scheme under less strict COP constraints.

Similar results can be obtained from Fig. 4.10, which shows that the PC-based scheme outperforms the AN-based scheme if either the transmit power of the AN-based scheme or the SOP constraint is small. Otherwise, the AN-based scheme outperforms the PC-based scheme. However, the results obtained from Fig. 4.11 are different. We can see from Fig. 4.11 that the AN-based scheme outperforms the PC-based scheme when adopting a large transmit power (i.e., $P_a = -15$ dB), while it achieves worse CSR performance than the PC-based scheme when adopting a small transmit power (i.e., $P_a = -20$ dB). Based on the above observations from Fig. 4.9, Fig. 4.10 and 4.11, we can conclude that when the transmit power is not a big concern, transmitters may prefer the AN-based transmission scheme to achieve better CSR performance, especially for less strict covertness, secrecy and transmission performance constraints. On the other hand, when the transmit power is constrained (e.g., in IoT and sensor networks), the PC-based scheme is more preferable for transmitters.

4.5 Discussion

In this chapter, our work represents a significant research progress in the joint guarantees of covertness and secrecy for wireless communications, and contributes a basic understanding on the covertness-secrecy interplay. To understand the more fundamental interplay between the covertness and secrecy, this work examines a general secure wireless communication paradigm where the detection and eavesdropping attacks co-exist in wireless communications. Regarding the comparison with latest works in 2020 [104, 105], in particular, this paradigm carefully takes into consideration the relationship between the eavesdropper and detector (like the independent

relationship or friend relationship), and adopts a general assumption on channel state information (CSI) of the attackers (i.e., unknown instantaneous CSI). We also explore both the artificial noise (AN)-based technique and power control (PC)-based technique in the paradigm for covertness and secrecy guarantees.

Although we have completed this work, there are still some parts that can be improved. We consider a common assumption that the instantaneous CSI is unknown to the detector, which is not practical, and thus, in our future work, we can assume that the instantaneous CSI is known to the detector due to his more powerful capabilities. Regarding the results of the performance comparison between two secure transmission schemes in the numerical results section, the better scheme can be observed because of the transmit power of the transmitter and the constraints of covertness, secrecy and transmission performances. In future work, we can consider a self-adaptive secure transmission mode, where the transmitter always adopts the best scheme according to some conditions, such as transmit power, location, and performance constraints. In addition, we achieve one-hop secure wireless communication paradigm in this work, while the results cannot extend to a long distance transmission because of the signal fading. Thus, we can investigate the secure paradigm in the multi-hop and more complex wireless communications.

4.6 Summary

This chapter explores a new secure wireless communication paradigm, where the physical layer security technology is applied to ensure both the covertness and secrecy of the communication. We define a novel metric of covert secrecy rate (CSR) to depict the security performance of the new paradigm, and also provide solid theoretical analysis on CSR under two transmission schemes (i.e., artificial noise (AN)-based one and power control (PC)-based one) and two detector-eavesdropper relationships (i.e., independence and friend). The results in this work indicate that in general

the CSR performance can be improved when the constraints on covertness, secrecy and transmission performance become less strict. In particular, the PC-based transmission scheme outperforms the AN-based transmission scheme in terms of the CSR performance when strict constraints are applied to the covertness, secrecy and transmission performance. On the other hand, when these constraints become less strict, the AN-based scheme may achieve better CSR performance than the PC-based one by properly adjusting the message transmit power. We expect that this work can shed light on the future studies of new secure wireless communication paradigms.

CHAPTER V

Covertness and Secrecy Guarantees in Wireless Communications with Active Attackers

This chapter extends the secure wireless communication paradigm proposed in Chapter IV to the active attacker scenario where attackers perform jamming and detection/eavesdropping simultaneously. Both detection and eavesdropping attacks need to be counteracted in the wireless communication, such that the covertness and secrecy guarantees in wireless communication can be achieved. To understand the covertness, secrecy and transmission performances in the active attacker scenario, we first provide theoretical modeling for covertness outage probability, secrecy outage probability and transmission probability, respectively. Based on the theoretical model, we further conduct detailed theoretical analysis to identify the covert secrecy rate (CSR) in this scenario under two secure transmission schemes adopted by transmitters. Finally, extensive numerical results are provided to reveal the impact of the active attackers on the CSR under each transmission scheme, and illustrate the achievable performances under the active attacker scenario in the secure wireless communication paradigm.

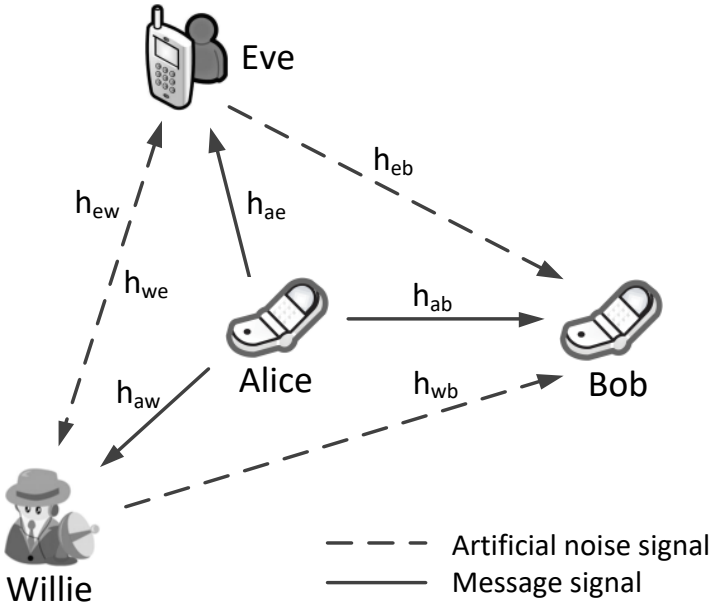


Figure 5.1: System model regarding covertness and secrecy guarantees in wireless communication with active attackers.

5.1 System Model

In this section, we introduce the channel model, the secure transmission schemes and the attacking model of the secure wireless communication paradigm scenario with active attackers, and then give the signal transmission case in this scenario.

5.1.1 Channel Model

This work considers a secure wireless communication paradigm scenario with active attackers, where the attackers (i.e., detector and eavesdropper) perform detection/eavesdropping and jamming simultaneously. As illustrated in Fig. 5.1, a transmitter Alice sends messages to a receiver Bob in the presence of an active detector Willie and an active eavesdropper Eve. In addition to continuously transmitting artificial noise (AN) signals for jamming, Willie attempts to detect the existence of

the signals transmitted from Alice, while Eve targets the messages contained in the signals. Alice and Bob operate in the half-duplex mode, while Willie and Eve can operate in the full-duplex mode. The self-interference caused by the full-duplex mode can be canceled by adopting the perfect self-interference cancellation technique [106]. Alice and Bob are assumed to be equipped with a single omnidirectional antenna, while besides the single receiving antenna, both Willie and Eve use an additional antenna for transmission of AN in order to deliberately interfere with the secure wireless communication between Alice and Bob. For notation simplicity, we use a, b, e and w to represent Alice, Bob, Eve and Willie, respectively, throughout this chapter.

Time is divided into successive slots with equal duration that is long enough for Alice to transmit multiple symbols. We assume that the wireless channels are subject to the quasi-static Rayleigh fading channel model, where the channel coefficients remain constant in one slot and change independently from one slot to another at random. We use h_{ij} to denote the coefficient of the channel from i to j, where $i \in \{a, b, e, w\}$ and $j \in \{a, b, e, w\}$. As assumed in [19], the corresponding channel gain $|h_{ij}|^2$ follows the exponential distribution with unit mean. We assume that Alice and Bob know the statistical characterizations of each channel coefficient including those of the attackers. In addition, Bob also knows the instantaneous channel coefficient h_{ab}, which makes the covert secrecy rate easy to analyze and also ensures a meaningful theoretical performance results. We also assume that Eve knows the instantaneous channel coefficient h_{ae} and the statistical channel coefficient h_{we}, while Willie knows only the statistical characterizations of h_{aw} and h_{ew}. These assumptions are widely used in previous research related to physical layer security (PLS) and covert communication.

5.1.2 Secure Transmission Schemes

Alice considers two transmission schemes according to power control (PC) and artificial noise (AN) injection, respectively. In the PC-based scheme, Alice controls

her transmit power P_a so as to hide the message signals into the background noise for the covertness and secrecy guarantees. In the AN-based scheme, Alice intentionally injects AN into the message signals to confuse Willie and Eve in order to weaken their attack effects. Unlike the PC-based scheme, in the AN-based scheme, Alice utilizes a constant transmit power (also denoted by P_a) and allocates the power between message and noise transmissions. We use ρP_a to denote the transmission power of message, where the parameter $\rho \in (0, 1]$, and the remaining power is used for the AN transmission. In addition to the above strategies on transmit power, Alice also adopts the well-known Wyner's encoding scheme [57] to resist the eavesdropping of Eve. To transmit a message, Alice chooses a target secrecy rate R_s for this message and another rate R_t for the whole transmitted codewords. The rate difference $R_t - R_s$ reflects the cost of securing the message transmission to confuse Eve.

Alice decides whether the transmission takes place according to an on-off transmission model, which only requires one-bit feedback transmitted from Bob to Alice. The condition of transmission in the model holds when the value of signal to interference plus noise ratio (SINR) at Bob γ_b exceeds a specific threshold μ [107, 108]. The SINR threshold μ is a function of different parameters in the communication system, including application, data rate, signal processing applied at transmitter/receiver sides, error correction coding, etc [109]. Note that Alice will set R_t arbitrarily close to C_b to ensure largest possible rate without incurring any decoding error at Bob, while causing as much confusion to Eve as possible. Thus, when Alice adopts the on-off transmission model, the transmission probability (TP) in a certain time slot can be defined as

$$p_{tx} = \mathbb{P}(\gamma_b \geq \mu). \tag{5.1}$$

Note that the TP p_{tx} can be interpreted as a metric to measure the transmission performance.

5.1.3 Attacking Model

In this chapter, we consider the active attackers (i.e., detector Willie and eavesdropper Eve) scenario, where the attackers intentionally radiate AN to interfere with the achieving of covertness and secrecy of wireless communication between Alice and Bob. In addition to radiating the AN, the main objective of Willie and Eve in each slot is to detect the existence of signals transmitted from Alice and eavesdrop the messages contained in the signals, respectively.

The detection scheme at the detector is to adopt the commonly-used likelihood ratio test [23], where Willie first decides a threshold θ and then measures the average power $\bar{P}_w$ of the symbols received from Alice in one slot. If $\bar{P}_w \geq \theta$, Willie accepts a hypothesis $\mathcal{H}_1$ that Alice transmitted messages to Bob in this slot. If $\bar{P}_w \leq \theta$, Willie accepts a hypothesis $\mathcal{H}_0$ that Alice did not transmit messages. Formally, the likelihood ratio test can be given by

$$\bar{P}_w \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \theta. \tag{5.2}$$

In general, the likelihood ratio test exists two types of detection errors. One is called false alarm, which means that Willie makes a decision in favor of $\mathcal{H}_1$ whilst the transmission does not exist in fact. The other is called missed detection, which means that Willie makes a decision in favor of $\mathcal{H}_0$ whilst the transmission exists indeed. We denote the probabilities of false alarm and missed detection by p_{FA} and p_{MD}, respectively. Note that $p_{FA} + p_{MD}$ can be interpreted as the total detection error probability of Willie. If neither false alarm nor missed detection occurs, the transmission from Alice to Bob will suffer from covertness outage. Thus, the covertness outage probability (COP) is given by

$$p_{co} = 1 - (p_{FA} + p_{MD}). \tag{5.3}$$

The covertness performance of transmission can be measured by COP. The smaller the COP is, the higher the covertness of the transmission is.

To intercept the transmitted messages, Eve tries to decode the signals received from Alice. When the perfect secrecy fails (i.e., Eve can recover the messages), the instantaneous secrecy capacity C_s [95] of the Alice-Bob channel cannot support the target secrecy rate R_s, such that the transmission between Alice and Bob suffers from secrecy outage. The secrecy outage considered in this chapter only occurs when Alice actually transmits a message (i.e., $\gamma_b \geq \mu$) [108]. Thus, the secrecy outage probability (SOP) as the conditional probability can be given by

$$p_{so} = \mathbb{P}(C_s < R_s \mid \gamma_b \geq \mu). \tag{5.4}$$

Similarly, the secrecy performance of transmission can be measured by SOP, where the smaller the SOP, the stronger the secrecy of the transmission.

5.1.4 Signal Transmission Case

In the active attacker scenario, Willie and Eve not only conduct the detection and the eavesdropping attack, but also generate AN to interfere with the secure transmission between Alice and Bob. Thus, under the PC-based transmission scheme, when Alice transmits, she sends n symbols to Bob, represented by a complex vector $\mathbf{x}$, where each symbol $\mathbf{x}[i]$ $(i = 1, 2, \cdots, n)$ is subject to the unit power constraint, i.e., $\mathbb{E}[|\mathbf{x}[i]|^2] = 1$. In addition to the information signals $\mathbf{x}$, Bob also receives ANs $\mathbf{v}_w$ and $\mathbf{v}_e$ from both Willie and Eve, respectively. Each AN symbol $\mathbf{v}_w[i]/\mathbf{v}_e[i]$ $(i = 1, 2, \cdots, n)$ is subject to the unit power constraint, i.e., $\mathbb{E}[|\mathbf{v}_w[i]|^2] = 1$ and $\mathbb{E}[|\mathbf{v}_e[i]|^2] = 1$. Thus, the received signal vector at Bob under the PC-based transmis-

sion scheme is given by

$$\mathbf{y}_{b,PC} = \sqrt{P_a} h_{ab} \mathbf{x} + \sqrt{P_w} h_{wb} \mathbf{v}_w + \sqrt{P_e} h_{eb} \mathbf{v}_e + \mathbf{n}_b, \tag{5.5}$$

where P_w and P_e denote the transmit powers of Willie and Eve, respectively, and $\mathbf{n}_b$ denotes the noise at Bob with the i-th element $\mathbf{n}_b[i]$ being the complex additive Gaussian noise with zero mean and variance σ_b^2, i.e., $\mathbf{n}_b[i] \sim \mathcal{CN}(0, \sigma_b^2)$. We assume that both Willie and Eve can eliminate the AN from itself. Thus, the received signal vectors at Willie and Eve under the PC-based transmission scheme are given by

$$\mathbf{y}_{w,PC}^1 = \sqrt{P_a} h_{aw} \mathbf{x} + \sqrt{P_e} h_{ew} \mathbf{v}_e + \mathbf{n}_w, \tag{5.6}$$

and

$$\mathbf{y}_{e,PC} = \sqrt{P_a} h_{ae} \mathbf{x} + \sqrt{P_w} h_{we} \mathbf{v}_w + \mathbf{n}_e. \tag{5.7}$$

Here, $\mathbf{n}_w$ and $\mathbf{n}_e$ represent the noise at Willie and Eve, where the i-th element $\mathbf{n}_w[i]$ and $\mathbf{n}_e[i]$ being the complex additive Gaussian noise with zero mean and variance σ_w^2 and σ_e^2, respectively, i.e., $\mathbf{n}_w[i] \sim \mathcal{CN}(0, \sigma_w^2)$ and $\mathbf{n}_e[i] \sim \mathcal{CN}(0, \sigma_e^2)$. When Alice does not transmit, Willie receives the AN from Eve together with his background noise, and thus the received signal vector at Willie under the PC-based scheme is given by

$$\mathbf{y}_{w,PC}^0 = \sqrt{P_e} h_{ew} \mathbf{v}_e + \mathbf{n}_w. \tag{5.8}$$

Based on the AN-based transmission scheme, when Alice transmits, in addition to the message symbols, she will also inject AN, represented by a complex vector $\mathbf{z}$, where each symbol $\mathbf{z}[i]$ $(i = 1, 2, \cdots, n)$ is subject to the unit power constraint, i.e., $\mathbb{E}[|\mathbf{z}[i]|^2] = 1$. Alice will use a fraction ρ of her transmit power P_a for message transmission and the remaining power for AN radiation. Thus, the received signal

vectors at Bob, Willie and Eve under the AN-based scheme are respectively given by

$$\mathbf{y}_{b,AN} = \sqrt{\rho P_a} h_{ab}\mathbf{x} + \sqrt{(1-\rho)P_a} h_{ab}\mathbf{z} + \sqrt{P_w} h_{wb}\mathbf{v}_w + \sqrt{P_e} h_{eb}\mathbf{v}_e + \mathbf{n}_b, \tag{5.9}$$

$$\mathbf{y}^1_{w,AN} = \sqrt{\rho P_a} h_{aw}\mathbf{x} + \sqrt{(1-\rho)P_a} h_{aw}\mathbf{z} + \sqrt{P_e} h_{ew}\mathbf{v}_e + \mathbf{n}_w, \tag{5.10}$$

and

$$\mathbf{y}_{e,AN} = \sqrt{\rho P_a} h_{ae}\mathbf{x} + \sqrt{(1-\rho)P_a} h_{ae}\mathbf{z} + \sqrt{P_w} h_{we}\mathbf{v}_w + \mathbf{n}_e. \tag{5.11}$$

When Alice does not transmit, Willie receives Alice and Eve's AN and his background noise, and thus the received signal vector at Willie under the AN-based transmission scheme is given by

$$\mathbf{y}^0_{w,AN} = \sqrt{(1-\rho)P_a} h_{aw}\mathbf{z} + \sqrt{P_e} h_{ew}\mathbf{v}_e + \mathbf{n}_w. \tag{5.12}$$

5.2 CSR Analysis under PC-Based Transmission Scheme

This section focuses on the covert secrecy rate (CSR) analysis when Alice and Bob adopt the PC-based transmission scheme to ensure the covertness and secrecy of wireless communication in the active attacker scenario.

5.2.1 Performance Analysis

As the secure transmission scheme mentioned in Section 5.1.2, Alice decides to transmit in a certain time slot based on the on-off transmission model. In this model, if the value of SINR at Bob γ_b is greater than a specific threshold μ, Bob will send Alice one-bit feedback representing transmission. To do this, based on (5.5), the SINR at Bob γ_b under PC-based scheme can be formulated by

$$\gamma_b = \frac{P_a|h_{ab}|^2}{P_w|h_{wb}|^2 + P_e|h_{eb}|^2 + \sigma_b^2}, \tag{5.13}$$

where $|h_{ab}|^2$, $|h_{wb}|^2$ and $|h_{eb}|^2$ are exponentially distributed. According to the definition in (5.1), to measure the transmission performance of wireless communication, the transmission probability p_{tx} of Alice can be given by

$$\begin{aligned} p_{tx}^{\mathrm{PC}}(P_a, R_s) &= \mathbb{P}\left(\gamma_b \geq \mu\right) = \mathbb{P}\left(\frac{P_a|h_{ab}|^2}{P_w|h_{wb}|^2 + P_e|h_{eb}|^2 + \sigma_b^2} \geq 2^{R_s} - 1\right) \\ &= \frac{P_a^2}{(P_a + (2^{R_s} - 1)P_w)(P_a + (2^{R_s} - 1)P_e)} \exp\left(-\frac{(2^{R_s} - 1)\sigma_b^2}{P_a}\right). \end{aligned} \quad (5.14)$$

Note that $\mu \geq 2^{R_s} - 1$ always holds, since the transmission only happen when the instantaneous capacity C_b of Alice-Bob channel can support the secrecy rate R_s.

Next, we analyze the covertness and secrecy performances of wireless communication in the active attacker scenario, respectively. We first analyze a significant metric COP in the covertness guarantee. When Alice chooses to transmit, according to the detection scheme in Section 5.1.3, Willie makes a decision on the transmission of message signals based on the average power $\bar{P}_w$ of the received symbols $\mathbf{y}_w$ in (5.6). In this case, $\bar{P}_w$ is given by

$$\begin{aligned} \bar{P}_w &= \frac{\sum_{i=1}^{n} |\mathbf{y}_w[i]|^2}{n} = \lim_{n\to\infty} (P_a|h_{aw}|^2 + P_e|h_{ew}|^2 + \sigma_w^2)\chi_{2n}^2/n \\ &= P_a|h_{aw}|^2 + P_e|h_{ew}|^2 + \sigma_w^2, \end{aligned} \quad (5.15)$$

where χ_{2n}^2 represents a chi-squared random variable with $2n$ degrees of freedom. By the Strong Law of Large Numbers [102], $\frac{\chi_{2n}^2}{n}$ converges in probability to 1 as n tends to infinity. If $\bar{P}_w \leq \theta$, Willie accepts the hypothesis $\mathcal{H}_0$ that Alice did not transmit messages, leading to a missed detection. Thus, based on (5.15), the probability of

missed detection p_{MD} under the PC-based scheme can be given by

$$\begin{aligned} p_{MD} &= \mathbb{P}\left(P_a|h_{aw}|^2 + P_e|h_{ew}|^2 + \sigma_w^2 \leq \theta\right) \\ &= \begin{cases} 1 + \frac{P_e}{P_a - P_e} \exp\left(-\frac{\theta - \sigma_w^2}{P_e}\right) - \frac{P_a}{P_a - P_e} \exp\left(-\frac{\theta - \sigma_w^2}{P_a}\right), & \theta > \sigma_w^2, \\ 0, & \theta \leq \sigma_w^2. \end{cases} \end{aligned} \tag{5.16}$$

In the covertness analysis, when Alice does not transmit, due to the received symbols $\mathbf{y}_w$ at Willie in (5.8), the average power $\bar{P}_w$ is given by

$$\bar{P}_w = P_e|h_{ew}|^2 + \sigma_w^2. \tag{5.17}$$

If $\bar{P}_w \geq \theta$, Willie accepts the hypothesis $\mathcal{H}_1$ that Alice transmitted messages, leading to a false alarm. Thus, based on (5.17), the probability of false alarm p_{FA} is given by

$$p_{FA} = \mathbb{P}\left(P_e|h_{ew}|^2 + \sigma_w^2 \geq \theta\right) = \begin{cases} \exp\left(-\frac{\theta - \sigma_w^2}{P_e}\right), & \theta > \sigma_w^2, \\ 1, & \theta \leq \sigma_w^2. \end{cases} \tag{5.18}$$

Combining the p_{MD} in (5.16) and the p_{FA} in (5.18) gives the COP p_{co}^{PC} under the PC-based scheme, which is

$$p_{co}^{\mathrm{PC}}(P_a, \theta) = \begin{cases} \frac{P_a}{P_a - P_e} \left[\exp\left(-\frac{\theta - \sigma_w^2}{P_a}\right) - \exp\left(-\frac{\theta - \sigma_w^2}{P_e}\right)\right], & \theta > \sigma_w^2, \\ 0, & \theta \leq \sigma_w^2. \end{cases} \tag{5.19}$$

Note that Willie will set a decision threshold greater than the variance of the received noise, to ensure that the covertness outage occurs with a certain probability. We can see from (5.19) that the optimal detection threshold θ_{PC}^* exists when $\theta > \sigma_w^2$ and can

be obtained by solving $\partial p_{co}^{\mathrm{PC}}/\partial\theta = 0$. Thus, θ_{PC}^{*} is given by

$$\theta_{\mathrm{PC}}^{*} = \frac{P_a P_e}{P_a - P_e} \ln \frac{P_a}{P_e} + \sigma_w^2. \tag{5.20}$$

Substituting the optimal detection threshold θ as $\theta = \theta^*$ in (5.20) into the COP in (5.19), the maximum COP caused by setting the optimal detection threshold at Willie can be rewritten as

$$p_{co}^{\mathrm{PC}}\ (P_a) = \left(\frac{P_a}{P_e}\right)^{\frac{P_e}{P_e - P_a}}. \tag{5.21}$$

As for the secrecy analysis, the eavesdropping effect of Eve, which only exists when Alice choose to transmit, depends on the instantaneous secrecy capacity C_s of the Alice-Bob channel. According to [95], C_s is the difference between the channel capacity of the Alice-Bob channel and that of the Alice-Eve channel. Thus, based on (5.5) and (5.7), we can formulate the secrecy capacity C_s as

$$C_s = \log\left(1 + \frac{P_a|h_{ab}|^2}{P_w|h_{wb}|^2 + P_e|h_{eb}|^2 + \sigma_b^2}\right) - \log\left(1 + \frac{P_a|h_{ae}|^2}{P_w|h_{we}|^2 + \sigma_e^2}\right), \tag{5.22}$$

where log is to the base of 2. Note that $|h_{ab}|^2$, $|h_{wb}|^2$ and $|h_{eb}|^2$ are random variables here. Based on the definition of the SOP in Section 5.1.3, the SOP under the PC-based scheme can be given by

$$\begin{aligned}
p_{so}^{\mathrm{PC}}(R_s) &= \frac{\mathbb{P}\left(\mu < \gamma_b < 2^{R_s}(1+\gamma_e) - 1\right)}{\mathbb{P}\left(\gamma_b > \mu\right)} = 1 - \frac{\mathbb{P}\left(\gamma_b > 2^{R_s}(1+\gamma_e) - 1\right)}{\mathbb{P}\left(\gamma_b > \mu\right)} \\
&= 1 - \frac{(P_a + (2^{R_s}-1)P_w)(P_a + (2^{R_s}-1)P_e)}{P_a^2} \exp\left(\frac{(2^{R_s}-1)\sigma_b^2}{P_a}\right) \\
&\quad \times \mathbb{P}\left(\frac{P_a|h_{ab}|^2}{P_w|h_{wb}|^2 + P_e|h_{eb}|^2 + \sigma_b^2} - \frac{2^{R_s}P_a|h_{ae}|^2}{P_w|h_{we}|^2 + \sigma_e^2} > 2^{R_s} - 1\right) \\
&= 1 - \int_0^\infty \int_0^\infty \frac{(P_w x + \sigma_e^2)^2}{(P_w x + \sigma_e^2 + \frac{2^{R_s}P_w y}{1+(2^{R_s}-1)\nu_w})(P_w x + \sigma_e^2 + \frac{2^{R_s}P_e y}{1+(2^{R_s}-1)\nu_e})} \\
&\quad \times \exp\left(-x - \frac{2^{R_s}\sigma_b^2 y}{P_w x + \sigma_e^2} - y\right) \mathrm{d}x\, \mathrm{d}y,
\end{aligned} \tag{5.23}$$

where γ_e is the SINR at Eve, $\nu_w = \frac{P_w}{P_a}$ and $\nu_e = \frac{P_e}{P_a}$.

5.2.2 CSR Optimization Problem

In order to understand the fundamental security performance under the covertness and secrecy guarantees in wireless communication, we consider the covert secrecy rate (CSR) defined as the maximum transmission rate under which both covertness, secrecy and transmission performances can be ensured. To obtain the CSR R_{cs}, we formulate an optimization problem for the PC-based transmission scheme, which is given by

$$\textbf{P1 (PC-based):} \quad R_{cs}^{\mathrm{PC}} = \max_{P_a, R_s} R_s\, p_{tx}^{\mathrm{PC}}(P_a, R_s), \tag{5.24a}$$

$$\text{s.t.} \quad p_{co}^{\mathrm{PC}}(P_a) \leq \epsilon_c, \tag{5.24b}$$

$$p_{so}^{\mathrm{PC}}(R_s) \leq \epsilon_s, \tag{5.24c}$$

$$p_{tx}^{\mathrm{PC}}(P_a, R_s) \geq 1 - \epsilon_t, \tag{5.24d}$$

where ϵ_c, ϵ_s and ϵ_t denote the requirements of covertness, secrecy and transmission performances. Note that Problem P1 optimizes the transmission rate constrained by the transmit power P_a and the secrecy rate R_s.

By solving the optimization problem P1, we obtain the CSR under the PC-based transmission scheme, and the result is summarized in the following theorem.

Theorem V.1 *Under the scenario where Willie and Eve are active attackers and Alice adopts the PC-based secure transmission scheme, the CSR of the system is*

$$R_{cs}^{\mathrm{PC}} = \frac{R_{s,\mathrm{PC}}^*}{(1 + (2^{R_{s,\mathrm{PC}}^*} - 1)\nu_w)(1 + (2^{R_{s,\mathrm{PC}}^*} - 1)\nu_e)} \exp\left(-\frac{(2^{R_{s,\mathrm{PC}}^*} - 1)\sigma_b^2}{P_{a,\mathrm{PC}}^*}\right), \tag{5.25}$$

where $\nu_w = \frac{P_w}{P^*_{a,\mathrm{PC}}}$ *and* $\nu_e = \frac{P_e}{P^*_{a,\mathrm{PC}}}$. *The optimal secrecy rate* $R^*_{s,\mathrm{PC}}$ *is given by*

$$R^*_{s,\mathrm{PC}} = \begin{cases} R^0_{s,\mathrm{PC}}(P^*_{a,\mathrm{PC}}), & R^0_{s,\mathrm{PC}} \leq \min\left\{R^{SOP}_{s,\mathrm{PC}}, R^{TP}_{s,\mathrm{PC}}\right\}, \\ R^{SOP}_{s,\mathrm{PC}}, & R^{SOP}_{s,\mathrm{PC}} \leq \min\left\{R^0_{s,\mathrm{PC}}, R^{TP}_{s,\mathrm{PC}}\right\}, \\ R^{TP}_{s,\mathrm{PC}}(P^*_{a,\mathrm{PC}}), & R^{TP}_{s,\mathrm{PC}} \leq \min\left\{R^0_{s,\mathrm{PC}}, R^{SOP}_{s,\mathrm{PC}}\right\}, \end{cases} \tag{5.26}$$

where the stationary point $R^0_{s,\mathrm{PC}}$ *can be obtained by solving* $\frac{\partial R^{\mathrm{PC}}_{cs}}{\partial R_s} = 0$, $R^{SOP}_{s,\mathrm{PC}}$ *and* $R^{TP}_{s,\mathrm{PC}}$ *are the solutions of* $p^{\mathrm{PC}}_{so}(R_s) = \epsilon_s$ *and* $p^{\mathrm{PC}}_{tx}(R_s) = 1-\epsilon_t$, *respectively. Here, the optimal transmit power* $P^*_{a,\mathrm{PC}}$ *is given by*

$$P^*_{a,\mathrm{PC}} = \frac{P_e \mathrm{W}_0(\epsilon_c \ln \epsilon_c)}{\ln \epsilon_c}, \tag{5.27}$$

where $\mathrm{W}_0(\cdot)$ *is the principal branch of Lambert's W function.*

Proof 5 *As can be seen from* (5.24a), *the optimal transmit power* P_a *and optimal target secrecy rate* R_s *are required to solve the optimization problem P1. We first derive the optimal* P_a. *It is easy to see from* (5.14) *that* p^{PC}_{tx} *monotonically increases as* P_a *increases. As for the monotonicity of* p^{PC}_{co}, *we take the first derivative of the function in* (5.21) *in terms of* P_a *gives*

$$\frac{\partial p^{\mathrm{PC}}_{co}}{\partial P_a} = \frac{1 + \frac{P_a}{P_e}\left(-1 + \ln \frac{P_a}{P_e}\right)}{\frac{P_a}{P_e}\left(1 - \frac{P_a}{P_e}\right)^2} \left(\frac{P_a}{P_e}\right)^{\frac{P_e}{P_e - P_a}}. \tag{5.28}$$

Due to the logarithmic inequality $1 - \frac{1}{x} \leq \ln x, \forall x > 0$, *the result in* (5.28) *indicates that* $\frac{\partial p^{\mathrm{PC}}_{co}}{\partial P_a} > 0$, *and thus* p^{PC}_{co} *is always an increasing function of* P_a. *Based on the COP constraint in* (5.24b) *and the TP constraint in* (5.24d), *an upper bound* $P^{\max}_{a,\mathrm{PC}}$ *and a lower bound* $P^{\min}_{a,\mathrm{PC}}$ *on* P_a *can be obtained, respectively. Since the objective function in* (5.24a) *is an increasing function of* P_a, *the optimal* P_a *is the upper bound, i.e.,* $P^*_{a,\mathrm{PC}} = P^{\max}_{a,\mathrm{PC}}$ *and* $P^*_{a,\mathrm{PC}}$ *is given in* (5.27).

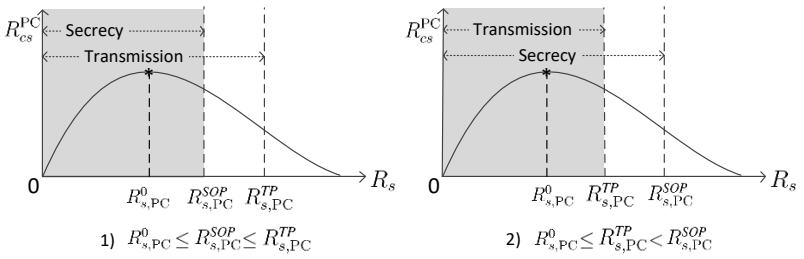


Figure 5.2: The feasible region of R_s for CSR in Case 1.

Next, we derive the optimal R_s by analyzing the feasible region of R_s and the monotonicity of the objective function with respect to R_s. We can see that as R_s increases, p_{tx}^{PC} in (5.14) *monotonically decreases while p_{so}^{PC} in* (5.23) *monotonically increases. Thus, based on the constraints* (5.24c) *and* (5.24d)*, the regions of R_s for ensuring secrecy and transmission performances are $[0, R_{s,\mathrm{PC}}^{SOP}]$ and $[0, R_{s,\mathrm{PC}}^{TP}]$, where $R_{s,\mathrm{PC}}^{SOP}$ and $R_{s,\mathrm{PC}}^{TP}$ can be obtained by solving $p_{so}^{\mathrm{PC}}(R_s) = \epsilon_s$ and $p_{tx}^{\mathrm{PC}}(R_s) = 1 - \epsilon_t$, respectively. Hence, the feasible region of R_s is $[0, \min\{R_{s,\mathrm{PC}}^{SOP}, R_{s,\mathrm{PC}}^{TP}\}]$. Taking the first derivative of the objective function in* (5.24a) *in terms of R_s and then letting $\frac{\partial R_{cs}^{\mathrm{PC}}}{\partial R_s} = 0$, we can obtain the stationary point R_s^0. We note that the objective function is increasing over $[0, R_s^0)$ and decreasing over $[R_s^0, \infty)$. This implies that if R_s^0 falls inside the feasible region of R_s, i.e., $R_s^0 \le \min\{R_{s,\mathrm{PC}}^{SOP}, R_{s,\mathrm{PC}}^{TP}\}$, the optimal R_s is $R_{s,\mathrm{PC}}^{*} = R_s^0$, as shown in Fig. 5.2. Otherwise, the optimal R_s is $R_{s,\mathrm{PC}}^{*} = \min\{R_{s,\mathrm{PC}}^{SOP}, R_{s,\mathrm{PC}}^{TP}\}$. Fig. 5.3 and Fig. 5.4 show the optimal R_s in this situation under different cases of $R_{s,\mathrm{PC}}^{SOP}$ and $R_{s,\mathrm{PC}}^{TP}$. Finally, substituting the optimal P_a and R_s into the objective function in* (5.24a) *completes the proof.*

5.3 CSR Analysis under AN-Based Transmission Scheme

In this section, we analyze the CSR performance based on the AN-based transmission scheme, in which Alice injects AN into the message signals to protect the wireless communication from the detection/eavesdropping in the active attacker scenario.

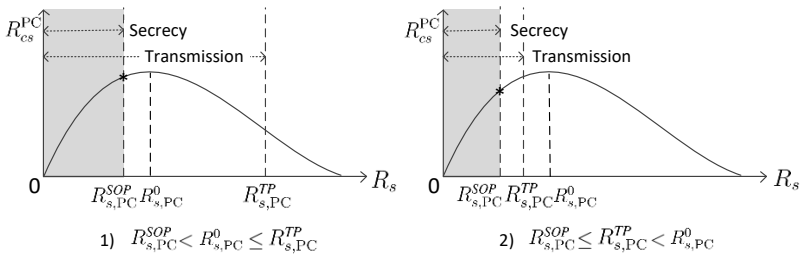


Figure 5.3: The feasible region of R_s for CSR in Case 2.

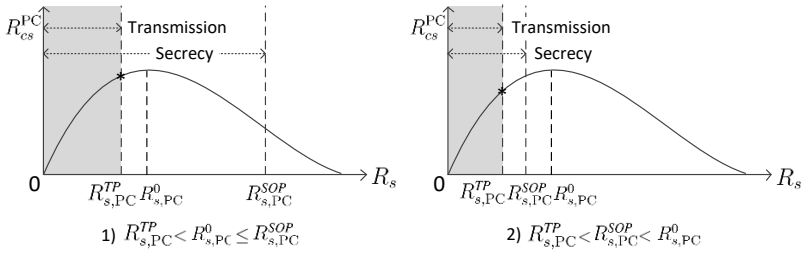


Figure 5.4: The feasible region of R_s for CSR in Case 3.

5.3.1 Performance Analysis

Under the AN-based transmission scheme, according to the decision condition in the on-off transmission model mentioned in Section 5.1.2 and the received signal vectors at Bob $\mathbf{y}_b$ in (5.9), the SINR at Bob can be given by

$$\gamma_b = \frac{\rho P_a |h_{ab}|^2}{(1-\rho)P_a|h_{ab}|^2 + P_w|h_{wb}|^2 + P_e|h_{eb}|^2 + \sigma_b^2}, \tag{5.29}$$

and thus Alice's transmission probability p_{tx} defined in (5.1) under AN-based scheme is given by

$$\begin{aligned} p_{tx}^{\mathrm{AN}}(\rho, R_s) &= \mathbb{P}\left(\frac{\rho P_a |h_{ab}|^2}{(1-\rho)P_a|h_{ab}|^2 + P_w|h_{wb}|^2 + P_e|h_{eb}|^2 + \sigma_b^2} \geq 2^{R_s} - 1\right) \\ &= \frac{(\rho P_a - (2^{R_s}-1)(1-\rho)P_a)^2}{(\rho P_a + (2^{R_s}-1)(P_w - (1-\rho)P_a))(\rho P_a + (2^{R_s}-1)(P_e - (1-\rho)P_a))} \\ &\quad \times \exp\left(-\frac{(2^{R_s}-1)\sigma_b^2}{\rho P_a - (2^{R_s}-1)(1-\rho)P_a}\right). \end{aligned} \tag{5.30}$$

When Alice chooses to transmit with the probability p_{tx}^{AN} in (5.30), the covertness and secrecy guarantees of wireless communication between Alice and Bob need to be considered. First, we analyze the metric COP in the covertness guarantee. Based on the detection scheme in Section 5.1.3, we can see from (5.10) that the average power $\bar{P}_w$ of the received symbols $\mathbf{y}_w$ at Willie is the same as that given in (5.15). Thus, the probability of missed detection p_{MD} under the AN-based transmission scheme can be given by (5.16).

In the covertness analysis, when Alice does not transmit, based on the signal vector $\mathbf{y}_w$ received at Willie as in (5.12), the average power $\bar{P}_w$ is given by

$$\bar{P}_w = (1-\rho)P_a|h_{aw}|^2 + P_e|h_{ew}|^2 + \sigma_w^2. \tag{5.31}$$

Based on (5.31), we can derive the probability of false alarm p_{FA} as

$$\begin{aligned} p_{FA} &= \mathbb{P}\left((1-\rho)P_a|h_{aw}|^2 + P_e|h_{ew}|^2 + \sigma_w^2 \geq \theta\right) \\ &= \begin{cases} \frac{(1-\rho)P_a}{(1-\rho)P_a - P_e}\exp\left(-\frac{\theta-\sigma_w^2}{(1-\rho)P_a}\right) - \frac{P_e}{(1-\rho)P_a-P_e}\exp\left(-\frac{\theta-\sigma_w^2}{P_e}\right), & \theta > \sigma_w^2, \\ 1, & \theta \leq \sigma_w^2, \end{cases} \end{aligned} \tag{5.32}$$

Combining the p_{MD} in (5.16) and p_{FA} in (5.32), we obtain the COP p_{co}^{AN} under the AN-based transmission scheme as

$$p_{co}^{\mathrm{AN}}(\rho,\theta) = \begin{cases} \frac{P_a}{P_a-P_e}\exp\left(-\frac{\theta-\sigma_w^2}{P_a}\right) - \frac{(1-\rho)P_a}{(1-\rho)P_a-P_e}\exp\left(-\frac{\theta-\sigma_w^2}{(1-\rho)P_a}\right) \\ \quad + \frac{\rho P_a P_e}{(P_a-P_e)((1-\rho)P_a-P_e)}\exp\left(-\frac{\theta-\sigma_w^2}{P_e}\right), & \theta > \sigma_w^2, \\ 0, & \theta \leq \sigma_w^2. \end{cases} \tag{5.33}$$

Note that the optimal detection threshold θ is difficult to obtain from (5.33).

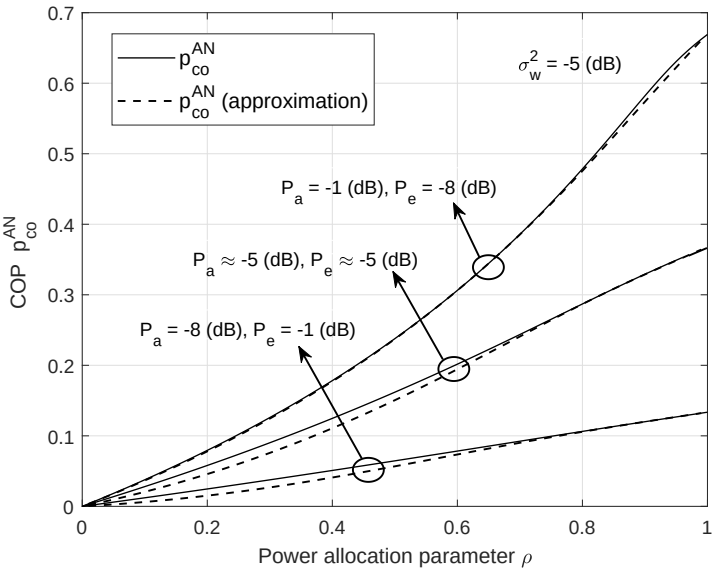


Figure 5.5: The COP and an approximation of COP with the approximation of optimal θ in (5.34).

Thus, we resort to an approximation, which can be given by

$$\theta_{\mathrm{AN}}^{*} \approx \sigma_w^2 + \frac{(\rho-1)P_a}{\rho}\ln(1-\rho) + \frac{\rho P_a P_e}{P_a - P_e}\ln\frac{P_a}{P_e}. \tag{5.34}$$

We can see from Fig. 5.5 that the COPs achieved at the optimal θ under different settings of P_a and P_e are close to those achieved at the approximation of optimal θ in (5.34). This implies that the approximation is accurate enough, and thus the optimal COP caused by setting the optimal detection threshold in Willie can be obtained by substituting $\theta = \theta_{\mathrm{AN}}^{*}$ in (5.34) into the COP in (5.33).

As for the secrecy analysis, according to (5.9) and (5.11), the secrecy capacity C_s can be given by

$$\begin{aligned} C_s = &\log\left(1 + \frac{\rho P_a |h_{ab}|^2}{(1-\rho)P_a|h_{ab}|^2 + P_w|h_{wb}|^2 + P_e|h_{eb}|^2 + \sigma_b^2}\right) \\ &- \log\left(1 + \frac{\rho P_a |h_{ae}|^2}{(1-\rho)P_a|h_{ae}|^2 + P_w|h_{we}|^2 + \sigma_e^2}\right). \end{aligned} \tag{5.35}$$

Thus, the SOP under the AN-based scheme can be derived as

$$
\begin{aligned}
p_{so}^{\mathrm{AN}}(\rho, R_s) &= 1 - \frac{(\rho P_a + (2^{R_s}-1)(P_w-(1-\rho)P_a))(\rho P_a + (2^{R_s}-1)(P_e-(1-\rho)P_a))}{(\rho P_a-(2^{R_s}-1)(1-\rho)P_a)^2} \\
&\quad \times \exp\left(\frac{(2^{R_s}-1)\sigma_b^2}{\rho P_a-(2^{R_s}-1)(1-\rho)P_a}\right) \mathbb{P}\left(-\frac{2^{R_s}\rho P_a|h_{ae}|^2}{(1-\rho)P_a|h_{ae}|^2 + P_w|h_{we}|^2 + \sigma_e^2}\right. \\
&\quad \left. + \frac{\rho P_a|h_{ab}|^2}{(1-\rho)P_a|h_{ab}|^2 + P_w|h_{wb}|^2 + P_e|h_{eb}|^2 + \sigma_b^2} > 2^{R_s} - 1\right) \\
&= 1 - \frac{(\rho P_a + (2^{R_s}-1)(P_w - (1-\rho)P_a))(\rho P_a + (2^{R_s}-1)(P_e - (1-\rho)P_a))}{(\rho - (2^{R_s}-1)(1-\rho))^2} \\
&\quad \times \exp\left(\frac{(2^{R_s}-1)\sigma_b^2}{\rho P_a - (2^{R_s}-1)(1-\rho)P_a}\right) \int_0^{\infty} \int_0^{\alpha(y)} \\
&\quad \frac{(\rho - (1-\rho)\beta(x,y))^2}{(\rho P_a + (P_w - (1-\rho)P_a)\beta(x,y))(\rho P_a + (P_e - (1-\rho)P_a)\beta(x,y))} \\
&\quad \times \exp\left(-x - \frac{\sigma_b^2\beta(x,y)}{(\rho - (1-\rho)\beta(x,y))P_a} - y\right) \mathrm{d}x\,\mathrm{d}y, \qquad (5.36)
\end{aligned}
$$

where $\alpha(y) = \frac{(1-2^{R_s}(1-\rho))(P_w y+\sigma_e^2)}{(2^{R_s}-1)(1-\rho)P_a}$ and $\beta(x,y) = \frac{2^{R_s}\rho P_a x}{(1-\rho)P_a x + P_w y + \sigma_e^2} + 2^{R_s} - 1$.

5.3.2 CSR Optimization Problem

To analyze the fundamental security performance in the new paradigm that ensures the covertness, secrecy and transmission performances jointly, we propose an optimization problem to derive the CSR under AN-based transmission scheme as follow.

$$
\begin{aligned}
\textbf{P2 (AN-based):} \quad R_{cs}^{\mathrm{AN}} = \max_{\rho\in[0,1], R_s} \; & R_s\, p_{tx}^{\mathrm{AN}}(\rho, R_s), && \text{(5.37a)} \\
\text{s.t.} \; & p_{co}^{\mathrm{AN}}(\rho) \le \epsilon_c, && \text{(5.37b)} \\
& p_{so}^{\mathrm{AN}}(\rho, R_s) \le \epsilon_s, && \text{(5.37c)} \\
& p_{tx}^{\mathrm{AN}}(\rho, R_s) \ge 1 - \epsilon_t, && \text{(5.37d)}
\end{aligned}
$$

where ϵ_c, ϵ_s and ϵ_t denote the requirements of covertness, secrecy and transmission performances. Note that Problem P2 conducts the optimization over the power allo-

cation parameter ρ and the secrecy rate R_s.

After solving the optimization problem P2, we obtain the CSR under the AN-based transmission scheme, which is given in the following theorem.

Theorem V.2 *Under the scenario where Willie and Eve are active attackers and Alice adopts the AN-based secure transmission scheme, the CSR of the system is*

$$R_{cs}^{\mathrm{AN}} = \frac{R_{s,\mathrm{AN}}^{*}(\rho_{\mathrm{AN}}^{*})\left(\rho_{\mathrm{AN}}^{*}P_a - (2^{R_{s,\mathrm{AN}}^{*}(\rho_{\mathrm{AN}}^{*})}-1)(1-\rho_{\mathrm{AN}}^{*})P_a\right)^2}{\left(\rho_{\mathrm{AN}}^{*}P_a+(2^{R_{s,\mathrm{AN}}^{*}(\rho_{\mathrm{AN}}^{*})}-1)(P_w-(1-\rho_{\mathrm{AN}}^{*})P_a)\right)\left(\rho_{\mathrm{AN}}^{*}P_a+(2^{R_{s,\mathrm{AN}}^{*}(\rho_{\mathrm{AN}}^{*})}-1)(P_e-(1-\rho_{\mathrm{AN}}^{*})P_a)\right)} \times \exp\left(-\frac{(2^{R_{s,\mathrm{AN}}^{*}(\rho_{\mathrm{AN}}^{*})}-1)\sigma_b^2}{\rho_{\mathrm{AN}}^{*}P_a-(2^{R_{s,\mathrm{AN}}^{*}(\rho_{\mathrm{AN}}^{*})}-1)(1-\rho_{\mathrm{AN}}^{*})P_a}\right), \tag{5.38}$$

where the optimal power allocation parameter ρ_{AN}^{*} solves $p_{co}^{\mathrm{AN}}(\rho,\theta_{\mathrm{AN}}^{*})=\epsilon_c$ with θ_{AN}^{*} given by (5.34)*. Here, the optimal secrecy rate $R_{s,\mathrm{AN}}^{*}$ can be obtained under three cases respectively and is given by*

$$R_{s,\mathrm{AN}}^{*}(\rho_{\mathrm{AN}}^{*}) = \begin{cases} R_{s,\mathrm{AN}}^{0}(\rho_{\mathrm{AN}}^{*}), & R_{s,\mathrm{AN}}^{0} \le \min\left\{R_{s,\mathrm{AN}}^{SOP}, R_{s,\mathrm{AN}}^{TP}\right\}, \\ R_{s,\mathrm{AN}}^{SOP}(\rho_{\mathrm{AN}}^{*}), & R_{s,\mathrm{AN}}^{SOP} \le \min\left\{R_{s,\mathrm{AN}}^{0}, R_{s,\mathrm{AN}}^{TP}\right\}, \\ R_{s,\mathrm{AN}}^{TP}(\rho_{\mathrm{AN}}^{*}), & R_{s,\mathrm{AN}}^{TP} \le \min\left\{R_{s,\mathrm{AN}}^{0}, R_{s,\mathrm{AN}}^{SOP}\right\}, \end{cases} \tag{5.39}$$

where the stationary point $R_{s,\mathrm{AN}}^{0}$ can be obtained by solving $\frac{\partial R_{cs}^{\mathrm{AN}}}{\partial R_s}=0$, $R_{s,\mathrm{AN}}^{SOP}$ and $R_{s,\mathrm{AN}}^{TP}$ are the solutions of $p_{so}^{\mathrm{AN}}(R_s)=\epsilon_s$ and $p_{tx}^{\mathrm{AN}}(R_s)=1-\epsilon_t$, respectively.

Proof 6 *As can be seen from* (5.37a)*, the power allocation parameter ρ and the target secrecy rate R_s are required to solve the optimization problem P2. We first derive the optimal ρ. We can see that as ρ increases, both the objective function in* (5.37a) *and the COP p_{co}^{AN} in* (5.33) *increase, while SOP p_{so}^{AN} in* (5.36) *and TP p_{tx}^{AN} in* (5.30) *decrease. Thus, based on the covertness constraint in* (5.37b)*, the optimal power allocation parameter ρ_{AN}^{*} can be obtained by solving $p_{co}^{\mathrm{AN}}(\rho,\theta_{\mathrm{AN}}^{*})=\epsilon_c$.*

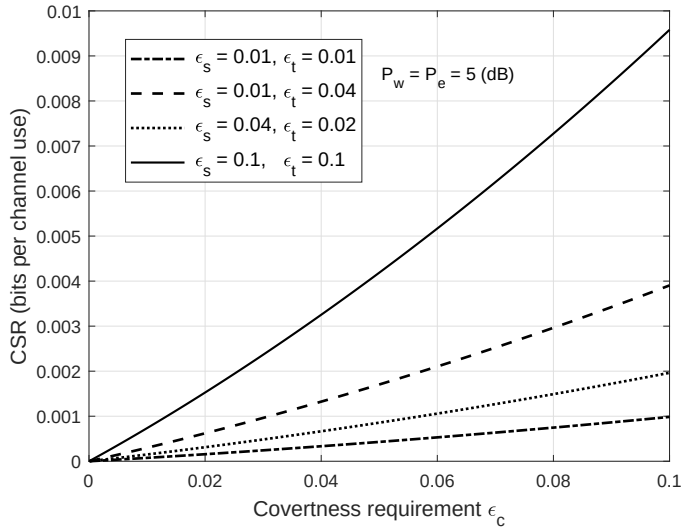
Next, we derive the optimal R_s by analyzing the feasible region of R_s and the monotonicity of the objective function with respect to R_s. We can see that as R_s increases, p_{tx}^{AN} in (5.30) *monotonically decreases while p_{so}^{AN} in* (5.36) *monotonically increases. Thus, based on the constraints* (5.37d) *and* (5.37c)*, the regions of R_s for ensuring secrecy and transmission performances are $[0, R_{s,\mathrm{AN}}^{TP}]$ and $[0, R_{s,\mathrm{AN}}^{SOP}]$, where $R_{s,\mathrm{AN}}^{TP}$ and $R_{s,\mathrm{AN}}^{SOP}$ are the solutions of $p_{tx}^{\mathrm{AN}}(R_s) = 1 - \epsilon_t$ and $p_{so}^{\mathrm{AN}}(R_s) = \epsilon_s$, respectively. Hence, the feasible region of R_s is $[0, \min\{R_{s,\mathrm{AN}}^{TP}, R_{s,\mathrm{AN}}^{SOP}\}]$. In addition, we can obtain the stationary point $R_{s,\mathrm{AN}}^{0}$ by solving $\frac{\partial R_{cs}^{\mathrm{AN}}}{\partial R_s} = 0$, and thus the objective function first increases over $[0, R_{s,\mathrm{AN}}^{0})$ and then decreases over $(R_{s,\mathrm{AN}}^{0}, \infty)$.*

The analyses regarding the feasible region of R_s and the optimal R_s is similar to that in Theorem V.1 and thus omitted here. Substituting the optimal power allocation parameter ρ_{AN}^{*} and the target secrecy rate $R_{s,\mathrm{AN}}^{*}$ into the objective function in (5.37a) *completes the proof.*

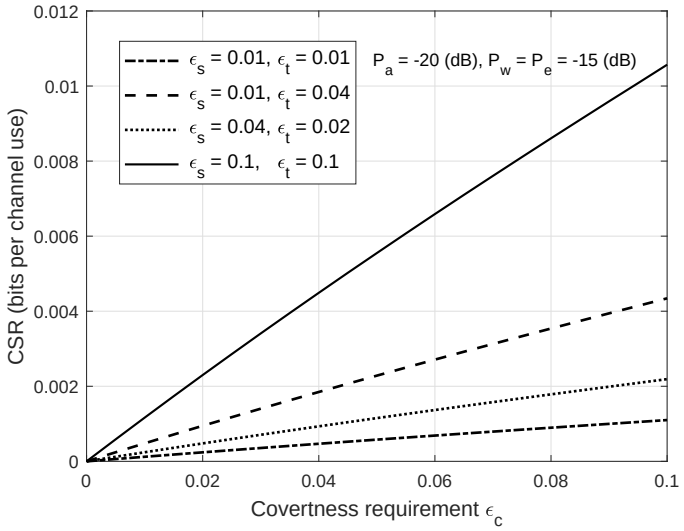
5.4 Numerical Results

In this section, we provide extensive numerical results to illustrate the CSR performances based on two transmission schemes in the new secure communication paradigm with active attackers. We also show the impacts of various system parameters (e.g., covertness requirement ϵ_c, secrecy requirement ϵ_s, transmission requirement ϵ_t and transmit power P_a) on the CSR performances. Unless otherwise stated, we set the noise powers at Bob, Willie and Eve to $\sigma_b^2 = -20$ (dB) and $\sigma_w^2 = \sigma_e^2 = 0$ (dB).

To explore the impact of the covertness requirement ϵ_c, secrecy requirement ϵ_s and transmission requirement ϵ_t on the CSR performance, we show in Fig. 5.6 R_{cs} vs. ϵ_c under the PC-based and AN-based transmission schemes, respectively. We set the transmit power of ANs from Willie and Eve to $P_w = P_e = 5$ dB in Fig. 5.6(a) and that to $P_w = P_e = -15$ dB in Fig. 5.6(b). We also set the transmit power of Alice to $P_a = -20$ dB in Fig. 5.6(b). In each subfigure of Fig. 5.6(a) and Fig. 5.6(b), we plot



(a) PC-based transmission scheme.



(b) AN-based transmission scheme.

Figure 5.6: Impacts of covertness requirement ϵ_c, secrecy requirement ϵ_s and transmission requirement ϵ_t on CSR R_{cs}.

the CSR curves under different settings of secrecy requirement ϵ_s and transmission requirement ϵ_t. We can see from Fig. 5.6(a) and Fig. 5.6(b) that the CSRs achieved under different secrecy and transmission requirements always increase as ϵ_c increases. This is because a looser covertness requirement results in a larger optimal transmit power in the PC-based scheme (resp. a larger optimal power allocation parameter in

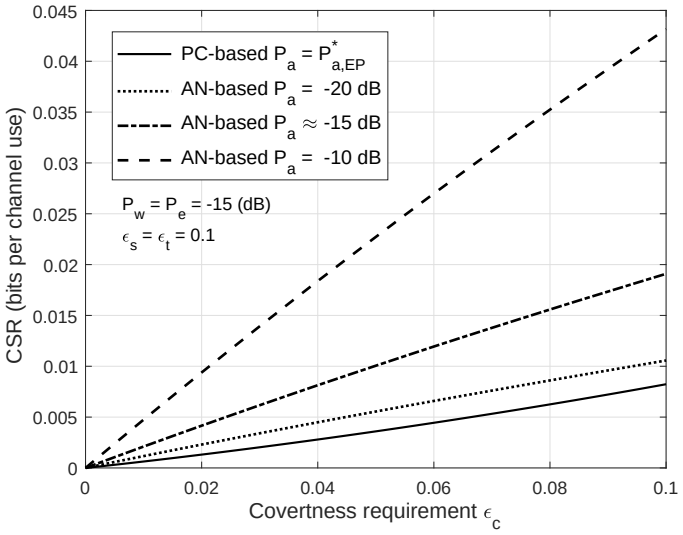
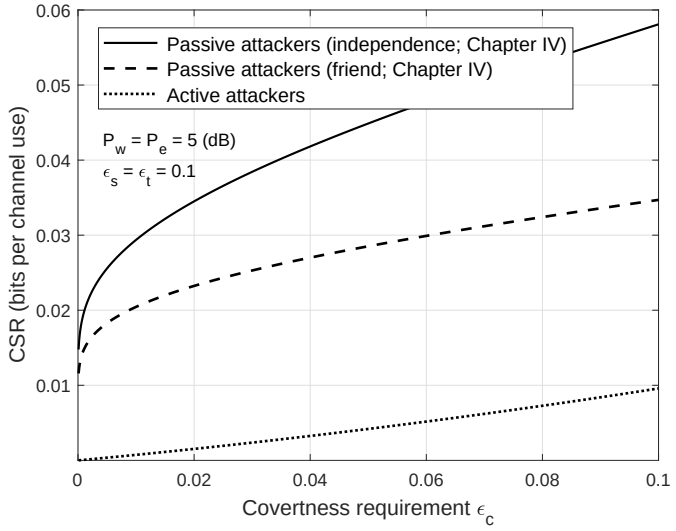


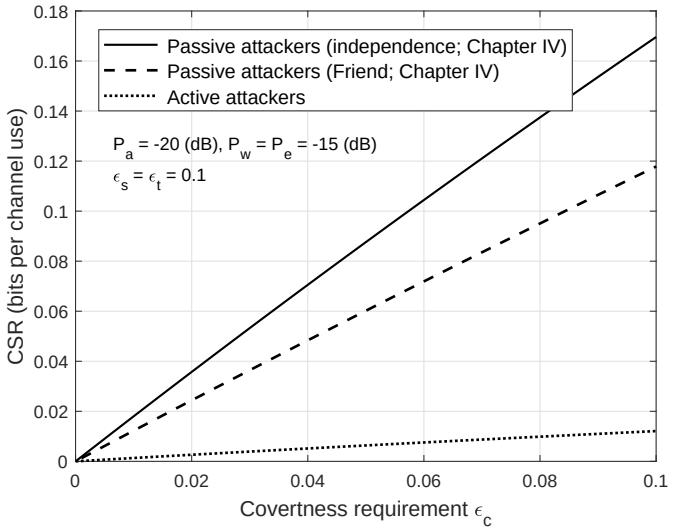
Figure 5.7: Comparisons of the CSR performances in the PC-based and AN-based transmission schemes.

the AN-based scheme) and thus a larger CSR. We can also see from the Fig. 5.6 that, under the same secrecy requirement ϵ_s, CSR is larger when transmission requirement ϵ_t is larger. This is because the optimal target secrecy rate is $R^*_{s,\mathrm{PC}} = R^{\mathrm{TP}}_{s,\mathrm{PC}}$ for ϵ_t, which increases as ϵ_t increases. In addition, the similar phenomena can be observed for the impact of secrecy requirement ϵ_s to CSR in Fig. 5.6. The above observations indicate that when any one of ϵ_c, ϵ_s or ϵ_t is looser, the CSR performance can always be improved.

We next explore the impacts of the PC-based and AN-based transmission schemes on the CSR performance with various values of transmit power of Alice P_a under the active attacker scenario in Fig. 5.7. We set the secrecy requirement and transmission requirement to $\epsilon_s = \epsilon_t = 0.1$ and the transmit power of Willie and Eve to $P_w = P_e = -15$ (dB) in Fig. 5.7. Comparing the curves of AN-based cases in Fig. 5.7, we can see that, as P_a increases, the CSRs for both AN-based schemes in the active attacker scenario increase. We can also observe that, under the different setting of P_a, the CSRs in AN-based always larger than that in PC-based at any ϵ_c. The above observations indicate that the AN-based scheme outperforms the PC-based scheme



(a) PC-based transmission scheme.



(b) AN-based transmission scheme.

Figure 5.8: Comparisons of the CSR performances under the passive and active attacker scenarios.

by adjusting the message transmit power.

Finally, we compare the CSR performances under the passive attacker scenario studied in Chapter IV and the active attacker scenario considered in this chapter. We set the transmit power of ANs from Willie and Eve to $P_w = P_e = 5$ dB in Fig. 5.8(a) and that to $P_w = P_e = -15$ dB in Fig. 5.8(b). We set the transmit power

of Alice to $P_a = -20$ dB in Fig. 5.8(b). We also set the secrecy requirement and transmission requirement to $\epsilon_s = \epsilon_t = 0.1$ in Fig. 5.8. From each subfigure, we can see that the CSR in the active attacker scenario is always smaller than that in the passive attacker scenario. The observation indicates that sending jamming signals and attacking simultaneously can reduce the CSR and thus impair the performance of new secure communication paradigm.

5.5 Discussion

This work represents a significant research progress in the joint guarantees of covertness and secrecy for wireless communications, and contributes an in-depth research on the proposed secure paradigm in Chapter IV. We, for the first time, consider the active attackers in the secure wireless communication paradigm scenario, where two attackers (i.e., detector and eavesdropper) perform ANs and detection/eavesdropping simultaneously. In addition to a motivation that ANs from attackers can degrade decoding performance of the receiver, the ANs can also be jamming signals to weaken the attack performance of another attacker. This is motivated by the fact that competitive or hostile relationships may exist between detectors and eavesdroppers as the members of different alliances.

Based on the work in this chapter, in the future we can consider that the active detector/eavesdropper performs ANs to destroy the training phase of the pilot-based channel estimation design in wireless communications. More specifically, before transmitting information signals, when the transmitter sends a pilot signal to the receiver, the active detector/eavesdropper performs ANs to interfere with the channel estimation at the receiver, resulting in an incorrect design of the transmitter's pre-coder, so that the detection/eavesdropping performance can be improved. In addition, we consider a common assumption that the instantaneous channel state information (CSI) is unknown to the detector, which is not practical, and thus in future work we

can assume that the instantaneous CSI is known to the detector because of its more powerful capabilities. We also assume that the transmit power of AN from detector/eavesdropper is fixed, while in future work we can further consider the case of randomly varying transmit power from detector/eavesdropper so as to implement the new secure paradigm in a more complex wireless communication scenario.

5.6 Summary

In this chapter, we considered a secure wireless communication paradigm with active attacker scenario, where attackers perform detection/eavesdropping and jamming simultaneously. In the scenario, we applied physical layer security technology to counteract both detection and eavesdropping attacks, such that the covertness and secrecy guarantee in wireless communication can be achieved. To understand the covertness, secrecy and transmission performances in the active attacker scenario, we conducted theoretical analyses to identify the covert secrecy rate (CSR) under power control (PC)-based and artificial noise (AN)-based transmission schemes, respectively. The results in this chapter showed that relaxing the covertness, secrecy and transmission requirements can improve the CSR performances, and utilizing AN-based scheme is a better choice than using the PC-based scheme by adjusting the message transmit power. In addition, the comparisons of CSR performance in passive and active attacker scenarios indicated that the active detection/eavesdropping attacks can impair the CSR performance in the new secure communication paradigm.

CHAPTER VI

Conclusion

In this thesis, we explored the joint guarantee of covertness and secrecy properties in wireless communications and thus proposed a new secure wireless communication paradigm in which the physical layer security technology is applied to counteract both detection and eavesdropping attacks. We first studied the covertness guarantee and the performance limit of covert throughput in two-way two-hop wireless communication systems. We then explored a new secure wireless communication paradigm where the critical covertness and secrecy properties of communication are jointly guaranteed under passive detection/eavesdropping attacks. Finally, we extended the secure wireless communication paradigm to the active attacker scenario, where attackers perform detection/eavesdropping and jamming simultaneously.

For the covertness guarantee in two-way two-hop wireless communication systems, we studied in Chapter III the performance of two-way relay communication systems, where two sources wish to covertly exchange information through a relay without being detected from a detector. We first propose covertness strategies for the systems, and then derive scaling law results of the covert throughput for various scenarios with different relaying patterns (i.e., four-slot, three-slot and two-slot), and prior knowledge of the legitimate nodes and detector. The main results in Chapter III showed that covert throughput of the concerned two-way two-hop wireless systems follows the

$\mathcal{O}(\sqrt{n})$ scaling law, which is independent of the relaying patterns, detection schemes, covertness strategies, and prior knowledge of the sources and detector.

For the joint guarantee of covertness and secrecy in wireless communications, we explored in Chapter IV a new secure wireless communication paradigm, where the physical layer security technology is applied to ensure both covertness and secrecy of the communication. We define a novel metric of covert secrecy rate (CSR) to depict the security performance of the new paradigm, and also provide solid theoretical analysis on CSR under two transmission schemes (i.e., artificial noise (AN)-based one and power control (PC)-based one) and two detector-eavesdropper relationships (i.e., independence and friend). The main results in Chapter IV indicated that in general, the CSR performance can be improved when the constraints on covertness, secrecy, and transmission performance become less strict. In particular, the PC-based transmission scheme outperforms the AN-based transmission scheme in terms of the CSR performance when strict constraints are applied to the covertness, secrecy, and transmission performance. While these constraints become less strict, the AN-based scheme may achieve better CSR performance than the PC-based one by properly adjusting the message transmit power.

In Chapter V, we extended the secure wireless communication paradigm in Chapter IV to the active attacker scenario where attackers perform detection/eavesdropping and jamming simultaneously. In this active attacker scenario, we apply physical layer security technology to counteract both detection and eavesdropping attacks, such that the covertness and secrecy guarantees in wireless communication can be achieved. To understand the covertness, secrecy, and transmission performances in the active attacker scenario, we conduct theoretical analyses to identify the CSR under PC-based and AN-based transmission schemes, respectively. The main results in Chapter V demonstrated that relaxing the covertness, secrecy, and transmission requirements can improve the CSR performances, and utilizing AN-based scheme is a better choice

than using the PC-based scheme by adjusting the message transmit power. In addition, the comparisons of CSR performances in passive and active attacker scenarios indicated that active detection/eavesdropping attacks can impair the CSR performance in the new secure communication paradigm.

It is notable that, this thesis considers relatively simple communication scenarios, while practical communication scenarios are more complex and changeable. Therefore, one of the interesting and important future work is to achieve covertness and secrecy guarantees and study the new secure communication paradigm in large-scale wireless networks. In the end, we still expect that the work of this thesis can shed light on the future studies of new secure wireless communication paradigms.

BIBLIOGRAPHY

BIBLIOGRAPHY

[1] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, 2016.

[2] P. Yang, Y. Xiao, M. Xiao, and S. Li, "6G wireless communications: Vision and potential techniques," *IEEE Network*, vol. 33, no. 4, pp. 70–75, 2019.

[3] D. Djenouri, L. Khelladi, and A. N. Badache, "A survey of security issues in mobile ad hoc and sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 7, no. 4, 2020.

[4] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, "Hiding information in noise: Fundamental limits of covert wireless communication," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 26–31, 2015.

[5] S. Yan, X. Zhou, J. Hu, and S. V. Hanly, "Low probability of detection communication: Opportunities and challenges," *IEEE Wireless Communications*, vol. 26, no. 5, pp. 19–25, 2019.

[6] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1878–1911, 2018.

[7] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1773–1828, 2018.

[8] J. Lubacz, W. Mazurczyk, and K. Szczypiorski, "Principles and overview of network steganography," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 225–229, 2014.

[9] M. Barni, "Steganography in digital media: Principles, algorithms, and applications (fridrich, j. 2010)[book reviews]," *IEEE Signal Processing Magazine*, vol. 28, no. 5, pp. 142–144, 2011.

[10] M. Simon, J. Omura, R. Scholtz, and B. Levitt, *Spread spectrum communications handbook*. McGraw-Hill Education, 2002.

[11] D. R. Stinson and M. Paterson, *Cryptography: theory and practice*. CRC Press, 2018.

[12] M. S. BenSaleh, R. Saida, Y. H. Kacem, and M. Abid, "Wireless sensor network design methodologies: A survey," *Journal of Sensors*, vol. 2020, 2020.

[13] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020.

[14] L. Gyongyosi and S. Imre, "A survey on quantum computing technology," *Computer Science Review*, vol. 31, pp. 51–71, 2019.

[15] Y. Liu, H.-H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 347–376, 2016.

[16] Y. Liang, H. V. Poor, S. Shamai *et al.*, "Information theoretic security," *Foundations and Trends® in Communications and Information Theory*, vol. 5, no. 4–5, pp. 355–580, 2009.

[17] B. A. Forouzan, *Cryptography & network security*. McGraw-Hill, Inc., 2007.

[18] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[19] J. Hu, S. Yan, X. Zhou, F. Shu, J. Li, and J. Wang, "Covert communication achieved by a greedy relay in wireless networks," *IEEE Transactions on Wireless Communications*, vol. 17, no. 7, pp. 4766–4779, 2018.

[20] M. Forouzesh, P. Azmi, N. Mokari, and D. Goeckel, "Robust power allocation in covert communication: Imperfect CDI," *arXiv preprint arXiv:1901.04914*, 2019.

[21] K. Shahzad, X. Zhou, S. Yan, J. Hu, F. Shu, and J. Li, "Achieving covert wireless communications using a full-duplex receiver," *IEEE Transactions on Wireless Communications*, vol. 17, no. 12, pp. 8517–8530, 2018.

[22] M. Zheng, A. Hamilton, and C. Ling, "Covert communications with a full-duplex receiver in non-coherent rayleigh fading," *IEEE Transactions on Communications*, 2020.

[23] T. V. Sobers, B. A. Bash, S. Guha, D. Towsley, and D. Goeckel, "Covert communication in the presence of an uninformed jammer," *IEEE Transactions on Wireless Communications*, vol. 16, no. 9, pp. 6193–6206, 2017.

[24] K. Li, P. A. Kelly, and D. Goeckel, "Optimal power adaptation in covert communication with an uninformed jammer," *IEEE Transactions on Wireless Communications*, vol. 19, no. 5, pp. 3463–3473, 2020.

[25] S.-H. Lee, L. Wang, A. Khisti, and G. W. Wornell, "Covert communication with channel-state information at the transmitter," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2310–2319, 2018.

[26] D. Goeckel, B. Bash, S. Guha, and D. Towsley, "Covert communications when the warden does not know the background noise power," *IEEE Communications Letters*, vol. 20, no. 2, pp. 236–239, 2016.

[27] B. He, S. Yan, X. Zhou, and V. K. Lau, "On covert communication with noise uncertainty," *IEEE Communications Letters*, vol. 21, no. 4, pp. 941–944, 2017.

[28] K. Shahzad, X. Zhou, and S. Yan, "Covert wireless communication in presence of a multi-antenna adversary and delay constraints," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 12, pp. 12 432–12 436, 2019.

[29] T.-X. Zheng, H.-M. Wang, D. W. K. Ng, and J. Yuan, "Multi-antenna covert communications in random wireless networks," *IEEE Transactions on Wireless Communications*, vol. 18, no. 3, pp. 1974–1987, 2019.

[30] D. Kibloff, S. M. Perlaza, and L. Wang, "Embedding covert information on a given broadcast code," in *2019 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2019, pp. 2169–2173.

[31] M. Tahmasbi and M. R. Bloch, "Covert secret key generation with an active warden," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1026–1039, 2019.

[32] C. Gao, B. Yang, X. Jiang, H. Inamura, and M. Fukushi, "Covert communication in relay-assisted IoT systems," *IEEE Internet of Things Journal*, 2021.

[33] Y. Su, H. Sun, Z. Zhang, Z. Lian, Z. Xie, and Y. Wang, "Covert communication with relay selection," *IEEE Wireless Communications Letters*, 2020.

[34] L. Sun, T. Xu, S. Yan, J. Hu, X. Yu, and F. Shu, "On resource allocation in covert wireless communication with channel estimation," *IEEE Transactions on Communications*, vol. 68, no. 10, pp. 6456–6469, 2020.

[35] Y. Zhang, Y. Shen, X. Jiang, and S. Kasahara, "Secure millimeter-wave ad hoc communications using physical layer security," *IEEE Transactions on Information Forensics and Security*, pp. 1–1, 2021.

[36] F. Sarkohaki, R. Fotohi, and V. Ashrafian, "An efficient routing protocol in mobile ad-hoc networks by using artificial immune system," *arXiv preprint arXiv:2003.00869*, 2020.

[37] Y. Zhang, Y. Shen, X. Jiang, and S. Kasahara, "Mode selection and spectrum partition for D2D inband communications: A physical layer security perspective," *IEEE Transactions on Communications*, vol. 67, no. 1, pp. 623–638, 2018.

[38] M. H. Khoshafa, T. M. Ngatched, M. H. Ahmed, and A. Ibrahim, "Secure transmission in wiretap channels using full-duplex relay-aided D2D communications with outdated CSI," *IEEE Wireless Communications Letters*, vol. 9, no. 8, pp. 1216–1220, 2020.

[39] Z. Peng, Z. Zhang, C. Pan, L. Li, and A. L. Swindlehurst, "Multiuser full-duplex two-way communications via intelligent reflecting surface," *IEEE Transactions on Signal Processing*, 2021.

[40] Z. H. Abbas, G. Abbas, M. S. Haroon, and F. Muhammad, "Analysis of interference management in heterogeneous cellular networks in the presence of wideband jammers," *IEEE Communications Letters*, vol. 24, no. 5, pp. 1138–1141, 2020.

[41] Y. Zhang, Y. Shen, H. Wang, J. Yong, and X. Jiang, "On secure wireless communications for IoT under eavesdropper collusion," *IEEE Transactions on Automation Science and Engineering*, vol. 13, no. 3, pp. 1281–1293, 2015.

[42] W. U. Khan, F. Jameel, M. A. Jamshed, H. Pervaiz, S. Khan, and J. Liu, "Efficient power allocation for NOMA-enabled IoT networks in 6G era," *Physical Communication*, vol. 39, p. 101043, 2020.

[43] S. Zhao, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, "Secure beamforming for full-duplex MIMO two-way untrusted relay systems," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3775–3790, 2020.

[44] X. Huanga, A. T. Leb, and Y. J. Guoc, "Transmit beamforming for communication and self-interference cancellation in full duplex MIMO systems: A trade-off analysis," *IEEE Transactions on Wireless Communications*, 2021.

[45] Q. Wang, F. Zhou, R. Q. Hu, and Y. Qian, "Energy efficient robust beamforming and cooperative jamming design for IRS-assisted MISO networks," *IEEE Transactions on Wireless Communications*, 2020.

[46] J. He, J. Liu, Y. Shen, X. Jiang, and N. Shiratori, "Link selection for security-QoS tradeoffs in buffer-aided relaying networks," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1347–1362, 2019.

[47] Y. Feng, S. Yan, C. Liu, Z. Yang, and N. Yang, "Two-stage relay selection for enhancing physical layer security in non-orthogonal multiple access," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, pp. 1670–1683, 2018.

[48] Y. Liu, W. Wang, H.-H. Chen, L. Wang, N. Cheng, W. Meng, and X. Shen, "Secrecy rate maximization via radio resource allocation in cellular underlaying V2V communications," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 7, pp. 7281–7294, 2020.

[49] Y. Wu, J. Shi, K. Ni, L. Qian, W. Zhu, Z. Shi, and L. Meng, "Secrecy-based delay-aware computation offloading via mobile edge computing for internet of things," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4201–4213, 2018.

[50] W. Wu, F. Zhou, R. Q. Hu, and B. Wang, "Energy-efficient resource allocation for secure NOMA-enabled mobile edge computing networks," *IEEE Transactions on Communications*, vol. 68, no. 1, pp. 493–505, 2019.

[51] J. Sarangapani, *Wireless ad hoc and sensor networks: protocols, performance, and control*. CRC Press, 2017.

[52] B. Rashid and M. H. Rehmani, "Applications of wireless sensor networks for urban areas: A survey," *Journal of network and computer applications*, vol. 60, pp. 192–219, 2016.

[53] S. Narayanan, "Two-hop forwarding in wireless networks," Ph.D. dissertation, Polytechnic University, 2006.

[54] R. H. Louie, Y. Li, and B. Vucetic, "Practical physical layer network coding for two-way relay channels: performance analysis and comparison," *IEEE Transactions on Wireless Communications*, vol. 9, no. 2, 2010.

[55] B. A. Bash, D. Goeckel, and D. Towsley, "Square root law for communication with low probability of detection on AWGN channels," in *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*. IEEE, 2012, pp. 448–452.

[56] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 8, pp. 3693–3704, 2012.

[57] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[58] 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.

[59] A. Carleial and M. Hellman, "A note on Wyner's wiretap channel (corresp.)," *IEEE Transactions on Information Theory*, vol. 23, no. 3, pp. 387–390, 1977.

[60] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *AT&T Bell Laboratories Technical Journal*, vol. 63, no. 10, pp. 2135–2157, 1984.

[61] 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.

[62] H. Xing, L. Liu, and R. Zhang, "Secrecy wireless information and power transfer in fading wiretap channel," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 1, pp. 180–190, 2015.

[63] S. Allipuram, P. Mohapatra, and S. Chakrabarti, "Secrecy performance of an artificial noise assisted transmission scheme with active eavesdropper," *IEEE Communications Letters*, 2020.

[64] I. Bang, S. M. Kim, and D. K. Sung, "Artificial noise-aided user scheduling from the perspective of secrecy outage probability," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 8, pp. 7816–7820, 2018.

[65] B. Li, Y. Zou, J. Zhou, F. Wang, W. Cao, and Y.-D. Yao, "Secrecy outage probability analysis of friendly jammer selection aided multiuser scheduling for wireless networks," *IEEE Transactions on Communications*, vol. 67, no. 5, pp. 3482–3495, 2019.

[66] X. Li, Y. Zhang, S. Zhao, Y. Shen, and X. Jiang, "Exact secrecy throughput capacity study in mobile ad hoc networks," *Ad Hoc Networks*, vol. 72, pp. 105–114, 2018.

[67] Y. Zhang, Y. Shen, and X. Jiang, "Friendship-based cooperative jamming for secure communication in poisson networks," *Wireless Networks*, vol. 25, no. 7, pp. 4077–4095, 2019.

[68] P. Zhang, Y. Shen, X. Jiang, and B. Wu, "Physical layer authentication jointly utilizing channel and phase noise in MIMO systems," *IEEE Transactions on Communications*, 2020.

[69] Y. Zou, T. Wu, M. Sun, J. Zhu, M. Qian, and C. Liu, "Secrecy outage analysis of non-orthogonal spectrum sharing for heterogeneous cellular networks," *IEEE Transactions on Communications*, vol. 67, no. 9, pp. 6626–6640, 2019.

[70] H. Ma, J. Cheng, and X. Wang, "Proportional fair secrecy beamforming for MISO heterogeneous cellular networks with wireless information and power transfer," *IEEE Transactions on Communications*, vol. 67, no. 8, pp. 5659–5673, 2019.

[71] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1921–1930, 2013.

[72] B. Haeupler, P. Kamath, and A. Velingker, "Communication with partial noiseless feedback," in *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2015)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2015.

[73] G. Wang, Y. Qin, and C. Chang, "Communication with partial noisy feedback," in *2017 IEEE Symposium on Computers and Communications (ISCC)*. IEEE, 2017, pp. 602–607.

[74] K. Efremenko, R. Gelles, and B. Haeupler, "Maximal noise in interactive communication over erasure channels and channels with feedback," *IEEE Transactions on Information Theory*, vol. 62, no. 8, pp. 4575–4588, 2016.

[75] Z. Liu, J. Liu, Y. Zeng, Z. Ma, J. Ma, and Q. Huang, "Challenges in covert wireless communications with active warden on AWGN channels," *arXiv preprint arXiv:1901.03185*, 2019.

[76] P. H. Che, M. Bakshi, C. Chan, and S. Jaggi, "Reliable, deniable and hidable communication," in *Information Theory and Applications Workshop (ITA), 2014*. IEEE, 2014, pp. 1–10.

[77] M. Bloch, "A channel resolvability perspective on stealth communications," in *2015 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2015, pp. 2535–2539.

[78] L. Wang, G. W. Wornell, and L. Zheng, "Fundamental limits of communication with low probability of detection," *IEEE Transactions on Information Theory*, vol. 62, no. 6, pp. 3493–3503, 2016.

[79] B. A. Bash, D. Goeckel, and D. Towsley, "LPD communication when the warden does not know when," in *Information Theory (ISIT), 2014 IEEE International Symposium on*. IEEE, 2014, pp. 606–610.

[80] R. Soltani, D. Goeckel, D. Towsley, B. Bash, and S. Guha, "Covert wireless communication with artificial noise generation," *arXiv preprint arXiv:1709.07096*, 2017.

[81] B. A. Bash, D. Goeckel, and D. Towsley, "Covert communication gains from adversary's ignorance of transmission time," *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 8394–8405, 2016.

[82] S. Yan, B. He, X. Zhou, Y. Cong, and A. L. Swindlehurst, "Delay-intolerant covert communications with either fixed or random transmit power," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 1, pp. 129–140, 2019.

[83] J. Hu, S. Yan, X. Zhou, F. Shu, and J. Li, "Covert wireless communications with channel inversion power control in rayleigh fading," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 12, pp. 12 135–12 149, 2019.

[84] K. S. K. Arumugam and M. R. Bloch, "Covert communication over a k-user multiple-access channel," *IEEE Transactions on Information Theory*, vol. 65, no. 11, pp. 7020–7044, 2019.

[85] V. Y. Tan and S.-H. Lee, "Time-division is optimal for covert communication over some broadcast channels," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 5, pp. 1377–1389, 2019.

[86] K. S. K. Arumugam and M. R. Bloch, "Embedding covert information in broadcast communications," *IEEE Transactions on Information Forensics and Security*, 2019.

[87] J. Wang, W. Tang, Q. Zhu, X. Li, H. Rao, and S. Li, "Covert communication with the help of relay and channel uncertainty," *IEEE Wireless Communications Letters*, vol. 8, no. 1, pp. 317–320, 2018.

[88] H. Wu, Y. Zhang, X. Liao, Y. Shen, and X. Jiang, "On covert throughput performance of two-way relay covert wireless communications," *Wireless Networks*, pp. 1–15, 2020.

[89] H. Wu, X. Liao, Y. Dang, Y. Shen, and X. Jiang, "Limits of covert communication on two-hop AWGN channels," in *Networking and Network Applications (NaNA), 2017 International Conference on.* IEEE, 2017, pp. 42–47.

[90] A. Sheikholeslami, M. Ghaderi, D. Towsley, B. A. Bash, S. Guha, and D. Goeckel, "Multi-hop routing in covert wireless networks," *IEEE Transactions on Wireless Communications*, 2018.

[91] R. Miao and Y. Huang, "An approach of covert communication based on the adaptive steganography scheme on voice over IP," in *2011 IEEE International Conference on Communications (ICC).* IEEE, 2011, pp. 1–5.

[92] H. Zhao, Y. Q. Shi, and N. Ansari, "Hiding data in multimedia streaming over networks," in *2010 8th Annual Communication Networks and Services Research Conference.* IEEE, 2010, pp. 50–55.

[93] O. I. Abdullaziz, V. T. Goh, H.-C. Ling, and K. Wong, "Network packet payload parity based steganography," in *2013 IEEE Conference on Sustainable Utilization and Development in Engineering and Technology (CSUDET).* IEEE, 2013, pp. 56–59.

[94] E. L. Lehmann and J. P. Romano, *Testing statistical hypotheses.* Springer Science & Business Media, 2006.

[95] T. M. Cover and J. A. Thomas, *Elements of information theory.* John Wiley & Sons, 2012.

[96] S. Lang, *Undergraduate analysis.* Springer Science & Business Media, 2013.

[97] S. Kullback, *Information theory and statistics*. Courier Corporation, 1997.

[98] T. Filler, A. D. Ker, and J. Fridrich, "The square root law of steganographic capacity for markov covers," in *Media Forensics and Security*, vol. 7254. International Society for Optics and Photonics, 2009, p. 725408.

[99] U. Madhow, *Fundamentals of digital communication*. Cambridge University Press, 2008.

[100] B. Rankov and A. Wittneben, "Achievable rate regions for the two-way relay channel," in *Information theory, 2006 IEEE international symposium on*. IEEE, 2006, pp. 1668–1672.

[101] T. H. Cormen, *Introduction to Algorithms*. MIT press, 2009.

[102] A. Browder, *Mathematical analysis: an introduction*. Springer Science & Business Media, 2012.

[103] 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.

[104] M. Forouzesh, P. Azmi, A. Kuhestani, and P. L. Yeoh, "Joint information theoretic secrecy and covert communication in the presence of an untrusted user and warden," *IEEE Internet of Things Journal*, vol. 8, no. 9, pp. 7170–7181, 2020.

[105] M. Forouzesh, P. Azmi, A. Kuhestani, and P. L. Yeoh, "Covert communication and secure transmission over untrusted relaying networks in the presence of multiple wardens," *IEEE Transactions on Communications*, vol. 68, no. 6, pp. 3737–3749, 2020.

[106] S. Bameri, R. H. Gohary, and S. Talebi, "Perfect self-interference cancellation based on mode-switching for differential channel-unaware two-way relay networks," *IEEE Transactions on Wireless Communications*, vol. 18, no. 11, pp. 5269–5283, 2019.

[107] S. Allipuram, P. Mohapatra, and S. Chakrabarti, "Secrecy performance of an artificial noise assisted transmission scheme with active eavesdropper," *IEEE Communications Letters*, vol. 24, no. 5, pp. 971–975, 2020.

[108] X. Zhou, M. R. McKay, B. Maham, and A. Hjorungnes, "Rethinking the secrecy outage formulation: A secure transmission design perspective," *IEEE Communications Letters*, vol. 15, no. 3, pp. 302–304, 2011.

[109] A. K. Sadek, K. R. Liu, and A. Ephremides, "Cognitive multiple access via cooperation: Protocol design and performance analysis," *IEEE Transactions on Information Theory*, vol. 53, no. 10, pp. 3677–3696, 2007.

Publications

Journal Articles

[1] Huihui Wu, Yuanyu Zhang, Xuening Liao, Yulong Shen and Xiaohong Jiang. On covert throughput performance of two-way relay covert wireless communications. *Wireless Networks*, 26: 3275-3289 (2020).

[2] Huihui Wu, Yuanyu Zhang, Yulong Shen and Xiaohong Jiang. Achieving covertness and secrecy: A new paradigm for secure wireless communication. *IEEE Transactions on Communications*, in peer review (2021); Published online: arXiv preprint arXiv:2008.00147.

[3] Huihui Wu, Yuanyu Zhang, Yulong Shen and Xiaohong Jiang. Covertness and secrecy guarantees in wireless communications with active attackers. *In preparation*, (2021).

Conference Papers

[4] Huihui Wu, Xuening Liao, Yongchao Dang, Yulong Shen and Xiaohong Jiang. Limits of covert communication on two-hop AWGN channels. 2017 International Conference on Networking and Network Applications (NaNA), pp. 42-47, 2017.