Wireless Networks

Feng Shu
Jiangzhou Wang

Intelligent Reflecting Surface-Aided Physical-Layer Security

Springer

Wireless Networks

Series Editor

Xuemin Sherman Shen, University of Waterloo, Waterloo, ON, Canada

The purpose of Springer's Wireless Networks book series is to establish the state of the art and set the course for future research and development in wireless communication networks. The scope of this series includes not only all aspects of wireless networks (including cellular networks, WiFi, sensor networks, and vehicular networks), but related areas such as cloud computing and big data. The series serves as a central source of references for wireless networks research and development. It aims to publish thorough and cohesive overviews on specific topics in wireless networks, as well as works that are larger in scope than survey articles and that contain more detailed background information. The series also provides coverage of advanced and timely topics worthy of monographs, contributed volumes, textbooks and handbooks.

Feng Shu • Jiangzhou Wang

Intelligent Reflecting Surface-Aided Physical-Layer Security

Springer

Feng Shu
School of Information and Communication
Engineering, Hainan University
Haikou, China

Jiangzhou Wang
School of Engineering
University of Kent
Canterbury, UK

ISSN 2366-1186 ISSN 2366-1445 (electronic)
Wireless Networks
ISBN 978-3-031-41811-2 ISBN 978-3-031-41812-9 (eBook)
https://doi.org/10.1007/978-3-031-41812-9

Preface

With the explosive growth of the smart devices and data traffic, more data security and privacy protection services are needed to be supported in wireless communication networks. Because of the inherent broadcasting characteristic, diversity and complexity of wireless communication, electromagnetic waves spread around, which leads confidential messages to be easily intercepted or eavesdropped by unauthorized receivers. Therefore, compared with the conventional wired transmission, the wireless communication network is more vulnerable to be attacked.

The primary principle of designing a wireless communication system is to ensure the security of wireless data transmission. The conventional cryptography technology is so heavily dependent on the complex encryption and decryption protocols and key management mechanisms that it cannot friendly support the large-scale devices. Different from cryptography schemes, the physical-layer secure (PLS) technology including channel coding and precoding takes full advantage of the physical characteristics (i.e. noise, fading, interference) of wireless channel to obtain a secure and efficient data transmission. The traditional error correction coding can be modified by the channel coding technology to have the abilities to correct error and keep security, and the quality of eavesdropping channels can be poor by precoding technology to improve the security rate of the wireless communication system, so that a lightweight secure transmission scheme can be provided by the above two PLS technologies for the resource-constrained devices.

Recently, intelligent reflecting surface (IRS) has become a hot topic of research. By adjusting the reflection amplitude and phase of each IRS element, friendly multipaths can be created to achieve energy consumption reduction, signal enhancement and coverage extension. In view of these advantages, IRS has been applied to the PLS communication in some recent research. The IRS-aided PLS communication can be viewed as a new research direction, which has drawn much attention from research community.

As far as we know, there is no book focusing on the IRS-aided PLS communication networks. This book presents concepts and technologies, which are related to the topic of IRS-aided PLS communication in different application

scenarios. Additionally, some insightful discussions and effective recommendations are available in this book. The book is organized as follows:

Chapter 1 presents the overviews of PLS and IRS. The survey of the PLS research on various promising mobile technologies from secure key generation and keyless technique, including secure key generation, directional modulation, spatial modulation, covert communication and IRS-aided communication, are first introduced, followed by organization of the monograph.

Chapter 2 considers the enhanced secrecy rate maximization for directional modulation networks via IRS. The directional modulation and IRS first introduced, followed by the IRS-aided directional modulation model, the high-performance general alternating iterative (GAI)-based maximization methods, including the SR (Max-SR) method and low-complexity null-space projection (NSP)-based Max-SR method.

Chapter 3 investigates the high-performance estimation of jamming covariance matrix for IRS-aided directional modulation network with a malicious attacker, directional modulation and IRS are first introduced, followed by IRS-aided directional modulation network with malicious attacker model and three estimation methods.

Chapter 4 studies the beamforming and power allocation for double-IRS-aided two-way directional modulation network. The double-IRS-aided two-way directional modulation system model is first established, and the two transmit beamforming methods and a hybrid iterative closed-form power allocation strategy are proposed.

Chapter 5 explores the beamforming and transmit power design for IRS-aided secure spatial modulation. The spatial modulation and IRS are first introduced, followed by the IRS-aided secure spatial modulation system model, the joint optimization of IRS beamforming and transmit power design.

Chapter 6 considers the IRS-aided covert wireless communications with delay constraint. The IRS and covert communication technique are first introduced, followed by IRS-assisted wireless covert communication system model, the covert communication design with global channel state information (CSI) and covert communication design without Willie's instantaneous CSI.

Chapter 7 presents the IRS-aided secure transmission with colluding eavesdroppers. Secure communication system with colluding eavesdroppers (Eves) is first introduced, followed by an IRS-aided secure communication system model with colluding Eves, the semidefinite relaxation (SDR)-based method and low-complexity alternating optimization algorithm.

Chapter 8 develops the secure multigroup multicast communication systems via IRS. The secure multigroup multicast communication system is first introduced, followed by the IRS-aided secure multigroup multicast communication system model, the SDR-based alternating optimization method and low-complexity second-order cone programming (SOCP)-based algorithm.

Chapter 9 considers the beamforming design of IRS-aided decode-and-forward (DF) relay wireless network. The IRS and relay technology are first introduced,

followed by IRS-aided multi-antenna DF relay network model and three high-performance beamforming schemes.

Chapter 10 explores the performance analysis of wireless network aided by discrete-phase-shifter IRS. Some application scenarios of IRS-aided wireless network under line of sight (LoS) and Rayleigh channels are first introduced, followed by the performance loss (PL) derivation and analysis in the LoS channels and Rayleigh channels.

Chapter 11 concludes some promising directions, aiming to promote future research outcomes in the field of IRS-aided PLS communication.

The writing and publication of this book is supported in part by the National Natural Science Foundation of China (Nos.U22A2002, and 62071234), the Hainan Province Science and Technology Special Fund (ZDKJ2021022), and the Scientific Research Fund Project of Hainan University under Grant KYQD(ZR)-21008. Here, we expresses our sincere gratitude.

Haikou, China — Feng Shu
Canterbury, UK — Jiangzhou Wang
March 15, 2023

Acknowledgments

It has taken seven months to complete this book on IRS-aided PLS communication. We appreciate our graduate students' generous help and strong support.

We sincerely would like to thank the students for their hard work. Firstly, we thank the students who have made contribution to the writing of this book. The following names are listed to express our gratitude: Weiping Shi, Yin Teng, Hangjia He, Rongen Dong, Lili Yang, Xiaobo Zhou, Yang Wang and Xuehui Wang. We also thank the students who have made editing work for this book: Yifan Zhao, Zhilin Chen, Sihao Lai and Qiankun Cheng. Meanwhile, special thanks to Xuehui Wang and Yifan Zhao.

Finally, thanks also to Springer-Nature Publishing for its support and completion of the publication of this book.

Haikou, China — Feng Shu
Canterbury, UK — Jiangzhou Wang
March 15, 2023

Contents

About the Authors

Feng Shu received the Ph.D. degree in Information and Communication Engineering from Southeast University, China, in 2002. From September 2009 to September 2010, he was a Visiting Post-doctor with the University of Texas at Dallas, Richardson, TX, USA. From October 2005 to November 2020, he was with the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing, where he was promoted from Associate Professor to a Full Professor of supervising Ph.D. students in 2013. Since December 2020, he has been with the School of Information and Communication Engineering, Hainan University, Haikou, China, where he is currently a Professor and supervisor of Ph.D. and graduate students. His research interests include wireless networks, wireless location, and array signal processing. He is awarded with the Leading-talent Plan of Hainan Province in 2020, Fujian hundred-talent plan of Fujian Province in 2018, and Mingjian Scholar Chair Professor in 2015. He has authored or coauthored more than 300 in archival journals with more than 120 papers on IEEE Journals and 200 SCI-indexed papers. His citations are 4386. He holds 30 Chinese patents and also are PI or CoPI for 7 national projects. He was an IEEE Transactions on Communications Exemplary Reviewer for 2020. He is currently the Editor of *IEEE Wireless Communications Letters* and was an editor for the *IEEE Systems Journal*.

Jiangzhou Wang is a Professor with the University of Kent, UK. He has published more than 400 papers and 4 books. His research focuses on mobile communications. He was a recipient of the 2022 IEEE Communications Society Leonard G. Abraham Prize and IEEE Globecom2012 Best Paper Award. He was the Technical Program Chair of the 2019 IEEE International Conference on Communications (ICC2019), Shanghai, Executive Chair of the IEEE ICC2015, London, and Technical Program Chair of the IEEE WCNC2013. He is/was the editor of a number of international journals, including *IEEE Transactions on Communications* from 1998 to 2013. Professor Wang is a Fellow of the Royal Academy of Engineering, UK, Fellow of the IEEE, and Fellow of the IET.

List of Abbreviations

2D-ES	Two-dimensional exhaustive search
3D	Three-dimensional
4G	Fourth Generation
5G	Fifth Generation
6G	Sixth Generation
AF	Amplify-and-forward
AI	Alternately iterative
AIS	Alternately iterative structure
AN	Artificial noise
AO	Alternating optimization
AP	Access point
APL	Approximate performance loss
AR	Achievable rate
AWGN	Additive white Gaussian noise
BCD	Block coordinate descent
BER	Bit error rate
BLAST	Bell laboratories layer space-time
BS	Base station
BSs	Base stations
CBS	Confidential bit stream
CBSs	Confidential bit streams
CM	Confidential message
CMS	Confidential message stream
CMs	Confidential messages
CRLB	Cramer-Rao lower bound
CSCG	Circularly symmetric complex Gaussian
CSI	Channel state information
DA	Dual ascent
DF	Decode-and-forward
DM	Directional modulation
DOA	Direction of arrival

DR	Data rate
EH	Energy harvesting
EHR	Energy harvesting receiver
eMBB	Enhanced mobile broadband
EMI	Ergodic mutual information
EPA	Equal power allocation
ES	Exhaustive search
ESR	Ergodic secrecy rate
EVD	Eigenvalue decomposition
Eve	Eavesdropper
Eves	Eavesdroppers
FD	Full-duplex
FDA	Frequency diverse array
FLOPs	Float-point operations
FSPL	Free-space path loss
GAI	General alternating iterative
GD	Gradient descend
GL	Generalized leakage
GNCP	Generalized nonlinear convex programming
GPG	Geometric parallelogram
GPI	Generalized power iteration
HAD	Hybrid analog-digital
HD	Half-duplex
HICF	Hybrid iterative closed-form
i.i.d.	Independent and identically distributed
IAS	Inter-antenna synchronization
ICI	Inter-channel interference
IoT	Internet of things
IRS	Intelligent reflecting surface
IRS-SSM	Intelligent reflecting surface-assisted secure spatial modulation
IRSES	Intelligent reflecting surface element selection
JCM	Jamming covariance matrix
KKT	Karush-Kuhn-Tucker
KL	Kullback-Leibler
LANSR	Leakage-artificial noise-to-signal ratio
LC-AO	Low-complexity alternating optimization
LMI	Linear matrix inequality
LoP	Line-of-propagation
LoS	Line-of-sight
Max-NASR-DA	Maximizing newly fitting secrecy rate via dual ascent
Max-NASR-SCA	Maximizing newly fitting secrecy rate via successive convex approximation
Max-RP	Maximizing receive power
Max-SLNR	Maximizing signal-to-leakage-noise ratio
Max-SR	Maximize the secrecy rate

Max-SV	Maximizing singular value
Max-TASR-SDR	Maximizing traditional approximate secrecy rate via semidefinite relaxation
MIMO	Multiple-input multiple-output
MISO	Multiple-input single-output
MM	Majorization-minimization
mmWave	Millimeter wave
MPSK	M-ary phase shift keying
MQAM	M-ary quadrature amplitude modulation
MRC	Maximum ratio combining
NASR	Newly fitting secrecy rate
NMSE	Normalized mean squared error
NS	Null-space
NSP	Null-space projection
PA	Power allocation
PEM-AO	Parametric estimation method by alternating optimization
PEM-GD	Parametric estimation method by gradient descend
PL	Performance loss
PLS	Physical layer security
PSCA	Penalty successive convex approximation
PSK	Phase shifted keying
PSM	Phase-shift matrix
QAM	Quadrature amplitude modulation
QE	Quantization error
QPSK	Quadrature phase shift keying
RBF	Receive beamforming
RCML	Rank-constrained maximum likelihood
RF	Radio frequency
RMCG	Riemannian manifold conjugate gradient
RS	Relay station
RSM	Receive spatial modulation
RSS	Received signal strength
SCA	Successive convex approximation
SCM	Sample covariance matrix
SDP	Semidefinite programming
SDR	Semidefinite relaxation
SINR	Signal to interference plus noise ratio
SM	Spatial modulation
SNR	Signal-to-noise ratio
SOC	Second-order cone
SOCP	Second-order cone programming
SR	Secrecy rate
SSM	Secure spatial modulation
SSR	Sum secrecy rate
STC	Space time coding

SVD	Singular value decomposition
SWIPT	Simultaneous wireless information and power transfer
TASR	Traditional approximate secrecy rate
TPD	Transmit power design
TSM	Transmit spatial modulation
TVBs	Transmit beamforming vectors
TWDM	Two-way directional modulation
UAV	Unmanned aerial vehicle
UDN	Ultra-dense network
URLLC	Ultra-reliable low-latency communications
WSN	Wireless sensor network
ZF	Zero-forcing

Chapter 1
Intelligent Reflecting Surface-Aided Physical-Layer Security Communications

1.1 Overview of Physical-Layer Security

The broadcast nature of wireless communication systems makes wireless transmission extremely susceptible to eavesdropping and even malicious interference. Physical layer security technology can effectively protect the private information sent by the transmitter from being listened to by illegal eavesdroppers, thus ensuring the privacy and security of communication between the transmitter and legitimate users. Thus, the main design goal of physical layer security is to increase the performance difference between the link of the legitimate receiver and that of the eavesdropper by using well-designed transmission schemes. The development of mobile communication presents new challenges to physical layer security research. Wireless mobile communications has been developing very fast [1–5]. The fifth generation (5G) mobile systems have been started to be deployed worldwide. Due to the broadcast nature of wireless media, information security has been a critical issue in wireless communication. The traditional method of addressing communication security is to adopt the secret key encryption. The secure transmission of private data is achieved by designing various encryption algorithms in the upper protocol stack. However, cryptography is of computational security and its security level depends on the hardness of the underlying mathematical problem it employs. Once an effective method is developed to solve its mathematical problem, the security of the encryption method will be seriously compromised [6]. The physical layer is the lowest one in the open system interconnect (OSI) model of computer and communication networks. physical layer deals with hardware specifications, encoding and signalling, Data transmission and reception, and finally topology and physical network design [7]. Moreover, with the development of sixth generation (6G) research, it is realized that the key issues facing future wireless communication will be the high cost of hardware, the high complexity of wireless communication networks, and the increasing energy consumption. Intelligent reflecting surface (IRS) is the key technology that has received the most attention in 6G research due

F. Shu, J. Wang, *Intelligent Reflecting Surface-Aided Physical-Layer Security*,
Wireless Networks, https://doi.org/10.1007/978-3-031-41812-9_1

to its low cost, low energy consumption and programmable nature [8]. Thus, spatial modulation (SM) and directional modulation (DM) are used to protect the privacy of the transmitted content, and covert communication protects the transmitted behavior, and IRS is introduced to further improve the security of the system while reducing the cost.

Physical layer security technology has become an effective solution to the wireless communication security problem. As shown in Fig. 1.1, the transmitter (i.e., Alice) sends a confidential message to the legitimate receiver (i.e., Bob), while the eavesdropper (i.e., Eve) receives the signal and intends to decode it. The key idea of physical layer security technology is to exploit the inherent propagation characteristics of wireless channels (such as the difference between the main channel and the eavesdropping channel, randomness, and reciprocity) from the perspective of information theory. By reasonably designing the transmit signal so that it improves the amount of mutual information between the transmitter and the desired user at the physical layer while reducing the amount of information in the eavesdropping channel. Compared with traditional encryption technology, physical layer security technology has the following notable features and advantages: First, physical layer security includes not only secure key generation techniques but also keyless techniques (i.e., no encryption and decryption operations are required). Second, physical layer security techniques can take advantage of the time-varying and random nature of wireless channels.

The physical layer security technology can effectively protect the content of private messages sent by the transmitter from being eavesdropped by illegal eavesdroppers (Eves) [9] and protect the behavior of signal transmission from being detected or the presence of the user from being discovered by surveillant [10].

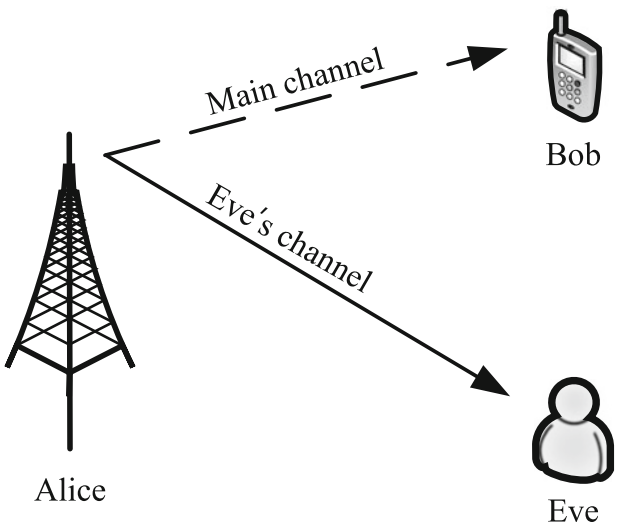


Fig. 1.1 A three-node secure communication model

Specifically, key generation-based physical layer security technology mainly relies on the reciprocity and randomness of the wireless channel to generate channel keys, ensuring that legitimate users can dynamically generate the corresponding keys under the observation of the transceiver link [11]. The study of keyless physical layer security techniques originated from Wyner's Wire-tap wireless communication eavesdropping channel model, which shows that when the Eve's channel is the degenerate channel of the legitimate receiver, there is some way to maximise the transmission rate from the sender to the legitimate receiver without giving away any information to the Eve. This eavesdropping channel model has been extended to broadcast and Gaussian channels by Csiszar, Korner and Leung-Yan-Cheong, Hellman, respectively [12, 13]. In particular, signal processing techniques are employed to design reasonable beamforming or power allocation strategies from the transmitter's perspective to improve the security performance of wireless communication systems [14]. Based on the above advantages, solving the communication security problem from the physical layer has aroused widespread concern. The authors in [13] studied the secure transmission of private information on Gaussian channels, and proved that expanding the difference between the main channel and the eavesdropping channel can achieve low probability interception and low probability detection for Eves. Wang et al. [15] further researched the keyless physical layer secure transmission technology over fading channels. The use of multiple antennas can add additional degrees of freedom and further improve the security performance of the wireless network [16, 17]. In addition, by generating random artificial noise (AN) at the transmitter to interfere with Eves, the security of the system can be further improved [18]. Currently, scenarios where Eves exist are considered in various wireless communication systems. The basic physical layer security techniques have been summarized comprehensively in the literatures [6, 7, 9, 14].

Specifically, secure key generation technology is an encryption method that uses the random characteristics of the physical channel of wireless transmission to generate a key and combines it with traditional upper layer encryption mechanisms to achieve security. It places no restrictions on the eavesdropping party's computing power, eliminating the dangers present in traditional wireless key negotiation, allowing independent key generation and extraction, and providing unconditional security, circumventing the risks of pre-distributed keys [11]. The difficulty lies in designing a key sequence that reflects the uniqueness, reciprocity and randomness of the channel to ensure that both communicating parties in a legitimate channel can identify the key sequence accurately and unambiguously [19]. Keyless physical layer security does not need to generate keys. Advanced signal processing techniques such as antenna selection, beamforming, relay selection and cooperative jamming are used to increase the transmission difference between legitimate and eavesdropping links, so as to enhance the secure transmission capability of the system. For keyless physical layer security, firstly, satellite communications, marine communications, millimeter wave (mmWave) communications, and unmanned aerial vehicle (UAV) networks have been widely used in current 5G networks, and their communication channels are mainly dominated by line-of-sight (LoS)

components, DM is very suitable for LoS channels to achieve a strong directive transmission because it can guarantee secure transmission in the desired direction while distorting the constellation diagram in all other directions [20]. Secondly, for the conventional multiple-input multiple-output (MIMO) technology, the large number of radio frequency (RF) chains leads to high system energy consumption, while SM provides a low-cost, low-energy and high-performance communication technology. SM also uses antenna sequences and modulation symbols to transmit bit information, which reduces the design complexity of transmitters and receivers and reduces the RF link overhead. Therefore, SM has become a promising technology for MIMO systems [21]. While these aforementioned techniques are able to solve security problems in many scenarios by protecting the content of the message. It is worth noting that the behavior of the transmission itself exposes the connection between the parties involved in that communication process, which can trigger further investigation and attacks. The task of covert communication is to protect the behaviour of wireless transmissions, thereby reducing the probability that a watcher will discover the communication behavior in a wireless network. It achieves a higher level of security compared to cryptography and traditional physical layer security techniques [10].

1.2 Overview of Intelligent Reflecting Surface

Due to the significant increase in the number of wireless communication devices, various novel technologies have been proposed in the literature to improve the spectrum and energy efficiencies, as well as the security and reliability of wireless communication systems. Future wireless networks are expected to support high (energy and spectrum) efficiency, security, reliability, and flexible design for emerging applications of 6G and beyond [22]. Relentless efforts have been made in research and development of wireless communications to achieve this goal. However, overall progress has been relatively sluggish due to the fact that traditional wireless communication designers have focused only on the transmitter and receiver sides, while treating the wireless communication environment as an uncontrollable factor. Recently, IRS has been considered as a promising new technology for the next-generation wireless communications, which can reconfigure the wireless propagation environment via controlling reflection with software [8]. Specifically, an IRS composes a large number of low-cost passive reflecting elements, each of which can induce a phase change to the incident signal independently. By smartly adjusting the phase shift of the reflecting elements, the IRS reflected signals and the signals from other paths can be combined constructively to enhance the desired signal power or destructively to suppress undesired signals such as co-channel interference, which thus significantly improves the communication performance [23, 24]. IRS is particularly suitable for indoor applications with high density of users (such as stadium, shopping mall, exhibition center, airport, etc.). For physical layer security, when the distance from the Eve to the Alice is smaller than the

distance from the legitimate user to the Alice, or when the Eve is in the same direction as the legitimate user, IRS can be deployed near the Eve, and the signal reflected by IRS can be tuned to cancel out the (non-IRS-reflected) signal from Alice at the Eve, thus effectively reducing the information leakage. IRS transforms the traditional uncontrollable and random wireless communication environment into a programmable and relatively deterministic transmission space, and plays an active role in the signal transmission process [25]. By introducing IRS into the security system, the security of the system can be further enhanced.

Compared to amplify-and-forward (AF) trunking, IRS does not use an RF transceiver and only passively reflects the incoming signal without any complex signal processing operations. As a result, IRS is much cheaper to operate in terms of hardware and power consumption compared to traditional relays. In addition, active AF trunking typically operates in half-duplex (HD) mode and is therefore less spectrally efficient than IRS that operates in full-duplex (FD) mode [26]. Although AF relaying can also operate in FD mode, it is subject to severe self-interference, which requires effective interference cancellation techniques. Due to the passive nature of the reflective elements, IRS can be manufactured with light weight and thin layer thickness. As a result, they can be easily installed in both indoor and outdoor environments. In indoor environments, IRS can be attached to ceilings, walls, furniture, and even behind paintings/decorations, thereby increasing coverage and enhancing received signal strength. This is particularly attractive for Enhanced Mobile Broadband (eMBB) and mass IoT communication applications in factories, stadiums, shopping malls, airports, etc. In outdoor environments, IRS can be mounted on building facades, light poles, billboards, and even on the surfaces of fast-moving vehicles to support applications such as ultra-reliable low-latency communications (URLLC) by effectively compensating for the Doppler effect for remote control and intelligent transportation [27, 28]. Thus, IRS is a promising technology to make our current communication environment intelligent, which has the potential to benefit a wide range of 5G/6G verticals, such as transportation, manufacturing, smart cities, etc.

The main advantage of having IRS in a communication system is the capability to execute passive beamforming, which can be done at the midpoint of the channel, unlike the traditional active beamforming at the Alice [29]. This additional degree of freedom has been shown to improve system performance in several metrics, including physical layer security, which is entirely dependent on the ability of the system to precisely direct the signal beam to the expected path (or eliminate it). In addition, the coverage area can be further increased with the assistance of IRS. However, the employment of IRS increases the complexity of the system. For example, in physical layer security applications, traditional active beamforming is optimized in order to maintain the confidentiality of the system. In contrast, the presence of IRS in the system requires joint optimization of active and passive beamforming, and the performance of the system depends greatly on the quality of the acquired channel state information (CSI). Moreover, under the far-field propagation assumption, the communication channel of the IRS link suffers from

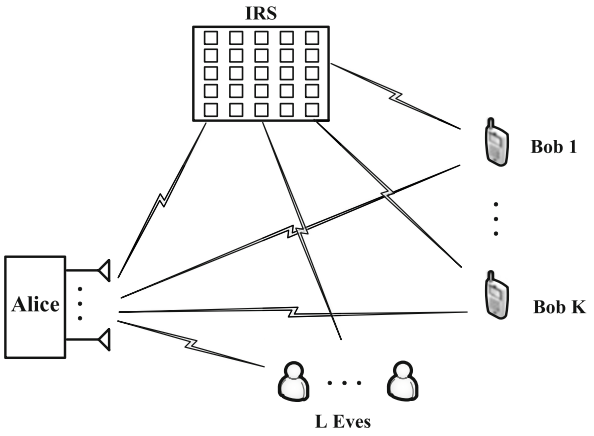


Fig. 1.2 IRS-assisted secure communication system

a dual path loss, the so-called product-distance path loss model, which needs to be compensated in the link budget or by increasing the number of reflective elements.

In traditional multi-antenna cellular networks, the beamforming design mainly consists of precoding and equalization matrices for the transceivers of multiple antennas to achieve directional signal transmission, while the introduction of IRS will make the beamforming design more complex. The IRS-assisted secure communication system is shown in Fig. 1.2. As shown in the figure, Alice to each user passes through a series of three components: Alice-IRS link, the IRS reflection link, and the IRS-user link. Each reflecting element of the IRS receives a combined signal from the transmitter and scatters the combined signal with adjustable amplitude and/or phase to produce a "multiplicative" channel model. The introduction of IRS in the system can increase the achievable rate of legitimate users (i.e., Bobs) while suppressing the achievable rate of illegal users (i.e., Eves), ultimately improving the security performance of the system. Hence, IRS can be used for strengthening the system security under the wiretap channel, especially when the channel of the eavesdropping communication link is stronger than that of the legitimate link. In particular, by denoting the reflecting coefficient matrix of the IRS as $\boldsymbol{\Theta} = \text{diag}[\mathbf{e}^{j\theta_1}, \ldots, \mathbf{e}^{j\theta_N}]$, and the transmit beamforming at the base station (BS) as $\mathbf{x} = \sum_{k=1}^{K} \mathbf{w}_k s_k$, the achievable SR of user k is

$$R_{s,k} = \log_2\left(1 + \frac{\left|\left(\mathbf{h}_{ib,k}^H \boldsymbol{\Theta}\mathbf{G} + \mathbf{h}_{ab,k}^H\right)\mathbf{w}_k\right|^2}{\sum_{j\neq k}\left|\left(\mathbf{h}_{ib,k}^H \boldsymbol{\Theta}\mathbf{G} + \mathbf{h}_{ab,j}^H\right)\mathbf{w}_j\right|^2 + \sigma_k^2}\right) \tag{1.1}$$

$$- \log_2\left(1 + \frac{\left|\left(\mathbf{h}_{ie,l}^H \boldsymbol{\Theta}\mathbf{G} + \mathbf{h}_{ae,l}^H\right)\mathbf{w}_k\right|^2}{\sum_{j\neq k}\left|\left(\mathbf{h}_{ie,l}^H \boldsymbol{\Theta}\mathbf{G} + \mathbf{h}_{ae,l}^H\right)\mathbf{w}_j\right|^2 + \sigma_e^2}\right),$$

where $\mathbf{G}$, $\mathbf{h}_{ib,k}$, $\mathbf{h}_{ab,k}$, $\mathbf{h}_{ie,l}$, and $\mathbf{h}_{ae,l}$ are the channel from the Alice to the IRS, from the IRS to user k, form the Alice to user k, from the IRS to Eve l, and from the Alice to Eve l, respectively. Notice that unlike the traditional model that contains only direct paths, the IRS is introduced with the addition of reflected paths, i.e., terms that contain $\boldsymbol{\Theta}$. In the optimization process, we not only optimize the active beamforming $\mathbf{w}_k$ at the Alice but also optimize the phase shift matrix $\boldsymbol{\Theta}$ of the IRS, i.e., passive beamforming.

Given these advantages of the IRS, many recent studies have utilized IRS to secure the physical layer of wireless communications. The authors in [30–32] investigated an IRS-aided secure wireless system where a multi-antenna transmitter communicates with a single-antenna receiver in the presence of an Eve. In [30–32], the SR was maximized by jointly optimizing the transmit beamforming and the IRS phase shifts. Specifically, the authors in [30] proposed an alternating optimization (AO) algorithm to design two variables alternately, in which the optimal solution to the transmit beamforming was computed directly and the IRS phase shifts were optimized by using semidefinite relaxation (SDR) method. In [31], the transmit beamforming and the IRS phase shifts were also optimized in an alternating manner. In each iteration, the solution to the transmit beamforming was achieved in closed form, while a semi-closed form solution to the IRS phase shifts was obtained by adopting the majorization-minimization (MM) algorithm. The element-wise block coordinate descent (BCD) and AO-MM algorithms were developed for solving the problem efficiently in [32]. Furthermore, the authors in [33] investigated a minimum-SR maximization problem in a secure IRS-aided multiuser multiple-input single-output (MISO) broadcast system with multiple Eves. The problem was successfully solved by applying the path-following algorithm and AO technique in an iterative manner. Moreover, two suboptimal algorithms with closed-form solutions were developed to further reduce the computational complexity. To further enhance the security, the AN is designed to disturb Eve. In [34], AN was firstly considered in an IRS-aided secure communication system. Specifically, the achievable SR of the system was maximized by jointly optimizing the transmit beamforming with AN and IRS phase shifts. An efficient algorithm based on AO was developed to solve the problem sub-optimally. The authors in [35] considered the resource allocation design in an IRS-aided multiuser MISO communication system. Aiming to maximize the system sum SR, the beamforming vectors, AN covariance matrix at the BS and phase shift matrix at the IRS were jointly optimized by applying AO, SDR and manifold optimization. The authors in [36] investigated a secure IRS-aided multigroup multicast MISO communication system to minimize the transmit power subject to the SR constraints. First, an SDR-based AO algorithm was proposed and a high-quality solution was obtained. Then, to reduce the high computation complexity, a low-complexity AO algorithm based on second-order cone programming (SOCP) was presented. Moreover, secure IRS-aided simultaneous wireless information and power transfer (SWIPT) system were studied in [37]. To maximize the harvested power of energy harvesting receiver (EHR), the secure transmit beamforming at Alice and phase shifts at the IRS are optimized subject to the SR and the reflecting phase shifts at the IRS constraints. The

SDR and the low-complexity AO algorithms are proposed, and the harvested power with the help of IRS approximately double that of the existing method without IRS. All of the above literature showed that the inclusion of IRS in the protection of private content achieves a significant increase in the security rate of the system. To investigate the effect of IRS in covert communication systems, Zhou et al. [38] studied IRS-assisted covert wireless communications, and proved that the perfect covertness can be achieved if the channel quality of the reflected path is higher than that of the direct path. This also demonstrated that IRSs are also effective in protecting transmission behaviour.

1.3 Organization of the Monograph

The remainder of this monograph is organized as follows. In Chap. 2, the enhanced secrecy rate maximization for directional modulation networks via IRS will be investigated. In Chap. 3, the high-performance estimation of jamming covariance matrix for IRS-aided directional modulation network with a malicious attacker will be comprehensively analyzed. In Chap. 4, the beamforming and power allocation for double-IRS-aided two-way directional modulation network will be studied. In Chap. 5, the beamforming and transmit power design for IRS-aided secure spatial modulation will be explored. The IRS-aided covert wireless communications with delay constraint will be considered in Chap. 6. Chapter 7 will study the IRS aided secure transmission with colluding eavesdroppers. The secure multigroup multicast communication systems via IRS will be developed in Chap. 8. Chapter 9 will consider the beamforming design for IRS-aided decode-and-forward relay wireless network. The performance analysis of wireless network aided by discrete-phase-shifter IRS will be explored in Chap. 10. Finally, Chap. 11 will close up with some promising directions, aiming to promote future research outcomes in the field of IRS-aided physical layer secure communication.

References

1. Zhu, H., Wang, J.: Chunk-based resource allocation in OFDMA systems - Part I, chunk allocation. IEEE Trans. Commun. **57**(9), 2734–2744 (2009)
2. Zhu, H., Wang, J.: Chunk-based resource allocation in OFDMA systems - Part II, joint chunk, power and bit allocation. IEEE Trans. Commun. **60**(2), 499–509 (2012)
3. Wang, J., Zhu, H., Gomes, N.: Distributed antenna systems for mobile communications in high speed trains. IEEE J. Sel. Areas Commun. **30**, 675–683 (2012)
4. Zhou, Y., Wang, J., Sawahashi, M.: Downlink transmission of broadband OFCDM systems - Part I, Hybrid Detection. IEEE Trans. Commun. **53**(4), 718–729 (2005)
5. Zhou, Y., Liu, H., Pan, Z., Tian, L., Shi, J., Yang, G.: Two-stage cooperative multicast transmission with optimized power consumption and guaranteed coverage. IEEE JSAC SEED **32**(2), 274–284 (2014)

6. Wu, Y., Khisti, A., Xiao, C., Caire, G., Wong, K.K., Gao, X.: A survey of physical layer security techniques for 5G wireless networks and challenges ahead. IEEE J. Sel. Areas Commun. **36**(4), 679–695 (2018)
7. Abdelgader, A.M., Lenan, W.: The physical layer of the IEEE 802.11 p WAVE communication standard, the specifications and challenges. In: Proceedings of the WCECS (2014)
8. Wu, Q., Zhang, R.: Towards smart and reconfigurable environment, Intelligent reflecting surface aided wireless network. IEEE Commun. Mag. **58**(1), 106–112 (2020)
9. Chen, X., Ng, D.W.K., Gerstacker, W.H., Chen, H.H.: A survey on multiple-antenna techniques for physical layer security. IEEE Commun. Surv. Tutorials **19**(2), 1027–1053 (2017)
10. Hu, J., Yan, S., Zhou, X., Shu, F., Li, J., Wang, J.: Covert communication achieved by a greedy relay in wireless networks. IEEE Trans. Wireless Commun. **17**(7), 4766–4779 (2018)
11. Chou, T.H., Draper, S.C., Sayeed, A.M.: Secret key generation from sparse wireless channels, ergodic capacity and secrecy outage. IEEE J. Sel. Areas Commun. **31**(9), 1751–1764 (2013)
12. Csiszar, I., Korner, J.: Broadcast channels with confidential messages. IEEE Trans. Inf. Theory **24**(3), 339–348 (1978)
13. Leung-Yan-Cheong, S., Hellman, M.: The Gaussian wire-tap channel. IEEE Trans. Inf. Theory **24**(4), 451–456 (1978)
14. Wang, D., Bai, B., Zhao, W., Han, Z.: A survey of optimization approaches for wireless physical layer security. IEEE Commun. Surv. Tutorials **21**(2), 1878–1911 (2019)
15. Wang, X., Tao, M., Mo, J., Xu, Y.: Power and subcarrier allocation for physical-layer security in OFDM-based broadband wireless networks. IEEE Trans. Inf. Forensics Secur. **61**(6), 693–702 (2011)
16. Ng, D.W.K., Lo, E.S., Schober, R.: Energy-efficient resource allocation for secure OFDM systems. IEEE Trans. Veh. Technol. **61**(6), 2572–2585 (2012)
17. Jeong, C., Kim, I.-M.: Optimal power allocation for secure multicarrier relay systems. IEEE Trans. Signal Process. **59**(11), 5428–5442 (2011)
18. Goel, S., Negi, R.: Guaranteeing secrecy using artificial noise. IEEE Trans. Wireless Commun. **7**(6), 2180–2189 (2008)
19. Abdelgader, A., Wu, L.: A secret key extraction technique applied in vehicular networks. In: IEEE 17th International Conference on Computational Science and Engineering, pp. 1396–1403 (2014)
20. Daly, M.P., Bernhard, J.T.: Beamsteering in pattern reconfigurable arrays using directional modulation. IEEE Trans. Antennas Propag. **58**(7), 2259–2265 (2010)
21. Mesleh, R.Y., Haas, H., Sinanovic, S., Ahn, C.W., Yun, S.: Spatial modulation. IEEE Trans. Veh. Technol. **57**(4), 2228–2241 (2008)
22. Wu, Q., Zhang, R.: Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming. IEEE Trans. Wireless Commun. **18**(11), 5394–5409 (2019)
23. Dong, L., Wang, H.-M.: Secure MIMO transmission via intelligent reflecting surface. IEEE Wirel. Commun. Lett. **9**(6), 787–790 (2020)
24. Jiang, W., Zhang, Y., Wu, J., Feng, W., Jin, Y.: Intelligent reflecting surface assisted secure wireless communications with multiple-transmit and multiple-receive antennas. IEEE Access **8**, 86 659–86 673 (2020)
25. Hong, S., Pan, C., Ren, H., Wang, K., Nallanathan, A.: Artificial-noise-aided secure MIMO wireless communications via intelligent reflecting surface. IEEE Trans. Commun. **68**(12), 7851–7866 (2020)
26. Shu, F., Teng, Y., Li, J., Huang, M., Shi, W., Li, J., Wu, Y.: Enhanced secrecy rate maximization for directional modulation networks via IRS. IEEE Trans. Commun. **69**(12), 8388–8401 (2021)
27. Wu, Q., Zhang, R.: Towards smart and reconfigurable environment, Intelligent reflecting surface aided wireless network. IEEE Commun. Mag. **58**(1), 106–112 (2020)
28. Huang, C., Mo, R., Yuen, C.: Reconfigurable intelligent surface assisted multiuser MISO systems exploiting deep reinforcement learning. IEEE J. Sel. Areas Commun. **38**(8),1839–1850 (2020)
29. Niu, H., Lei, N.: Intelligent reflect surface aided secure transmission in MIMO channel with SWIPT. IEEE Access **8**, 192132–192140 (2020)

30. Cui, M., Zhang, G., Zhang, R.: Secure wireless communication via intelligent reflecting surface. IEEE Wirel. Commun. Lett. **8**(5), 1410–1414 (2019)
31. Shen, H., Xu, W., Gong, S., He, Z., Zhao, C.: Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications. IEEE Commun. Lett. **23**(9), 1488–1492 (2020)
32. Yu, X., Xu, D., Schober, R.: Enabling secure wireless communications via intelligent reflecting surfaces. In: IEEE Global Communications Conference (GLOBECOM), pp. 1–6 (2019)
33. Chen, J., Liang, Y.-C., Pei, Y., Guo, H.: Intelligent reflecting surface, A programmable wireless environment for physical layer security. IEEE Access **7**, 82 599–82 612 (2019)
34. Guan, X., Wu, Q., Zhang, R.: Intelligent reflecting surface assisted secrecy communication, Is artificial noise helpful or not? IEEE Wirel. Commun. Lett. **9**(6), 778–782 (2020)
35. Xu, D., Yu, X., Sun, Y., Ng, D.W.K., Schober, R.: Resource allocation for secure IRS-assisted multiuser MISO systems. In: IEEE Globecom Workshops (GC Wkshps), pp. 1–6 (2019)
36. Shi, W., Li, J., Xia, G., Wang, Y., Zhou, X., Zhang, Y., Shu, F.: Secure multigroup multicast communication systems via intelligent reflecting surface. China Commun. **18**(3), 39–51 (2021)
37. Shi, W., Zhou, X., Jia, L., Wu, Y., Shu, F., Wang, J.: Enhanced secure wireless information and power transfer via intelligent reflecting surface. IEEE Commun. Lett. **25**(4), 1084–1088 (2020)
38. Zhou, X., Yan, S., Wu, Q., Shu, F., Ng, D.W.K.: Intelligent reflecting surface (IRS)-aided covert wireless communications with delay constraint. IEEE Trans. Wirel. Commun. **21**(1), 532–547 (2022)

Chapter 2
Enhanced Secrecy Rate Maximization for Directional Modulation Networks via IRS

IRS is of low-cost and energy-efficiency and will be a promising technology for the future wireless communications like sixth generation. To address the problem of conventional DM that Alice only transmits single confidential bit stream (CBS) to Bob with multiple antennas in a LoS channel in this chapter, IRS is proposed to create friendly multipaths for DM such that two confidential bit streams (CBSs) can be transmitted from Alice to Bob. This will significantly enhance the secrecy rate (SR) of DM. To maximize the SR (Max-SR), a general non-convex optimization problem is formulated with the unit-modulus constraint of IRS phase-shift matrix (PSM), and the general alternating iterative (GAI) algorithm is proposed to jointly obtain the transmit beamforming vectors (TBVs) and PSM by alternately optimizing one and fixing another. To reduce its high complexity, a low-complexity iterative algorithm for Max-SR is proposed by placing the constraint of null-space (NS) on the TBVs, called NS projection (NSP). Here, each CBS is transmitted separately in the NSs of other CBS and AN channels. Simulation results show that the SRs of the proposed GAI and NSP can approximately double that of IRS-based DM with single CBS for massive IRS in the high signal-to-noise ratio region.

2.1 Introduction

With the commercialization of 5G and the requirements of 6G pre-research, physical layer security increasingly becomes an extremely important and prominent problem. Techniques such as massive MIMO, mmWave mobile communication and hybrid beamforming have been investigated in cellular systems, internet of things (IoT), UAV, and satellite communications [1–7]. However, the network energy consumption and hardware cost still remain critical issues. For example, 5G system has a much higher energy consumption than the fourth generation (4G) system [8, 9]. Therefore, the importance of green communication becomes increasingly

F. Shu, J. Wang, *Intelligent Reflecting Surface-Aided Physical-Layer Security*,
Wireless Networks, https://doi.org/10.1007/978-3-031-41812-9_2

significant for the future wireless communications. Many related technologies are in the pace of research, such as SWIPT, which can enhance the energy efficiency and solve energy-limited issues of wireless networks [10–12].

For physical layer security, Wyner [13] proposed the concept of secrecy capacity in a discrete memoryless wiretap channel. With the aid of artificial noise (AN), the security can be improved against the overhearing of potential eavesdroppers [14]. As one of the most attractive technology in physical layer security DM is to apply signal processing methods like beamforming and AN in RF frontend or baseband, so that the signal in the desired direction can be restored as completely as possible, while the constellation diagram of signal in the undesired direction is distorted [15–17]. Here, the AN is usually projected onto the null-space of the desired steering vectors with energy focus along the directions of eavesdroppers. By doing so, the eavesdroppers will be seriously interfered such that the confidential messages cannot be recovered correctly. In particular, for DM, if the desired direction angles are available, it is not hard to design the beamforming vector of confidential messages and AN projection matrix. Traditional DM synthesis formed an orthogonal vector or projection matrix in the null space (NS) of channel along the desired direction, which can be seen as a kind of NS projection (NSP) schemes [18]. Sun et al. [19] proposed an energy-efficient alternating iterative scheme and discussed the secure energy efficiency for DM system. In [20, 21], the authors proposed robust DM synthesis schemes in the presence of direction of arrival (DOA) measurement errors. To achieve the high-resolution estimation of DOA for practical DM, Shu et al. [22] proposed three high-performance estimators of DOA for hybrid MIMO structure. Furthermore, a practical DM scheme with random frequency diverse array was proposed in [23], inspiring a new concept birth of secure and precise wireless transmission to achieve a higher-level physical layer security [24].

As wireless networks develop rapidly, a large number of active devices will result in a serious problem of energy consumption. Therefore, how to introduce passive devices and achieve a trade-off between spectrum utilization and energy efficiency with low hardware costs becomes a necessity for achieving sustainable wireless network evolution. Moreover, the improvement of propagation environment and coverage of BS also become one of the important research areas of next-generation wireless communications. Its main aim is to create a smart environment for transmitting BS signals. Now IRS has become a promising and emerging technology with great potential of significant energy consumption reduction and spectrum efficient enhancement [25–27]. A power efficient scheme was proposed in [28] to design the secure transmit power allocation and the surface reflecting phase shift. It is a planer array consisting of a large number of reconfigurable passive elements, where each of them can be controlled by an attached smart controller and thus induce a certain phase shift independently on incident signal to change the reflected signal propagation. This reveals the potential of enhancing the signal transmission and coverage. Due to the passive forwarding and full-duplex characteristics without self-interference, IRS can play an important role in coverage improvement, spectrum and energy efficiency enhancement, and the complexity and power consumption reduction of wireless networks.

Existing algorithms for IRS-based system implementation focus on the improvement of energy efficiency and secure capacity. The phase-shifters of IRS with constant modulus makes it difficult to solve the optimization problem. In [29], the authors proposed the energy efficiency maximization of IRS-aid MISO system when the phase-shifters of IRS are of low resolution, while [30] investigated the case of infinite resolution. The authors in [31] and [32] focused on the design of transmit beamforming by active antenna array and reflect beamforming by passive IRS to minimize the total transmit power, and discussed the cases of continuous and discrete phase-shifter. The efficient algorithms with SDR and alternating optimization techniques in [31] were proposed to make a tradeoff between the system performance and computational complexity. As for the IRS-aided MIMO system, Zhang and Zhang [33] aimed to characterize the fundamental capacity limit and developed efficient alternating optimization algorithms both in narrow band and broadband scenarios. In [34], IRS was proposed to be employed in mmWave massive MIMO in practice. Since all the above works focused on one-way communications, Zhang et al. [35] proposed the sum rate optimization of IRS-aided full-duplex MIMO two-way communications through jointly optimizing the source precoders and the IRS phase-shift matrix. Reconfigurable IRS was mentioned in [36–39] as a promising technology for the next generation wireless networks. Apart from the above traditional communication situations, IRS can also be applied in some special cases, such as UAV communications and SWIPT [40–42]. Shen and Yu [43] aimed to extend the use of fractional programming (FP) to solve the optimization problems of power control, beamforming and user scheduling in the design of communication systems.

In IRS-based secure wireless communications, confidential message (CM) can be transmitted by direct path and reflected by reflect path. However, the CM could be leaked to the undesired directions, which may reduce the secure performance. In this case, the scheme of IRS-based in secure communication should be treated seriously. Cui et al. [44] investigated an IRS-based secure system with multi-antenna transmitter Alice, single-antenna receiver Bob and single-antenna eavesdropper Eve. The authors applied alternating optimization and SDR methods to maximize the secrecy rate (SR). Shen et al. [45] proposed an iterative algorithm for designing the transmit covariance matrix in a closed form and IRS phase-shift matrix in a semi-closed form, respectively. Some recent work on robust design in IRS-aided communication systems based on imperfect CSI can be found in [46–48]. Guan et al. [49] and Dong and Wang [50] investigated the potential of AN in IRS-aided communications in which AN can be an effective means to help improve the SR with IRS deployed in practice, especially for multi-eavesdroppers.

In traditional DM networks, the signal should be transmitted in a LoS channel to enhance the directivity of transmission. This will lead to a drawback of DM that only single bit stream may be sent from Alice to Bob. To overcome the limitation, employing IRS in DM network will generate multipath to achieve a smart environment of transmitting controllable multiple parallel bit streams from Alice to Bob. In other words, due to IRS, spatial multiplexing gains are created for DM. This means that the SR performance can be dramatically improved. Moreover,

IRS can ensure a low energy consumption of DM system compared with other active forwarding devices like relays, which will make a good balance between spectrum efficiency and energy efficiency. Compared with traditional IRS-based MIMO secure communication in [51], AN in DM system not only interferes with eavesdropping, but also faces the hard problem of gathering AN to legitimate users through the uncontrolled reflected paths in multipath, called the effect of gathering AN. Although DM is only suitable to the LoS channels, it still has several potential future applications such as deep space channel, satellite communication channel, UAV communication channel, and even the future 6G mmWave and THz channels. In summary, different from conventional MIMO system, DM is only suitable for the LoS channels due to its effect of gathering AN to Bob in multipath channels. Its main advantage is its directive property. This property may improve the physical-layer security and achieve a high energy efficiency. Its main disadvantages are as follows: (a) Alice with transmit antennas only transmits one confidential message stream (CMS) towards Bob with multiple receive antennas due to the rank-one property of the channel matrix from Alice and Bob in line-of-propagation channel; (b) The effect of gathering AN towards Bob will significantly degrade the SR performance of Bob.

To address the above two problems with the help of IRS are the two main motivations. In this chapter, we consider an IRS-based DM network, where all Alice, Bob and Eve are employed with multiple antennas. In a direct way and a reflective way with the help of IRS, the suitably phase-shifted versions of transmitted signals are forwarded towards Bob and interfere with Eve seriously. Additionally, IRS is equipped with a large number of controllable reflecting elements with continuous phase-shifters. The contributions of this book chapter are summarized as follows:

To overcome the limitation of DM that Alice only transmits single CBS to Bob with multiple antennas in LoS channel and also combats the effect of gathering AN in multipath fading channels with uncontrolled multipaths, the IRS-based DM network, and the corresponding system model are established. With the help of IRS, useful controlled multipaths are created between Alice and Bob by adjusting the phases and magnitudes of IRS elements. As such, multiple parallel CBSs may be transmitted from Alice to Bob by using DM. This will result in a significant improvement in SR. As shown in what follows, when two parallel independent CBSs are sent from Alice to Bob as an example, the proposed IRS-based DM framework can harvest up to 75% SR gain over single CBS as the number of IRS elements tends to large-scale. This IRS-aided DM scheme utilizes the static multipath environment to enhance the physical layer security. It is anticipated that when the number of CBSs increases, the SR performance gain gradually increases.

To maximize the SR (Max-SR) of system, a general algorithm is proposed. Since the objective problem is non-convex for the unit-modulus constraint of IRS phase-shift matrix, we propose the general alternating iterative (GAI) algorithm to jointly obtain the transmit beamforming vectors and IRS phase-shift matrix by optimizing one and fixing another. It is assumed that AN is in the null-space (NS) of Alice-to-Bob channel and Alice-to-IRS channel, that is, only interferes with Eve. In the proposed GAI, the closed-form expression of transmit beamforming vector

corresponding to each CBS is derived, and the iterative gradient ascent algorithm is adopted to optimize the IRS phase-shift matrix. The proposed GAI performs much better than random phase, no-IRS, and IRS with single CBS in terms of SR. Its SR approximately doubles that of the IRS with single CBS. Additionally, its convergence rate is fast.

To reduce the high computational complexity of the proposed GAI, a low-complexity iterative Max-SR is proposed by imposing NS constraints on all beamforming vectors. In this case, each CBS is transmitted separately in the NSP of other CBS channels transmitter-to-receiver links. It is interesting that the IRS phase-shift matrix has a semi-closed form. In the risk of a little SR performance, this method can achieve a low computation complexity, especially when the number of IRS elements is large. Compared to the proposed GAI, the proposed NSP shows a little SR performance loss but its low-complexity is very attractive. Moreover, by simulation, we find the location of IRS has an important impact on the SR performance of methods and is preferred to be close to Alice or Bob in order to enhance better security.

The remainder of this chapter is organized as follows. Section 2.2 describes the system model and secrecy maximization problem. In Sect. 2.3, the general alternating iterative algorithm is proposed. Section 2.4 describes another low-complexity algorithm for special scenario. Simulation results and related analysis are presented in Sect. 2.5. Finally, we make our conclusions in Sect. 2.6.

Notations throughout the chapter, matrices, vectors, and scalars are denoted by letters of bold upper case, bold lower case, and lower case, respectively. Signs $(\cdot)^T$, $(\cdot)^H$, $(\cdot)^{-1}$, $(\cdot)^\dagger$ and $|\cdot|$ denote transpose, conjugate transpose, inverse, pseudo-inverse and matrix determinant, respectively. $\mathbf{I}_N$ denotes the $N \times N$ identity matrix, $\mathbf{0}_{N\times M}$ denotes the $N \times M$ matrix of all zeros.

2.2 System Model

As shown in Fig. 2.1, we consider a system, where Alice is equipped with N antennas, IRS is equipped with M low-cost passive reflecting elements, Bob and Eve are equipped with K_B, K_E antennas, $K_B = K_E = K$, respectively. In the following, we assume that the IRS reflects signal only one time. In this chapter, we assume there exists the LoS path. The transmit baseband signal is expressed as

$$\mathbf{s} = \sqrt{\beta_1 P_s}\mathbf{v}_1 x_1 + \sqrt{\beta_2 P_s}\mathbf{v}_2 x_2 + \sqrt{(1-\beta_1-\beta_2)P_s}\mathbf{P}_{AN}\mathbf{z}, \tag{2.1}$$

where P_s is the total transmit power, β_1, β_2 and $(1-\beta_1-\beta_2)$ are the power allocation parameters of confidential messages (CMs) and AN, respectively. $\mathbf{v}_1 \in \mathbb{C}^{N\times 1}$ and $\mathbf{v}_2 \in \mathbb{C}^{N\times 1}$ are the beamforming vector of forcing the two CMs to the desired user Bob, where $\mathbf{v}_1^H\mathbf{v}_1 = 1$, $\mathbf{v}_2^H\mathbf{v}_2 = 1$. $\mathbf{P}_{AN}$ is the projection matrix for controlling the direction of AN. x_1 and x_2 are CM which satisfy $\mathbb{E}\left[\|x_1\|^2\right] = 1$, $\mathbb{E}\left[\|x_2\|^2\right] = 1$,

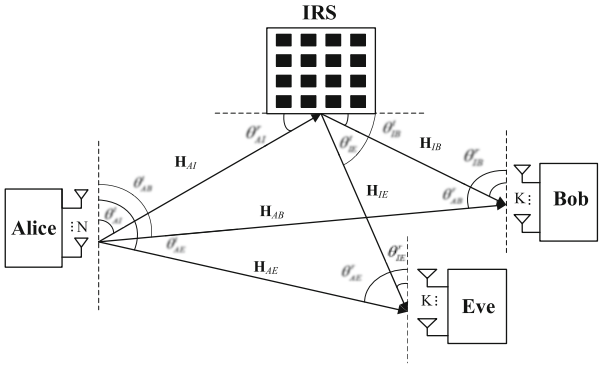


Fig. 2.1 Block diagram for IRS-based DM network

and $\mathbf{z}$ is vector AN with complex Gaussian distribution, i.e., $\mathbf{z} \sim \mathcal{CN}(0,\ \mathbf{I}_N)$. The received signal at Bob is given by

$$\begin{aligned}\mathbf{y}_B &= \left(\sqrt{g_{AIB}}\mathbf{H}_{IB}^H\boldsymbol{\Theta}\mathbf{H}_{AI} + \sqrt{g_{AB}}\mathbf{H}_{AB}^H\right)\mathbf{s} + \mathbf{n}_B \\ &= \sqrt{\beta_1 P_s}\left(\sqrt{g_{AIB}}\mathbf{H}_{IB}^H\boldsymbol{\Theta}\mathbf{H}_{AI} + \sqrt{g_{AB}}\mathbf{H}_{AB}^H\right)\mathbf{v}_1 x_1 \\ &\quad + \sqrt{\beta_2 P_s}\left(\sqrt{g_{AIB}}\mathbf{H}_{IB}^H\boldsymbol{\Theta}\mathbf{H}_{AI} + \sqrt{g_{AB}}\mathbf{H}_{AB}^H\right)\mathbf{v}_2 x_2 \\ &\quad + \sqrt{(1-\beta_1-\beta_2)P_s}\left(\sqrt{g_{AIB}}\mathbf{H}_{IB}^H\boldsymbol{\Theta}\mathbf{H}_{AI} + \sqrt{g_{AB}}\mathbf{H}_{AB}^H\right)\mathbf{P}_{AN}\mathbf{z} + \mathbf{n}_B,\end{aligned} \tag{2.2}$$

where $\mathbf{H}_{IB} \in \mathbb{C}^{M\times K}$ represents the IRS-to-Bob channel, $\boldsymbol{\Theta} = \text{diag}(e^{j\phi_1}, \cdots, e^{j\phi_m}, \cdots, e^{j\phi_M})$ is a diagonal matrix with the phase shift ϕ_m incurred by the m-th reflecting element of the IRS, $\mathbf{H}_{AI} \in \mathbb{C}^{M\times N}$ represents the Alice-to-IRS channel, $\mathbf{H}_{AB} \in \mathbb{C}^{N\times K}$ represents Alice-to-Bob channel, and $\mathbf{n}_B \sim \mathcal{CN}(\mathbf{0}, \sigma_B^2\mathbf{I}_K)$ denotes the complex additive white Gaussian noise (AWGN) at Bob. g_{AB} denotes the path loss coefficient between Alice and Bob, whereas $g_{AIB} = g_{AI}g_{IB}$ is the equivalent path loss coefficient of Alice-to-IRS channel and IRS-to-Bob channel. Similarly, the received signal at Eve can be written as

$$\begin{aligned}\mathbf{y}_E &= \left(\sqrt{g_{AIE}}\mathbf{H}_{IE}^H\boldsymbol{\Theta}\mathbf{H}_{AI} + \sqrt{g_{AE}}\mathbf{H}_{AE}^H\right)\mathbf{s} + \mathbf{n}_E \\ &= \sqrt{\beta_1 P_s}\left(\sqrt{g_{AIE}}\mathbf{H}_{IE}^H\boldsymbol{\Theta}\mathbf{H}_{AI} + \sqrt{g_{AE}}\mathbf{H}_{AE}^H\right)\mathbf{v}_1 x_1 \\ &\quad + \sqrt{\beta_2 P_s}\left(\sqrt{g_{AIE}}\mathbf{H}_{IE}^H\boldsymbol{\Theta}\mathbf{H}_{AI} + \sqrt{g_{AE}}\mathbf{H}_{AE}^H\right)\mathbf{v}_2 x_2\end{aligned}$$

$$+\sqrt{(1-\beta_1-\beta_2)P_s}\left(\sqrt{g_{AIE}}\mathbf{H}_{IE}^H\boldsymbol{\Theta}\mathbf{H}_{AI}+\sqrt{g_{AE}}\mathbf{H}_{AE}^H\right)\mathbf{P}_{AN}\mathbf{z}+\mathbf{n}_E, \tag{2.3}$$

where $\mathbf{H}_{IE}\in\mathbb{C}^{M\times K}$ represents the IRS-to-Eve channel, $\mathbf{H}_{AE}\in\mathbb{C}^{N\times K}$ represents the Alice-to-Eve channel, and $\mathbf{n}_E\sim\mathcal{CN}(\mathbf{0},\sigma_E^2\mathbf{I}_K)$ denotes AWGN at Eve. Here, g_{AIE} and g_{AE} denote the path loss coefficient between Alice and Eve, where $g_{AIE}=g_{AI}g_{IE}$ is the equivalent path loss coefficient of Alice-to-IRS channel and IRS-to-Eve channel, g_{AE} is the path loss coefficient of Alice-to-Eve channel. In the following, we assume that $\sigma_B^2=2\sigma_E^2$, and the channel matrices can be expressed respectively as

$$\mathbf{H}_{AB}^H=\mathbf{h}(\theta_{AB}^r)\mathbf{h}^H(\theta_{AB}^t),\quad \mathbf{H}_{AI}^H=\mathbf{h}(\theta_{AI}^r)\mathbf{h}^H(\theta_{AI}^t),$$

$$\mathbf{H}_{IE}^H=\mathbf{h}(\theta_{IE}^r)\mathbf{h}^H(\theta_{IE}^t), \tag{2.4a}$$

$$\mathbf{H}_{IB}^H=\mathbf{h}(\theta_{IB}^r)\mathbf{h}^H(\theta_{IB}^t),\quad \mathbf{H}_{AE}^H=\mathbf{h}(\theta_{AE}^r)\mathbf{h}^H(\theta_{AE}^t), \tag{2.4b}$$

and the normalized steering vector $\mathbf{h}(\theta)$ is defined as

$$\mathbf{h}(\theta)=\frac{1}{\sqrt{N}}[e^{j2\pi\Psi_\theta(1)},\ldots,e^{j2\pi\Psi_\theta(n)},\ldots,e^{j2\pi\Psi_\theta(N)}]^T, \tag{2.5}$$

where the phase function $\Psi_\theta(n)$ is defined

$$\Psi_\theta(n)\triangleq-\left(n-\frac{N+1}{2}\right)\frac{d\cos\theta}{\lambda},\quad n=1,\cdots,N, \tag{2.6}$$

where θ is the direction of arrival or departure, n is the index of antenna, d represents the element spacing in the transmit antenna array, and λ is the wavelength.

Due to the LoS assumption, if we can estimate the position of Eve, the steering vectors and path losses from Alice to Eve, Eve to Alice, Bob to Eve, Eve to Bob, and IRS to Eve are readily computed. By using the computing results, it can directly give the channel matrices from Alice to Eve, Eve to Alice, Bob to Eve, Eve to Bob, and IRS to Eve. Now, we show how to estimate the position of Eve when Eve emits signal or reflects echoes. Eve behaves as an emitter when it emits signal, i.e., it transmits the intercepted confidential messages to its data collector such as UAV. When Eve does not emit a signal, it can be regarded as a reflector. In this case, it reflects the electromagnetic energy from Alice or IRS to Alice or Bob. By observing the echoes returned from Eve, its position can be measured by Alice or Bob with multiple antennas. Regardless of emitting signal or the echoes of Eve, the localization principle of Eve is identical. In general, a localization method using the received signal strength (RSS) rule in [52] may be adopted to find the position of Eve. Given the estimated position of Eve together with known positions of Alice, IRS and Bob, it is easy to compute all channel matrices defined in (2.4a) and (2.4b) via Fig. 2.1 by using basic geometric knowledges.

Assuming that AN is only transmitted to Eve for interference, then $\mathbf{P}_{AN}$ should satisfy the condition that

$$\mathbf{H}_{AI}\mathbf{P}_{AN} = \mathbf{0}_{M\times N},\ \mathbf{H}_{AB}^{H}\mathbf{P}_{AN} = \mathbf{0}_{K\times N}. \tag{2.7}$$

Let us define a large virtual CM channel $\mathbf{H}_{CM} = \left[\mathbf{H}_{AI}^{T}\ \mathbf{H}_{AB}^{*}\right]^{T}$, then $\mathbf{P}_{AN}$ can be expressed as

$$\mathbf{P}_{AN} = \mathbf{I}_N - \mathbf{H}_{CM}^{H}\left[\mathbf{H}_{CM}\mathbf{H}_{CM}^{H}\right]^{\dagger}\mathbf{H}_{CM}. \tag{2.8}$$

In this case, (2.2) and (2.3) can be rewritten by applying (2.8) as,

$$\begin{aligned}\mathbf{y}_B &= \sqrt{\beta_1 P_s}\left(\sqrt{g_{AIB}}\mathbf{H}_{IB}^{H}\boldsymbol{\Theta}\mathbf{H}_{AI} + \sqrt{g_{AB}}\mathbf{H}_{AB}^{H}\right)\mathbf{v}_1 x_1 \\ &\quad + \sqrt{\beta_2 P_s}\left(\sqrt{g_{AIB}}\mathbf{H}_{IB}^{H}\boldsymbol{\Theta}\mathbf{H}_{AI} + \sqrt{g_{AB}}\mathbf{H}_{AB}^{H}\right)\mathbf{v}_2 x_2 + \mathbf{n}_B, \qquad (2.9)\\ \mathbf{y}_E &= \sqrt{\beta_1 P_s}\left(\sqrt{g_{AIE}}\mathbf{H}_{IE}^{H}\boldsymbol{\Theta}\mathbf{H}_{AI} + \sqrt{g_{AE}}\mathbf{H}_{AE}^{H}\right)\mathbf{v}_1 x_1 \\ &\quad + \sqrt{\beta_2 P_s}\left(\sqrt{g_{AIE}}\mathbf{H}_{IE}^{H}\boldsymbol{\Theta}\mathbf{H}_{AI} + \sqrt{g_{AE}}\mathbf{H}_{AE}^{H}\right)\mathbf{v}_2 x_2 \\ &\quad + \sqrt{(1-\beta_1-\beta_2)P_s}\sqrt{g_{AE}}\mathbf{H}_{AE}^{H}\mathbf{P}_{AN}\mathbf{z} + \mathbf{n}_E. \qquad (2.10)\end{aligned}$$

We jointly optimize beamforming vectors and IRS phase-shift matrix $\boldsymbol{\Theta}$ based on the secrecy rate maximization scheme. The achievable rates from Alice to Bob and to Eve can be expressed as (2.11) and (2.12)

$$\begin{aligned}R_B &= \log_2\left|\mathbf{I}_K + \frac{1}{\sigma_B^2}\left(\beta_1 P_s\mathbf{H}_B\mathbf{v}_1\mathbf{v}_1^{H}\mathbf{H}_B^{H} + \beta_2 P_s\mathbf{H}_B\mathbf{v}_2\mathbf{v}_2^{H}\mathbf{H}_B^{H}\right)\right| \\ &= \log_2\left|\mathbf{I}_K + \mathbf{H}_{B1}\mathbf{v}_1\mathbf{v}_1^{H}\mathbf{H}_{B1}^{H} + \mathbf{H}_{B2}\mathbf{v}_2\mathbf{v}_2^{H}\mathbf{H}_{B2}^{H}\right| \qquad (2.11)\\ R_E &= \log_2\left|\mathbf{I}_K + (\beta_1 P_s\mathbf{H}_E\mathbf{v}_1\mathbf{v}_1^{H}\mathbf{H}_E^{H} + \beta_2 P_s\mathbf{H}_E\mathbf{v}_2\mathbf{v}_2^{H}\mathbf{H}_E^{H})\right. \\ &\quad \left.\cdot\left((1-\beta_1-\beta_2)P_s g_{AE}\mathbf{H}_{AE}^{H}\mathbf{P}_{AN}\mathbf{P}_{AN}^{H}\mathbf{H}_{AE} + \sigma_E^2\mathbf{I}_K\right)^{-1}\right| \\ &= \log_2\left|\mathbf{I}_K + \left(\mathbf{H}_{E1}\mathbf{v}_1\mathbf{v}_1^{H}\mathbf{H}_{E1}^{H} + \mathbf{H}_{E2}\mathbf{v}_2\mathbf{v}_2^{H}\mathbf{H}_{E2}^{H}\right)\mathbf{B}^{-1}\right|, \qquad (2.12)\end{aligned}$$

where

$$\begin{aligned}\mathbf{H}_B &= \sqrt{g_{AIB}}\mathbf{H}_{IB}^{H}\Theta\mathbf{H}_{AI} + \sqrt{g_{AB}}\mathbf{H}_{AB}^{H}, \\ \mathbf{H}_{B1} &= \frac{\sqrt{\beta_1 P_s}}{\sigma_B}\left(\sqrt{g_{AIB}}\mathbf{H}_{IB}^{H}\boldsymbol{\Theta}\mathbf{H}_{AI} + \sqrt{g_{AB}}\mathbf{H}_{AB}^{H}\right), \qquad (2.13)\end{aligned}$$

$$\mathbf{H}_{B2} = \frac{\sqrt{\beta_2 P_s}}{\sigma_B}\left(\sqrt{g_{AIB}}\mathbf{H}_{IB}^H \mathbf{\Theta} \mathbf{H}_{AI} + \sqrt{g_{AB}}\mathbf{H}_{AB}^H\right),$$

$$\mathbf{H}_E = \sqrt{g_{AIE}}\mathbf{H}_{IE}^H \Theta \mathbf{H}_{AI} + \sqrt{g_{AE}}\mathbf{H}_{AE}^H, \tag{2.14}$$

$$\mathbf{H}_{E1} = \frac{\sqrt{\beta_1 P_s}}{\sigma_E}\left(\sqrt{g_{AIE}}\mathbf{H}_{IE}^H \mathbf{\Theta} \mathbf{H}_{AI} + \sqrt{g_{AE}}\mathbf{H}_{AE}^H\right), \tag{2.15}$$

$$\mathbf{H}_{E2} = \frac{\sqrt{\beta_2 P_s}}{\sigma_E}\left(\sqrt{g_{AIE}}\mathbf{H}_{IE}^H \mathbf{\Theta} \mathbf{H}_{AI} + \sqrt{g_{AE}}\mathbf{H}_{AE}^H\right), \tag{2.16}$$

$$\mathbf{B} = \frac{(1-\beta_1-\beta_2)P_s g_{AE}}{\sigma_E^2}\mathbf{H}_{AE}^H \mathbf{P}_{AN}\mathbf{P}_{AN}^H \mathbf{H}_{AE} + \mathbf{I}_K. \tag{2.17}$$

The achievable SR R_s can be written as

$$\begin{aligned} R_s &= \max\{0, R_B - R_E\} \\ &= \log_2 \frac{\left|\mathbf{I}_K + \mathbf{H}_{B1}\mathbf{v}_1\mathbf{v}_1^H\mathbf{H}_{B1}^H + \mathbf{H}_{B2}\mathbf{v}_2\mathbf{v}_2^H\mathbf{H}_{B2}^H\right|}{\left|\mathbf{I}_K + \left(\mathbf{H}_{E1}\mathbf{v}_1\mathbf{v}_1^H\mathbf{H}_{E1}^H + \mathbf{H}_{E2}\mathbf{v}_2\mathbf{v}_2^H\mathbf{H}_{E2}^H\right)\mathbf{B}^{-1}\right|}. \end{aligned} \tag{2.18}$$

The achievable SR given by optimization problem can be formulated as follows:

$$(\text{P0}): \max_{\mathbf{v}_1,\mathbf{v}_2,\mathbf{\Theta}} \quad R_s(\mathbf{v}_1, \mathbf{v}_2, \mathbf{\Theta}) \tag{2.19a}$$

$$\text{s.t.} \quad \mathbf{v}_1^H\mathbf{v}_1 = 1, \mathbf{v}_2^H\mathbf{v}_2 = 1, \tag{2.19b}$$

$$|\Theta_i| = 1, \arg(\Theta_i) \in [0, 2\pi),\ i = 1, \cdots, M, \tag{2.19c}$$

s the i-th diagonal of $\mathbf{\Theta}$. It is hard to solve the problem since the unit modulus constraint is hard to handle. In this case, we propose the alternating algorithm to calculate the beamforming vectors and IRS phase shift matrix separatively.

2.3 Proposed High-Performance GAI-Based Max-SR Method

In this section, we propose an optimal alternating algorithm for secrecy rate maximization problem to determine the beamforming vectors for CM and AN, and IRS phase-shift matrix $\mathbf{\Theta}$. To simplify the expression of R_s, let us first define

$$\mathbf{C}_{B1} = \mathbf{H}_{B1}\mathbf{v}_1\mathbf{v}_1^H\mathbf{H}_{B1}^H, \quad \mathbf{C}_{B2} = \mathbf{H}_{B2}\mathbf{v}_2\mathbf{v}_2^H\mathbf{H}_{B2}^H, \tag{2.20}$$

$$\mathbf{C}_{E1} = \mathbf{H}_{E1}\mathbf{v}_1\mathbf{v}_1^H\mathbf{H}_{E1}^H, \quad \mathbf{C}_{E2} = \mathbf{H}_{E2}\mathbf{v}_2\mathbf{v}_2^H\mathbf{H}_{E2}^H \tag{2.21}$$

for Bob and Eve.

2.3.1 *Optimize the Beamforming Vectors* $\mathbf{v}_1$ *and* $\mathbf{v}_2$ *Given the IRS Phase-Shift Matrix* $\boldsymbol{\Theta}$

To simplify the expression of R_s related to beamforming vectors, we regard $\boldsymbol{\Theta}$ as a given constant matrix, and define that

$$\begin{aligned} R_B(\mathbf{v}_1) &\overset{(a)}{=} \log_2 |\mathbf{I}_K + \mathbf{C}_{B2}| + \log_2 |\mathbf{I}_K + (\mathbf{I}_K + \mathbf{C}_{B2})^{-1}\mathbf{H}_{B1}\mathbf{v}_1\mathbf{v}_1^H\mathbf{H}_{B1}^H| \\ &\overset{(b)}{=} \log_2 |\mathbf{I}_K + \mathbf{C}_{B2}| + \log_2 \left(1 + \mathbf{v}_1^H\mathbf{H}_{B1}^H(\mathbf{I}_K + \mathbf{C}_{B2})^{-1}\mathbf{H}_{B1}\mathbf{v}_1\right), \end{aligned} \tag{2.22}$$

$$\begin{aligned} R_E(\mathbf{v}_1) &\overset{(a)}{=} \log_2 |\mathbf{I}_K + \mathbf{C}_{E2}\mathbf{B}^{-1}| + \log_2 |\mathbf{I}_K + (\mathbf{I}_K + \mathbf{C}_{E2}\mathbf{B}^{-1})^{-1}\mathbf{H}_{E1}\mathbf{v}_1\mathbf{v}_1^H\mathbf{H}_{E1}^H\mathbf{B}^{-1}| \\ &\overset{(b)}{=} \log_2 |\mathbf{I}_K + \mathbf{C}_{E2}\mathbf{B}^{-1}| + \log_2 \left(1 + \mathbf{v}_1^H\mathbf{H}_{E1}^H\mathbf{B}^{-1}(\mathbf{I}_K + \mathbf{C}_{E2}\mathbf{B}^{-1})^{-1}\mathbf{H}_{E1}\mathbf{v}_1\right), \end{aligned} \tag{2.23}$$

where (a) holds due to the fact that $|\mathbf{XY}| = |\mathbf{X}||\mathbf{Y}|$ and (b) holds due to $|\mathbf{I}_M + \mathbf{XY}| = |\mathbf{I}_N + \mathbf{YX}|$ for $\mathbf{X} \in \mathbb{C}^{M\times N}$ and $\mathbf{Y} \in \mathbb{C}^{N\times M}$. Rewrite (2.18) by applying (2.22) and (2.23),

$$R_s(\mathbf{v}_1) = \log_2 |\mathbf{I}_K + \mathbf{C}_{B2}| - \log_2 |\mathbf{I}_K + \mathbf{C}_{E2}\mathbf{B}^{-1}| + \log_2 \frac{\mathbf{v}_1^H\tilde{\mathbf{C}}_{B2}\mathbf{v}_1}{\mathbf{v}_1^H\tilde{\mathbf{C}}_{E2}\mathbf{v}_1}, \tag{2.24}$$

where $\tilde{\mathbf{C}}_{B2} = \mathbf{I}_N + \mathbf{H}_{B1}^H(\mathbf{I}_K + \mathbf{C}_{B2})^{-1}\mathbf{H}_{B1}$, $\tilde{\mathbf{C}}_{E2} = \mathbf{I}_N + \mathbf{H}_{E1}^H\mathbf{B}^{-1}(\mathbf{I}_K + \mathbf{C}_{E2}\mathbf{B}^{-1})^{-1}\mathbf{H}_{E1}$. Since the first two items of (2.24) are independent of $\mathbf{v}_1$, the subproblem to optimize $\mathbf{v}_1$ can be expressed as follows:

$$(\mathrm{P0}-1): \max_{\mathbf{v}_1} \ \frac{\mathbf{v}_1^H\tilde{\mathbf{C}}_{B2}\mathbf{v}_1}{\mathbf{v}_1^H\tilde{\mathbf{C}}_{E2}\mathbf{v}_1} \qquad \text{s.t.} \quad \mathbf{v}_1^H\mathbf{v}_1 = 1 \tag{2.25}$$

According to the Rayleigh-Ritz theorem, the optimal $\mathbf{v}_1$ can be obtained from the eigenvector corresponding to the largest eigenvalue of the matrix $\tilde{\mathbf{C}}_{E2}^{-1}\tilde{\mathbf{C}}_{B2}$.

Similarly, given the determined or known $\mathbf{v}_1$ and $\boldsymbol{\Theta}$, let us define $\tilde{\mathbf{C}}_{B1} = \mathbf{I}_N + \mathbf{H}_{B2}^H(\mathbf{I}_K + \mathbf{C}_{B1})^{-1}\mathbf{H}_{B2}$ and $\tilde{\mathbf{C}}_{E1} = \mathbf{I}_N + \mathbf{H}_{E2}^H\mathbf{B}^{-1}(\mathbf{I}_K + \mathbf{C}_{E1}\mathbf{B}^{-1})^{-1}\mathbf{H}_{E2}$. The subproblem to optimize $\mathbf{v}_2$ can be expressed as follows:

$$(\mathrm{P0}-2): \max_{\mathbf{v}_2} \ \frac{\mathbf{v}_2^H\tilde{\mathbf{C}}_{B1}\mathbf{v}_2}{\mathbf{v}_2^H\tilde{\mathbf{C}}_{E1}\mathbf{v}_2} \qquad \text{s.t.} \quad \mathbf{v}_2^H\mathbf{v}_2 = 1 \tag{2.26}$$

According to the Rayleigh-Ritz theorem, the optimal $\mathbf{v}_2$ can be obtained from the eigenvector corresponding to the largest eigenvalue of the matrix $\tilde{\mathbf{C}}_{E1}^{-1}\tilde{\mathbf{C}}_{B1}$.

2.3.2 Optimize IRS Phase-Shift Matrix $\boldsymbol{\Theta}$ Given the Beamforming Vectors

To simplify the expression of R_s in this subsection, we define the IRS phase-shift vector containing all the elements on the diagonal of $\boldsymbol{\Theta}$, that is,

$$\boldsymbol{\theta} = [e^{j\phi_1}, \cdots, e^{j\phi_m}, \cdots, e^{j\phi_M}]^T, \quad \boldsymbol{\Theta} = \text{diag}\{\boldsymbol{\theta}\}. \tag{2.27}$$

Letting $\theta_i = e^{j\phi_i}$ be the i-th element of $\boldsymbol{\theta}$, the IRS phase-shift vector $\boldsymbol{\theta}$ should satisfy the condition that

$$|\theta_i| = 1, \quad \arg(\theta_i) \in [0, 2\pi), \quad i = 1, \cdots, M. \tag{2.28}$$

Here, let us define

$$\mathbf{g}_1 = \mathbf{H}_{AI}\mathbf{v}_1, \quad \mathbf{g}_2 = \mathbf{H}_{AI}\mathbf{v}_2,$$

$$\mathbf{h}_{B1} = \frac{\sqrt{\beta_1 P_s g_{AB}}}{\sigma_B}\mathbf{H}_{AB}^H\mathbf{v}_1, \quad \mathbf{h}_{B2} = \frac{\sqrt{\beta_2 P_s g_{AB}}}{\sigma_B}\mathbf{H}_{AB}^H\mathbf{v}_2, \tag{2.29}$$

$$\mathbf{h}_{E1} = \frac{\sqrt{\beta_1 P_s g_{AE}}}{\sigma_E}\mathbf{H}_{AE}^H\mathbf{v}_1, \quad \mathbf{h}_{E2} = \frac{\sqrt{\beta_2 P_s g_{AE}}}{\sigma_E}\mathbf{H}_{AE}^H\mathbf{v}_2. \tag{2.30}$$

Given that

$$\begin{aligned}\mathbf{H}_{B1}\mathbf{v}_1 &= \frac{\sqrt{\beta_1 P_s}}{\sigma_B}(\sqrt{g_{AIB}}\mathbf{H}_{IB}^H\boldsymbol{\Theta}\mathbf{H}_{AI}\mathbf{v}_1 + \sqrt{g_{AB}}\mathbf{H}_{AB}^H\mathbf{v}_1) \\ &\overset{(c)}{=} \frac{\sqrt{\beta_1 P_s g_{AIB}}}{\sigma_B}\mathbf{H}_{IB}^H\text{diag}\{\mathbf{g}_1\}\boldsymbol{\theta} + \mathbf{h}_{B1},\end{aligned} \tag{2.31}$$

where (c) holds due to the fact that $\text{diag}\{\mathbf{a}\}\mathbf{b} = \text{diag}\{\mathbf{b}\}\mathbf{a}$ for $\mathbf{a}, \mathbf{b} \in \mathbb{C}^{M\times 1}$. To simplify the above equation, we define

$$\mathbf{T}_{B1} = \frac{1}{\sigma_B}\sqrt{\beta_1 P_s g_{AIB}}\mathbf{H}_{IB}^H\text{diag}\{\mathbf{g}_1\}, \mathbf{T}_{B2} = \frac{1}{\sigma_B}\sqrt{\beta_2 P_s g_{AIB}}\mathbf{H}_{IB}^H\text{diag}\{\mathbf{g}_2\}, \tag{2.32}$$

$$\mathbf{T}_{E1} = \frac{1}{\sigma_E}\sqrt{\beta_1 P_s g_{AIE}}\mathbf{H}_{IE}^H\text{diag}\{\mathbf{g}_1\}, \mathbf{T}_{E2} = \frac{1}{\sigma_E}\sqrt{\beta_2 P_s g_{AIE}}\mathbf{H}_{IE}^H\text{diag}\{\mathbf{g}_2\}. \tag{2.33}$$

Then (2.31) can be rewritten as $\mathbf{H}_{B1}\mathbf{v}_1 = \mathbf{T}_{B1}\boldsymbol{\theta} + \mathbf{h}_{B1}$. For the sake of simplicity, we define $\mathbf{t}_{hb1} \triangleq \mathbf{H}_{B1}\mathbf{v}_1 = \mathbf{T}_{B1}\boldsymbol{\theta} + \mathbf{h}_{B1}$. Similarly, the expression like $\mathbf{H}_{B1}\mathbf{v}_1$ can also be defined as $\mathbf{t}_{hb2} \triangleq \mathbf{H}_{B2}\mathbf{v}_2 = \mathbf{T}_{B2}\boldsymbol{\theta} + \mathbf{h}_{B2}$, $\mathbf{t}_{he1} \triangleq \mathbf{H}_{E1}\mathbf{v}_1 = \mathbf{T}_{E1}\boldsymbol{\theta} + \mathbf{h}_{E1}$, $\mathbf{t}_{he2} \triangleq \mathbf{H}_{E2}\mathbf{v}_2 = \mathbf{T}_{E2}\boldsymbol{\theta} + \mathbf{h}_{E2}$. In this case, we rewrite (2.11) and (2.12) as (2.34)

and (2.35) as follow

$$\begin{aligned} R_B(\boldsymbol{\theta}) &= \log_2 \left| \mathbf{I}_K + \mathbf{t}_{hb1}\mathbf{t}_{hb1}^H + \mathbf{t}_{hb2}\mathbf{t}_{hb2}^H \right| \\ &= \log_2 \left| \left(\mathbf{I}_K + \mathbf{t}_{hb2}\mathbf{t}_{hb2}^H \right) \left(\mathbf{I}_K + \left(\mathbf{I}_K + \mathbf{t}_{hb2}\mathbf{t}_{hb2}^H \right)^{-1} \mathbf{t}_{hb1}\mathbf{t}_{hb1}^H \right) \right| \\ &= \log_2 \left(1 + \mathbf{t}_{hb2}^H \mathbf{t}_{hb2} \right) + \log_2 \left(1 + \mathbf{t}_{hb1}^H \left(\mathbf{I}_K + \mathbf{t}_{hb2}\mathbf{t}_{hb2}^H \right)^{-1} \mathbf{t}_{hb1} \right) \end{aligned} \tag{2.34}$$

$$\begin{aligned} R_E(\boldsymbol{\theta}) &= \log_2 \left| \mathbf{I}_K + (\mathbf{t}_{he1}\mathbf{t}_{he1}^H + \mathbf{t}_{he2}\mathbf{t}_{he2}^H)\mathbf{B}^{-1} \right| \\ &= \log_2 \left| \left(\mathbf{I}_K + \mathbf{t}_{he2}\mathbf{t}_{he2}^H\mathbf{B}^{-1} \right) \left(\mathbf{I}_K + \left(\mathbf{I}_K + \mathbf{t}_{he2}\mathbf{t}_{he2}^H\mathbf{B}^{-1} \right)^{-1} \mathbf{t}_{he1}\mathbf{t}_{he1}^H\mathbf{B}^{-1} \right) \right| \\ &= \log_2 \left(1 + \mathbf{t}_{he2}^H\mathbf{B}^{-1}\mathbf{t}_{he2} \right) + \log_2 \left(1 + \mathbf{t}_{he1}^H\mathbf{B}^{-1} \left(\mathbf{I}_K + \mathbf{t}_{he2}\mathbf{t}_{he2}^H\mathbf{B}^{-1} \right)^{-1} \mathbf{t}_{he1} \right) \end{aligned} \tag{2.35}$$

The SR in terms of $\boldsymbol{\theta}$ can be rewritten as

$$(2.34)\text{–}(2.35) = \log_2 \frac{f_1(\boldsymbol{\theta}) f_2(\boldsymbol{\theta})}{g_1(\boldsymbol{\theta}) g_2(\boldsymbol{\theta})}, \tag{2.36}$$

where

$$\begin{aligned} f_1(\boldsymbol{\theta}) &= 1 + \mathbf{t}_{hb2}^H \mathbf{t}_{hb2}, \quad g_1(\boldsymbol{\theta}) = 1 + \mathbf{t}_{he2}^H \mathbf{B}^{-1} \mathbf{t}_{he2}, \\ f_2(\boldsymbol{\theta}) &= 1 + \mathbf{t}_{hb1}^H \left(\mathbf{I}_K + \mathbf{t}_{hb2}\mathbf{t}_{hb2}^H \right)^{-1} \mathbf{t}_{hb1} \\ &\overset{(d)}{=} 1 + \mathbf{t}_{hb1}^H \left(\mathbf{I}_K - \mathbf{t}_{hb2}(1 + \mathbf{t}_{hb2}^H \mathbf{t}_{hb2})^{-1} \mathbf{t}_{hb2}^H \right) \mathbf{t}_{hb1} \\ &= 1 + \mathbf{t}_{hb1}^H \mathbf{t}_{hb1} - \frac{\mathbf{t}_{hb1}^H \mathbf{t}_{hb2} \mathbf{t}_{hb2}^H \mathbf{t}_{hb1}}{1 + \mathbf{t}_{hb2}^H \mathbf{t}_{hb2}}, \\ g_2(\boldsymbol{\theta}) &= 1 + \mathbf{t}_{he1}^H \mathbf{B}^{-1} \left(\mathbf{I}_K + \mathbf{t}_{he2}\mathbf{t}_{he2}^H \mathbf{B}^{-1} \right)^{-1} \mathbf{t}_{he1} \\ &\overset{(d)}{=} 1 + \mathbf{t}_{he1}^H \mathbf{B}^{-1} \left(\mathbf{I}_K - \frac{\mathbf{t}_{he2}\mathbf{t}_{he2}^H \mathbf{B}^{-1}}{1 + \mathbf{t}_{he2}^H \mathbf{B}^{-1} \mathbf{t}_{he2}} \right) \mathbf{t}_{he1} \\ &= 1 + \mathbf{t}_{he1}^H \mathbf{B}^{-1} \mathbf{t}_{he1} - \frac{\mathbf{t}_{he1}^H \mathbf{B}^{-1} \mathbf{t}_{he2} \mathbf{t}_{he2}^H \mathbf{B}^{-1} \mathbf{t}_{he1}}{1 + \mathbf{t}_{he2}^H \mathbf{B}^{-1} \mathbf{t}_{he2}}, \end{aligned} \tag{2.37}$$

where (d) holds the fact that $(\mathbf{I}_M+\mathbf{XY})^{-1}=\mathbf{I}_M-\mathbf{X}(\mathbf{I}_N+\mathbf{YX})^{-1}\mathbf{Y}$ for $\mathbf{X}\in\mathbb{C}^{M\times N}$ and $\mathbf{Y}\in\mathbb{C}^{N\times M}$. To simplify the expression, let us define that

$$\begin{aligned} f(\boldsymbol{\theta}) &= f_1(\boldsymbol{\theta})f_2(\boldsymbol{\theta}) = f_{t1}(\boldsymbol{\theta}) - f_{t2}(\boldsymbol{\theta}), \\ g(\boldsymbol{\theta}) &= g_1(\boldsymbol{\theta})g_2(\boldsymbol{\theta}) = g_{t1}(\boldsymbol{\theta}) - g_{t2}(\boldsymbol{\theta}), \end{aligned} \tag{2.38}$$

where $f_{t1}(\boldsymbol{\theta})=(1+\mathbf{t}_{hb1}^H\mathbf{t}_{hb1})(1+\mathbf{t}_{hb2}^H\mathbf{t}_{hb2})$, $f_{t2}(\boldsymbol{\theta})=\mathbf{t}_{hb1}^H\mathbf{t}_{hb2}\mathbf{t}_{hb2}^H\mathbf{t}_{hb1}$, $g_{t1}(\boldsymbol{\theta})=(1+\mathbf{t}_{he1}^H\mathbf{B}^{-1}\mathbf{t}_{he1})(1+\mathbf{t}_{he2}^H\mathbf{B}^{-1}\mathbf{t}_{he2})$, $g_{t2}(\boldsymbol{\theta})=\mathbf{t}_{he1}^H\mathbf{B}^{-1}\mathbf{t}_{he2}\mathbf{t}_{he2}^H\mathbf{B}^{-1}\mathbf{t}_{he1}$. Then the subproblem to optimize $\boldsymbol{\theta}$ can be formulated as

$$(\mathrm{P0}-3):\max_{\boldsymbol{\theta}}\ \frac{f(\boldsymbol{\theta})}{g(\boldsymbol{\theta})}=\frac{f_{t1}(\boldsymbol{\theta})-f_{t2}(\boldsymbol{\theta})}{g_{t1}(\boldsymbol{\theta})-g_{t2}(\boldsymbol{\theta})}\qquad \text{s.t.}\quad (2.28). \tag{2.39}$$

Since (2.36) is a non-convex function of $\boldsymbol{\theta}$, and all elements in $\boldsymbol{\theta}$ are of constant modulus constraint, thus, a gradient ascent (GA) method is used to compute the IRS phase-shift matrix $\boldsymbol{\Theta}=\mathrm{diag}\{\boldsymbol{\theta}\}$. The gradient of the objective function in (2.39) with respect to $\boldsymbol{\theta}$ can be expressed as

$$\nabla_{\boldsymbol{\theta}}=\frac{f^{'}(\boldsymbol{\theta})g(\boldsymbol{\theta})-f(\boldsymbol{\theta})g^{'}(\boldsymbol{\theta})}{g^2(\boldsymbol{\theta})}, \tag{2.40}$$

where

$$f^{'}(\boldsymbol{\theta})=f_{t1}^{'}(\boldsymbol{\theta})-f_{t2}^{'}(\boldsymbol{\theta}),\ g^{'}(\boldsymbol{\theta})=g_{t1}^{'}(\boldsymbol{\theta})-g_{t2}^{'}(\boldsymbol{\theta}), \tag{2.41}$$

$$\begin{aligned} f_{t1}^{'}(\boldsymbol{\theta}) =\ & (1+\mathbf{t}_{hb2}^H\mathbf{t}_{hb2})(\mathbf{T}_{B1}^H\mathbf{T}_{B1}\boldsymbol{\theta}+\mathbf{T}_{B1}^H\mathbf{h}_{B1}) \\ & +(1+\mathbf{t}_{hb1}^H\mathbf{t}_{hb1})(\mathbf{T}_{B2}^H\mathbf{T}_{B2}\boldsymbol{\theta}+\mathbf{T}_{B2}^H\mathbf{h}_{B2}), \end{aligned} \tag{2.42}$$

$$\begin{aligned} f_{t2}^{'}(\boldsymbol{\theta}) =\ & \mathbf{t}_{hb2}^H\mathbf{t}_{hb1}(\mathbf{T}_{B2}^H\mathbf{T}_{B1}\boldsymbol{\theta}+\mathbf{T}_{B2}^H\mathbf{h}_{B1}) \\ & +\mathbf{t}_{hb1}^H\mathbf{t}_{hb2}(\mathbf{T}_{B1}^H\mathbf{T}_{B2}\boldsymbol{\theta}+\mathbf{T}_{B1}^H\mathbf{h}_{B2}), \end{aligned} \tag{2.43}$$

$$\begin{aligned} g_{t1}^{'}(\boldsymbol{\theta}) =\ & (1+\mathbf{t}_{he2}^H\mathbf{B}^{-1}\mathbf{t}_{he2})(\mathbf{T}_{E1}^H\mathbf{B}^{-1}\mathbf{T}_{E1}\boldsymbol{\theta}+\mathbf{T}_{E1}^H\mathbf{B}^{-1}\mathbf{h}_{E1}) \\ & +(1+\mathbf{t}_{he1}^H\mathbf{B}^{-1}\mathbf{t}_{he1})(\mathbf{T}_{E2}^H\mathbf{B}^{-1}\mathbf{T}_{E2}\boldsymbol{\theta}+\mathbf{T}_{E2}^H\mathbf{B}^{-1}\mathbf{h}_{E2}), \end{aligned} \tag{2.44}$$

$$\begin{aligned} g_{t2}^{'}(\boldsymbol{\theta}) =\ & \mathbf{t}_{he2}^H\mathbf{B}^{-1}\mathbf{t}_{he1}(\mathbf{T}_{E2}^H\mathbf{B}^{-1}\mathbf{T}_{E1}\boldsymbol{\theta}+\mathbf{T}_{E2}^H\mathbf{B}^{-1}\mathbf{h}_{E1}) \\ & +\mathbf{t}_{he1}^H\mathbf{B}^{-1}\mathbf{t}_{he2}(\mathbf{T}_{E1}^H\mathbf{B}^{-1}\mathbf{T}_{E2}\boldsymbol{\theta}+\mathbf{T}_{E1}^H\mathbf{B}^{-1}\mathbf{h}_{E2}). \end{aligned} \tag{2.45}$$

After obtaining $\nabla_{\boldsymbol{\theta}}$, we will renew the value $\boldsymbol{\theta}^{(t)}$ of $\boldsymbol{\theta}$ by $\boldsymbol{\theta}^{(t-1)}+\alpha\nabla_{\boldsymbol{\theta}}$ with α being the searching step, which can be obtained by a backtracking line search [53]. The detailed process of GA algorithm proposed is listed in Algorithm 1. The convergence can be guaranteed as the step size can be determined well in each iteration by the backtracking line search, which guarantees the objective function

value of problem (P0-3) monotonically increases in each step and each iteration. Thus we can obtain the IRS phase-shift matrix $\boldsymbol{\Theta}$ with $\boldsymbol{\Theta} = \text{diag}\{\boldsymbol{\theta}\}$.

Algorithm 1 GA algorithm to compute the phase-shift vector $\boldsymbol{\theta}$ using the Max-SR rule

1: Initialize $\boldsymbol{\theta}^{(0)}$, initialize $\mathbf{v}_1$, $\mathbf{v}_2$ based on (2.25) and (2.26), compute $R_s^{(0)}$.
2: Set $t = 1$, threshold value ϵ.
3: **repeat**
4: Compute $\nabla_{\boldsymbol{\theta}}^{(t-1)}$ according to (2.40). Obtain the step size $\alpha^{(t)}$ by backtracking line search.
5: $\boldsymbol{\theta}^{(t)} = \boldsymbol{\theta}^{(t-1)} + \alpha^{(t)} \nabla_{\boldsymbol{\theta}}^{(t-1)}$, reform $\boldsymbol{\theta}^{(t)} = \exp\{j \angle(\boldsymbol{\theta}^{(t)})\}$.
6: Compute $R_s^{(t)}$ using $\mathbf{v}_1$, $\mathbf{v}_2$ and $\boldsymbol{\theta}^{(t)}$.
7: $t = t + 1$.
8: **until** $R_s^{(t)} - R_s^{(t-1)} \leq \epsilon$
9: $\boldsymbol{\theta}^{(t)}$ is the optimal phase-shift vector.

2.3.3 Overall Algorithm

Algorithm 2 Proposed GAI algorithm

1: Initialize $\mathbf{v}_1^{(0)}$, $\mathbf{v}_2^{(0)}$ and $\boldsymbol{\Theta}^{(0)}$, compute $R_s^{(0)}$ according to (2.18).
2: Set $p = 0$, threshold ϵ.
3: **repeat**
4: Given $(\boldsymbol{\Theta}^{(p)}, \mathbf{v}_2^{(p)})$, solve problem (2.25) to determine $\mathbf{v}_1^{(p+1)}$ based on the Rayleigh-Ritz theorem.
5: Given $(\boldsymbol{\Theta}^{(p)}, \mathbf{v}_1^{(p+1)})$, solve problem (2.26) to determine $\mathbf{v}_2^{(p+1)}$ based on the Rayleigh-Ritz theorem.
6: Given $(\mathbf{v}_1^{(p+1)}, \mathbf{v}_2^{(p+1)})$, solve problem (2.39) to determine $\boldsymbol{\Theta}^{(p+1)}$ based on GA method in Algorithm 1.
7: Compute $R_s^{(p+1)}$ using $\mathbf{v}_1^{(p+1)}$, $\mathbf{v}_2^{(p+1)}$ and $\boldsymbol{\Theta}^{(p+1)}$.
8: $p = p + 1$;
9: **until** $R_s^{(p)} - R_s^{(p-1)} \leq \epsilon$
10: $\boldsymbol{\Theta}^{(p)}$, $\mathbf{v}_1^{(p)}$ and $\mathbf{v}_2^{(p)}$ are the optimal value that we need, and $R_s^{(p)}$ is the optimal achievable secrecy rate.

So far, we have completed the design of beamforming vectors and IRS phase-shift matrix. Our iterative idea can be described as follows: given a fixed matrix $\boldsymbol{\Theta}$, the corresponding beamforming vectors can be computed in a closed-form expression iteratively; for two given beamforming vectors $\mathbf{v}_1$ and $\mathbf{v}_2$, the GA method is used to find the value of IRS phase-shift matrix $\boldsymbol{\Theta}$. The alternative iteration process among $\mathbf{v}_1$, $\mathbf{v}_2$, and $\boldsymbol{\Theta}$ is repeated until the stop criterion is satisfied, that is, $R_s^{p+1} - R_s^p \leq \epsilon$ with p being the iteration index. The proposed method is summarized in Algorithm 2.

The computational complexity of Algorithm 2 is

$$O\Big(D\big(8N^3+2N+D_1(12M^3K+10M^3+12M^2K+16 \\ M^2K^2-18M^2+12MK^2+28MK-16M)\log_2(1/\kappa)\big)\Big) \tag{2.46}$$

float-point operations (FLOPs), where D denotes the maximum number of alternating iterations for Algorithm 2, D_1 denotes the maximum iterative number of Algorithm 1, κ denotes the accuracy or, in other words, the convergence threshold of backtracking line search, and $\log_2(1/\kappa)$ denotes the maximum iterative number of backtracking line search.

2.4 Proposed Low-Complexity NSP-Based Max-SR Method

In the previous section, the proposed GAI is general, its computational complexity is still very high because of GA algorithm with lots of FLOPs for obtaining the gradient and stepsize. In this section, we will propose one low-complexity algorithm named NSP to reduce the complexity of the proposed GAI, especially for the case of a large number of IRS elements. In this section, the three beamforming vectors for two CMs and AN are designed well such that any one of them is confined to the NSs of the remaining two channels. This guarantees that two CMs will be not allowed to leak to Eve at the transmitter end, and AN is only transmitted to Eve for interference.

Applying the NSP principle in [20], the beamforming vectors $\mathbf{v}_1$ and $\mathbf{v}_2$ can be determined by

$$\begin{aligned} &\mathbf{H}_{AB}^H\mathbf{v}_1=\mathbf{0}_{K\times 1}, \quad \mathbf{H}_{AE}^H\mathbf{v}_1=\mathbf{0}_{K\times 1}, \\ &\mathbf{H}_{AI}\mathbf{v}_2=\mathbf{0}_{M\times 1}, \quad \mathbf{H}_{AE}^H\mathbf{v}_2=\mathbf{0}_{K\times 1}, \end{aligned} \tag{2.47}$$

which means that x_1 is only reflected to users by IRS, and x_2 reaches users through the direct path. The achievable rates from Alice to Bob and to Eve can be expressed as (2.48) and (2.49).

$$\begin{aligned} R_B=\log_2 t|\mathbf{I}_K+\frac{1}{\sigma_B^2}[&\beta_1 P_s g_{AIB}\mathbf{H}_{IB}^H\boldsymbol{\Theta}\mathbf{H}_{AI}\mathbf{v}_1\mathbf{v}_1^H\left(\mathbf{H}_{IB}^H\boldsymbol{\Theta}\mathbf{H}_{AI}\right)^H \\ &+\beta_2 P_s g_{AB}\mathbf{H}_{AB}^H\mathbf{v}_2\mathbf{v}_2^H\mathbf{H}_{AB}]| \end{aligned} \tag{2.48}$$

$$\begin{aligned} R_E=\log_2\Big|\mathbf{I}_K+\big(&\beta_1 P_s g_{AIE}\mathbf{H}_{IE}^H\boldsymbol{\Theta}\mathbf{H}_{AI}\mathbf{v}_1\mathbf{v}_1^H\left(\mathbf{H}_{IE}^H\boldsymbol{\Theta}\mathbf{H}_{AI}\right)^H\big) \\ &\cdot\big((1-\beta_1-\beta_2)P_s g_{AE}\mathbf{H}_{AE}^H\mathbf{P}_{AN}\mathbf{P}_{AN}^H\mathbf{H}_{AE}+\sigma_E^2\mathbf{I}_K\big)^{-1}\Big|. \end{aligned} \tag{2.49}$$

Let us define two new large channel matrices

$$\mathbf{H}_1 = \left[\mathbf{H}_{AB}^* \, \mathbf{H}_{AE}^*\right]^T, \quad \mathbf{H}_2 = \left[\mathbf{H}_{AI}^T \, \mathbf{H}_{AE}^*\right]^T, \tag{2.50}$$

then (2.47) can be expressed as $\mathbf{H}_1\mathbf{v}_1 = \mathbf{0}$ and $\mathbf{H}_2\mathbf{v}_2 = \mathbf{0}$ which means the beamforming vectors $\mathbf{v}_1$ and $\mathbf{v}_2$ can be solved by using the zero-forcing (ZF) scheme as $\mathbf{P}_1$ and $\mathbf{P}_2$ are the corresponding projection matrix, where

$$\begin{aligned}\mathbf{P}_1 &= \mathbf{I}_N - \mathbf{H}_1^H \left[\mathbf{H}_1\mathbf{H}_1^H\right]^\dagger \mathbf{H}_1, \\ \mathbf{P}_2 &= \mathbf{I}_N - \mathbf{H}_2^H \left[\mathbf{H}_2\mathbf{H}_2^H\right]^\dagger \mathbf{H}_2.\end{aligned} \tag{2.51}$$

For convenience of derivation below, let us define two new vectors $\mathbf{w}_1 \in \mathbb{C}^{N\times 1}$ and $\mathbf{w}_2 \in \mathbb{C}^{N\times 1}$

$$\mathbf{v}_1 = \mathbf{P}_1\mathbf{w}_1, \quad \mathbf{v}_2 = \mathbf{P}_2\mathbf{w}_2. \tag{2.52}$$

As for the condition (2.19c) of the problem (2.19), we rewrite it by applying (2.52), that is, $\mathbf{w}_1^H\mathbf{P}_1^H\mathbf{P}_1\mathbf{w}_1 = 1$ and $\mathbf{w}_2^H\mathbf{P}_2^H\mathbf{P}_2\mathbf{w}_2 = 1$. (2.53) and (2.54) are rewritten as follows

$$\begin{aligned}\mathbf{y}_B &= \sqrt{\beta_1 P_s g_{AIB}}\mathbf{H}_{IB}^H\boldsymbol{\Theta}\mathbf{H}_{AI}\mathbf{v}_1 x_1 + \sqrt{\beta_2 P_s g_{AB}}\mathbf{H}_{AB}^H\mathbf{v}_2 x_2 + \mathbf{n}_B \\ &= \sqrt{\beta_1 P_s g_{AIB}}\mathbf{H}_{IB}^H\boldsymbol{\Theta}\mathbf{H}_{AI}\mathbf{P}_1\mathbf{w}_1 x_1 + \sqrt{\beta_2 P_s g_{AB}}\mathbf{H}_{AB}^H\mathbf{P}_2\mathbf{w}_2 x_2 + \mathbf{n}_B,\end{aligned} \tag{2.53}$$

$$\begin{aligned}\mathbf{y}_E &= \sqrt{\beta_1 P_s g_{AIE}}\mathbf{H}_{IE}^H\boldsymbol{\Theta}\mathbf{H}_{AI}\mathbf{v}_1 x_1 + \sqrt{(1-\beta_1-\beta_2) P_s g_{AE}}\mathbf{H}_{AE}^H\mathbf{P}_{AN}\mathbf{z} + \mathbf{n}_E \\ &= \sqrt{\beta_1 P_s g_{AIE}}\mathbf{H}_{IE}^H\boldsymbol{\Theta}\mathbf{H}_{AI}\mathbf{P}_1\mathbf{w}_1 x_1 + \sqrt{(1-\beta_1-\beta_2) P_s g_{AE}}\mathbf{H}_{AE}^H\mathbf{P}_{AN}\mathbf{z} + \mathbf{n}_E.\end{aligned} \tag{2.54}$$

In what follows, we can calculate the beamforming vectors and IRS phase-shift matrix by calculating $\mathbf{w}_1$, $\mathbf{w}_2$ and $\boldsymbol{\Theta}$ alternately.

2.4.1 *Optimization of Beamforming Vectors Given IRS Phase-Shift Matrix* $\boldsymbol{\Theta}$

Substituting (2.52) in (2.48) yields

$$R_B = \log_2 |\mathbf{I}_K + \mathbf{A}_1\mathbf{w}_1\mathbf{w}_1^H\mathbf{A}_1^H + \mathbf{A}_2\mathbf{w}_2\mathbf{w}_2^H\mathbf{A}_2^H|, \tag{2.55}$$

where $\mathbf{A}_1 = \frac{\sqrt{\beta_1 P_s g_{AIB}}}{\sigma_B}\mathbf{H}_{IB}^H\boldsymbol{\Theta}\mathbf{H}_{AI}\mathbf{P}_1$, $\mathbf{A}_2 = \frac{\sqrt{\beta_2 P_s g_{AB}}}{\sigma_B}\mathbf{H}_{AB}^H\mathbf{P}_2$, Similarly, substituting (2.52) in (2.49) yields

$$R_E = \log_2 |\mathbf{I}_K + \mathbf{A}_3 \mathbf{w}_1 \mathbf{w}_1^H \mathbf{A}_3^H \mathbf{B}^{-1}| \overset{(b)}{=} \log_2 \left(1 + \mathbf{w}_1^H \mathbf{A}_3^H \mathbf{B}^{-1} \mathbf{A}_3 \mathbf{w}_1\right), \tag{2.56}$$

where $\mathbf{A}_3 = \frac{\sqrt{\beta_1 P_s g_{AIE}}}{\sigma_E} \mathbf{H}_{IE}^H \mathbf{\Theta} \mathbf{H}_{AI} \mathbf{P}_1$, $\mathbf{B}$ owns the same definition as (2.17), and (b) holds due to $|\mathbf{I}_M + \mathbf{XY}| = |\mathbf{I}_N + \mathbf{YX}|$ for $\mathbf{X} \in \mathbb{C}^{M \times N}$ and $\mathbf{Y} \in \mathbb{C}^{N \times M}$. Then the NSP-based Max-SR can be formulated as follows:

$$(\text{P1}): \max_{\mathbf{w}_1, \mathbf{w}_2, \mathbf{\Theta}} \quad R_s(\mathbf{w}_1, \mathbf{w}_2, \mathbf{\Theta}) = (2.55)\text{-}(2.56) \tag{2.57a}$$

$$\text{s.t.} \quad \mathbf{w}_1^H \mathbf{P}_1^H \mathbf{P}_1 \mathbf{w}_1 = 1, \quad \mathbf{w}_2^H \mathbf{P}_2^H \mathbf{P}_2 \mathbf{w}_2 = 1, \quad (2.19c). \tag{2.57b}$$

It is clear to see that R_B in (2.55) is related to $\mathbf{w}_1$, $\mathbf{w}_2$ and $\mathbf{\Theta}$, while R_E in (2.56) is only related to $\mathbf{w}_1$ and $\mathbf{\Theta}$. Since the expression of (2.55) is similar to (2.11), (2.55) can be expressed as the function of $\mathbf{w}_1$ in (2.58) with known $\mathbf{w}_2$ and $\mathbf{\Theta}$, and the function of $\mathbf{w}_2$ in (2.59) with known $\mathbf{w}_1$ and $\mathbf{\Theta}$

$$R_B(\mathbf{w}_1) = \log_2 |\mathbf{I}_K + \mathbf{A}_2 \mathbf{w}_2 \mathbf{w}_2^H \mathbf{A}_2^H| + \log_2 \left(1 + \mathbf{w}_1^H \mathbf{A}_1^H (\mathbf{I}_K + \mathbf{A}_2 \mathbf{w}_2 \mathbf{w}_2^H \mathbf{A}_2^H)^{-1} \mathbf{A}_1 \mathbf{w}_1\right), \tag{2.58}$$

$$R_B(\mathbf{w}_2) = \log_2 |\mathbf{I}_K + \mathbf{A}_1 \mathbf{w}_1 \mathbf{w}_1^H \mathbf{A}_1^H| + \log_2 \left(1 + \mathbf{w}_2^H \mathbf{A}_2^H (\mathbf{I}_K + \mathbf{A}_1 \mathbf{w}_1 \mathbf{w}_1^H \mathbf{A}_1^H)^{-1} \mathbf{A}_2 \mathbf{w}_2\right), \tag{2.59}$$

respectively. Since $R_B(\mathbf{w}_1)$ in (2.58) is independent of $\mathbf{w}_2$, the NSP-based Max-SR of optimizing $\mathbf{w}_1$ is casted as

$$(\text{P1}-1): \max_{\mathbf{w}_1} \quad \frac{\mathbf{w}_1^H \tilde{\mathbf{A}}_1 \mathbf{w}_1}{\mathbf{w}_1^H \tilde{\mathbf{B}}_1 \mathbf{w}_1} \qquad \text{s.t.} \quad \mathbf{w}_1^H \mathbf{P}_1^H \mathbf{P}_1 \mathbf{w}_1 = 1, \tag{2.60}$$

where $\tilde{\mathbf{A}}_1 = \mathbf{P}_1^H \mathbf{P}_1 + \mathbf{A}_1^H (\mathbf{I}_K + \mathbf{A}_2 \mathbf{w}_2 \mathbf{w}_2^H \mathbf{A}_2^H)^{-1} \mathbf{A}_1$ and $\tilde{\mathbf{B}}_1 = \mathbf{P}_1^H \mathbf{P}_1 + \mathbf{A}_3^H \mathbf{B}^{-1} \mathbf{A}_3$. Since $\frac{\mathbf{w}_1^H \tilde{\mathbf{A}}_1 \mathbf{w}_1}{\mathbf{w}_1^H \tilde{\mathbf{B}}_1 \mathbf{w}_1}$ is insensitive to the scaling of $\mathbf{w}_1$, via ignoring the constraint on $\mathbf{w}_1$, we will find a general solution, and then scale it to satisfy

$$\mathbf{w}_1^H \mathbf{P}_1^H \mathbf{P}_1 \mathbf{w}_1 \leq 1. \tag{2.61}$$

It can be observed that the optimization problem in (2.60) belongs to the type of nonlinear fractional optimization problem. To solve this problem, we introduce the Dinkelbach method, and then transform it into a DC programming similar to [54]. Since the numerator and denominator of the objective function in problem (2.60) are convex, we introduce ν into it and transform it as $\mathbf{w}_1^H \tilde{\mathbf{A}}_1 \mathbf{w}_1 - \nu \mathbf{w}_1^H \tilde{\mathbf{B}}_1 \mathbf{w}_1$. Then the objective function of (2.60) can be achieved if and only if

$$\max_{\mathbf{w}_1 \in \mathbb{D}} \quad \mathbf{w}_1^H \tilde{\mathbf{A}}_1 \mathbf{w}_1 - \nu^* \mathbf{w}_1^H \tilde{\mathbf{B}}_1 \mathbf{w}_1$$
$$= \mathbf{w}_1^{*H} \tilde{\mathbf{A}}_1 \mathbf{w}_1^* - \nu^* \mathbf{w}_1^{*H} \tilde{\mathbf{B}}_1 \mathbf{w}_1^* = 0, \tag{2.62}$$

for $\mathbf{w}_1^H \tilde{\mathbf{A}}_1 \mathbf{w}_1 \geq 0$ and $\mathbf{w}_1^H \tilde{\mathbf{B}}_1 \mathbf{w}_1 \geq 0, \forall \mathbf{w}_1 \in \mathbb{D}$, where $\mathbb{D}$ denotes the feasible domain of the problem (2.60). This transformation can be proved in [54]. Therefore, we can rewrite the optimization problem (2.60) as

$$(\mathrm{P1}-1.1): \max_{\mathbf{w}_1, \nu} \quad \mathbf{w}_1^H \tilde{\mathbf{A}}_1 \mathbf{w}_1 - \nu \mathbf{w}_1^H \tilde{\mathbf{B}}_1 \mathbf{w}_1 \qquad \text{s.t.} \quad (2.61). \tag{2.63}$$

However, problem (2.63) is still not convex in terms of $\mathbf{w}_1$ due to the fact that its objective function is the difference of two convex functions, which is nonconvex. Hence, we linearize the objective function $\mathbf{w}_1^H \tilde{\mathbf{A}}_1 \mathbf{w}_1$ by the first term of its Taylor series expansion at a given vector of $\tilde{\mathbf{w}}_1$ as follows

$$\mathbf{w}_1^H \tilde{\mathbf{A}}_1 \mathbf{w}_1 \geq 2\Re\{\tilde{\mathbf{w}}_1^H \tilde{\mathbf{A}}_1 \mathbf{w}_1\} - \tilde{\mathbf{w}}_1^H \tilde{\mathbf{A}}_1 \tilde{\mathbf{w}}_1. \tag{2.64}$$

Then the problem (2.60) can be rewritten as

$$(\mathrm{P1}-1.2): \max_{\mathbf{w}_1, \nu} \quad 2\Re\{\tilde{\mathbf{w}}_1^H \tilde{\mathbf{A}}_1 \mathbf{w}_1\} - \tilde{\mathbf{w}}_1^H \tilde{\mathbf{A}}_1 \tilde{\mathbf{w}}_1 - \nu \mathbf{w}_1^H \tilde{\mathbf{B}}_1 \mathbf{w}_1$$
$$\text{s.t.} \quad (2.61). \tag{2.65}$$

which is a convex optimization problem. Then it can be readily solved by Boyd and Vandenberghe [53].

The optimization subproblem of NSP-based Max-SR with respect to $\mathbf{w}_2$ can be modeled as

$$(\mathrm{P1}-2): \max_{\mathbf{w}_2} \quad \mathbf{w}_2^H \tilde{\mathbf{A}}_2 \mathbf{w}_2 \qquad \text{s.t.} \quad \mathbf{w}_2^H \mathbf{P}_2^H \mathbf{P}_2 \mathbf{w}_2 = 1, \tag{2.66}$$

where $\tilde{\mathbf{A}}_2 = \mathbf{P}_2^H \mathbf{P}_2 + \mathbf{A}_2^H (\mathbf{I}_K + \mathbf{A}_1 \mathbf{w}_1 \mathbf{w}_1^H \mathbf{A}_1^H)^{-1} \mathbf{A}_2$. Similarly, the constraint can be scaled as (2.61). Since $\tilde{\mathbf{A}}_2 \succeq \mathbf{0}$, $\mathbf{w}_2^H \tilde{\mathbf{A}}_2 \mathbf{w}_2$ is a convex function with respect to $\mathbf{w}_2$, we can get the following inequality by performing the first-order Taylor expansion on $\mathbf{w}_2^H \tilde{\mathbf{A}}_2 \mathbf{w}_2$ at the point $\tilde{\mathbf{w}}_2$ like (2.64). Then the problem (2.66) can be rewritten as

$$(\mathrm{P1}-2.1): \max_{\mathbf{w}_2} \quad 2\Re\{\tilde{\mathbf{w}}_2^H \tilde{\mathbf{A}}_2 \mathbf{w}_2\} - \tilde{\mathbf{w}}_2^H \tilde{\mathbf{A}}_2 \tilde{\mathbf{w}}_2$$
$$\text{s.t.} \quad \mathbf{w}_2^H \mathbf{P}_2^H \mathbf{P}_2 \mathbf{w}_2 \leq 1. \tag{2.67}$$

We can see that the objective function in the optimization problem (2.67) is concave and the constraint is convex. Thus (2.67) is a convex optimization problem, which can be solved by Boyd and Vandenberghe [53].

2.4.2 Optimization of IRS Phase-Shift Matrix $\boldsymbol{\Theta}$ with Given Beamforming Vectors

Now, we optimize the IRS phase-shift matrix $\boldsymbol{\Theta}$ by using NSP-based Max-SR method. By applying (2.27), (2.48) and (2.49) are represented as

$$R_B(\boldsymbol{\theta}) = \log_2 |\mathbf{I}_K + \mathbf{T}_{B1}\boldsymbol{\theta}\boldsymbol{\theta}^H\mathbf{T}_{B1}^H + \mathbf{h}_{B2}\mathbf{h}_{B2}^H| \tag{2.68}$$

and

$$R_E(\boldsymbol{\theta}) = \log_2 |\mathbf{I}_K + \mathbf{T}_{E1}\boldsymbol{\theta}\boldsymbol{\theta}^H\mathbf{T}_{E1}^H\mathbf{B}^{-1}|, \tag{2.69}$$

where $\mathbf{T}_{B1}$, $\mathbf{h}_{B2}$, $\mathbf{T}_{E1}$, and $\mathbf{B}$ have the same forms as before. Then the subproblem to optimize $\boldsymbol{\Theta}$ can be equivalently changed as to optimize the IRS phase-shift vector $\boldsymbol{\theta}$, formulated as,

$$(\text{P1}-3): \max_{\boldsymbol{\theta}} \quad (2.68)\text{–}(2.69) \qquad \text{s.t.} \quad (2.28). \tag{2.70}$$

Due to the fact that $|\mathbf{XY}| = |\mathbf{X}||\mathbf{Y}|$ and $|\mathbf{I}_M + \mathbf{XY}| = |\mathbf{I}_N + \mathbf{YX}|$ for $\mathbf{X} \in \mathbb{C}^{M\times N}$ and $\mathbf{Y} \in \mathbb{C}^{N\times M}$, (2.68) and (2.69) can be rewritten as

$$R_B(\boldsymbol{\theta}) = \log_2(1+\boldsymbol{\theta}^H\mathbf{T}_{B1}^H(\mathbf{I}_K+\mathbf{h}_{B2}\mathbf{h}_{B2}^H)^{-1}\mathbf{T}_{B1}\boldsymbol{\theta})+\log_2|\mathbf{I}_K+\mathbf{h}_{B2}\mathbf{h}_{B2}^H|, \tag{2.71}$$

and

$$R_E(\boldsymbol{\theta}) = \log_2(1+\boldsymbol{\theta}^H\mathbf{T}_{E1}^H\mathbf{B}^{-1}\mathbf{T}_{E1}\boldsymbol{\theta}). \tag{2.72}$$

Since $\log_2|\mathbf{I}_K + \mathbf{h}_{B2}\mathbf{h}_{B2}^H|$ is independent of $\boldsymbol{\theta}$, problem (2.70) can be formulated as

$$(\text{P1}-3.1): \max_{\boldsymbol{\theta}} \quad \frac{\boldsymbol{\theta}^H\tilde{\mathbf{T}}_B\boldsymbol{\theta}}{\boldsymbol{\theta}^H\tilde{\mathbf{B}}_E\boldsymbol{\theta}} \qquad \text{s.t.} \quad (2.28), \tag{2.73}$$

where $\tilde{\mathbf{T}}_B = \frac{1}{M}\mathbf{I}_M + \mathbf{T}_{B1}^H(\mathbf{I}_K + \mathbf{h}_{B2}\mathbf{h}_{B2}^H)^{-1}\mathbf{T}_{B1}$ and $\tilde{\mathbf{B}}_E = \frac{1}{M}\mathbf{I}_M + \mathbf{T}_{E1}^H\mathbf{B}^{-1}\mathbf{T}_{E1}$. Rewrite problem (2.73) as

$$(\text{P1}-3.2): \min_{\boldsymbol{\theta}} \quad \frac{\boldsymbol{\theta}^H\tilde{\mathbf{B}}_E\boldsymbol{\theta}}{\boldsymbol{\theta}^H\tilde{\mathbf{T}}_B\boldsymbol{\theta}} \qquad \text{s.t.} \quad (2.28). \tag{2.74}$$

Obviously, the above optimization problem belongs to fractional programming. Introducing a new parameter $\mu \geqslant 0$ forms the corresponding parametric program as follows:

$$(\mathrm{P1}-3.3):\min_{\boldsymbol{\theta}}\ \boldsymbol{\theta}^H\tilde{\mathbf{B}}_E\boldsymbol{\theta}-\mu\boldsymbol{\theta}^H\tilde{\mathbf{T}}_B\boldsymbol{\theta}\qquad \text{s.t.}\quad (2.28). \tag{2.75}$$

As [54] showed, the optimal solution to problem (2.75) is the unique root of $\boldsymbol{\theta}^H\tilde{\mathbf{B}}_E\boldsymbol{\theta}-\mu\boldsymbol{\theta}^H\tilde{\mathbf{T}}_B\boldsymbol{\theta}=0$. Without the constant mode constraint of $\boldsymbol{\theta}$, this kind of problem can be solved by SDR as problem (2.65) performs. In this case, we minimize an upper bound of its objective function following [55] and [56] as

$$\begin{aligned}\boldsymbol{\theta}^H\tilde{\mathbf{B}}_E\boldsymbol{\theta}-\mu\boldsymbol{\theta}^H\tilde{\mathbf{T}}_B\boldsymbol{\theta}&=\boldsymbol{\theta}^H(\tilde{\mathbf{B}}_E-\mu\tilde{\mathbf{T}}_B)\boldsymbol{\theta}\\&\leqslant\lambda_{\max}(\boldsymbol{\Psi})\|\boldsymbol{\theta}\|^2-2\Re\{\boldsymbol{\theta}^H\big(\lambda_{\max}(\boldsymbol{\Psi})\mathbf{I}_M-\boldsymbol{\Psi}\big)\tilde{\boldsymbol{\theta}}\}\\&\quad+\tilde{\boldsymbol{\theta}}^H\big(\lambda_{\max}(\boldsymbol{\Psi})\mathbf{I}_M-\boldsymbol{\Psi}\big)\tilde{\boldsymbol{\theta}}\end{aligned} \tag{2.76}$$

where $\boldsymbol{\Psi}=\tilde{\mathbf{B}}_E-\mu\tilde{\mathbf{T}}_B$, $\tilde{\boldsymbol{\theta}}$ is the solution to $\boldsymbol{\theta}$ obtained in the previous iteration of the alternating algorithm. Since $|\boldsymbol{\theta}_i|^2=1$ and $\|\boldsymbol{\theta}\|^2=M$, $\lambda_{\max}(\boldsymbol{\Psi})\|\boldsymbol{\theta}\|^2$ and $\tilde{\boldsymbol{\theta}}^H\big(\lambda_{\max}(\boldsymbol{\Psi})\mathbf{I}_M-\boldsymbol{\Psi}\big)\tilde{\boldsymbol{\theta}}$ are determined here. Then the simplified optimization problem reduces to

$$(\mathrm{P1}-3.4):\max_{\boldsymbol{\theta}}\ \Re\{\boldsymbol{\theta}^H\boldsymbol{\delta}\}\qquad \text{s.t.}\quad (2.28), \tag{2.77}$$

where $\boldsymbol{\delta}=\big(\lambda_{\max}(\boldsymbol{\Psi})\mathbf{I}_M-\boldsymbol{\Psi}\big)\tilde{\boldsymbol{\theta}}$. In this case, $\Re\{\boldsymbol{\theta}^H\boldsymbol{\delta}\}$ is maximized when the phases of θ_i and δ_i are equal, where δ_i is the i-th element of $\boldsymbol{\delta}$. Thus the optimal solution to the problem with given μ is

$$\boldsymbol{\theta}^*(\mu)=[e^{j\arg(\delta_1)},\cdots,e^{j\arg(\delta_M)}]^T. \tag{2.78}$$

Substituting $\boldsymbol{\theta}^*(\mu)$ into the objective function of problem (2.75), we have the result $\varphi^*(\mu)$. Since $\varphi^*(\mu)$ is a strictly decreasing function for the optimal $\boldsymbol{\theta}$, with $\varphi^*(0)>0$ and $\varphi^*(+\infty)<0$, which has been confirmed in [45], the optimal μ^* can be found by $\varphi^*(\mu^*)=0$ via bisection search. Thus we can obtain the solution to $\boldsymbol{\theta}$ by $\boldsymbol{\theta}^*(\mu^*)$. The above problem has a closed form, which is more convenient for implementation and requires much lower complexity especially for large M.

2.4.3 Overall Algorithm

The proposed NSP algorithm is divided into two parts: the beamforming vectors and the IRS phase-shift matrix. The iterative idea can be described as follows: for given matrix $\boldsymbol{\Theta}$, anyone of the beamforming vectors can be expressed as an unknown vector multiplied by a known matrix, which can be computed by CVX

iteratively as the other is fixed; for given two beamforming vectors $\mathbf{v}_1$ and $\mathbf{v}_2$, the closed-form expression of IRS phase-shift vector $\boldsymbol{\theta}$ can be expressed as (2.78). The alternative iterations among $\mathbf{v}_1$, $\mathbf{v}_2$ and $\boldsymbol{\Theta}$ is repeated until the stop criterion satisfies, that is, $R_s^{p+1} - R_s^p \leq \epsilon$ with p being the iteration index. The proposed method is summarized in Algorithm 3. The computational complexity of Algorithm 3 is

$$O\Big(L\big(2\sqrt{2}[(N+1)^3 + N^2(N+1)]\ln(1/\epsilon) + L_1(M^3 + 4M^2 K - 2M - 2MK + 4MK^2 + K^2)\log_2((\lambda_{max} - \lambda_{min})/\epsilon)\big)\Big) \tag{2.79}$$

FLOPs, where L denotes the maximum number of alternating iterations, L_1 denotes the iterative number of the subproblem (P1-3), ϵ denotes the accuracy or the convergence threshold of the algorithm, and λ_{max} and λ_{min} are the upper-bound and lower-bound of bisection method, respectively. $\log_2((\lambda_{max} - \lambda_{min})/\epsilon)$ is the maximum iterative number of bisection search.

Compared with the complexity of the proposed GAI in (2.46), the complexity of the proposed NSP in (2.79) is greatly reduced especially for large M by taking the convergence analysis in Sect. 2.5 into account. This is the benefit of NSP. However, the NSP is only suitable for the case that three streams are transmitted separately and directively, and requires that the number of transmit antennas is greater than the number of receive antennas. This is its limit. Additionally, compared to the GAI, the proposed NSP algorithm will suffer from a performance loss (PL) due to its strict NS constraints. This will reduce the spatial multiplexing gain of CMs. In summary, the proposed NSP can strike an appreciated good balance between SR performance and computational complexity.

Algorithm 3 Proposed NSP algorithm

1: Initialize $\mathbf{v}_1^{(0)}$, $\mathbf{v}_2^{(0)}$ and $\boldsymbol{\Theta}^{(0)}$, compute $R_s^{(0)}$ according to (2.48) and (2.49).
2: Set $p = 0$, threshold ϵ.
3: **repeat**
4: Given $(\boldsymbol{\Theta}^{(p)}, \mathbf{v}_2^{(p)})$ and (2.52), solve problem (2.65) to determine $\mathbf{v}_1^{(p+1)}$.
5: Given $(\boldsymbol{\Theta}^{(p)}, \mathbf{v}_1^{(p+1)})$ and (2.52), solve problem (2.67) to determine $\mathbf{v}_2^{(p+1)}$.
6: Given $(\mathbf{v}_1^{(p+1)}, \mathbf{v}_2^{(p+1)})$ and (2.52), $\boldsymbol{\theta}^{(p+1)}$ can be determined by (2.78), $\boldsymbol{\Theta}^{(p+1)} = \text{diag}\{\boldsymbol{\theta}^{(p+1)}\}$.
7: Compute $R_s^{(p+1)}$ using $\mathbf{v}_1^{(p+1)}$, $\mathbf{v}_2^{(p+1)}$ and $\boldsymbol{\Theta}^{(p+1)}$.
8: $p = p + 1$;
9: **until** $R_s^{(p)} - R_s^{(p-1)} \leq \epsilon$
10: $\boldsymbol{\Theta}^{(p)}$, $\mathbf{v}_1^{(p)}$ and $\mathbf{v}_2^{(p)}$ are the optimal value that we need, and $R_s^{(p)}$ is the optimal achievable secrecy rate.

2.5 Simulation and Discussion

In this section, we provide numeral results to examine the performance of our proposed algorithms. As for the MIMO system model, the array response is modeled as $\mathbf{a}_t(\theta_t) \in \mathbb{C}^{n_t \times 1}$, with $[\mathbf{a}_t(\theta_t)]_{n_{ti}} = \exp(-j2\pi(n_{ti}-1)d_A \cos\theta_{ti}/\lambda)$, where $\theta_r \in [0, \pi)$ denotes the angle-of-arrival (AoA), and $\mathbf{a}_r(\theta_r) \in \mathbb{C}^{n_r \times 1}$, with $[\mathbf{a}_r(\theta_r)]_{n_{ri}} = \exp(-j2\pi(n_{ri}-1)d_A \cos\theta_{ri}/\lambda)$, where $\theta_t \in [0, \pi)$ denotes the angle-of-departure (AoD). Both transmit array at Alice and receive array at Bob are uniformly spaced linear arrays with element pacing $d_A = \lambda/2$. The LoS channel matrix can be expressed as $\mathbf{H} = \mathbf{a}_r(\theta_r)\mathbf{a}_t^H(\theta_t)$. The path loss model is given by $g_{TR} = \left(\frac{c}{4\pi d_{TR} f}\right)^2$, where d_{TR} denotes the distance between the transmitter and the receiver. Under this model, the path loss coefficient g_{AB}, g_{AE}, g_{AIB} and g_{AIE} can be derived respectively.

Simulation parameters are set as follows: $P_s = 30$ dBm, $\sigma_B^2 = 2\sigma_E^2$. $N = 16$, $K = 4$. The distances of Alice-to-IRS link, Alice-to-Bob link, and Alice-to-Eve link are set as $d_{AI} = 10$ m, $d_{AB} = 100$ m and $d_{AE} = 50$ m, respectively. The AoDs of each channel are set as $\theta_{AI}^t = \pi/6$, $\theta_{AB}^t = 11\pi/36$ and $\theta_{AE}^t = \pi/3$, respectively. With given AoDs and distances of each channel, the AoAs and distances of IRS-to-Bob link and IRS-to-Eve link can be determined, thus the channel matrix can be derived respectively. The PA factors are set as $\beta_1 = \beta_2 = 0.4$, $\beta_3 = 0.2$. As for the algorithm setup, the convergence thresholds in terms of the relative increment in the objective value are set as tolerance of $\epsilon = 10^{-4}$.

First, by simulation, we make an investigation of the convergence behaviour of the proposed GAI in Algorithm 2 and NSP in Algorithm 3. Figure 2.2 shows the SR versus the number of iterations for various number of phase shifter, i.e., for $M = 10, 20$. It can be seen from the figure that GAI requires about 4 iterations to converge the SR ceil, while the proposed NSP requires about 3 iterations to converge. Thus, we make a conclusion that the proposed NSP has a more rapid convergence rate than

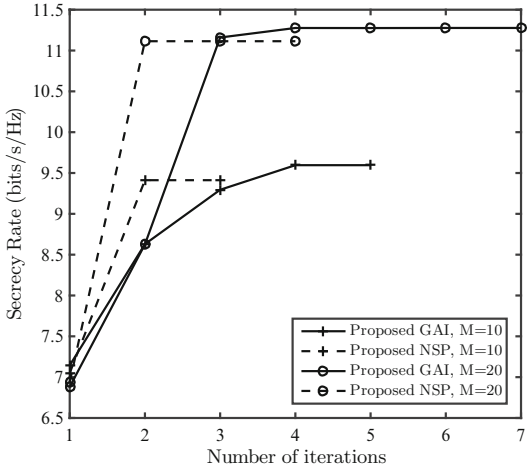


Fig. 2.2 Convergence of proposed algorithm at different number of IRS phase-shift elements ($d_{AB} = 100$ m)

GAI. Using the convergence results in Fig. 2.2, the complexity (2.46) of GAI and complexity (2.79) of NSP reduce to the magnitude orders $40M^3$ and $3M^3$ FLOPs respectively as M goes to large-scale. Clearly, the complexity of NSP is far lower than that of GAI. In the following, we compare our proposed algorithms to the following benchmark schemes:

1. **No-IRS**: Obtain the maximum SR by optimizing the beamforming vectors with the IRS phase-shift matrix set to zero, i.e., $\boldsymbol{\Theta} = \mathbf{0}_{M\times M}$.
2. **Random Phase**: Obtain the maximum SR by optimizing the beamforming vectors with all the phase for each reflection element uniformly and independently generated from $[0, 2\pi)$.
3. **IRS with Single CBS**: Obtain the maximum SR by Algorithm 2 with single CBS, as $\beta_1 = 0, \beta_2 = 1 - \beta_3$ or $\beta_2 = 0, \beta_1 = 1 - \beta_3$. In this case, we also fix PA factor of the AN as $\beta_3 = 0.2$.

2.5.1 *Impact of the Number of IRS Phase-Shift Elements*

For comparison, we consider two scenarios of Alice-to-Bob distance given by $d_{AB} = 300$ m and $d_{AB} = 50$ m, which correspond to the low-SNR regime and high-SNR regime, respectively. For these two cases, the SR performance versus the number of reflecting elements M for the proposed algorithms and the benchmark schemes are presented as Figs. 2.3 and 2.4.

From Figs. 2.3 and 2.4, it can be seen that the proposed two schemes GAI and NSP can improve the SR performance whether in the ow-SNR regime or the high-SNR regime. As the number of IRS elements increases, the SR gains achieved by

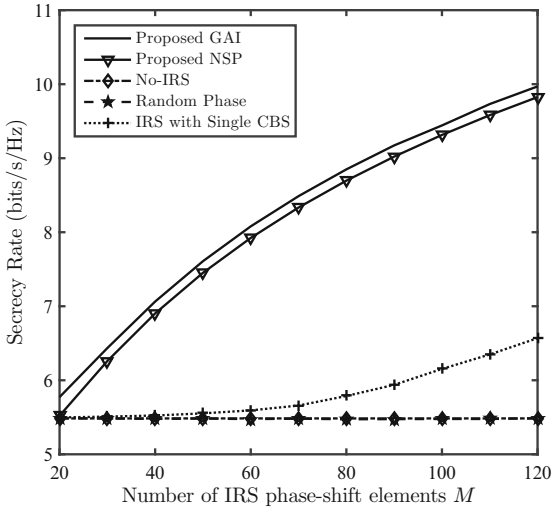


Fig. 2.3 Secrecy rate versus the number of IRS phase-shift elements M in the low-SNR regime ($d_{AB} = 300$ m)

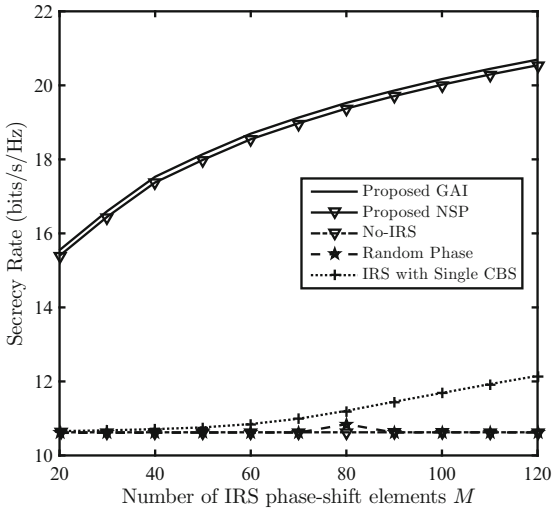


Fig. 2.4 Secrecy rate versus the number of IRS phase-shift elements M in the high-SNR regime ($d_{AB} = 50\,\text{m}$)

GAI and NSP over no-IRS, random phase and IRS with single CBS grow gradually and become more significant.

Compared with the No-IRS scheme and Random-Phase scheme, the IRS phase-shift-optimization schemes (i.e., GAI, NSP) performs much better, especially with a large value of M. This reveals the importance of the optimization of the phase-shift design. Even with a value of M as $M = 30$, our proposed scheme can also perform better than that scheme without the IRS phase-shift-optimization (e.g., by 17.3% in the low-SNR regime and 56.3% in the high-SNR regime).

Under the condition that the total power is equally allocated between two independent CBSs, the proposed GAI performs a bit better than the proposed NSP. This shows that the proposed NSP scheme sacrifices a little SR performance by an obvious computational complexity reduction.

Compared with the case of IRS with single CBS, the SR performance in the case of dual CM stream plus AN (i.e., GAI and NSP scheme) is much better whether in the low-SNR regime or in the high-SNR regime (e.g., by 16.6% higher in the low-SNR regime and 55.6% higher in the high-SNR regime when $M = 30$). This proves the superiority of our proposed schemes in the dual CM stream case due to the diversity gain in LoS channel. Furthermore, even with IRS aided, Alice transmitting single CBS can not achieve better security performance than the case without IRS, unless the IRS equips with more phase-shift elements. This is because the path loss of the IRS-forward link is more serious than the direct link in LoS channel. If there is no more IRS phase-shift elements, IRS may not forward single CBS to the legitimate user more strongly. In this case, it is suggested to transmit dual CBSs or more CM streams with IRS aided, which requires more in-depth researches in the future.

On the other hand, the performance gap between our proposed schemes and other schemes increases as the IRS phase-shift elements M and receive SNR increases, which reveals the superiority of our proposed schemes.

2.5.2 *Impact of the IRS Location*

With fixed positions of Alice, Bob and Eve, the IRS position only depends on the AoD θ_{AI}^{t} and the distance d_{AI} of Alice-to-IRS link. To simplify the analysis, assume that Alice and IRS are on a straight line l_{AI} parallel to the straight line l_{BE} with Bob and Eve. The distances and AoDs of Alice-to-Bob link and Alice-to-Eve link are computed as before, thus θ_{AI}^{t} can be determined as

$$\theta_{AI}^{t} = \theta_{AB}^{t} - \arcsin\left(\frac{d_{AE}}{d_{BE}}\sin\theta_{BAE}\right), \tag{2.80}$$

where $d_{BE} = \sqrt{d_{AB}^2 + d_{AE}^2 - 2d_{AB}d_{AE}\cos\theta_{BAE}}$ and $\theta_{BAE} = \theta_{AE}^{t} - \theta_{AB}^{t}$. The vertical distance d_v of the two lines l_{AI} and l_{BE} can be computed as $d_v = d_{AE}\sin\left(\theta_{AE}^{t} - \theta_{AI}^{t}\right)$. Figure 2.5 shows the location scenario. Define the point S_A is the projection point on l_{BE}, which means $l_{\mathrm{AS}_A} \perp l_{BE}$. Then the distances between S_A and Eve, S_A and Bob can be expressed as $d_{\mathrm{S}_A\mathrm{E}} = \sqrt{d_{AE}^2 - d_v^2}$, $d_{\mathrm{S}_A\mathrm{B}} = \sqrt{d_{AB}^2 - d_v^2}$, respectively. Based on the above conditions, $\theta_{AI}^{t} = 5\pi/18$, the distance of $d_{\mathrm{S}_A\mathrm{E}}$ and $d_{\mathrm{S}_A\mathrm{B}}$ can be calculated as $d_{\mathrm{S}_A\mathrm{E}} = 49.2$ m, $d_{\mathrm{S}_A\mathrm{B}} = 99.6$ m.

Figure 2.6 depicts the SR versus d_{AI} when $M = 80$ as shown in the scenario in (2.5). Here, IRS moves from the position of Alice along the line l_{AI} near Bob. As IRS gets closer to Eve but still far away from Bob, the achievable SR decreases gradually. When IRS is on top of Eve, the minimum SR value is available. In this moment, when IRS is the nearest to Eve, Eve has the strongest eavesdropping ability. As IRS moves away along the line l_{AI} from Eve, it get closer and closer to Bob, the SR value increases up to the largest until IRS is on top of Bob. Furthermore, as IRS moves away along the line l_{AI} Bob, both Eve and Bob get less energy reflected from IRS, thus the SR decreases gradually.

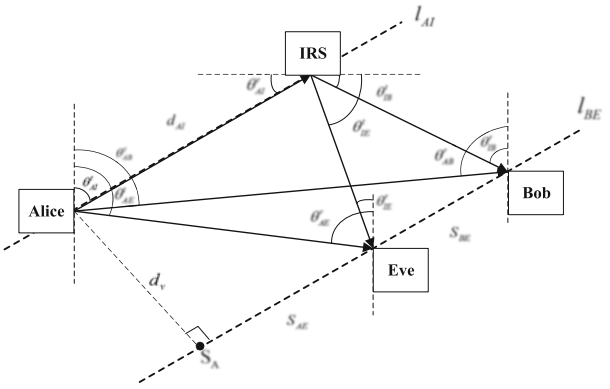


Fig. 2.5 Special scenario for adjusting the position of IRS (l_{AI} is parallel to l_{BE})

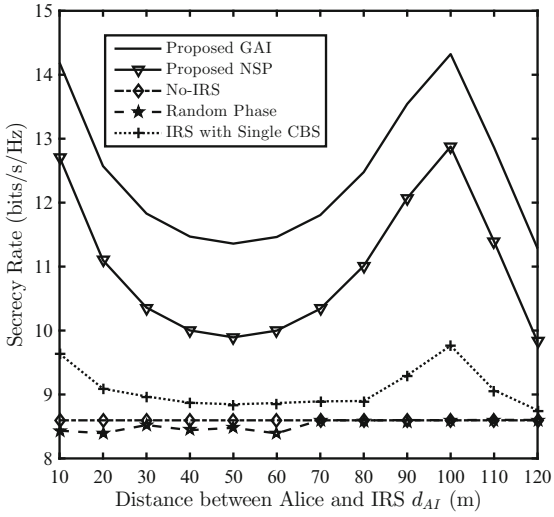


Fig. 2.6 Secrecy rate versus distance between Alice and IRS d_{AI} ($M = 80$)

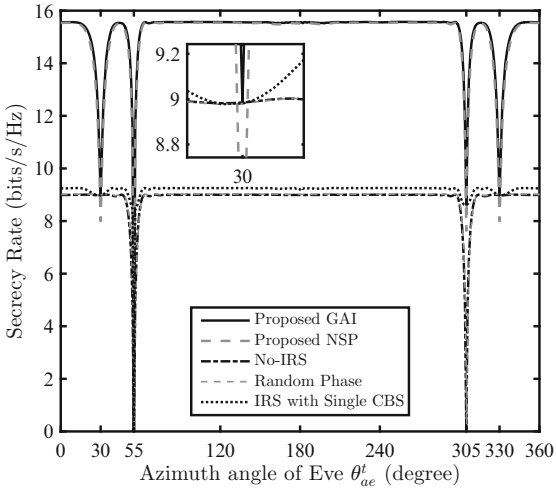


Fig. 2.7 Secrecy rate versus the azimuth angle of Eve θ_{ae}^t when M = 80

Figure 2.7 shows the SR versus the azimuth angle θ_{ae}^t of Eve where θ_{ae}^t changes from 0 to 2π with $M = 80$. Observing this figure, we conclude that once Eve has the same azimuth as that of Bob or IRS, i.e., $\theta_{ae}^t = \theta_{ai}^t$ or $\theta_{ae}^t = \theta_{ab}^t$, SR will degrade rapidly. This means that Eve can eavesdrop a large amount of confidential messages when it locates on one of the two lines of Alice-to-IRS and Alice-to-Bob. In terms of SR, the proposed GAI is much better than the proposed NSP. In other words, the proposed GAI is more robust than the proposed NSP. In particular, for the single CBS case, the SR PL is more serious. Since the transmitter and receiver are both linear arrays, when $\theta_{ae}^t \in (\pi,\ 2\pi)$ and $\theta_{ae}^t \in (0,\ \pi)$ are symmetrical each other.

2.6 Conclusion

In this chapter, we have made an extensive investigation of secure transmit beamforming and phase shifting at IRS in a secure IRS-based DM Networks, where two parallel independent CBSs are transmitted from Alice to Bob with multiple receive antennas. Using the criterion of Max-SR, two alternating iterative algorithms, GAI and NSP, have been proposed. The former is of high-performance and the latter is of low-complexity. From simulation, we find the IRS can make a dramatic enhancement on the SR of DM by using two CBSs compared to single CBS. For example, with the aid of IRS, the proposed two methods can approximately double the SR of existing method with single CBS in the case of medium-scale and large-scale IRS. Additionally, the impact of IRS position on SR is also analyzed in the simulation. It is recommended that the IRS is placed close to the transmitter or the target receiver to achieve a higher SR performance. Moreover, the optimal position of IRS also exists.

References

1. Larsson, E.G., Edfors, O., Tufvesson, F., Marzetta, T.L.: Massive MIMO for next generation wireless systems. IEEE Commun. Mag. **52**(2), 186–195 (2014)
2. Rappaport, T.S., Sun, S., Mayzus, R., Zhao, H., Azar, Y., Wang, K., Wong, G.N., Schulz, J.K., Samimi, M., Gutierrez, F.: Millimeter wave mobile communications for 5G cellular: It will work! IEEE Access **1**(1), 335–349 (2013)
3. Ahmed, I., Khammari, H., Shahid, A., Musa, A., Kim, K.S., DePoorter, E., Moerman, I.: A survey on hybrid beamforming techniques in5G: architecture and system model perspectives. IEEE Commun. Surv. Tutorials **20**(4), 3060–3097 (2018)
4. Khuwaja, A.A., Chen, Y., Zhao, N., Alouini, M., Dobbins, P.: A survey of channel modeling for UAV communications. IEEE Commun. Surv. Tutorials **20**(4), 2804–2821 (2018)
5. Lei, H., Gao, C., Ansari, I.S., Guo, Y., Zou, Y., Pan, G., Qaraqe, K.A.: Secrecy outage performance of transmit antenna selection for MIMO underlay cognitive radio systems over Nakagami-*m* channels. IEEE Trans. Veh. Technol. **66**(3), 2237–2250 (2017)
6. Wang, C., Wang, H.: Physical layer security in millimeter wave cellular networks. IEEE Trans. Wirel. Commun. **15**(8), 5569–5585 (2016)
7. Chen, X., Wang, X., Chen, X.: Energy-efficient optimization for wireless information and power transfer in large-scale MIMO systems employing energy beamforming. IEEE Wirel. Commun. Lett. **2**(6), 667–670 (2013)
8. Zhu, H., Wang, J.: Chunk-based resource allocation in OFDMA systems - Part I: chunk allocation. IEEE Trans. Commun. **57**(9), 2734–2744 (2009)
9. Zhu, H., Wang, J.: Chunk-based resource allocation in OFDMA systems - Part II: joint chunk, power and bit allocation. IEEE Trans. Commun. **60**(2), 499–509 (2012)
10. Li, Q., Zhang, Q., Qin, J.: Secure relay beamforming for SWIPT in amplify-and-forward two-way relay networks. IEEE Trans. Veh. Technol. **65**(11), 9006–9019 (2016)
11. Wu, Q., Li, G.Y., Chen, W., Ng, D.W.K., Schober, R.: An overview of sustainable green 5G networks. IEEE Wirel. Commun. **24**(4), 72–80 (2017)
12. Min, M., Xiao, L., Chen, Y., Cheng, P., Wu, D., Zhuang, W.: Learning-based computation offloading for IoT devices with energy harvesting. IEEE Trans. Veh. Technol. **68**(2), 1930–1941 (2019)
13. Wyner, A.D.: The wire-tap channel. Bell. Syst. Tech. J. **54**(8), 1355–1387 (1975)

14. Yan, S., Yang, N., Land, I., Malaney, R., Yuan, J.: Three artificial-noise-aided secure transmission schemes in wiretap channels. IEEE Trans. Veh. Technol. **67**(4), 3669–3673 (2018)
15. Daly, M.P., Bernhard, J.T.: Directional modulation technique for phased arrays. IEEE Trans. Antennas Propag. **57**(9), 2633–2640 (2009)
16. Cheng, Q., Fusco, V., Zhu, J., Wang, S., Wang, F.: WFRFT-aided power-efficient multi-beam directional modulation schemes based on frequency diverse array. IEEE Trans. Wirel. Commun. **18**(11), 5211–5226 (2019)
17. Qiu, B., Tao, M., Wang, L., Xie, J., Wang, Y.: Multi-beam directional modulation synthesis scheme based on frequency diverse array. IEEE Trans. Inf. Forensics Secur. **14**(10), 2593–2606 (2019)
18. Ding, Y., Fusco, V.F.: A vector approach for the analysis and synthesis of directional modulation transmitters. IEEE Trans. Antennas Propag. **62**(1), 361–370 (2014)
19. Sun, L., Li, J., Zhang, Y., Wang, Y., Gui, L., Li, F., Li, H., Zhuang, Z., Shu, F.: Energy-efficient alternating iterative secure structure of maximizing secrecy rate for directional modulation networks. Phys. Commun. **38**, 100949 (2020)
20. Hu, J., Shu, F., Li, J.: Robust synthesis method for secure directional modulation with imperfect direction angle. IEEE Commun. Lett. **20**(6), 1084–1087 (2016)
21. Shu, F., Xu, L., Wang, J., Zhu, W., Xiaobo, Z.: Artificial-noise-aided secure multicast precoding for directional modulation systems. IEEE Trans. Veh. Technol. **67**(7), 6658–6662 (2018)
22. Shu, F., Qin, Y., Liu, T., Gui, L., Zhang, Y., Li, J., Han, Z.: Low-complexity and high-resolution DOA estimation for hybrid analog and digital massive MIMO receive array. IEEE Trans. Commun. **66**(6), 2487–2501 (2018)
23. Hu, J., Yan, S., Shu, F., Wang, J., Li, J., Zhang, Y.: Artificial-noise-aided secure transmission with directional modulation based on random frequency diverse arrays. IEEE Access **5**(1), 1658–1667 (2017)
24. Shu, F., Wu, X., Hu, J., Li, J., Chen, R., Wang, J.: Secure and precise wireless transmission for random-subcarrier-selection-based directional modulation transmit antenna array. IEEE J. Sel. Areas Commun. **36**(4), 890–904 (2018)
25. Wu, Q., Zhang, R.: Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network. IEEE Commun. Mag. **58**(1), 106–112 (2020)
26. Bereyhi, A., Asaad, S., Müller, R.R., Schaefer, R.F., Poor, H.V.: Secure transmission in IRS-assisted MIMO systems with active eavesdroppers. In: 54th Asilomar Conference on Signals, Systems, and Computers, pp. 718–725 (2020)
27. Yu, X., Xu, D., Sun, Y., Ng, D.W.K., Schober, R.: Robust and secure wireless communications via intelligent reflecting surfaces. IEEE J. Sel. Areas Commun. **38**(11), 2637–2652 (2020)
28. Chu, Z., Hao, W., Xiao, P., Shi, J.: Intelligent reflecting surface aided multi-antenna secure transmission. IEEE Wirel. Commun. Lett. **9**(1), 108–112 (2020)
29. Huang, C., Alexandropoulos, G.C., Zappone, A., Debbah, M., Yuen, C.: Energy efficient multi-user MISO communication using low resolution large intelligent surfaces. In: IEEE Globecom Workshops (GC Wkshps), pp. 1–6 (2018)
30. Huang, C., Zappone, A., Alexandropoulos, G.C., Debbah, M., Yuen, C.: Reconfigurable intelligent surfaces for energy efficiency in wireless communication. IEEE Trans. Wirel. Commun. **18**(8), 4157–4170 (2019)
31. Wu, Q., Zhang, R.: Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming. IEEE Trans. Wirel. Commun. **18**(11), 5394–5409 (2019)
32. Wu, Q., Zhang, R.: Beamforming optimization for wireless network aided by intelligent reflecting surface with discrete phase shifts. IEEE Trans. Commun. **68**(3), 1838–1851 (2020)
33. Zhang, S., Zhang, R.: Capacity characterization for intelligent reflecting surface aided MIMO communication. Available via arXiv. https://arxiv.org/abs/1910.01573
34. Jamali, V., Tulino, A.M., Fischer, G., Müller, R., Schober, R.: Intelligent surface-aided transmitter architectures for millimeter wave ultra massive MIMO systems. IEEE Open J. Commun. Soc. **2**, 144–167 (2020)
35. Zhang, Y., Zhong, C., Zhang, Z., Lu, W.: Sum rate optimization for two way communications with intelligent reflecting surface. IEEE Commun. Lett. **24**(5), 1090–1094 (2020)

36. Alghamdi, R., Alhadrami, R., Alhothali, D., Almorad, H., Faisal, A., Helal, S., Shalabi, R., Asfour, R., Hammad, N., Shams, A., Saeed, N., Dahrouj, H., Al-Naffouri, T.Y., Alouini, M.-S.: Intelligent surfaces for 6g wireless networks: a survey of optimization and performance analysis techniques. IEEE Access **8**(202), 795–202 (2020)
37. Basar, E., Di Renzo, M., De Rosny, J., Debbah, M., Alouini, M.-S., Zhang, R.: Wireless communications through reconfigurable intelligent surfaces. IEEE Access **7**(116), 753–116 (2019)
38. Kishk, M.A., Alouini, M.-S.: Exploiting randomly located blockages for large-scale deployment of intelligent surfaces. IEEE J. Sel. Areas Commun. **39**(4), 1043–1056 (2021)
39. Guo, H., Liang, Y.-C., Chen, J., Larsson, E.G.: Weighted sum-rate maximization for reconfigurable intelligent surface aided wireless networks. IEEE Trans. Wirel. Commun. **19**(5), 3064–3076 (2020)
40. Li, S., Duo, B., Yuan, X., Liang, Y., Di Renzo, M.: Reconfigurable intelligent surface assisted UAV communication: Joint trajectory design and passive beamforming. IEEE Wirel. Commun. Lett. **9**(5), 716–720 (2020)
41. Shi, W., Zhou, X., Jia, L., Wu, Y., Shu, F., Wang, J.: Enhanced secure wireless information and power transfer via intelligent reflecting surface. IEEE Commun. Lett. **25**(4), 1084–1088 (2021)
42. Pan, C., Ren, H., Wang, K., Elkashlan, M., Nallanathan, A., Wang, J.,Hanzo, L.: Intelligent reflecting surface aided MIMO broadcasting for simultaneous wireless information and power transfer. IEEE J. Sel. Areas Commun. **38**(8), 1719–1734 (2020)
43. Shen, K., Yu, W.: Fractional programming for communication systems - Part I: Power control and beamforming. IEEE Trans. Signal Process. **66**(10), 2616–2630 (2018)
44. Cui, M., Zhang, G., Zhang, R.: Secure wireless communication via intelligent reflecting surface. IEEE Wirel. Commun. Lett. **8**(5), 1410–1414 (2019)
45. Shen, H., Xu, W., Gong, S., He, Z., Zhao, C.: Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications. IEEE Commun. Lett. **23**(9), 1488–1492 (2019)
46. Zhou, G., Pan, C., Ren, H., Wang, K., Renzo, M.D., Nallanathan, A.: Robust beamforming design for intelligent reflecting surface aided MISO communication systems. IEEE Wirel. Commun. Lett. **9**(10), 1658–1662 (2020)
47. Zhou, G., Pan, C., Ren, H., Wang, K., Nallanathan, A.: A framework of robust transmission design for IRS-Aided MISO communications with imperfect cascaded channels. IEEE Trans. Signal Process. **68**(1), 5092–5106 (2020)
48. Hong, S., Pan, C., Ren, H., Wang, K., Chai, K.K., Nallanathan, A.: Robust transmission design for intelligent reflecting surface aided secure communication systems with imperfect cascaded CSI. IEEE Trans. Wirel. Commun. **20**(4), 2487–2501 (2021)
49. Guan, X., Wu, Q., Zhang, R.: Intelligent reflecting surface assisted secrecy communication: Is artificial noise helpful or not? IEEE Wirel. Commun. Lett. **9**(6), 778–782 (2020)
50. Dong, L., Wang, H.M.: Enhancing secure MIMO transmission via intelligent reflecting surface. IEEE Trans. Wirel. Commun. **19**(11), 7543–7556 (2020)
51. Dong, L., Wang, H.: Secure MIMO transmission via intelligent reflecting surface. IEEE Wirel. Commun. Lett. **9**(6), 787–790 (2020)
52. Wang, S., Inkol, R., Jackson, B.R.: Relationship between the maximum likelihood emitter location estimators based on received signal strength (RSS) and received signal strength difference (RSSD). In: 26th Biennial Symposium on Communications (QBSC), pp. 64–69 (2012)
53. Boyd, S., Vandenberghe, L.: Convex Optimization. Cambridge University Press, Cambridge (2004)
54. Dinkelbach, W.: On nonlinear fractional programming. Manag. Sci. **13**(7), 492–498 (1967)
55. Song, J., Babu, P., Palomar, D.P.: Optimization methods for designing sequences with low autocorrelation sidelobes. IEEE Trans. Signal Process. **63**(15), 3998–4009 (2015)
56. Pan, C., Ren, H., Wang, K., Xu, W., Elkashlan, M., Nallanathan, A., Hanzo, L.: Multicell MIMO communications relying on intelligent reflecting surfaces. IEEE Trans. Wirel. Commun. **19**(8), 5218–5233 (2020)

Chapter 3
High-Performance Estimation of Jamming Covariance Matrix for IRS-Aided Directional Modulation Network with a Malicious Attacker

In this chapter, we investigate the anti-jamming problem of a DM system with the aid of IRS. As an efficient tool to combat malicious jamming, receive beamforming (RBF) is usually designed by using the statistical properties of the jamming received by Bob. Thus, it is very necessary to estimate the receive jamming covariance matrix (JCM) at Bob. To achieve a precise JCM estimation, three JCM estimation methods, including eigenvalue decomposition (EVD), parametric estimation method by gradient descend (PEM-GD) and parametric estimation method by alternating optimization (PEM-AO), are proposed. Here, the proposed EVD is derived according to the rank-2 constraint of JCM. The PEM-GD method fully explores the structure features of JCM and the PEM-AO is proposed to decrease the computational complexity of the former via dimensionality reduction. The simulation results show that the proposed three methods perform better than directly using sample covariance matrix. Additionally, the proposed PEM-GD and PEM-AO outperform EVD method and the clutter and disturbance covariance estimator Rank-constrained maximum likelihood (RCML).

3.1 Introduction

While wireless communication develops rapidly in recent years, high hardware complexity as well as energy consumption is a critical issue yet [1]. Under such circumstance, the IRS is believed to be a promising new technology, which can smartly reconfigure the wireless propagation environment at lower cost. So far, there has been extensive research on IRS-assisted secure communication, e.g., joint optimization of transmit beamforming and IRS phase shift [2], beamforming design in the case of imperfect CSI [3] or discrete IRS phase shift [4], channel estimation in IRS communication systems [5]. And in [6], the authors investigated the joint optimization problem under time-varying channel conditions based on

F. Shu, J. Wang, *Intelligent Reflecting Surface-Aided Physical-Layer Security*,
Wireless Networks, https://doi.org/10.1007/978-3-031-41812-9_3

recent advances of machine learning. When combining IRS and DM [7, 8], which can send signals directionally and purposely distort the signals in other directions to improve physical layer security (PLS), the communication system can achieve better performance than conventional DM [9, 10], since the assistance of IRS makes it possible for DM to transmit two or more confidential bit streams.

However, most of the aforementioned works focus on avoiding leakage of CM, while the receiver may also be subject to malicious jamming. And since IRS may reflect malicious jamming, as mentioned in [11], the deployment of IRS may also cause harmful interference to wireless communications. The authors in [12–14] resisted interference by configuring the phase shift of the IRS. All these researches deal with the situation with receivers equipped with single antenna, and when receivers are equipped with multiple antennas, RBF is an efficient anti-jamming scheme. The authors in [15] presented scenarios with a FD malicious attacker, and they proposed several RBF methods, which can solve the anti-jamming problem with good performance.

In this book chapter, we consider an IRS-aided DM network with a malicious attacker Mallory, where Alice, Mallory, and Bob are equipped with multiple antennas. Although RBF methods can be extended to this system to eliminate jamming from Mallory, since Mallory is a non-cooperative unit, the estimation of JCM from Mallory to Bob is needed. Thus, three methods are proposed to estimate the JCM from sample covariance matrix (SCM). The main contributions of this book chapter are summarized as follows:

To estimate JCM precisely, minimizing the Euclidean distance between estimated JCM and SCM under different constraints is established as an optimization rule. The rank of ideal JCM is derived to be two, and an EVD method is proposed with a rank-2 constraint. Simulation results show that the proposed EVD method performs better than existing method of directly using the definition of SCM, but it is inferior to RCML in [16]. However, RCML requires the knowledge of receiver noise variance while the proposed EVD can estimate it when this parameter is unknown. Thus, the proposed EVD is more practical.

To achieve a better estimation, we then exploit the structure properties of JCM. By observing the expression of ideal JCM, we extract the unknown parameters, integrate and decompose them to four vectors, and then the estimation problem is converted into a problem of optimizing four unknown vectors, forming the PEM-GD. The JCM estimated by the proposed PEM-GD is independent of the phase changes of IRS. To reduce the complexity of PEM-GD, a dimensionality-reduction method with fewer optimization variables, called PEM-AO, is proposed. Simulation results show that the proposed PEM-GD and PEM-AO have the same normalized mean squared error (NMSE) performance with the latter having lower complexity, and outperform EVD and RCML.

The remainder is organized as follows. Section 3.2 presents the system model and three estimation methods are proposed in Sect. 3.3. In Sect. 3.4, numerical simulations are presented, and Sect. 3.5 draws our conclusion.

Notations In this book chapter, matrices, vectors, and scalars are denoted by uppercase bold, lowercase bold, and lowercase letters, respectively. Signs $(\cdot)^H$, $(\cdot)^T$ $tr(\cdot)$ and $\mathrm{E}[\cdot]$ stand for the conjugate transpose, transpose, trace and expectation operation respectively. $\|\cdot\|_F$ denotes the Frobenius norm of a matrix, and $\Re\{\cdot\}$ represents the real part of a variable.

3.2 System Model

Figure 3.1 shows an IRS-aided DM wireless communication, where Alice equipped with N_A antennas sends CM to Bob with N_B antennas. The transmission is assisted by an IRS with M passive reflecting elements. Mallory with N_M antennas works in FD mode, which means that it can eavesdrop the message and send malicious jamming simultaneously. In such a scenario, the transmit beamforming and phase shift of the IRS are first optimized to prevent eavesdropping, and then with the optimized IRS phase shift, RBF will be used to eliminate jamming after estimating JCM.

The transmitted baseband signal from Alice is

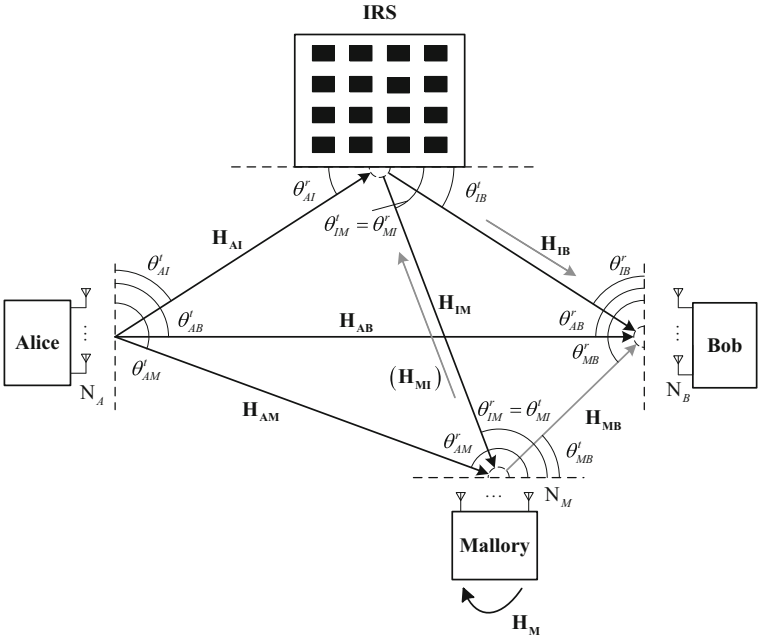


Fig. 3.1 Block diagram of IRS-aided DM network with malicious attacker

$$\mathbf{s}_A = \sqrt{\beta P_A}\mathbf{v}x + \sqrt{(1-\beta)P_A}\mathbf{T}_{A,AN}\mathbf{z}_{A,AN}, \tag{3.1}$$

where P_A denotes the total transmit power and $\beta \in [0,1]$ is the power allocation factor. $\mathbf{v} \in \mathbb{C}^{N_A \times 1}$ and $\mathbf{T}_{A,AN} \in \mathbb{C}^{N_A \times N_A}$ denote the transmit beamforming vector and projection of artificial noise (AN) respectively, with the nature of $\mathbf{v}^H\mathbf{v} = 1$ and $tr(\mathbf{T}_{A,AN}\mathbf{T}_{A,AN}^H) = 1$, and AN is designed in accordance with the null-space projection. x is the transmitted symbol satisfying $\mathrm{E}[|x|^2] = 1$, and $\mathbf{z}_{A,AN} \in \mathbb{C}^{N_A \times 1}$ represents the AN vector with distribution $\mathbf{z}_{A,AN} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_A})$.

The malicious jamming signal from Mallory is

$$\mathbf{s}_M = \sqrt{P_M}\mathbf{T}_{M,AN}\mathbf{z}_{M,AN}, \tag{3.2}$$

where P_M is the transmit power of Mallory, $\mathbf{T}_{M,AN} \in \mathbb{C}^{N_M \times N_J}$ denotes the projection of jamming, $N_J \in [1, N_M - 1]$, and $\mathbf{z}_{M,AN} \sim \mathcal{CN}(\mathbf{0}, \mathbf{I}_{N_J})$ indicates the jamming symbol from Mallory with complex Gaussian distribution.

The received signal at Bob can be written as

$$\begin{aligned}
\mathbf{r}_B = \mathbf{v}_{BR}^H[&(\underbrace{\sqrt{g_{AIB}}\mathbf{H}_{IB}^H\mathbf{\Theta}\mathbf{H}_{AI}^H + \sqrt{g_{AB}}\mathbf{H}_{AB}^H}_{\mathbf{H}_{A1}})\mathbf{s}_A \\
&+ (\underbrace{\sqrt{g_{MIB}}\mathbf{H}_{IB}^H\mathbf{\Theta}\mathbf{H}_{MI}^H + \sqrt{g_{MB}}\mathbf{H}_{MB}^H}_{\mathbf{H}_{M1}})\mathbf{s}_M + \mathbf{n}_B] \\
= \mathbf{v}_{BR}^H[&\sqrt{\beta P_A}\mathbf{H}_{A1}\mathbf{v}x + \sqrt{(1-\beta)P_A}\mathbf{H}_{A1}\mathbf{T}_{A,AN}\mathbf{z}_{A,AN} \\
&+ \underbrace{\sqrt{P_M}\mathbf{H}_{M1}\mathbf{T}_{M,AN}\mathbf{z}_{M,AN}}_{\mathbf{n}_{MB}} + \mathbf{n}_B],
\end{aligned} \tag{3.3}$$

where $\mathbf{v}_{BR} \in \mathbb{C}^{N_B \times 1}$ is the receive beamforming vector of Bob, $\mathbf{n}_B \in \mathbb{C}^{N_B \times 1}$ denotes the complex additive white Gaussian noise (AWGN) vector, following the distribution $\mathbf{n}_B \sim \mathcal{CN}(\mathbf{0}, \sigma_B^2\mathbf{I}_{N_B})$, and $\mathbf{\Theta} = diag\{[e^{j\phi_1}, \ldots, e^{j\phi_i}, \ldots, e^{j\phi_M}]\}$ is a diagonal matrix with ϕ_i symbolizing the phase shift of the i-th element at IRS. g_{AIB}, g_{AB}, g_{MIB}, and g_{MB} denote the path loss coefficients of four path: Alice to Bob through IRS, Alice to Bob, Mallory to Bob through IRS and Mallory to Bob.

Besides, $\mathbf{H}_{IB}^H \in \mathbb{C}^{N_B \times M}$, $\mathbf{H}_{AI}^H \in \mathbb{C}^{M \times N_A}$, $\mathbf{H}_{AB}^H \in \mathbb{C}^{N_B \times N_A}$, $\mathbf{H}_{MI}^H \in \mathbb{C}^{M \times N_M}$, and $\mathbf{H}_{MB}^H \in \mathbb{C}^{N_B \times N_M}$ denote the channel matrices of IRS to Bob, Alice to IRS, Alice to Bob, Mallory to IRS and Mallory to Bob respectively. In DM, transmitter and receiver are deployed with N-element linear antenna arrays with spacing d, the normalized steering vector is

$$\mathbf{h}(\theta) = \frac{1}{\sqrt{N}}\left[e^{j2\pi\Psi_\theta(1)}, \ldots, e^{j2\pi\Psi_\theta(n)}, \ldots, e^{j2\pi\Psi_\theta(N)}\right]^T, \tag{3.4}$$

where $\Psi_\theta(n) = -(n - \frac{N+1}{2})\frac{d\cos\theta}{\lambda}, n = 1 \ldots N$. θ represents the angle of arrival or departure of signal, n is the index of antenna and λ represents the wavelength. Then, the channel can be given by $\mathbf{H}^H(\theta) = \mathbf{h}(\theta_r)\mathbf{h}^H(\theta_t)$, which also indicates that the rank of each channel is 1. In (3.3), for convenience, we set $\mathbf{H}_{A1}$ and $\mathbf{H}_{M1}$ as the equivalent channel matrices of Alice to Bob and Mallory to Bob.

The received JCM at Bob is

$$\begin{aligned}\mathbf{R}_i &= \mathrm{E}\left[\mathbf{n}_{MB}\mathbf{n}_{MB}^H\right] \\ &= P_M(\sqrt{g_{MIB}}\mathbf{H}_{IB}^H\boldsymbol{\Theta}\mathbf{H}_{MI}^H + \sqrt{g_{MB}}\mathbf{H}_{MB}^H)\mathbf{T}_{M,AN}\cdot \\ &\quad \mathbf{T}_{M,AN}^H(\sqrt{g_{MIB}}\mathbf{H}_{IB}^H\boldsymbol{\Theta}\mathbf{H}_{MI}^H + \sqrt{g_{MB}}\mathbf{H}_{MB}^H)^H. \end{aligned} \tag{3.5}$$

Specially, using the matrix inequalities $rank(\mathbf{A}+\mathbf{B}) \leqslant rank(\mathbf{A}) + rank(\mathbf{B})$, and $rank(\mathbf{AB}) \leqslant \min\{rank(\mathbf{A}), rank(\mathbf{B})\}$, it can be derived that $rank(\mathbf{R}_i) \leqslant 2$. In other words, the rank of ideal JCM will not be greater than 2.

To estimate JCM, once Alice detects the jamming signal, or IRS phase shift changes and JCM re-estimation is needed, Alice will keep silent, and then the received signal at Bob is

$$\mathbf{y}_B = \underbrace{\sqrt{P_M}\mathbf{H}_{M1}\mathbf{T}_{M,AN}\mathbf{z}_{M,AN}}_{\mathbf{n}_{MB}} + \mathbf{n}_B. \tag{3.6}$$

After Bob receives K samples, SCM can be directly given by

$$\hat{\mathbf{R}} = \frac{1}{K}\sum_{k=1}^{K}\mathbf{y}_B[k]\mathbf{y}_B^H[k]. \tag{3.7}$$

As K tends to infinity, $\hat{\mathbf{R}} \approx \mathbf{R}_i + \sigma_B^2\mathbf{I}_{N_B}$, which means, when K is large enough, SCM is a valid estimator. However, in the small-sample scenario, it has poor performance. To improve the performance of estimation, the properties of ideal JCM should be used, such as rank-2 or rank-1 channel matrices mentioned above. In the following, the criterion of minimizing the Euclidean distance between SCM minus noise covariance matrix $\mathbf{S} = \hat{\mathbf{R}} - \sigma_B^2\mathbf{I}_{N_B}$ and estimated JCM is cast as

$$\min_{\mathbf{R}} \quad \|\mathbf{R} - \mathbf{S}\|_F, \tag{3.8}$$

which is constrained by the properties of JCM.

To compare the SR performance of JCM estimated by different schemes, we extend NSP-based Max-WFRP RBF method in [15] to our model, which is cast as

$$\max_{\mathbf{v}_{BR}} \quad \mathbf{v}_{BR}^H\mathbf{H}_{A1}\mathbf{v}\mathbf{v}^H\mathbf{H}_{A1}^H\mathbf{v}_{BR} \tag{3.9a}$$

$$\text{s.t.} \quad \mathbf{v}_{BR}^H\mathbf{R} = \mathbf{0}_{1\times N_B}, \mathbf{v}_{BR}^H\mathbf{v}_{BR} = 1. \tag{3.9b}$$

3.3 Proposed Three Estimation Methods

In this section, by exploring the features of ideal JCM, including its rank and composition, three estimation methods named EVD, PEM-GD and PEM-AO are proposed to improve the performance, and their complexities are also compared.

3.3.1 Proposed EVD Method

We first consider the rank constraint of JCM, the ideal JCM can be expanded as

$$\mathbf{R}_i = \lambda_{r1}\mathbf{v}_{r1}\mathbf{v}_{r1}^H + \lambda_{r2}\mathbf{v}_{r2}\mathbf{v}_{r2}^H, \tag{3.10}$$

where $\lambda_{r1}, \lambda_{r2}$ are the eigenvalues of $\mathbf{R}_i$, and $\mathbf{v}_{r1}, \mathbf{v}_{r2}$ are the corresponding eigenvectors. Meanwhile, the covariance matrix of $\mathbf{y}_B$ is given by

$$\mathbf{R}_y = \mathrm{E}[\mathbf{y}_B\mathbf{y}_B^H] = \mathbf{R}_i + \sigma_B^2\mathbf{I}_{N_B}, \tag{3.11}$$

whose eigenvalues have the order $\lambda_{y1} \geq \ldots \geq \lambda_{yN_B}$, and $\mathbf{v}_1, ldots, \mathbf{v}_{N_B}$ are the corresponding eigenvectors. Here, $\lambda_{y1} = \lambda_{r1} + \sigma_B^2, \lambda_{y2} = \lambda_{r2} + \sigma_B^2$, and $\lambda_{y3} = \ldots = \lambda_{yN_B} = \sigma_B^2$ and $\mathbf{v}_1 = \mathbf{v}_{r1}, \mathbf{v}_2 = \mathbf{v}_{r2}$, i.e. $\mathbf{R}_y$ can be rewritten as

$$\mathbf{R}_y = (\lambda_{r1} + \sigma_B^2)\mathbf{v}_1\mathbf{v}_1^H + (\lambda_{r2} + \sigma_B^2)\mathbf{v}_2\mathbf{v}_2^H + \sum_{i=3}^{N_B}\sigma_B^2\mathbf{v}_i\mathbf{v}_i^H. \tag{3.12}$$

Since $\mathbf{R}_y$ and $\hat{\mathbf{R}}$ give the covariance and sample covariance of $\mathbf{y}_B$ respectively, after finding the eigenvalues and eigenvectors of $\hat{\mathbf{R}}$, represented as $\lambda_1 \geq \ldots \geq \lambda_{N_B}$ and $\mathbf{u}_1, \ldots, \mathbf{u}_{N_B}$, the receiver noise variance and JCM are estimated as

$$\hat{\sigma}_B^2 = \frac{\sum_{i=3}^{N_B}\lambda_i}{N_B - 2}, \tag{3.13}$$

and

$$\mathbf{R}_{EVD} = (\lambda_1 - \hat{\sigma}_B^2)\mathbf{u}_1\mathbf{u}_1^H + (\lambda_2 - \hat{\sigma}_B^2)\mathbf{u}_2\mathbf{u}_2^H. \tag{3.14}$$

3.3.2 Proposed PEM-GD Method

Now, we turn to consider the structure of $\mathbf{R}_i$ and propose a method to estimate JCM by its parameters. It can be derived from (3.5) that $\mathbf{R}_i = \mathbf{F}\mathbf{F}^H$, where

$$\begin{aligned}\mathbf{F} &= \sqrt{P_M}(\sqrt{g_{MIB}}\mathbf{H}_{IB}^H\boldsymbol{\Theta}\mathbf{H}_{MI}^H + \sqrt{g_{MB}}\mathbf{H}_{MB}^H)\mathbf{T}_{M,AN} \\ &= \mathbf{H}_{IB}^H\boldsymbol{\Theta}\underbrace{(\sqrt{P_M g_{MIB}}\mathbf{H}_{MI}^H\mathbf{T}_{M,AN})}_{\mathbf{T}_1} + \underbrace{\sqrt{P_M g_{MB}}\mathbf{H}_{MB}^H\mathbf{T}_{M,AN}}_{\mathbf{T}_2},\end{aligned} \tag{3.15}$$

where matrices $\mathbf{T}_1 \in \mathbb{C}^{M\times N_J}$ and $\mathbf{T}_2 \in \mathbb{C}^{N_B\times N_J}$ describe the unknown parameters in $\mathbf{R}_i$. Since both $\mathbf{T}_1$ and $\mathbf{T}_2$ are rank-1 matrices, they can be decomposed into $\mathbf{T}_1 = \boldsymbol{\alpha}\boldsymbol{\beta}^H$, $\mathbf{T}_2 = \boldsymbol{\omega}\boldsymbol{\nu}^H$, where $\boldsymbol{\alpha} \in \mathbb{C}^{M\times 1}$, $\boldsymbol{\omega} \in \mathbb{C}^{N_B\times 1}$, and $\boldsymbol{\beta}, \boldsymbol{\nu} \in \mathbb{C}^{N_J\times 1}$. Then, JCM is constructed as

$$\mathbf{R}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\omega}, \boldsymbol{\nu}) = (\mathbf{H}_{IB}^H\boldsymbol{\Theta}\boldsymbol{\alpha}\boldsymbol{\beta}^H + \boldsymbol{\omega}\boldsymbol{\nu}^H)(\mathbf{H}_{IB}^H\boldsymbol{\Theta}\boldsymbol{\alpha}\boldsymbol{\beta}^H + \boldsymbol{\omega}\boldsymbol{\nu}^H)^H, \tag{3.16}$$

which transforms the optimization problem in (3.8) into

$$\min_{\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\omega},\boldsymbol{\nu}} \quad \|\mathbf{R}(\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\omega}, \boldsymbol{\nu}) - \mathbf{S}\|_F^2. \tag{3.17}$$

It is an unconstrained non-convex optimization problem, then the gradient descend (GD) method is applied to get the unknown parameters in (3.16). The gradients of the objective function with respect to $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$, $\boldsymbol{\omega}$ and $\boldsymbol{\nu}$ are as follows:

$$\nabla_{\boldsymbol{\alpha}^*} = \boldsymbol{\Theta}^H\mathbf{H}_{IB}(\mathbf{R} - \mathbf{S})^H(\mathbf{H}_{IB}^H\boldsymbol{\Theta}\boldsymbol{\alpha}\boldsymbol{\beta}^H + \boldsymbol{\omega}\boldsymbol{\nu}^H)\boldsymbol{\beta}, \tag{3.18a}$$

$$\nabla_{\boldsymbol{\beta}^*} = (\boldsymbol{\nu}\boldsymbol{\omega}^H + \boldsymbol{\beta}\boldsymbol{\alpha}^H\boldsymbol{\Theta}^H\mathbf{H}_{IB})(\mathbf{R} - \mathbf{S})^H\mathbf{H}_{IB}^H\boldsymbol{\Theta}\boldsymbol{\alpha}, \tag{3.18b}$$

$$\nabla_{\boldsymbol{\omega}^*} = (\mathbf{R} - \mathbf{S})^H(\mathbf{H}_{IB}^H\boldsymbol{\Theta}\boldsymbol{\alpha}\boldsymbol{\beta}^H + \boldsymbol{\omega}\boldsymbol{\nu}^H)\boldsymbol{\nu}, \tag{3.18c}$$

$$\nabla_{\boldsymbol{\nu}^*} = (\boldsymbol{\beta}\boldsymbol{\alpha}^H\boldsymbol{\Theta}\mathbf{H}_{IB} + \boldsymbol{\nu}\boldsymbol{\omega}^H)(\mathbf{R} - \mathbf{S})^H\boldsymbol{\omega}. \tag{3.18d}$$

In the above GD algorithm, we first initialize the parameters $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$, $\boldsymbol{\omega}$ and $\boldsymbol{\nu}$, and noting that N_J is unknown in a practical scene, $\boldsymbol{\beta}$ and $\boldsymbol{\nu}$ are initialized to vectors of dimension $\tilde{N}_J$ greater than the surmised number of Mallory's antennas. Next, all parameters are updated as $\mathbf{x}^{(m)} = \mathbf{x}^{(m-1)} - t_{\mathbf{x}}^{(m)}\nabla_{\mathbf{x}^*}^{(m-1)}$ in each iteration until convergence, where $\mathbf{x}$ can be replaced by $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$, $\boldsymbol{\omega}$ and $\boldsymbol{\nu}$. It should be aware that $t_{\mathbf{x}}$ denotes the step of each update, which can be obtained by a backtracking line search in [17], and it guarantees that the objective function declines in each iteration. Thus, the estimated JCM $\mathbf{R}_{PEM-GD}$ can be obtained, and it can adapt to the phases change of IRS since the estimated vectors are independent of $\boldsymbol{\Theta}$.

3.3.3 Proposed PEM-AO Method

However, while backtracking line search and a sufficiently large initial step size in each search make it possible to get a global minimum point for PEM-GD, the GD method of four vectors and backtracking line search cause a large computational

amount. Therefore, below, improving the work in the previous subsection, a low-complexity parametric estimation method is proposed. From (3.16), the JCM can be given by

$$\begin{aligned}\mathbf{R}(\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\omega},\boldsymbol{\nu}) &= \mathbf{H}_{IB}^{H}\boldsymbol{\Theta}\boldsymbol{\alpha}\boldsymbol{\beta}^{H}\boldsymbol{\beta}\boldsymbol{\alpha}^{H}\boldsymbol{\Theta}^{H}\mathbf{H}_{IB} \\ &\quad+\mathbf{H}_{IB}^{H}\boldsymbol{\Theta}\boldsymbol{\alpha}\boldsymbol{\beta}^{H}\boldsymbol{\nu}\boldsymbol{\omega}^{H}+\boldsymbol{\omega}\boldsymbol{\nu}^{H}\boldsymbol{\beta}\boldsymbol{\alpha}^{H}\boldsymbol{\Theta}^{H}\mathbf{H}_{IB}+\boldsymbol{\omega}\boldsymbol{\nu}^{H}\boldsymbol{\nu}\boldsymbol{\omega}^{H}.\end{aligned} \tag{3.19}$$

To reduce unknown optimization variables, let us define three new variables $\boldsymbol{\beta}^{H}\boldsymbol{\beta}=c_1$, $\boldsymbol{\nu}^{H}\boldsymbol{\beta}=c_2$, $\boldsymbol{\nu}^{H}\boldsymbol{\nu}=c_3$, and the association of three newly defined variables can be derived as $c_1c_3cos^2\theta=c_2c_2^*$, where θ is the included angle between $\boldsymbol{\beta}$ and $\boldsymbol{\nu}$. Since $\mathbf{H}_{IB}^{H}=\mathbf{h}(\theta_{IB}^{r})\mathbf{h}^{H}(\theta_{IB}^{t})$, we can set $\boldsymbol{\alpha}^{H}\boldsymbol{\Theta}^{H}\mathbf{h}(\theta_{IB}^{t})=b$, then the estimated JCM turns into

$$\begin{aligned}\mathbf{R}(c_1,c_2,c_3,b,\boldsymbol{\omega}) &= c_1b^{*}b\mathbf{h}(\theta_{IB}^{r})\mathbf{h}^{H}(\theta_{IB}^{r}) \\ &\quad+c_2^{*}b^{*}\mathbf{h}(\theta_{IB}^{r})\boldsymbol{\omega}^{H}+c_2b\boldsymbol{\omega}\mathbf{h}^{H}(\theta_{IB}^{r})+c_3\boldsymbol{\omega}\boldsymbol{\omega}^{H}.\end{aligned} \tag{3.20}$$

And to further reduce the unknown variables, let us define $\tilde{\boldsymbol{\omega}}=\sqrt{c_3}\boldsymbol{\omega}$, $\tilde{c}_1=c_1b^{*}b$, $\tilde{c}_2=\frac{c_2b}{\sqrt{c_3}}$. Thus, the estimated JCM is formed as

$$\begin{aligned}\mathbf{R}(\tilde{c}_1,\tilde{c}_2,\tilde{\boldsymbol{\omega}}) &= \tilde{c}_1\mathbf{h}(\theta_{IB}^{r})\mathbf{h}^{H}(\theta_{IB}^{r})+\tilde{c}_2^{*}\mathbf{h}(\theta_{IB}^{r})\tilde{\boldsymbol{\omega}}^{H} \\ &\quad+\tilde{c}_2\tilde{\boldsymbol{\omega}}\mathbf{h}^{H}(\theta_{IB}^{r})+\tilde{\boldsymbol{\omega}}\tilde{\boldsymbol{\omega}}^{H},\end{aligned} \tag{3.21}$$

where $\tilde{c}_1cos^2\theta=\tilde{c}_2\tilde{c}_2^{*}$. Consequently, the optimization problem is recast as

$$\min_{\tilde{c}_1,\tilde{c}_2,\tilde{\boldsymbol{\omega}}}\ \|\mathbf{R}(\tilde{c}_1,\tilde{c}_2,\tilde{\boldsymbol{\omega}})-\mathbf{S}\|_{\mathbf{F}}^{2}\qquad\text{s.t.}\quad\tilde{c}_1\geq\tilde{c}_2\tilde{c}_2^{*}. \tag{3.22}$$

Noting that it is hard to solve (3.22) directly due to the coupled variables and its non-convex properties, we apply AO algorithm and optimize $(\tilde{c}_1,\tilde{c}_2)$, $\tilde{\boldsymbol{\omega}}$ alternately. First, by fixing $\tilde{\boldsymbol{\omega}}$, the sub-optimization problem of $(\tilde{c}_1,\tilde{c}_2)$ is cast as

$$\min_{\tilde{c}_1,\tilde{c}_2}\quad f(\tilde{c}_1,\tilde{c}_2)\qquad\text{s.t.}\quad\tilde{c}_1\geq\tilde{c}_2\tilde{c}_2^{*}, \tag{3.23}$$

where

$$\begin{aligned}f(\tilde{c}_1,\tilde{c}_2) &= \Re\{\tilde{c}_1^{2}+2(\tilde{c}_2^{*})^{2}a^{2}+4\tilde{c}_1\tilde{c}_2^{*}a+2\tilde{c}_1aa^{*} \\ &\quad+2\tilde{c}_2\tilde{c}_2^{*}e+4\tilde{c}_2^{*}ae-2\tilde{c}_1\tau-4\tilde{c}_2\gamma\},\end{aligned} \tag{3.24}$$

with $\tilde{\boldsymbol{\omega}}^{H}\mathbf{h}(\theta_{IB}^{r})=a$, $\tilde{\boldsymbol{\omega}}^{H}\tilde{\boldsymbol{\omega}}=e$, $\mathbf{h}^{H}(\theta_{IB}^{r})\mathbf{S}\tilde{\boldsymbol{\omega}}=\gamma$, and $\mathbf{h}(\theta_{IB}^{r})\mathbf{S}\mathbf{h}(\theta_{IB}^{r})=\tau$ for brevity.

This sub-optimization problem can be solved by the Karush-Kuhn-Tucker (KKT) conditions. By setting $m = aa^* - e - v/2$, where v is the Lagrange multiplier associated with the inequality constraint, the result of each iteration is

$$\tilde{c}_1 = \tau + \frac{v}{2} - aa^* - \tilde{c}_2^* a - \tilde{c}_2 a^*, \quad \tilde{c}_2 = \frac{(\tau - m)a - \gamma^*}{m}, \tag{3.25}$$

with $v = 0$ for $l_3 \geq 0$, and v being a positive real root of $v^3 + l_1 v^2 + l_2 v + l_3 = 0$ when $l_3 < 0$, where

$$l_1 = 4e + 2\tau - 4aa^*, \tag{3.26a}$$

$$l_2 = 4a^2(a^*)^2 - 8aa^* e - 8aa^*\tau + 4e^2 + 8e\tau, \tag{3.26b}$$

$$l_3 = 8a^2(a^*)^2\tau - 16aa^* e\tau - 8aa^*\tau^2 + 8\gamma a\tau, \tag{3.26c}$$

$$+ 8\gamma^* a^*\tau + 8e^2\tau - 8\gamma\gamma^*. \tag{3.26d}$$

For given $\tilde{c}_1, \tilde{c}_2$, we have to solve a non-convex unconstrained optimization problem about $\tilde{\boldsymbol{\omega}}$. Then we apply GD method as before, and the gradient of the objective function with respect to $\tilde{\boldsymbol{\omega}}$ is as follows,

$$\nabla_{\tilde{\boldsymbol{\omega}}^*} = (\mathbf{R} - \mathbf{S})(\tilde{c}_2^* \mathbf{h}(\theta_{MB}^r) + \tilde{\boldsymbol{\omega}}). \tag{3.27}$$

Finally, by alternately calculating $(\tilde{c}_1, \tilde{c}_2)$ and $\tilde{\boldsymbol{\omega}}$ until convergence, the estimated JCM is obtained as $\mathbf{R}_{PEM-AO}$.

3.3.4 Computational Complexity Analysis and CRLBs

Now, we analyse the complexities of the proposed methods. The complexities of EVD, PEM-GD, and PEM-AO are $O(N_B^3 + 2N_B^2 + 2N_B)$, $O(L_1(2M^2 N_B + MN_B^2 + M\tilde{N}_J N_B + 3M\tilde{N}_J + 3\tilde{N}_J N_B)log_2(1/\kappa))$, and $O(L_2(L_3(N_B^2 + N_B)log_2(1/\kappa) + 3N_B^2 + 2N_B + 25) + 41L_4)$ respectively, where L_1 and L_3 denote the iterative number of GD in PEM-GD and PEM-AO, with $\log_2(1/\kappa)$ the maximum iterative number of backtracking line search, L_2 and L_4 are the numbers of alternating iterations and occurrences of $l_3 < 0$ in PEM-AO. Besides, the complexity of RCML in [16] is $O(N_B^3 + 4N_B^2 + 2)$. Therefore, the complexities of these methods have an decreasing order as PEM-GD, PEM-AO, RCML, and EVD.

Additionally, the CRLBs of JCM is defined as the sum of the Cramer-Rao Lower Bound (CRLB) of each element in JCM to give a lower bound for NMSE. And the CRLBs is directly given by

$$CRLBs = \|\mathbf{R}_i\|_F^{-2} \sum_{j=1}^{N_B} [\mathbf{I}^{-1}(\mathbf{R})]_{jj}, \tag{3.28}$$

with $\mathbf{I}(\mathbf{R})$ denoting the Fisher information matrix.

3.4 Simulation Results and Discussions

In this section, the performance of the proposed estimation methods are compared through numerical simulations. Simulation parameters are set as follows: $\beta = 0.9$, $P_A = P_M = 1W$, $N_A = N_B = N_M = 8$, $M = 16$, $\sigma_B^2 = \sigma_M^2$, $K = 5$, JNR=5dB and Alice, IRS, Bob, Mallory are located at (0,0), (50,50), (500,0), (400, -50) respectively. JNR and SNR represent the ratio of received jamming to noise and signal to noise. The path loss model is given by $g = (\frac{c}{4\pi f d})^2$, where d is the distance between transmitter and receiver. For convenience, we set $(\frac{c}{4\pi f})^2 = 10^{-2}$. In addition, the convergence threshold for PEM-GD and PEM-AO is set as 10^{-20}, and for PEM-GD, $\tilde{N}_J = 3N_B$.

Figure 3.2 shows the CPU time versus N_B of the proposed methods and RCML. It gives a more intuitive form for the complexity comparison of these methods and reveals that the complexity of PEM-GD is much higher than that of EVD and RCML, while the complexity of PEM-AO is between them.

Figure 3.3 depicts the convergence of PEM-GD and PEM-AO, where, specially, since PEM-AO contains two loops, the iteration refers to the innermost iteration for PEM-AO. Obviously, the proposed PEM-GD and PEM-AO converge to approximate constant floor values, but the proposed PEM-AO has a faster convergence rate.

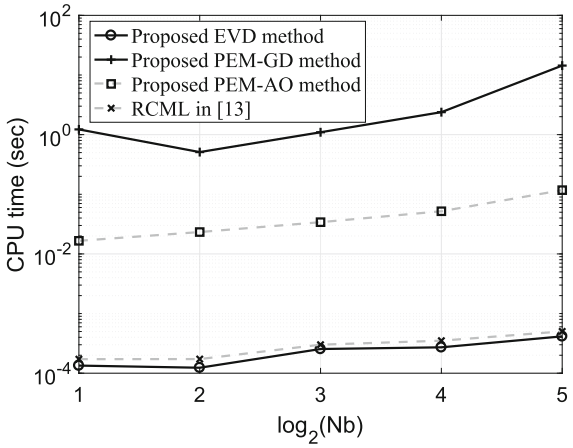


Fig. 3.2 CPU time versus N_B

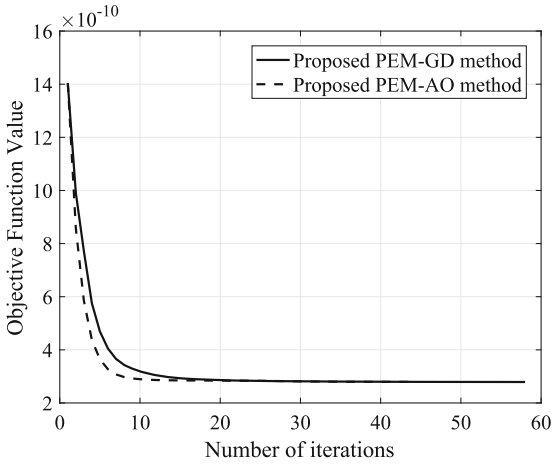


Fig. 3.3 Objective function value versus number of iterations

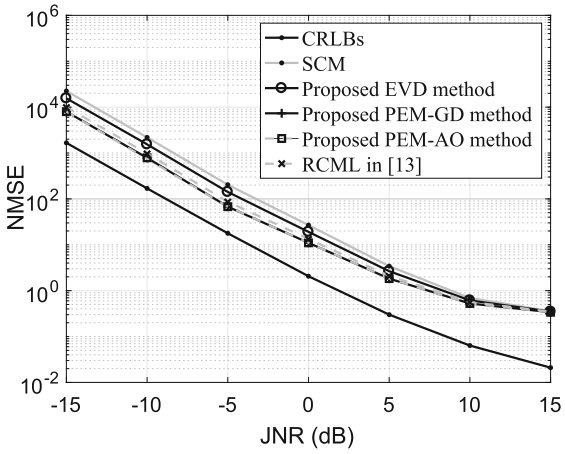


Fig. 3.4 NMSE versus JNR

Figure 3.4 plots the NMSE versus JNR of three proposed methods with CRLBs, SCM and RCML in [16] as benchmarks. It is observed that in the low and medium regions of JNR, the proposed methods make better estimations than SCM while the RCML is better than EVD method but inferior to PEM-GD and PEM-AO. Additionally, as JNR increases, the performance gap between these methods decreases, since estimation difficulty decreases as well.

Figure 3.5 shows the NMSE versus N_B. It is seen that as the dimension of the JCM matrix increases, with the same amount of samples, the performance of all methods deteriorates, since in low training scenarios, the requirements for estimation schemes are more stringent. And as their NMSE gaps are further widened, the advantages of PEM-GD and PEM-AO over other methods will become more significant.

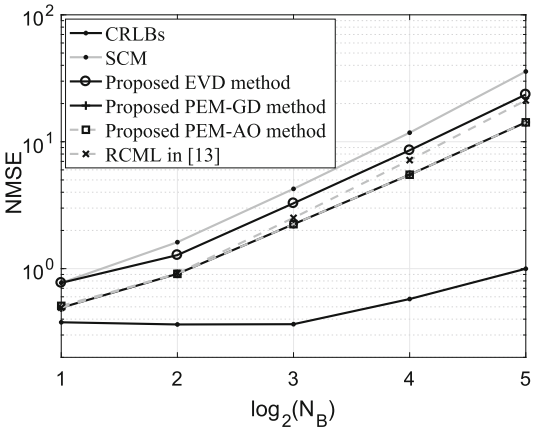


Fig. 3.5 NMSE versus N_B

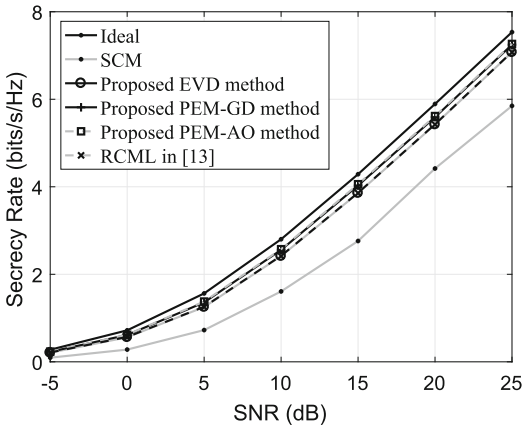


Fig. 3.6 SR versus SNR

Figure 3.6 demonstrates the SR versus SNR with different JCM in RBF, where SNR is increased by adjusting P_A and JNR is fixed. Additionally, in this figure, transmit beamforming and phase shift of IRS are jointly optimized using GAI-based Max-SR method in [10]. The figure shows that using JCM estimated by PEM-AO or PEM-GD achieves higher SR than other estimation methods, and EVD, RCML have approximate performance when applied to RBF. This outcome is consistent with those in Figs. 3.4 and 3.5.

3.5 Conclusion

In this chapter, three methods: EVD, PEM-GD and PEM-AO have been proposed to estimate JCM before employing RBF methods to eliminate the active jamming from Mallory on Bob in an IRS-aided DM network. Simulation results showed that

the three proposed methods perform better than SCM in the low and medium JNR regions in terms of NMSE and SR, while the proposed PEM-GD and PEM-AO outperform RCML and EVD. Specially, EVD can estimate the noise variance of receiver and the JCM estimated by PEM-GD can adapt to the phase shift change of IRS. Among the three proposed methods, the proposed EVD has the lowest complexity and the complexity of PEM-AO is lower than PEM-GD, without loss of performance.

References

1. Wu, Q., Zhang, R.: Towards smart and reconfigurable environment: intelligent reflecting surface aided wireless network. IEEE Commun. Mag. **58**(1), 106–112 (2020)
2. Wu, Q., Zhang, R.: Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming. IEEE Trans. Wirel. Commun. **18**(11), 5394–5409 (2019)
3. Zhou, G., Pan, C., Ren, H., Wang, K., Renzo, M.D., Nallanathan, A.: Robust beamforming design for intelligent reflecting surface aided MISO communication systems. IEEE Wirel. Commun. Lett. **9**(10), 1658–1662 (2020)
4. Wu, Q., Zhang, R.: Beamforming optimization for wireless network aided by intelligent reflecting surface with discrete phase shifts. IEEE Trans. Wirel. Commun. **68**(3), 1838–1851 (2020)
5. Guan, X., Wu, Q., Zhang, R.: Anchor-assisted channel estimation for intelligent reflecting surface aided multiuser communication. IEEE Trans. Wirel. Commun. **21**(6), 3764–3778 (2022)
6. Yang, H., Xiong, Z., Zhao, J., Niyato, D., Xiao, L., Wu, Q.: Deep reinforcement learning-based intelligent reflecting surface for secure wireless communications. IEEE Trans. Wirel. Commun. **20**(1), 375–388 (2021)
7. Daly, M.P., Bernhard, J.T.: Directional modulation technique for phased arrays. IEEE Trans. Antennas Propag. **57**(9), 2633–2640 (2009)
8. Cheng, Q., Fusco, V., Zhu, J., Wang, S., Wang, F.: WFRFT-aided power-efficient multi-beam directional modulation schemes based on frequency diverse array. IEEE Trans. Wireless Commun. **18**(11), 5211–5226 (2019)
9. Lai, L., Hu, J., Chen, Y., Zheng, H., Yang, N.: Directional modulation-enabled secure transmission with intelligent reflecting surface. In: IEEE International Conference on Information Communication and Signal Processing (ICICSP), pp. 450–453 (2020)
10. Shu, F., Teng, Y., Li, J., Huang, M., Shi, W., Li, J., Wu, Y., Wang, J.: Enhanced secrecy rate maximization for directional modulation networks via IRS. IEEE Trans. Commun. **69**(12), 8388–8401 (2021)
11. Lyu, B., Hoang, D.T., Gong, S., Niyato, D., Kim, D.I., IRS-based wireless jamming attacks: When jammers can attack without power. IEEE Wirel. Commun. Lett. **9**(10), 1663–1667 (2020)
12. Yang, H., Xiong, Z., Zhao, J., Niyato, D., Wu, Q., Poor, H.V., Tornatore, M.: Intelligent reflecting surface assisted anti-jamming communications: a fast reinforcement learning approach. IEEE Trans. Wirel. Commun. **20**(3), 1963–1974 (2021)
13. Sun, Y., An, K., Luo, J., Zhu, Y., Zheng, G., Chatzinotas, S.: Intelligent reflecting surface enhanced secure transmission against both jamming and eavesdropping attacks. IEEE Trans. Veh. Technol. **70**(10), 11017–11022 (2021)
14. Tang, X., Wang, D., Zhang, R., Chu, Z., Han, Z.: Jamming mitigation via aerial reconfigurable intelligent surface: passive beamforming and deployment optimization. IEEE Trans. Veh. Technol. **70**(6), 6232–6237 (2021)

15. Teng, Y., Li, J., Liu, L., Xia, G., Zhou, X., Shu, F., Wang, J., You, X.: Low-complexity and high-performance receive beamforming for secure directional modulation networks against an eavesdropping-enabled full-duplex attacker. Sci. China Inform. Sci. **65**(1), 1–2 (2022)
16. Kang, B., Monga, V., Rangaswamy, M.: Rank-constrained maximum likelihood estimation of structured covariance matrices. IEEE Trans. Aerosp. Electron. Syst. **50**(1), 501–515 (2014)
17. Boyd, S., Boyd, S.P., Vandenberghe, L.: Convex Optimization. Cambridge University Press, Cambridge (2004)

Chapter 4
Beamforming and Power Allocation for Double-IRS-Aided Two-Way Directional Modulation Network

To improve the information exchange rate between Alice and Bob in traditional two-way directional modulation (TWDM) network, a new double-IRS-aided TWDM network is proposed in this chapter. To achieve the low-complexity transmitter design, two analytical precoders, one closed-form method of adjusting the IRS phase-shifting matrices, and semi-iterative power allocation (PA) strategy of maximizing secrecy sum rate (SSR) are proposed. First, the geometric parallelogram (GPG) criterion is employed to give the phase-shifting matrices of IRSs. Then, two precoders, called maximizing singular value (Max-SV) and maximizing signal-to-leakage-noise ratio (Max-SLNR), are proposed to enhance the SSR. Evenly, the maximizing SSR PA with hybrid iterative closed-form (HICF) is further proposed to improve the SSR and derived to be one root of a sixth-order polynomial computed by: (1) the Newton-Raphson algorithm is repeated twice to reduce the order of the polynomial from six to four; (2) the remaining four feasible solutions can be directly obtained by the Ferrari's method. Simulation results show that using the proposed Max-SV and Max-SLNR, the proposed GPG makes a significant SSR improvement over random phase and no IRS. Given GPG, the proposed Max-SV outperforms the proposed leakage for small-scale or medium-scale IRS. Particularly, the proposed HICF PA strategy shows about 10% performance gain over equal PA.

4.1 Introduction

DM, as a key method of physical layer security (PLS), is attracting much attention from academia and industry due to its future great promising applications in civil and military [1–12]. Its basic idea is as follows: in line-of-propagation channel, transmit beamforming and AN are two main ways to improve the secure performance. The former uses the beamforming vector to enhance the confidential

F. Shu, J. Wang, *Intelligent Reflecting Surface-Aided Physical-Layer Security*,
Wireless Networks, https://doi.org/10.1007/978-3-031-41812-9_4

message along the desired direction while the latter is projected along the undesired direction to severely degrade the performance at Eve.

In [13], the authors proposed a dual-beam DM scheme, in which the in-phase and quadrature baseband signals were used to excite two different antennas. In [14], a general PA strategy of maximizing secrecy rate (Max-SR), given the NSP beamforming method, was proposed for secure DM network. In [15], the authors considered a scenario for DM network with a FD malicious attacker, where three high-performance receive beamforming methods were proposed to alleviate the impact of the jamming signal on the desired user. In DM, the beamforming vector and AN projection matrix are intimately related to the desired and undesired directions, Alice should behave as a receiver to make DOA measurements before performing a beamforming operation. In [16], to achieve low-complexity and high-resolution DOA estimation for practical DM, a fast root multiple signal classification hybrid analog-digital (HAD) phase alignment method of DOA in hybrid MIMO structure were proposed. In [17], using the probability density function of measured DOA of a desired user, an AN-aided robust HAD plus DM transmitter was presented, and a robust and secure physical-layer transmission was achieved. In fact, for DM, the direction angle is not always perfect, for the imperfect direction angle, a low-complexity robust synthesis method for secure DM was proposed to make an one-order improvement on bit error ate performance compared to non-robust ones in [18].

To address the secure risk of DM that Eve moves to the desired main-beam from Alice to Bob and may eavesdrop the CM due to its property of only depending on angle dimension, in [19], a random frequency diverse array (FDA)-based DM scheme of randomly allocating frequencies to transmit antennas was proposed to implement a two-dimensional secure transmission of depending on both angle and range. In [20], combining the orthogonal frequency division multiplexing and DM, a new secure precise wireless transmission concept was proposed to make it easy to implement in practice by replacing random frequency diverse with random subcarrier selection. A FDA-based DM aided by AN was proposed in [21], the AN projection matrix was calculated to minimize the effect of AN on legitimate user in the cases of known and unknown Eve locations. In [22], a single-point AN-aided FDA DM scheme was proposed, where the FDA was analyzed in three-dimensional (i.e., range, azimuth angle, and elevation angle). Compared with the conventional zero-forcing and singular value decomposition methods, this method reduced the memory consumption significantly.

With the rapid development of wireless networks, there is a strong demand for a wireless network with lower implementation cost and energy consumption. IRS, consisting of a large number of small and low-cost reconfigurable passive elements, will meet this demand [23–25]. Actually, IRS is a passive forwarding device, which is viewed as a low-cost and low-energy-consumption reflecting relay. An IRS-aided SWIPT for MISO system was presented in [26] to maximize the harvested energy by jointly optimizing the transmit beamforming and IRS phase shift. In [27], an IRS-aided FD communication system was established to maximize the sum rate of two-way transmissions. Compared with the Arimoto-Blahut method, this

method achieved a faster convergence rate and lower computational complexity. An IRS-aided decode-and-forward (DF) relay network system was investigated with multiple antennas at relay station in [28], three maximizing receive power methods were proposed to achieve a high rate. In a double-IRS-aided multi-user system [29], the maximizing the minimum signal-to-interference-plus-noise ratio of all users was proposed to jointly optimize the (active) receiving beamforming of the base station and (passive) cooperative reflection beamforming of the two distributed IRSs. A double-IRS-assisted wireless system was proposed in [30], using the particle swarm optimization algorithm, the transmit and passive beamforming vectors on the two IRSs were cooperatively optimized to maximize the received signal power.

To explore the security of IRS-assisted wireless system, in [31], the authors analyzed whether AN is helpful to enhance PLS, and identified the most beneficial practical scenario for using AN. In [32], the authors investigated the improved security of an IRS-assisted MISO system, the oblique manifold and Majorization-Minimization algorithms were proposed to jointly optimize the transmit beamforming at transmitter and phase shifts at IRS. In [33], the IRS was used to enhance the security performance in MIMO system in order to maximize SR. Here, the block coordinate descent algorithm was proposed to alternately update the transmit precoding, AN covariance, and IRS phase shifting matrix. An IRS-aided secure spatial modulation system was presented in [34], and three IRS beamforming methods and two transmit power design methods were proposed to improve the SR. A robust transmission design for an IRS-aided secure system in the presence of transceiver hardware impairments was investigated in [35], and an alternate optimization method was proposed to maximize the SR.

To enhance the energy efficiency and overcome the limitation of only one confidential signal being transmitted to legitimate user in the traditional DM network, in [36], with the help of an IRS, the DM system has implemented two parallel independent CBS transmission from Alice to Bob, where the GAI algorithm and low-complexity NSP algorithm were proposed to maximize the SR. They showed that the proposed two-stream transmission approximately doubles the SR of conventional DM system in terms of SR. In [37], an IRS-aided DM with AN scheme was proposed to achieve an enhanced secure single-stream transmission, and its closed-form expression for SR was derived. Although two CBSs in [36] were independently and concurrently transmitted from Alice to Bob with the aid of IRS, only one-way information was sent from Alice to Bob. In this chapter, we propose a completely distinct new network, i.e., a new kind of two-way DM network aided by IRS. In other words, Alice and Bob exchange their messages each other via two IRSs at the same time, which will be shown to significantly improve the SR of the traditional two-way DM network without IRSs in this book chapter.

In this book chapter, to enhance the SSR performance and energy efficiency in the traditional DM networks, a double-IRS-aided two-way DM system is established. Here, both Alice and Bob work in FD mode, and friendly multipaths between Alice and Bob are created and controlled by the two IRSs. To maximize the SSR of this system, the phase-shifting matrices of two IRSs are firstly designed and optimized by using the GPG criterion, i.e., each IRS phase-shifting matrix is chosen to be

negative to the phase part of a synthesis vector of two channel vectors independently reflected from IRS to Alice and Bob. In the simulation, it is verified compared to random phase method, the proposed GPG method can make a substantial SSR enhancement.

Given that IRS phase-shifting matrix has been designed by GPG strategy, one transmit beamforming scheme, called Max-SV, is proposed. Here, the right singular corresponding the maximum singular-value is used as the beamforming vector of the CM while the AN beamforming vector is designed on the null-space of the remaining singular vectors. Additionally, the Max-SLNR is generalized to the double-IRS-aided two-way DM network. At Eve, a ZF-based maximum ratio combining (MRC) method is proposed to achieve a high-performance receive beamforming. Simulation results show that the proposed Max-SV and generalized leakage methods outperform random phase and no IRS in terms of SSR.

To further improve SSR, a PA strategy of maximizing SSR is proposed, which is addressed by the HICF algorithm. Here, the optimal PA factor is shown to be one root of a sixth-order polynomial. The HICF method consists of two steps: In the first step, the Newton-Raphson algorithm is repeated twice to obtain two candidate roots and reduce the order of the polynomial from six to four, and the remaining four feasible solutions can be obtained by the Ferrari's method; secondly, the optimal root is obtained by maximizing the SSR over the set of six candidate roots and boundary points. Moreover, the two-dimensional exhaustive search (2D-ES) algorithm is presented as a performance benchmark. Simulation results show that the proposed HICF achieves about a 10% performance gain over equal PA (EPA).

The remainder of this chapter is organized as follows. Section 4.2 describes the system model and problem formulation of the double-IRS-aided two-way DM network. In Sect. 4.3, two transmit beamforming methods are presented. One PA scheme for maximizing SSR is given in Sect. 4.4. Numerical simulation results are presented in Sect. 4.5. Finally, we draw our conclusions in Sect. 4.6.

Notations throughout this chapter, boldface lower case and upper case letters represent vectors and matrices, respectively. Signs $(\cdot)^T$, $(\cdot)^*$, $(\cdot)^H$, $(\cdot)^{-1}$, $(\cdot)^\dagger$, $\mathrm{tr}(\cdot)$, and $\|\cdot\|$ denote the transpose operation, conjugate operation, conjugate transpose operation, inverse operation, pseudo inverse operation, trace operation, and 2-norm operation, respectively. The symbol $\mathbb{C}^{N\times N}$ is the space of $N \times N$ complex-valued matrix. The notation $\mathbf{I}_N$ is the $N \times N$ identity matrix. The sign $\mathbb{E}\{\cdot\}$ represents the expectation operation.

4.2 System Model and Problem Formulation

As shown in Fig. 4.1, a double-IRS-aided two-way DM system is considered, where Alice is equipped with N_a antennas, Bob is equipped with N_b antennas, and an eavesdropper (Eve) is equipped with N_e antennas, both of IRS-1 and IRS-2 are

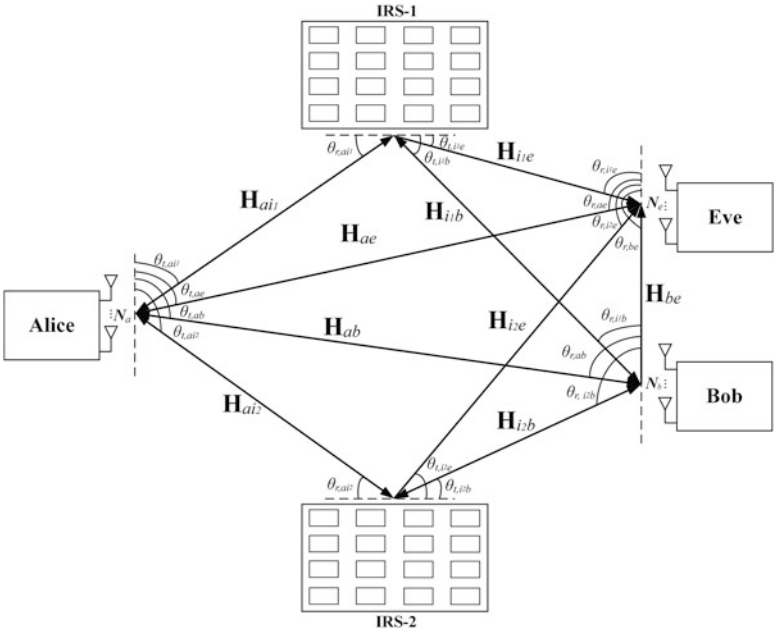


Fig. 4.1 System model diagram for double-IRS-aided two-way DM network

equipped with M low-cost passive reflecting elements. The IRS reflects signal only one time slot. Both of Alice and Bob work in FD model. For convenience of analysis and derivation below, it is assumed the self-interference is completely removed by the transmitters at Alice and Bob. The channels from Alice to IRS-1, Alice to IRS-2, Alice to Eve, Alice to Bob, IRS-1 to Eve, IRS-2 to Eve, Bob to Eve, IRS-1 to Bob, and IRS-2 to Bob are the line-of-propagation channels.

The transmit signal from Alice is

$$\mathbf{S}_a = \sqrt{\beta_1 P_a}\mathbf{v}_{at}x_1 + \sqrt{(1-\beta_1)P_a}\mathbf{w}_a, \tag{4.1}$$

where P_a denotes the total transmit power, β_1 and $(1-\beta_1)$ represent the PA parameters of CM and AN, respectively. $\mathbf{v}_{at} \in \mathbb{C}^{N_a \times 1}$ is the transmit beamforming vector of CM, and $\mathbf{w}_a \in \mathbb{C}^{N_a \times 1}$ denotes the beamforming vector for transmitting AN, where $\mathbf{v}_{at}^H \mathbf{v}_{at} = 1$, and $\mathbf{w}_a^H \mathbf{w}_a = 1$. x_1 is the CM with $\mathbb{E}[\|x_1\|^2] = 1$.

The transmit signal from Bob is given by

$$\mathbf{S}_b = \sqrt{\beta_2 P_b}\mathbf{v}_{bt}x_2 + \sqrt{(1-\beta_2)P_b}\mathbf{w}_b, \tag{4.2}$$

where P_b represents the total transmit power, β_2 and $(1-\beta_2)$ are the PA factors of CM and AN, respectively. $\mathbf{v}_{bt} \in \mathbb{C}^{N_b \times 1}$ is the transmit beamforming vector that

sends CM, and $\mathbf{w}_b \in \mathbb{C}^{N_b \times 1}$ denotes the AN beamforming vector, where $\mathbf{v}_{bt}^H \mathbf{v}_{bt} = 1$, and $\mathbf{w}_b^H \mathbf{w}_b = 1$. x_2 represents the CM with $\mathbb{E}[\|x_2\|^2] = 1$.

Taking the path loss into account, the received signal at Bob is

$$\begin{aligned} y_b &= \mathbf{v}_{br}^H \Big(\big(\sqrt{g_{ai_1b}} \mathbf{H}_{i_1b}^H \boldsymbol{\Theta}_1 \mathbf{H}_{ai_1} + \sqrt{g_{ai_2b}} \mathbf{H}_{i_2b}^H \boldsymbol{\Theta}_2 \mathbf{H}_{ai_2} + \sqrt{g_{ab}} \mathbf{H}_{ab}^H \big) \mathbf{S}_a \\ &\quad + \big(\sqrt{g_{bi_1b}} \mathbf{H}_{i_1b}^H \boldsymbol{\Theta}_1 \mathbf{H}_{bi_1} + \sqrt{g_{bi_2b}} \mathbf{H}_{i_2b}^H \boldsymbol{\Theta}_2 \mathbf{H}_{bi_2} \big) \mathbf{v}_{bt} x_2 + \mathbf{n}_b \Big) \\ &= \mathbf{v}_{br}^H \Big(\sqrt{\beta_1 P_a} \mathbf{H}_b(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2) \mathbf{v}_{at} x_1 + \big(\sqrt{g_{bi_1b}} \mathbf{H}_{i_1b}^H \boldsymbol{\Theta}_1 \mathbf{H}_{bi_1} \\ &\quad + \sqrt{g_{bi_2b}} \mathbf{H}_{i_2b}^H \boldsymbol{\Theta}_2 \mathbf{H}_{bi_2} \big) \mathbf{v}_{bt} x_2 + \sqrt{(1-\beta_1) P_a} \mathbf{H}_b(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2) \mathbf{w}_a + \mathbf{n}_b \Big), \end{aligned} \tag{4.3}$$

where $\boldsymbol{\Theta}_1$=diag$(e^{j\phi_1^1}, \cdots, e^{j\phi_m^1}, \cdots, e^{j\phi_M^1})$ and $\boldsymbol{\Theta}_2$=diag$(e^{j\phi_1^2}, \cdots, e^{j\phi_m^2}, \cdots, e^{j\phi_M^2})$ are the reflection-coefficient matrices of IRS-1 and IRS-2, respectively, where $\phi_m^1, \phi_m^2 \in [0, 2\pi]$ represent the phase shifts of m-th reflection element. $\mathbf{v}_{br}^H \in \mathbb{C}^{1 \times N_b}$ is the receive beamforming vector. $\mathbf{n}_b \in \mathbb{C}^{N_b \times 1}$ is the complex AWGN vector with its distribution as $\mathbf{n}_b \sim \mathcal{CN}(0, \sigma_b^2 \mathbf{I}_{N_b})$. $g_{ai_1b} = g_{ai_1} g_{i_1b}$, $g_{ai_2b} = g_{ai_2} g_{i_2b}$, $g_{bi_1b} = g_{bi_1} g_{i_1b}$ and $g_{bi_2b} = g_{bi_2} g_{i_2b}$ represent the equivalent path loss coefficients of Alice-IRS-1-Bob, Alice-IRS-2-Bob, Bob-IRS-1-Bob and Bob-IRS-2-Bob channels, respectively. g_{ab} denotes the path loss coefficient of Alice-to-Bob channel. In (4.3),

$$\mathbf{H}_b(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2) = \sqrt{g_{ai_1b}} \mathbf{H}_{i_1b}^H \boldsymbol{\Theta}_1 \mathbf{H}_{ai_1} + \sqrt{g_{ai_2b}} \mathbf{H}_{i_2b}^H \boldsymbol{\Theta}_2 \mathbf{H}_{ai_2} + \sqrt{g_{ab}} \mathbf{H}_{ab}^H, \tag{4.4}$$

where the channel matrices $\mathbf{H}_{ai_1} = \mathbf{h}(\theta_{r,ai_1}) \mathbf{h}^H(\theta_{t,ai_1}) \in \mathbb{C}^{M \times N_a}$, $\mathbf{H}_{i_1b}^H = \mathbf{h}(\theta_{r,i_1b}) \mathbf{h}^H(\theta_{t,i_1b}) \in \mathbb{C}^{N_b \times M}$, $\mathbf{H}_{ai_2} = \mathbf{h}(\theta_{r,ai_2}) \mathbf{h}^H(\theta_{t,ai_2}) \in \mathbb{C}^{M \times N_a}$, $\mathbf{H}_{i_2b}^H = \mathbf{h}(\theta_{r,i_2b}) \mathbf{h}^H(\theta_{t,i_2b}) \in \mathbb{C}^{N_b \times M}$, $\mathbf{H}_{ab}^H = \mathbf{h}(\theta_{r,ab}) \mathbf{h}^H(\theta_{t,ab}) \in \mathbb{C}^{N_b \times N_a}$, $\mathbf{H}_{bi_1} = \mathbf{h}(\theta_{r,bi_1}) \mathbf{h}^H(\theta_{t,bi_1}) \in \mathbb{C}^{M \times N_b}$, and $\mathbf{H}_{bi_2} = \mathbf{h}(\theta_{r,bi_2}) \mathbf{h}^H(\theta_{t,bi_2}) \in \mathbb{C}^{M \times N_b}$ are the Alice-to-IRS-1, IRS-1-to-Bob, Alice-to-IRS-2, IRS-2-to-Bob, Alice-to-Bob, Bob-to-IRS-1, and Bob-to-IRS-2 channels, respectively. The normalized steering vector $\mathbf{h}(\theta)$ is

$$\mathbf{h}(\theta) = \frac{1}{\sqrt{N}} [e^{j2\pi \Psi_\theta(1)}, \ldots, e^{j2\pi \Psi_\theta(n)}, \ldots, e^{j2\pi \Psi_\theta(N)}]^T, \tag{4.5}$$

and the phase function $\Psi_\theta(n)$ is given by

$$\Psi_\theta(n) \triangleq -\frac{(n - (N+1)/2) d \cos\theta}{\lambda}, n = 1, \ldots, N, \tag{4.6}$$

where θ represents the direction angle of arrival or departure, n denotes the index of antenna, d is the spacing of adjacent transmitting antennas, and λ stands for the

wavelength. Then (4.4) can be rewritten as

$$\begin{aligned}\mathbf{H}_b(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2) = &\sqrt{g_{ai_1b}}\mathbf{h}(\theta_{r,i_1b})\mathbf{h}^H(\theta_{t,i_1b})\boldsymbol{\Theta}_1\mathbf{h}(\theta_{r,ai_1})\mathbf{h}^H(\theta_{t,ai_1}) \\ &+ \sqrt{g_{ai_2b}}\mathbf{h}(\theta_{r,i_2b})\mathbf{h}^H(\theta_{t,i_2b})\boldsymbol{\Theta}_2\mathbf{h}(\theta_{r,ai_2})\mathbf{h}^H(\theta_{t,ai_2}) \\ &+ \sqrt{g_{ab}}\mathbf{h}(\theta_{r,ab})\mathbf{h}^H(\theta_{t,ab}).\end{aligned} \tag{4.7}$$

Assuming that the CSI of each link is perfectly known by Bob, similar to [27], the term in (4.3)

$$\mathbf{v}_{br}^H\left(\sqrt{g_{bi_1b}}\mathbf{H}_{i_1b}^H\boldsymbol{\Theta}_1\mathbf{H}_{bi_1} + \sqrt{g_{bi_2b}}\mathbf{H}_{i_2b}^H\boldsymbol{\Theta}_2\mathbf{H}_{bi_2}\right)\mathbf{v}_{bt}x_2$$

can be removed from the received signal y_b due to the fact that Bob knows its own data symbol x_2. Then the received signal (4.3) reduces to

$$y_b = \mathbf{v}_{br}^H\Big(\sqrt{\beta_1 P_a}\mathbf{H}_b(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2)\mathbf{v}_{at}x_1 + \underbrace{\sqrt{(1-\beta_1)P_a}\mathbf{H}_b(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2)\mathbf{w}_a + \mathbf{n}_b}_{\tilde{\mathbf{n}}_b}\Big). \tag{4.8}$$

Similar to the received signal at Bob, Alice knows its own data symbol x_1. Then the received signal at Alice is given by

$$\begin{aligned}y_a &= \mathbf{v}_{ar}^H\Big(\big(\sqrt{g_{ai_1b}}\mathbf{H}_{i_1a}^H\boldsymbol{\Theta}_1\mathbf{H}_{bi_1} + \sqrt{g_{ai_2b}}\mathbf{H}_{i_2a}^H\boldsymbol{\Theta}_2\mathbf{H}_{bi_2} + \sqrt{g_{ab}}\mathbf{H}_{ba}^H\big)\mathbf{S}_b + \mathbf{n}_a\Big) \\ &= \mathbf{v}_{ar}^H\Big(\sqrt{\beta_2 P_b}\mathbf{H}_a(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2)\mathbf{v}_{bt}x_2 + \underbrace{\sqrt{(1-\beta_2)P_b}\mathbf{H}_a(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2)\mathbf{w}_b + \mathbf{n}_a}_{\tilde{\mathbf{n}}_a}\Big)\end{aligned} \tag{4.9}$$

where

$$\mathbf{H}_a(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2) = \sqrt{g_{ai_1b}}\mathbf{H}_{i_1a}^H\boldsymbol{\Theta}_1\mathbf{H}_{bi_1} + \sqrt{g_{ai_2b}}\mathbf{H}_{i_2a}^H\boldsymbol{\Theta}_2\mathbf{H}_{bi_2} + \sqrt{g_{ab}}\mathbf{H}_{ba}^H, \tag{4.10}$$

$\mathbf{v}_{ar}^H \in \mathbb{C}^{1\times N_a}$ denotes the receive beamforming vector, $\mathbf{n}_a \in \mathbb{C}^{N_a\times 1}$ is the complex AWGN vector, distributed as $\mathbf{n}_a \sim \mathcal{CN}(0, \sigma_a^2\mathbf{I}_{N_a})$, the channel matrices $\mathbf{H}_{i_1a}^H = \mathbf{h}(\theta_{r,i_1a})\mathbf{h}^H(\theta_{t,i_1a}) \in \mathbb{C}^{N_a\times M}$, $\mathbf{H}_{i_2a}^H = \mathbf{h}(\theta_{r,i_2a})\mathbf{h}^H(\theta_{t,i_2a}) \in \mathbb{C}^{N_a\times M}$, and $\mathbf{H}_{ba}^H = \mathbf{h}(\theta_{r,ba})\mathbf{h}^H(\theta_{t,ba}) \in \mathbb{C}^{N_a\times N_b}$ represent the IRS-1-to-Alice, IRS-2-to-Alice, and Bob-to-Alice channels, respectively. Then (4.10) becomes as

$$\begin{aligned}\mathbf{H}_a(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2) = &\sqrt{g_{ai_1b}}\mathbf{h}(\theta_{r,i_1a})\mathbf{h}^H(\theta_{t,i_1a})\boldsymbol{\Theta}_1\mathbf{h}(\theta_{r,bi_1})\mathbf{h}^H(\theta_{t,bi_1}) \\ &+ \sqrt{g_{ai_2b}}\mathbf{h}(\theta_{r,i_2a})\mathbf{h}^H(\theta_{t,i_2a})\boldsymbol{\Theta}_2\mathbf{h}(\theta_{r,bi_2})\mathbf{h}^H(\theta_{t,bi_2}) \\ &+ \sqrt{g_{ab}}\mathbf{h}(\theta_{r,ba})\mathbf{h}^H(\theta_{t,ba}).\end{aligned} \tag{4.11}$$

The receive signal at Eve can be expressed as

$$\begin{aligned} y_e &= \mathbf{v}_{er}^H \Big(\big(\sqrt{g_{ai_1e}} \mathbf{H}_{i_1e}^H \boldsymbol{\Theta}_1 \mathbf{H}_{ai_1} + \sqrt{g_{ai_2e}} \mathbf{H}_{i_2e}^H \boldsymbol{\Theta}_2 \mathbf{H}_{ai_2} + \sqrt{g_{ae}} \mathbf{H}_{ae}^H \big) \mathbf{S}_a \\ &\quad + \big(\sqrt{g_{bi_1e}} \mathbf{H}_{i_1e}^H \boldsymbol{\Theta}_1 \mathbf{H}_{bi_1} + \sqrt{g_{bi_2e}} \mathbf{H}_{i_2e}^H \boldsymbol{\Theta}_2 \mathbf{H}_{bi_2} + \sqrt{g_{be}} \mathbf{H}_{be}^H \big) \mathbf{S}_b + \mathbf{n}_e \Big) \\ &= \mathbf{v}_{er}^H \Big(\sqrt{\beta_1 P_a} \mathbf{H}_{e_1}(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2) \mathbf{v}_{at} x_1 + \sqrt{\beta_2 P_b} \mathbf{H}_{e_2}(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2) \mathbf{v}_{bt} x_2 \\ &\quad + \sqrt{(1-\beta_1) P_a} \mathbf{H}_{e_1}(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2) \mathbf{w}_a + \sqrt{(1-\beta_2) P_b} \mathbf{H}_{e_2}(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2) \mathbf{w}_b + \mathbf{n}_e \Big) \\ &= \mathbf{v}_{er}^H \Big(\sqrt{\beta_1 P_a} \mathbf{H}_{e_1}(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2) \mathbf{v}_{at} x_1 + \sqrt{\beta_2 P_b} \mathbf{H}_{e_2}(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2) \mathbf{v}_{bt} x_2 + \bar{\mathbf{n}}_e \Big), \end{aligned} \tag{4.12}$$

where

$$\mathbf{H}_{e_1}(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2) = \sqrt{g_{ai_1e}} \mathbf{H}_{i_1e}^H \boldsymbol{\Theta}_1 \mathbf{H}_{ai_1} + \sqrt{g_{ai_2e}} \mathbf{H}_{i_2e}^H \boldsymbol{\Theta}_2 \mathbf{H}_{ai_2} + \sqrt{g_{ae}} \mathbf{H}_{ae}^H, \tag{4.13}$$

$$\mathbf{H}_{e_2}(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2) = \sqrt{g_{bi_1e}} \mathbf{H}_{i_1e}^H \boldsymbol{\Theta}_1 \mathbf{H}_{bi_1} + \sqrt{g_{bi_2e}} \mathbf{H}_{i_2e}^H \boldsymbol{\Theta}_2 \mathbf{H}_{bi_2} + \sqrt{g_{be}} \mathbf{H}_{be}^H, \tag{4.14}$$

$$\bar{\mathbf{n}}_e = \sqrt{(1-\beta_1) P_a} \mathbf{H}_{e_1}(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2) \mathbf{w}_a + \sqrt{(1-\beta_2) P_b} \mathbf{H}_{e_2}(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2) \mathbf{w}_b + \mathbf{n}_e, \tag{4.15}$$

$\mathbf{v}_{er}^H \in \mathbb{C}^{1 \times N_e}$ denotes the receive beamforming vector, $\mathbf{n}_e \in \mathbb{C}^{N_e \times 1}$ represents the AWGN vector, distributed as $\mathbf{n}_e \sim \mathcal{CN}(0, \sigma_e^2 \mathbf{I}_{N_e})$. $g_{ai_1e} = g_{ai_1} g_{i_1e}$, $g_{ai_2e} = g_{ai_2} g_{i_2e}$, $g_{bi_1e} = g_{bi_1} g_{i_1e}$, and $g_{bi_2e} = g_{bi_2} g_{i_2e}$ denote the equivalent path loss coefficients of Alice-IRS-1-Eve, Alice-IRS-2-Eve, Bob-IRS-1-Eve, and Bob-IRS-2-Eve channels, respectively. g_{ae} and g_{be} are the path loss coefficients of Alice-to-Eve and Bob-to-Eve channels, respectively. The channel matrices $\mathbf{H}_{ae}^H = \mathbf{h}(\theta_{r,ae}) \mathbf{h}^H(\theta_{t,ae}) \in \mathbb{C}^{N_e \times N_a}$, $\mathbf{H}_{be}^H = \mathbf{h}(\theta_{r,be}) \mathbf{h}^H(\theta_{t,be}) \in \mathbb{C}^{N_e \times N_b}$, $\mathbf{H}_{i_1e}^H = \mathbf{h}(\theta_{r,i_1e}) \mathbf{h}^H(\theta_{t,i_1e}) \in \mathbb{C}^{N_e \times M}$, and $\mathbf{H}_{i_2e}^H = \mathbf{h}(\theta_{r,i_2e}) \mathbf{h}^H(\theta_{t,i_2e}) \in \mathbb{C}^{N_e \times M}$ represent the Alice-to-Eve, Bob-to-Eve, IRS-1-to-Eve, and IRS-2-to-Eve channels, respectively. Then (4.13) and (4.14) can be rewritten as

$$\begin{aligned} \mathbf{H}_{e_1}(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2) &= \sqrt{g_{ai_1e}} \mathbf{h}(\theta_{r,i_1e}) \mathbf{h}^H(\theta_{t,i_1e}) \boldsymbol{\Theta}_1 \mathbf{h}(\theta_{r,ai_1}) \mathbf{h}^H(\theta_{t,ai_1}) \\ &\quad + \sqrt{g_{ai_2e}} \mathbf{h}(\theta_{r,i_2e}) \mathbf{h}^H(\theta_{t,i_2e}) \boldsymbol{\Theta}_2 \mathbf{h}(\theta_{r,ai_2}) \mathbf{h}^H(\theta_{t,ai_2}) \\ &\quad + \sqrt{g_{ae}} \mathbf{h}(\theta_{r,ae}) \mathbf{h}^H(\theta_{t,ae}) \end{aligned} \tag{4.16}$$

and

$$\begin{aligned} \mathbf{H}_{e_2}(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2) &= \sqrt{g_{bi_1e}} \mathbf{h}(\theta_{r,i_1e}) \mathbf{h}^H(\theta_{t,i_1e}) \boldsymbol{\Theta}_1 \mathbf{h}(\theta_{r,bi_1}) \mathbf{h}^H(\theta_{t,bi_1}) \\ &\quad + \sqrt{g_{bi_2e}} \mathbf{h}(\theta_{r,i_2e}) \mathbf{h}^H(\theta_{t,i_2e}) \boldsymbol{\Theta}_2 \mathbf{h}(\theta_{r,bi_2}) \mathbf{h}^H(\theta_{t,bi_2}) \end{aligned}$$

$$+\sqrt{g_{be}}\mathbf{h}(\theta_{r,be})\mathbf{h}^H(\theta_{t,be}), \tag{4.17}$$

respectively.

In this section, we characterize the SSR expression in this chapter. According to formulas (4.9), (4.8), and (4.12), the achievable rates at Alice, Bob, and Eve are

$$R_a = \log_2\left(1+\frac{\mathbf{v}_{ar}^H\mathbf{A}\mathbf{v}_{ar}}{\mathbf{v}_{ar}^H\mathbf{B}\mathbf{v}_{ar}+\sigma_a^2}\right), \tag{4.18}$$

$$R_b = \log_2\left(1+\frac{\mathbf{v}_{br}^H\mathbf{C}\mathbf{v}_{br}}{\mathbf{v}_{br}^H\mathbf{D}\mathbf{v}_{br}+\sigma_b^2}\right), \tag{4.19}$$

and

$$R_e = \log_2\left(1+\frac{\mathbf{v}_{er}^H\mathbf{E}\mathbf{v}_{er}}{\mathbf{v}_{er}^H(\mathbf{G}+\mathbf{J})\mathbf{v}_{er}+\sigma_e^2}\right)+\log_2\left(1+\frac{\mathbf{v}_{er}^H\mathbf{F}\mathbf{v}_{er}}{\mathbf{v}_{er}^H(\mathbf{G}+\mathbf{J})\mathbf{v}_{er}+\sigma_e^2}\right), \tag{4.20}$$

respectively, where

$$\mathbf{A} = \beta_2 P_b \mathbf{H}_a(\boldsymbol{\Theta}_1,\boldsymbol{\Theta}_2)\mathbf{v}_{bt}\mathbf{v}_{bt}^H\mathbf{H}_a^H(\boldsymbol{\Theta}_1,\boldsymbol{\Theta}_2), \tag{4.21a}$$

$$\mathbf{B} = (1-\beta_2) P_b \mathbf{H}_a(\boldsymbol{\Theta}_1,\boldsymbol{\Theta}_2)\mathbf{w}_b\mathbf{w}_b^H\mathbf{H}_a^H(\boldsymbol{\Theta}_1,\boldsymbol{\Theta}_2), \tag{4.21b}$$

$$\mathbf{C} = \beta_1 P_a \mathbf{H}_b(\boldsymbol{\Theta}_1,\boldsymbol{\Theta}_2)\mathbf{v}_{at}\mathbf{v}_{at}^H\mathbf{H}_b^H(\boldsymbol{\Theta}_1,\boldsymbol{\Theta}_2), \tag{4.21c}$$

$$\mathbf{D} = (1-\beta_1) P_a \mathbf{H}_b(\boldsymbol{\Theta}_1,\boldsymbol{\Theta}_2)\mathbf{w}_a\mathbf{w}_a^H\mathbf{H}_b^H(\boldsymbol{\Theta}_1,\boldsymbol{\Theta}_2), \tag{4.21d}$$

$$\mathbf{E} = \beta_1 P_a \mathbf{H}_{e_1}(\boldsymbol{\Theta}_1,\boldsymbol{\Theta}_2)\mathbf{v}_{at}\mathbf{v}_{at}^H\mathbf{H}_{e_1}^H(\boldsymbol{\Theta}_1,\boldsymbol{\Theta}_2), \tag{4.21e}$$

$$\mathbf{F} = \beta_2 P_b \mathbf{H}_{e_2}(\boldsymbol{\Theta}_1,\boldsymbol{\Theta}_2)\mathbf{v}_{bt}\mathbf{v}_{bt}^H\mathbf{H}_{e_2}^H(\boldsymbol{\Theta}_1,\boldsymbol{\Theta}_2), \tag{4.21f}$$

$$\mathbf{G} = (1-\beta_1)\, P_a \mathbf{H}_{e_1}(\boldsymbol{\Theta}_1,\boldsymbol{\Theta}_2)\mathbf{w}_a\mathbf{w}_a^H\mathbf{H}_{e_1}^H(\boldsymbol{\Theta}_1,\boldsymbol{\Theta}_2), \tag{4.21g}$$

$$\mathbf{J} = (1-\beta_2)\, P_b \mathbf{H}_{e_2}(\boldsymbol{\Theta}_1,\boldsymbol{\Theta}_2)\mathbf{w}_b\mathbf{w}_b^H\mathbf{H}_{e_2}^H(\boldsymbol{\Theta}_1,\boldsymbol{\Theta}_2). \tag{4.21h}$$

Then the achievable SSR can be written as

$$R = \max\{0,\, R_a + R_b - R_e\}. \tag{4.22}$$

4.3 Proposed Transmit Beamforming Methods

In this section, the GPG method is proposed to design the IRS phase-shifting firstly. Then two transmit beamforming methods at Alice and Bob, called Max-SV and Max-SLNR, are presented to enhance the SSR performance by fully exploiting the double-IRS.

4.3.1 Proposed GPG Method of Synthesizing the Phase-Shifting Matrices at Two IRSs

Observing (4.7) and (4.11), it is obvious that their first terms on the right sides are the linear functions of the IRS-1 phase-shifting matrix. To make a good balance between Alice and Bob, it is fairly reasonable to maximize the power sum of the two terms by a detailed design of $\mathbf{\Theta}_1$

$$\begin{aligned}
&\mathrm{tr}(\mathbf{h}^H(\theta_{t,i_1b})\mathbf{\Theta}_1\mathbf{h}(\theta_{r,ai_1})) + \mathrm{tr}(\mathbf{h}^H(\theta_{t,i_1a})\mathbf{\Theta}_1\mathbf{h}(\theta_{r,bi_1})) \\
&= \mathrm{tr}(\mathbf{\Theta}_1\mathbf{h}(\theta_{r,ai_1})\mathbf{h}^H(\theta_{t,i_1b})) + \mathrm{tr}(\mathbf{\Theta}_1\mathbf{h}(\theta_{r,bi_1})\mathbf{h}^H(\theta_{t,i_1a})) \\
&= \mathrm{tr}(\mathbf{\Theta}_1(\mathbf{h}(\theta_{r,ai_1})\mathbf{h}^H(\theta_{t,i_1b}) + \mathbf{h}(\theta_{r,bi_1})\mathbf{h}^H(\theta_{t,i_1a}))) \\
&= \frac{1}{M}\sum_{m=1}^{M} e^{j\phi_m^1}\left(e^{j2\pi\left(\Psi_{\theta_{r,ai_1}}(m)-\Psi_{\theta_{t,i_1b}}(m)\right)} + e^{j2\pi\left(\Psi_{\theta_{r,bi_1}}(m)-\Psi_{\theta_{t,i_1a}}(m)\right)}\right).
\end{aligned} \tag{4.23}$$

To make more clear, as shown in Fig. 4.2, let us define

$$\theta_1(m) = 2\pi(\Psi_{\theta_{r,ai_1}}(m) - \Psi_{\theta_{t,i_1b}}(m)), \tag{4.24}$$

$$\theta_2(m) = 2\pi(\Psi_{\theta_{r,bi_1}}(m) - \Psi_{\theta_{t,i_1a}}(m)). \tag{4.25}$$

In accordance with the angle relationship of parallelogram, we have

$$\theta_3(m) = \pi - \theta_2(m) + \theta_1(m). \tag{4.26}$$

Based on the cosine theorem, it is known that

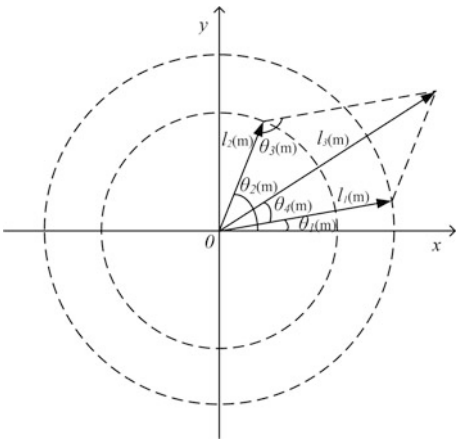


Fig. 4.2 Diagram of IRS-1 phase-shifting matrix designed

$$l_3(m) = \sqrt{l_1^2(m) + l_2^2(m) - 2l_1(m)l_2(m)\cos(\theta_3(m))}, \tag{4.27}$$

$$\theta_4(m) = \arccos\left(\frac{l_1^2(m) + l_3^2(m) - l_2^2(m)}{2l_1(m)l_3(m)}\right), \tag{4.28}$$

where $l_1(m)$ and $l_2(m)$ represent the weight coefficients of $\theta_1(m)$ and $\theta_2(m)$, respectively. Then we can obtain that

$$l_3(m)e^{j(\theta_1(m)+\theta_4(m))}e^{j\phi_m^1} = c(m), \tag{4.29}$$

where $c(m)$ is a constant, $l_3(m)$ represents the weight coefficient of ϕ_m^1. When $l_1(m) = l_2(m)$, (4.27) and (4.28) can be reduced to

$$l_3(m) = l_1(m)\sqrt{2 - 2\cos(\theta_3(m))} \tag{4.30}$$

and

$$\theta_4(m) = \frac{|\theta_2(m) - \theta_1(m)|}{2}, \tag{4.31}$$

respectively. To maximize the power sum via IRS-1, let us set

$$\theta_1(m) + \theta_4(m) + \phi_m^1 = 0, \tag{4.32}$$

then the optimal phase-shifting of m-th reflection element of $\mathbf{\Theta}_1$ is given by

$$\phi_m^1 = -(\theta_1(m) + \theta_4(m)). \tag{4.33}$$

Similarly, the optimal phase-shifting matrix of $\mathbf{\Theta}_2$ can also be obtained.

4.3.2 Proposed Max-SV Method

In this section, a Max-SV beamforming method is proposed. Here, we first perform singular-value decomposition (SVD) on the desired channel from Alice to Bob. Its right singular vector corresponding to the largest singular-value is used as the transmit beamforming vector. In the same manner, the receive beamforming vector is designed. The AN beamforming vector is constructed to maximizing the receive power at Eve on the null-space of this singular vector.

4.3.2.1 Design of the CM Beamforming Vectors at Alice and Bob

According to (4.8), the receive signal at Bob can be rewritten as

$$y_b = \mathbf{v}_{br}^H \left(\sqrt{\beta_1 P_a} \mathbf{H}_b(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2) \mathbf{v}_{at} x_1 + \bar{\mathbf{n}}_b \right). \tag{4.34}$$

Here, $\mathbf{H}_b(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2)$ has the following SVD form

$$\mathbf{H}_b(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2) = \mathbf{U}_{\mathbf{H}_b} \Sigma_{\mathbf{H}_b} \mathbf{V}_{\mathbf{H}_b}^H, \tag{4.35}$$

where both of $\mathbf{U}_{\mathbf{H}_b} \in \mathbb{C}^{N_b \times N_b}$ and $\mathbf{V}_{\mathbf{H}_b} \in \mathbb{C}^{N_a \times N_a}$ are unitary matrices, and $\Sigma_{\mathbf{H}_b} \in \mathbb{C}^{N_b \times N_a}$ is a matrix containing the singular values of $\mathbf{H}_b(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2)$ and along its main diagonal. The transmit beamforming vector $\mathbf{v}_{at}$ and receive beamforming vector $\mathbf{v}_{br}$ can be chosen as

$$\mathbf{v}_{at} = \mathbf{V}_{\mathbf{H}_b}(:, 1) \tag{4.36}$$

and

$$\mathbf{v}_{br} = \mathbf{U}_{\mathbf{H}_b}(:, 1), \tag{4.37}$$

respectively, where $\mathbf{V}_{\mathbf{H}_b}(:, 1)$ and $\mathbf{U}_{\mathbf{H}_b}(:, 1)$ respectively denote the first column vectors of the matrices $\mathbf{V}_{\mathbf{H}_b}$ and $\mathbf{U}_{\mathbf{H}_b}$.

In the same manner, the SVD form of $\mathbf{H}_a(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2)$ in (4.9) is

$$\mathbf{H}_a(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2) = \mathbf{U}_{\mathbf{H}_a} \Sigma_{\mathbf{H}_a} \mathbf{V}_{\mathbf{H}_a}^H, \tag{4.38}$$

where $\mathbf{U}_{\mathbf{H}_a} \in \mathbb{C}^{N_a \times N_a}$ and $\mathbf{V}_{\mathbf{H}_a} \in \mathbb{C}^{N_b \times N_b}$ are unitary matrices, and $\Sigma_{\mathbf{H}_a} \mathbb{C}^{N_a \times N_b}$ is a matrix containing the singular values of $\mathbf{H}_a(\boldsymbol{\Theta}_1, \boldsymbol{\Theta}_2)$ and along its main diagonal. The transmit beamforming vector $\mathbf{v}_{bt}$ and receive beamforming vector $\mathbf{v}_{ar}$ can be respectively designed as

$$\mathbf{v}_{bt} = \mathbf{V}_{\mathbf{H}_a}(:, 1), \quad \mathbf{v}_{ar} = \mathbf{U}_{\mathbf{H}_a}(:, 1). \tag{4.39}$$

4.3.2.2 Design the AN Transmit Beamforming Vectors

To reduce the effect of AN on the desired users, we limit the AN into the null-space of CM transmit space, and then the AN beamforming vector $\mathbf{w}_a$ at Alice can be casted as

$$\mathbf{w}_a = \mathbf{T}_a \mathbf{u}_a, \tag{4.40}$$

where $\mathbf{T}_a \in \mathbb{C}^{N_a \times N_a}$, $\mathbf{u}_a \in \mathbb{C}^{N_a \times 1}$ satisfies $\mathbf{u}_a^H \mathbf{u}_a = 1$. In other words, to minimize the AN power received by Bob, the $\mathbf{T}_a$ is a projector on the null-space of CM transmit beamforming vector at Alice constructed as follows

$$\mathbf{T}_a = \mathbf{I}_{N_a} - \mathbf{V}_{\mathbf{H}_b}(:,1)\mathbf{V}_{\mathbf{H}_b}(:,1)^H. \tag{4.41}$$

The problem of maximizing the AN power received by Eve is formulated as

$$\max_{\mathbf{u}_a} \quad \mathrm{tr}\{\mathbf{w}_a^H \mathbf{H}_{ae} \mathbf{H}_{ae}^H \mathbf{w}_a\} \tag{4.42a}$$

$$\text{s.t.} \quad \mathbf{u}_a^H \mathbf{u}_a = 1. \tag{4.42b}$$

Considering $\mathbf{H}_{ae}^H = \mathbf{h}(\theta_{r,ae})\mathbf{h}^H(\theta_{t,ae})$, the above optimization problem reduces to

$$\max_{\mathbf{u}_a} \quad \mathrm{tr}\{\mathbf{u}_a^H \mathbf{T}_a^H \mathbf{h}(\theta_{t,ae})\mathbf{h}^H(\theta_{t,ae})\mathbf{T}_a \mathbf{u}_a\} \tag{4.43a}$$

$$\text{s.t.} \quad \mathbf{u}_a^H \mathbf{u}_a = 1, \tag{4.43b}$$

which gives the associated Lagrangian

$$L(\mathbf{u}_a, \lambda_a) = \mathbf{u}_a^H \mathbf{T}_a^H \mathbf{h}(\theta_{t,ae})\mathbf{h}^H(\theta_{t,ae})\mathbf{T}_a \mathbf{u}_a - \lambda_a(\mathbf{u}_a^H \mathbf{u}_a - 1), \tag{4.44}$$

where λ_a is the Lagrange multiplier. We have the partial derivative of the Lagrangian function with respect to $\mathbf{u}_a^*$ and set as zero

$$\frac{\partial L(\mathbf{u}_a, \lambda_a)}{\partial \mathbf{u}_a^*} = (\mathbf{T}_a^H \mathbf{h}(\theta_{t,ae})\mathbf{h}^H(\theta_{t,ae})\mathbf{T}_a)\mathbf{u}_a - \lambda_a \mathbf{u}_a = 0, \tag{4.45}$$

which is rewritten as

$$\underbrace{\mathbf{T}_a^H \mathbf{h}(\theta_{t,ae})}_{\mathbf{t}} \underbrace{\mathbf{h}^H(\theta_{t,ae})\mathbf{T}_a \mathbf{u}_a}_{c} = c\mathbf{t} = \lambda_a \mathbf{u}_a, \tag{4.46}$$

which means that $\mathbf{u}_a$ is on the subspace spanned by the column vector $\mathbf{t}$ directly given by

$$\mathbf{u}_a = \frac{\mathbf{T}_a^H \mathbf{h}(\theta_{t,ae})}{\|\mathbf{T}_a^H \mathbf{h}(\theta_{t,ae})\|}. \tag{4.47}$$

Plugging (4.41) and (4.47) into (4.40), the AN beamforming vector $\mathbf{w}_a$ can be obtained completely.

Similarly, the AN beamforming vector $\mathbf{w}_b$ at Bob is given by

$$\mathbf{w}_b = \mathbf{T}_b \mathbf{u}_b, \tag{4.48}$$

where

$$\mathbf{T}_b = \mathbf{I}_{N_b} - \mathbf{V}_{\mathbf{H}_b}(:,1)\mathbf{V}_{\mathbf{H}_b}(:,1)^H, \tag{4.49}$$

$$\mathbf{u}_b = \frac{\mathbf{T}_b^H \mathbf{h}(\theta_{t,be})}{\|\mathbf{T}_b^H \mathbf{h}(\theta_{t,be})\|}. \tag{4.50}$$

4.3.2.3 Proposed ZF-Based MRC Receive Beamforming Method at Eve

Seeing Fig. 4.1, Eve may eavesdrop four-way signals from IRS-1, IRS-2, Alice and Bob. The four-way signals interfere with each other. It is very necessary for Eve to separate them and then combine them coherently. Below, the ZF receive beamforming method is first presented to separate them, and the MRC is adopted to combine their separate versions.

To completely cancel the interference among four-way signals, the total receive beamforming vector is decomposed as

$$\mathbf{v}_{er}^H \triangleq \underbrace{\left[w_{e_1}\ w_{e_2}\ w_{e_3}\ w_{e_4}\right]}_{\text{MRC}} \cdot \underbrace{\begin{bmatrix} \mathbf{v}_{er_1}^H \\ \mathbf{v}_{er_2}^H \\ \mathbf{v}_{er_3}^H \\ \mathbf{v}_{er_4}^H \end{bmatrix}}_{\text{ZF}}, \tag{4.51}$$

where w_{e_1}, w_{e_2}, w_{e_3}, and w_{e_4} are the weight coefficients of MRC, $\mathbf{v}_{er_1}^H$, $\mathbf{v}_{er_2}^H$, $\mathbf{v}_{er_3}^H$, $\mathbf{v}_{er_4}^H \in \mathbb{C}^{1\times N_e}$ are the receive sub-beamforming vectors of ZF. Substituting (4.51) in (4.12) yields

$$\begin{aligned} y_e &= \mathbf{v}_{er}^H\left(\sqrt{\beta_1 P_a}\mathbf{H}_{e_1}(\boldsymbol{\Theta}_1,\boldsymbol{\Theta}_2)\mathbf{v}_{at}x_1 + \sqrt{\beta_2 P_b}\mathbf{H}_{e_2}(\boldsymbol{\Theta}_1,\boldsymbol{\Theta}_2)\mathbf{v}_{bt}x_2 + \bar{\mathbf{n}}_e\right) \\ &= \left(w_{e_1}\mathbf{v}_{er_1}^H + w_{e_2}\mathbf{v}_{er_2}^H + w_{e_3}\mathbf{v}_{er_3}^H + w_{e_4}\mathbf{v}_{er_4}^H\right)\Big[\mathbf{h}(\theta_{r,i_1e})\mathbf{h}^H(\theta_{t,i_1e})\boldsymbol{\Theta}_1 \cdot \\ &\quad \left(\sqrt{\beta_1 P_a g_{ai_1e}}\mathbf{H}_{ai_1}\mathbf{v}_{at}x_1 + \sqrt{\beta_2 P_b g_{bi_1e}}\mathbf{H}_{bi_1}\mathbf{v}_{bt}x_2\right) + \mathbf{h}(\theta_{r,i_2e}) \cdot \\ &\quad \mathbf{h}^H(\theta_{t,i_2e})\boldsymbol{\Theta}_2\left(\sqrt{\beta_1 P_a g_{ai_2e}}\mathbf{H}_{ai_2}\mathbf{v}_{at}x_1 + \sqrt{\beta_2 P_b g_{bi_2e}}\mathbf{H}_{bi_2}\mathbf{v}_{bt}x_2\right) + \\ &\quad \sqrt{\beta_1 P_a g_{ae}}\mathbf{H}_{ae}^H\mathbf{v}_{at}x_1 + \sqrt{\beta_2 P_b g_{be}}\mathbf{H}_{be}^H\mathbf{v}_{bt}x_2\Big] + \Big(w_{e_1}\mathbf{v}_{er_1}^H + w_{e_2}\mathbf{v}_{er_2}^H \\ &\quad + w_{e_3}\mathbf{v}_{er_3}^H + w_{e_4}\mathbf{v}_{er_4}^H\Big)\bar{\mathbf{n}}_e. \end{aligned} \tag{4.52}$$

To design the sub-beamforming vector $\mathbf{v}_{er_1}^H$, it is assumed that $\mathbf{h}(\theta_{r,i_1e})$ is the only one useful channel for $\mathbf{v}_{er_1}^H$ to receive the reflected CM from IRS-1 and the remaining channels are useless, i.e., $\mathbf{v}_{er_1}^H$ satisfies

$$\mathbf{v}_{er_1}^H \mathbf{h}(\theta_{r,i_2e}) = 0, \quad \mathbf{v}_{er_1}^H \mathbf{h}(\theta_{r,ae}) = 0, \quad \mathbf{v}_{er_1}^H \mathbf{h}(\theta_{r,be}) = 0, \tag{4.53}$$

the actual CM channel can be defined as

$$\mathbf{H}_{er_{-1}} = \begin{bmatrix} \mathbf{h}^H(\theta_{r,i_2e}) \\ \mathbf{h}^H(\theta_{r,ae}) \\ \mathbf{h}^H(\theta_{r,be}) \end{bmatrix}, \tag{4.54}$$

then $\mathbf{v}_{er_1}$ can be set as

$$\mathbf{v}_{er_1} = \left(\mathbf{I}_{N_e} - \mathbf{H}_{er_{-1}}^H [\mathbf{H}_{er_{-1}} \mathbf{H}_{er_{-1}}^H]^\dagger \mathbf{H}_{er_{-1}}\right) \mathbf{h}(\theta_{r,i_1e}). \tag{4.55}$$

Likewise, $\mathbf{v}_{er_2}$, $\mathbf{v}_{er_3}$, and $\mathbf{v}_{er_4}$ are respectively set as follows

$$\mathbf{v}_{er_2} = \left(\mathbf{I}_{N_e} - \mathbf{H}_{er_{-2}}^H [\mathbf{H}_{er_{-2}} \mathbf{H}_{er_{-2}}^H]^\dagger \mathbf{H}_{er_{-2}}\right) \mathbf{h}(\theta_{r,i_2e}), \tag{4.56a}$$

$$\mathbf{v}_{er_3} = \left(\mathbf{I}_{N_e} - \mathbf{H}_{er_{-3}}^H [\mathbf{H}_{er_{-3}} \mathbf{H}_{er_{-3}}^H]^\dagger \mathbf{H}_{er_{-3}}\right) \mathbf{h}(\theta_{r,ae}), \tag{4.56b}$$

$$\mathbf{v}_{er_4} = \left(\mathbf{I}_{N_e} - \mathbf{H}_{er_{-4}}^H [\mathbf{H}_{er_{-4}} \mathbf{H}_{er_{-4}}^H]^\dagger \mathbf{H}_{er_{-4}}\right) \mathbf{h}(\theta_{r,be}), \tag{4.56c}$$

where

$$\mathbf{H}_{er_{-2}} = \begin{bmatrix} \mathbf{h}^H(\theta_{r,i_1e}) \\ \mathbf{h}^H(\theta_{r,ae}) \\ \mathbf{h}^H(\theta_{r,be}) \end{bmatrix}, \quad \mathbf{H}_{er_{-3}} = \begin{bmatrix} \mathbf{h}^H(\theta_{r,i_1e}) \\ \mathbf{h}^H(\theta_{r,i_2e}) \\ \mathbf{h}^H(\theta_{r,be}) \end{bmatrix}, \quad \mathbf{H}_{er_{-4}} = \begin{bmatrix} \mathbf{h}^H(\theta_{r,i_1e}) \\ \mathbf{h}^H(\theta_{r,i_2e}) \\ \mathbf{h}^H(\theta_{r,ae}) \end{bmatrix}. \tag{4.57}$$

According to the MRC rule, the weight coefficients $w_{e_1}, w_{e_2}, w_{e_3}, w_{e_4}$ are respectively given by

$$w_{e_1} = \frac{\left(\mathbf{v}_{er_1}^H \mathbf{H}_{i_1e}^H \mathbf{\Theta}_1 \left(\sqrt{\beta_1 P_a g_{ai_1e}} \mathbf{H}_{ai_1} \mathbf{v}_{at} + \sqrt{\beta_2 P_b g_{bi_1e}} \mathbf{H}_{bi_1} \mathbf{v}_{bt}\right)\right)^H}{\| \mathbf{v}_{er_1}^H \mathbf{H}_{i_1e}^H \mathbf{\Theta}_1 \left(\sqrt{\beta_1 P_a g_{ai_1e}} \mathbf{H}_{ai_1} \mathbf{v}_{at} + \sqrt{\beta_2 P_b g_{bi_1e}} \mathbf{H}_{bi_1} \mathbf{v}_{bt}\right) \|}, \tag{4.58a}$$

$$w_{e_2} = \frac{\left(\mathbf{v}_{er_2}^H \mathbf{H}_{i_2e}^H \mathbf{\Theta}_2 \left(\sqrt{\beta_1 P_a g_{ai_2e}} \mathbf{H}_{ai_2} \mathbf{v}_{at} + \sqrt{\beta_2 P_b g_{bi_2e}} \mathbf{H}_{bi_2} \mathbf{v}_{bt}\right)\right)^H}{\| \mathbf{v}_{er_2}^H \mathbf{H}_{i_2e}^H \mathbf{\Theta}_2 \left(\sqrt{\beta_1 P_a g_{ai_2e}} \mathbf{H}_{ai_2} \mathbf{v}_{at} + \sqrt{\beta_2 P_b g_{bi_2e}} \mathbf{H}_{bi_2} \mathbf{v}_{bt}\right) \|}, \tag{4.58b}$$

$$w_{e_3} = \frac{\left(\mathbf{v}_{er_3}^H \mathbf{H}_{ae}^H \mathbf{v}_{at}\right)^H}{\| \mathbf{v}_{er_3}^H \mathbf{H}_{ae}^H \mathbf{v}_{at} \|}, \quad w_{e_4} = \frac{\left(\mathbf{v}_{er_4}^H \mathbf{H}_{be}^H \mathbf{v}_{bt}\right)^H}{\| \mathbf{v}_{er_4}^H \mathbf{H}_{be}^H \mathbf{v}_{bt} \|}. \tag{4.58c}$$

Then Eq. (4.12) can be further converted to

$$
\begin{aligned}
y_e = {} & w_{e_1}\mathbf{v}_{er_1}^H\mathbf{H}_{i_1e}^H\boldsymbol{\Theta}_1\left(\sqrt{\beta_1 P_a g_{ai_1e}}\mathbf{H}_{ai_1}\mathbf{v}_{at}x_1+\sqrt{\beta_2 P_b g_{bi_1e}}\mathbf{H}_{bi_1}\mathbf{v}_{bt}x_2\right)\\
& + w_{e_2}\mathbf{v}_{er_2}^H\mathbf{H}_{i_2e}^H\boldsymbol{\Theta}_2\left(\sqrt{\beta_1 P_a g_{ai_2e}}\mathbf{H}_{ai_2}\mathbf{v}_{at}x_1+\sqrt{\beta_2 P_b g_{bi_2e}}\mathbf{H}_{bi_2}\mathbf{v}_{bt}x_2\right)\\
& + \sqrt{\beta_1 P_a g_{ae}}w_{e_3}\mathbf{v}_{er_3}^H\mathbf{H}_{ae}^H\mathbf{v}_{at}x_1+\sqrt{\beta_2 P_b g_{be}}w_{e_4}\mathbf{v}_{er_4}^H\mathbf{H}_{be}^H\mathbf{v}_{bt}x_2\\
& + \left(w_{e_1}\mathbf{v}_{er_1}^H+w_{e_2}\mathbf{v}_{er_2}^H+w_{e_3}\mathbf{v}_{er_3}^H+w_{e_4}\mathbf{v}_{er_4}^H\right)\bar{\mathbf{n}}_e.
\end{aligned}
\tag{4.59}
$$

4.3.3 Generalized Leakage Method

In this section, the leakage concept in [38, 39] is generalized to design the CM transmit beamforming vector and AN beamforming vector, and called a generalized leakage (GL) in what follows.

4.3.3.1 Design the CM Transmit Beamforming Vector

The $\mathbf{H}_{ai_1}$, $\mathbf{H}_{ai_2}$, and $\mathbf{H}_{ab}^H$ channels can be viewed as the desired channels, while $\mathbf{H}_{ae}^H$ viewed as the undesired channel. In accordance with [38, 39], the transmit beamforming vector $\mathbf{v}_{at}$ is designed by the optimization problem

$$
\max_{\mathbf{v}_{at}} \quad \mathrm{SLNR}(\mathbf{v}_{at}) \tag{4.60a}
$$

$$
\text{s.t.} \quad \mathbf{v}_{at}^H\mathbf{v}_{at}=1, \tag{4.60b}
$$

where

$$
\mathrm{SLNR}(\mathbf{v}_{at})=\beta_1 P_a\frac{\mathrm{tr}\left\{\mathbf{v}_{at}^H\left(g_{ai_1}\mathbf{H}_{ai_1}^H\mathbf{H}_{ai_1}+g_{ai_2}\mathbf{H}_{ai_2}^H\mathbf{H}_{ai_2}+g_{ab}\mathbf{H}_{ab}\mathbf{H}_{ab}^H\right)\mathbf{v}_{at}\right\}}{\mathrm{tr}\left\{\mathbf{v}_{at}^H\left(\beta_1 P_a g_{ae}\mathbf{H}_{ae}\mathbf{H}_{ae}^H+\sigma_e^2\mathbf{I}_{N_a}\right)\mathbf{v}_{at}\right\}}. \tag{4.61}
$$

According to the generalized Rayleigh-Ritz theorem [40], the transmit beamforming vector $\mathbf{v}_{at}$ at Alice is directly equal to the eigen-vector corresponding to the largest eigenvalue of the matrix

$$
\left[g_{ae}\mathbf{H}_{ae}\mathbf{H}_{ae}^H+(\beta_1 P_a)^{-1}\sigma_e^2\mathbf{I}_{N_a}\right]^{-1}\left(g_{ai_1}\mathbf{H}_{ai_1}^H\mathbf{H}_{ai_1}+g_{ai_2}\mathbf{H}_{ai_2}^H\mathbf{H}_{ai_2}+g_{ab}\mathbf{H}_{ab}\mathbf{H}_{ab}^H\right). \tag{4.62}
$$

Similarly, the transmit beamforming vector $\mathbf{v}_{bt}$ at Bob can be designed from the eigen-vector corresponding to the largest eigenvalue of the matrix

$$
\left[g_{be}\mathbf{H}_{be}\mathbf{H}_{be}^H+(\beta_2 P_b)^{-1}\sigma_e^2\mathbf{I}_{N_b}\right]^{-1}\left(g_{i_1b}\mathbf{H}_{bi_1}^H\mathbf{H}_{bi_1}+g_{i_2b}\mathbf{H}_{bi_2}^H\mathbf{H}_{bi_2}+g_{ab}\mathbf{H}_{ba}\mathbf{H}_{ba}^H\right). \tag{4.63}
$$

4.3.3.2 Design the AN Beamforming Vector

The $\mathbf{H}_{ae}^H$ can be viewed as the desired channel, while $\mathbf{H}_{ai_1}$, $\mathbf{H}_{ai_2}$, and $\mathbf{H}_{ab}^H$ channels are viewed as the undesired channel. In the following, we compute the AN beamforming vector at Alice by the following maximizing leakage-AN-to-signal ratio (LANSR) optimization problem

$$\max_{\mathbf{w}_a} \quad \text{LANSR}(\mathbf{w}_a) \tag{4.64a}$$

$$\text{s.t.} \quad \mathbf{w}_a^H \mathbf{w}_a = 1, \tag{4.64b}$$

where $\text{LANSR}(\mathbf{w}_a)$ is given by

$$\text{LANSR}(\mathbf{w}_a) = \tag{4.65}$$

$$\frac{(1-\beta_1) P_a \text{tr}\left\{ g_{ae} \mathbf{w}_a^H \mathbf{H}_{ae} \mathbf{H}_{ae}^H \mathbf{w}_a \right\}}{\text{tr}\left\{ \mathbf{w}_a^H \left[(1-\beta_1) P_a \left(g_{ai_1} \mathbf{H}_{ai_1}^H \mathbf{H}_{ai_1} + g_{ai_2} \mathbf{H}_{ai_2}^H \mathbf{H}_{ai_2} + g_{ab} \mathbf{H}_{ab} \mathbf{H}_{ab}^H \right) + \sigma_b^2 \mathbf{I}_{N_a} \right] \mathbf{w}_a \right\}}.$$

Similar to (4.60)–(4.62), $\mathbf{w}_a$ is equal to the eigen-vector corresponding to the largest eigenvalue of the matrix

$$\left[\left(g_{ai_1} \mathbf{H}_{ai_1}^H \mathbf{H}_{ai_1} + g_{ai_2} \mathbf{H}_{ai_2}^H \mathbf{H}_{ai_2} + g_{ab} \mathbf{H}_{ab} \mathbf{H}_{ab}^H \right) + \left((1-\beta_1) P_a \right)^{-1} \sigma_b^2 \mathbf{I}_{N_a} \right]^{-1} \cdot \left(g_{ae} \mathbf{H}_{ae} \mathbf{H}_{ae}^H \right). \tag{4.66}$$

In the same manner, the AN beamforming vector $\mathbf{w}_b$ at Bob is given by the eigen-vector corresponding to the largest eigenvalue of the matrix

$$\left[\left(g_{i_1 b} \mathbf{H}_{bi_1}^H \mathbf{H}_{bi_1} + g_{i_2 b} \mathbf{H}_{bi_2}^H \mathbf{H}_{bi_2} + g_{ab} \mathbf{H}_{ba} \mathbf{H}_{ba}^H \right) + \left((1-\beta_2) P_b \right)^{-1} \sigma_a^2 \mathbf{I}_{N_b} \right]^{-1} \cdot \left(g_{be} \mathbf{H}_{be} \mathbf{H}_{be}^H \right). \tag{4.67}$$

4.3.3.3 Design of the Receive Beamforming Vector

Considering that Bob receives three-way signals from IRS-1, IRS-2, and Alice, to combine them coherently, similar to the design of receive beamforming at Eve in (4.51), the ZF-based MRC receive beamforming method is still adopted as follows

$$\mathbf{v}_{br}^H = \left[w_{b_1} \; w_{b_2} \; w_{b_3} \right] \left[\mathbf{v}_{br_1}^* \; \mathbf{v}_{br_2}^* \; \mathbf{v}_{br_3}^* \right]^T, \tag{4.68}$$

where the receive sub-beamforming vectors $\mathbf{v}_{br_1}$, $\mathbf{v}_{br_2}$, $\mathbf{v}_{br_3} \in \mathbb{C}^{N_b \times 1}$ are respectively given as follows

$$\mathbf{v}_{br_1} = \left(\mathbf{I}_{N_b} - \mathbf{H}_{br_{-1}}^H [\mathbf{H}_{br_{-1}} \mathbf{H}_{br_{-1}}^H]^\dagger \mathbf{H}_{br_{-1}}\right) \mathbf{h}(\theta_{r,i_1 b}), \tag{4.69a}$$

$$\mathbf{v}_{br_2} = \left(\mathbf{I}_{N_b} - \mathbf{H}_{br_{-2}}^H [\mathbf{H}_{br_{-2}} \mathbf{H}_{br_{-2}}^H]^\dagger \mathbf{H}_{br_{-2}}\right) \mathbf{h}(\theta_{r,i_2 b}), \tag{4.69b}$$

$$\mathbf{v}_{br_3} = \left(\mathbf{I}_{N_b} - \mathbf{H}_{br_{-3}}^H [\mathbf{H}_{br_{-3}} \mathbf{H}_{br_{-3}}^H]^\dagger \mathbf{H}_{br_{-3}}\right) \mathbf{h}(\theta_{r,ab}), \tag{4.69c}$$

where

$$\mathbf{H}_{br_{-1}} = \begin{bmatrix} \mathbf{h}^H(\theta_{r,i_2 b}) \\ \mathbf{h}^H(\theta_{r,ab}) \end{bmatrix}, \ \mathbf{H}_{br_{-2}} = \begin{bmatrix} \mathbf{h}^H(\theta_{r,i_1 b}) \\ \mathbf{h}^H(\theta_{r,ab}) \end{bmatrix}, \ \mathbf{H}_{br_{-3}} = \begin{bmatrix} \mathbf{h}^H(\theta_{r,i_1 b}) \\ \mathbf{h}^H(\theta_{r,i_2 b}) \end{bmatrix}. \tag{4.70}$$

In (4.68), the weight coefficients w_{b_1}, w_{b_2}, and w_{b_3} can be respectively designed as follows

$$w_{b_1} = \frac{\left(\mathbf{v}_{br_1}^H \mathbf{H}_{i_1 b}^H \mathbf{\Theta}_1 \mathbf{H}_{ai_1} \mathbf{v}_{at}\right)^H}{\|\mathbf{v}_{br_1}^H \mathbf{H}_{i_1 b}^H \mathbf{\Theta}_1 \mathbf{H}_{ai_1} \mathbf{v}_{at}\|}, \tag{4.71a}$$

$$w_{b_2} = \frac{\left(\mathbf{v}_{br_2}^H \mathbf{H}_{i_2 b}^H \mathbf{\Theta}_2 \mathbf{H}_{ai_2} \mathbf{v}_{at}\right)^H}{\|\mathbf{v}_{br_2}^H \mathbf{H}_{i_2 b}^H \mathbf{\Theta}_2 \mathbf{H}_{ai_2} \mathbf{v}_{at}\|}, \tag{4.71b}$$

$$w_{b_3} = \frac{\left(\mathbf{v}_{br_3}^H \mathbf{H}_{ab}^H \mathbf{v}_{at}\right)^H}{\|\mathbf{v}_{br_3}^H \mathbf{H}_{ab}^H \mathbf{v}_{at}\|}. \tag{4.71c}$$

Therefore, (4.8) can be further converted to

$$\begin{aligned} y_b = \sqrt{\beta_1 P_a}\Big(&\sqrt{g_{ai_1 b}} w_{b_1} \mathbf{v}_{br_1}^H \mathbf{h}(\theta_{r,i_1 b}) \mathbf{h}^H(\theta_{t,i_1 b}) \mathbf{\Theta}_1 \mathbf{H}_{ai_1} + \sqrt{g_{ai_2 b}} w_{b_2} \mathbf{v}_{br_2}^H \cdot \\ &\mathbf{h}(\theta_{r,i_2 b}) \mathbf{h}^H(\theta_{t,i_2 b}) \mathbf{\Theta}_2 \mathbf{H}_{ai_2} + \sqrt{g_{ab}} w_{b_3} \mathbf{v}_{br_3}^H \mathbf{h}(\theta_{r,ab}) \mathbf{h}^H(\theta_{t,ab})\Big) \mathbf{v}_{at} x_1 \\ &+ (w_{b_1} \mathbf{v}_{br_1}^H + w_{b_2} \mathbf{v}_{br_2}^H + w_{b_3} \mathbf{v}_{br_3}^H) \bar{\mathbf{n}}_b. \end{aligned} \tag{4.72}$$

Similarly, the receive beamforming vector $\mathbf{v}_{ar}^H$ at Alice is

$$\mathbf{v}_{ar}^H = \begin{bmatrix} w_{a_1} & w_{a_2} & w_{a_3} \end{bmatrix} \begin{bmatrix} \mathbf{v}_{ar_1}^* & \mathbf{v}_{ar_2}^* & \mathbf{v}_{ar_3}^* \end{bmatrix}^T, \tag{4.73}$$

where the receive sub-beamforming vectors $\mathbf{v}_{ar_1}$, $\mathbf{v}_{ar_2}$, $\mathbf{v}_{ar_3} \in \mathbb{C}^{N_a \times 1}$ are respectively given by

$$\mathbf{v}_{ar_1} = \left(\mathbf{I}_{N_a} - \mathbf{H}_{ar_{-1}}^H [\mathbf{H}_{ar_{-1}} \mathbf{H}_{ar_{-1}}^H]^\dagger \mathbf{H}_{ar_{-1}}\right) \mathbf{h}(\theta_{r,i_1 a}), \tag{4.74a}$$

$$\mathbf{v}_{ar_2} = \left(\mathbf{I}_{N_a} - \mathbf{H}_{ar_{-2}}^H [\mathbf{H}_{ar_{-2}} \mathbf{H}_{ar_{-2}}^H]^\dagger \mathbf{H}_{ar_{-2}}\right) \mathbf{h}(\theta_{r,i_2 a}), \tag{4.74b}$$

$$\mathbf{v}_{ar_3} = \left(\mathbf{I}_{N_a} - \mathbf{H}_{ar_{-3}}^H [\mathbf{H}_{ar_{-3}} \mathbf{H}_{ar_{-3}}^H]^\dagger \mathbf{H}_{ar_{-3}}\right) \mathbf{h}(\theta_{r,ba}), \tag{4.74c}$$

and

$$\mathbf{H}_{ar_{-1}} = \begin{bmatrix} \mathbf{h}^H(\theta_{r,i_2 a}) \\ \mathbf{h}^H(\theta_{r,ba}) \end{bmatrix}, \ \mathbf{H}_{ar_{-2}} = \begin{bmatrix} \mathbf{h}^H(\theta_{r,i_1 a}) \\ \mathbf{h}^H(\theta_{r,ba}) \end{bmatrix}, \ \mathbf{H}_{ar_{-3}} = \begin{bmatrix} \mathbf{h}^H(\theta_{r,i_1 a}) \\ \mathbf{h}^H(\theta_{r,i_2 a}) \end{bmatrix}. \tag{4.75}$$

In (4.73), the weight coefficients w_{a_1}, w_{a_2}, and w_{a_3} are respectively constructed as follows

$$w_{a_1} = \frac{\left(\mathbf{v}_{ar_1}^H \mathbf{H}_{i_1 a}^H \mathbf{\Theta}_1 \mathbf{H}_{bi_1} \mathbf{v}_{bt}\right)^H}{\|\mathbf{v}_{ar_1}^H \mathbf{H}_{i_1 a}^H \mathbf{\Theta}_1 \mathbf{H}_{bi_1} \mathbf{v}_{bt}\|}, \tag{4.76a}$$

$$w_{a_2} = \frac{\left(\mathbf{v}_{ar_2}^H \mathbf{H}_{i_2 a}^H \mathbf{\Theta}_2 \mathbf{H}_{bi_2} \mathbf{v}_{bt}\right)^H}{\|\mathbf{v}_{ar_2}^H \mathbf{H}_{i_2 a}^H \mathbf{\Theta}_2 \mathbf{H}_{bi_2} \mathbf{v}_{bt}\|}, \tag{4.76b}$$

$$w_{a_3} = \frac{\left(\mathbf{v}_{ar_3}^H \mathbf{H}_{ba}^H \mathbf{v}_{bt}\right)^H}{\|\mathbf{v}_{ar_3}^H \mathbf{H}_{ba}^H \mathbf{v}_{bt}\|}. \tag{4.76c}$$

The received signal in (4.9) can be further converted to

$$\begin{aligned} y_a = \sqrt{\beta_2 P_b}\Big(&\sqrt{g_{ai_1 b}} w_{a_1} \mathbf{v}_{ar_1}^H \mathbf{h}(\theta_{r,i_1 a}) \mathbf{h}^H(\theta_{t,i_1 a}) \mathbf{\Theta}_1 \mathbf{H}_{bi_1} + \sqrt{g_{ai_2 b}} w_{a_2} \mathbf{v}_{ar_2}^H \cdot \\ &\mathbf{h}(\theta_{r,i_2 a}) \mathbf{h}^H(\theta_{t,i_2 a}) \mathbf{\Theta}_2 \mathbf{H}_{bi_2} + \sqrt{g_{ab}} w_{a_3} \mathbf{v}_{ar_3}^H \mathbf{h}(\theta_{r,ba}) \mathbf{h}^H(\theta_{t,ba})\Big) \mathbf{v}_{bt} x_2 \\ &+ (w_{a_1} \mathbf{v}_{ar_1}^H + w_{a_2} \mathbf{v}_{ar_2}^H + w_{a_3} \mathbf{v}_{ar_3}^H) \bar{\mathbf{n}}_a. \end{aligned} \tag{4.77}$$

This completes the construction of all beamforming methods.

4.4 Proposed HICF Power Allocation Strategy

In this section, given that all beamforming vectors are designed well in the previous section, we will optimize the PA between CM and AN to improve the SSR performance. The PA method of maximizing SSR is proposed. First, two exhaustive search (ES) methods including 2D and 1D are presented, and then a hybrid iterative

and closed-form solution is proposed to reduce the high computational complexity and approximately achieve the same SSR performance as ES method.

4.4.1 Problem Formulation

Given all beamforming vectors, maximizing the SSR in (4.22) over the PA factors forms the following optimization problem

$$\max_{\beta_1,\beta_2} \quad R(\beta_1,\beta_2) = R_a + R_b - R_e \tag{4.78a}$$

$$\text{s.t.} \quad 0 \le \beta_1 \le 1, 0 \le \beta_2 \le 1. \tag{4.78b}$$

Let us define

$$s_1 = P_b\|\mathbf{v}_{ar}^H\mathbf{H}_a(\boldsymbol{\Theta}_1,\boldsymbol{\Theta}_2)\mathbf{v}_{bt}\|^2, \quad s_2 = P_b\|\mathbf{v}_{ar}^H\mathbf{H}_a(\boldsymbol{\Theta}_1,\boldsymbol{\Theta}_2)\mathbf{w}_b\|^2, \tag{4.79a}$$

$$s_3 = P_a\|\mathbf{v}_{br}^H\mathbf{H}_b(\boldsymbol{\Theta}_1,\boldsymbol{\Theta}_2)\mathbf{v}_{at}\|^2, \quad s_4 = P_a\|\mathbf{v}_{br}^H\mathbf{H}_b(\boldsymbol{\Theta}_1,\boldsymbol{\Theta}_2)\mathbf{w}_a\|^2, \tag{4.79b}$$

$$s_5 = P_a\|\mathbf{v}_{er}^H\mathbf{H}_{e_1}(\boldsymbol{\Theta}_1,\boldsymbol{\Theta}_2)\mathbf{v}_{at}\|^2, \quad s_6 = P_b\|\mathbf{v}_{er}^H\mathbf{H}_{e_2}(\boldsymbol{\Theta}_1,\boldsymbol{\Theta}_2)\mathbf{v}_{bt}\|^2, \tag{4.79c}$$

$$s_7 = P_a\|\mathbf{v}_{er}^H\mathbf{H}_{e_1}(\boldsymbol{\Theta}_1,\boldsymbol{\Theta}_2)\mathbf{w}_a\|^2, \quad s_8 = P_b\|\mathbf{v}_{er}^H\mathbf{H}_{e_2}(\boldsymbol{\Theta}_1,\boldsymbol{\Theta}_2)\mathbf{w}_b\|^2. \tag{4.79d}$$

Then the objective function $R(\beta_1,\beta_2)$ can be rewritten as follows

$$\begin{aligned} R(\beta_1,\beta_2) = &\log_2\left(1+\frac{\beta_2 s_1}{(1-\beta_2)s_2+\sigma_a^2}\right) + \log_2\left(1+\frac{\beta_1 s_3}{(1-\beta_1)s_4+\sigma_b^2}\right) \\ &- \log_2\left(1+\frac{\beta_1 s_5}{(1-\beta_1)s_7+(1-\beta_2)s_8+\sigma_e^2}\right) \\ &- \log_2\left(1+\frac{\beta_2 s_6}{(1-\beta_1)s_7+(1-\beta_2)s_8+\sigma_e^2}\right). \end{aligned} \tag{4.80}$$

In what follows, let us consider two cases: $\beta_2 \neq \beta_2$ (different, 2D) and $\beta_1 = \beta_2$ (equal, 1D), which are called 2D-ES and 1D-ES, respectively.

4.4.2 2D-ES and 1D-ES PA Strategies

In this section, we first consider the case of $\beta_1 \neq \beta_2$, the 2D PA optimization problem in (4.78) can be recasted as

$$\max_{\beta_1,\beta_2} \quad R(\beta_1,\beta_2) = R_a + R_b - R_e \tag{4.81a}$$

$$\text{s.t.} \quad 0 \le \beta_1 \le 1, 0 \le \beta_2 \le 1, \tag{4.81b}$$

$$\beta_1 \ne \beta_2. \tag{4.81c}$$

Clearly, the above objective function is a non-concave function. Due to its three constraints, it is hard to obtain its closed-form solution. It is natural to use a 2D-ES algorithm to find its approximate solution over the 2D domain $[0, 1] \times [0, 1]$.

To reduce the computational complexity of the above 2D-ES algorithm and consider the symmetry of two-way network, β_1 is taken to be equal to β_2. Let us define $\beta_1 = \beta_2 = \beta$, then (4.78) reduces to

$$\max_{\beta} \quad R(\beta) = \log_2 \frac{Q_1}{Q_2} \tag{4.82a}$$

$$\text{s.t.} \quad 0 \le \beta_1, \beta_2 \le 1, \tag{4.82b}$$

where

$$\begin{aligned} Q_1 = &((s_1 - s_2)\beta + s_2 + \sigma_a^2)((s_3 - s_4)\beta + s_4 + \sigma_b^2) \\ &\cdot ((-s_7 - s_8)\beta + s_7 + s_8 + \sigma_e^2)^2, \end{aligned} \tag{4.83}$$

and

$$\begin{aligned} Q_2 = &(-s_2\beta + s_2 + \sigma_a^2)(-s_4\beta + s_4 + \sigma_b^2)((s_5 - s_7 - s_8)\beta \\ &+ s_7 + s_8 + \sigma_e^2)((s_6 - s_7 - s_8)\beta + s_7 + s_8 + \sigma_e^2). \end{aligned} \tag{4.84}$$

According to the derivation of Appendix 4.6 and (4.82) is equivalent to solving the following sixth-order polynomial

$$f(\beta) = \beta^6 + \alpha_1\beta^5 + \alpha_2\beta^4 + \alpha_3\beta^3 + \alpha_4\beta^2 + \alpha_5\beta + \alpha_6 = 0 \tag{4.85}$$

with the constraint $\beta \in [0, 1]$.

4.4.3 Proposed HICF PA Strategy

To the best of our knowledge, there is no closed-form expression for roots of a general polynomial with order more than four in (4.85). In what follows, we will propose a HICF method to solve this polynomial, and its basic idea is as follows: the Newton-Raphson algorithm in [41] is first employed twice to reduce its order from six to four with two candidate roots be computed iteratively, and the remaining

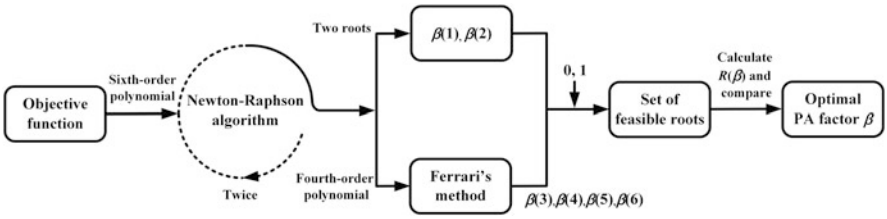


Fig. 4.3 Diagram for HICF power allocation strategy

four candidate roots can be obtained by the Ferrari's method. The more detailed procedure are sketched in Fig. 4.3.

Let us begin with the initialization of the Newton-Raphson method:

$$f_1(\beta) = \beta^6 + \alpha_1\beta^5 + \alpha_2\beta^4 + \alpha_3\beta^3 + \alpha_4\beta^2 + \alpha_5\beta + \alpha_6, \tag{4.86}$$

and its derivative

$$\begin{aligned} g_1(\beta) &= \frac{\partial f_1(\beta)}{\partial \beta} \\ &= 6\beta^5 + 5\alpha_1\beta^4 + 4\alpha_2\beta^3 + 3\alpha_3\beta^2 + 2\alpha_4\beta + \alpha_5. \end{aligned} \tag{4.87}$$

The iterative step of Newton-Raphson algorithm is as follows

$$\beta^{p+1} = \beta^p - \frac{f_1(\beta^p)}{g_1(\beta^p)}, \tag{4.88}$$

where p is the number of iterations, and setting the initial value $\beta^0 = 0.5$. Repeating the above iterate process until $|\beta^{p+1} - \beta^p| \leq 10^{-5}$ yields the first root $\beta(1)$, and (4.85) is decomposed as a product of an one-order factor and one fifth-order factor as follows

$$(\beta - \beta(1))(\beta^5 + \bar{\alpha}_1\beta^4 + \bar{\alpha}_2\beta^3 + \bar{\alpha}_3\beta^2 + \bar{\alpha}_4\beta + \bar{\alpha}_5) = 0, \tag{4.89}$$

where

$$\bar{\alpha}_1 = \alpha_1 + \beta(1),\ \bar{\alpha}_2 = \alpha_2 + \beta(1)\bar{\alpha}_1,\ \bar{\alpha}_3 = \alpha_3 + \beta(1)\bar{\alpha}_2, \tag{4.90a}$$

$$\bar{\alpha}_4 = \alpha_4 + \beta(1)\bar{\alpha}_3,\ \bar{\alpha}_5 = \alpha_5 + \beta(1)\bar{\alpha}_4. \tag{4.90b}$$

The remaining five roots of (4.85) can be found by solving the roots of fifth-order polynomial

$$\beta^5 + \bar{\alpha}_1\beta^4 + \bar{\alpha}_2\beta^3 + \bar{\alpha}_3\beta^2 + \bar{\alpha}_4\beta + \bar{\alpha}_5 = 0, \tag{4.91}$$

which is higher in order than four. We still need to use the Newton-Raphson algorithm one time. Let us define the objective function and its derivative as

$$f_2(\beta) = \beta^5 + \bar{\alpha}_1\beta^4 + \bar{\alpha}_2\beta^3 + \bar{\alpha}_3\beta^2 + \bar{\alpha}_4\beta + \bar{\alpha}_5, \tag{4.92}$$

and

$$g_2(\beta) = \frac{\partial f_2(\beta)}{\partial \beta} = 5\beta^4 + 4\bar{\alpha}_1\beta^3 + 3\bar{\alpha}_2\beta^2 + 2\bar{\alpha}_3\beta + \bar{\alpha}_4, \tag{4.93}$$

respectively. To avoid the increase of computational complexity caused by repeated search, we define a new reduced search domain initial value $(0, 0.5) \cup (\beta(1), 1)$, and the initial value β^0 is randomly chosen in this interval. Repeating the procession of computing $\beta(1)$ in (4.88), a root $\beta(2)$ of (4.91) is obtained in the same manner, which is the second root of (4.85). Making use of the values of $\beta(1)$ and $\beta(2)$, (4.85) has the following decomposition form

$$(\beta - \beta(1))(\beta - \beta(2))(\beta^4 + \hat{\alpha}_1\beta^3 + \hat{\alpha}_2\beta^2 + \hat{\alpha}_3\beta + \hat{\alpha}_4) = 0, \tag{4.94}$$

where

$$\hat{\alpha}_1 = \bar{\alpha}_1 + \beta(2),\ \hat{\alpha}_2 = \bar{\alpha}_2 + \beta(2)\hat{\alpha}_1, \tag{4.95a}$$

$$\hat{\alpha}_3 = \bar{\alpha}_3 + \beta(2)\hat{\alpha}_2,\ \hat{\alpha}_4 = \bar{\alpha}_4 + \beta(2)\hat{\alpha}_3. \tag{4.95b}$$

Now, the two roots of (4.85) have been found. The problem of finding the remaining solutions can be converted to the one of solving the roots of the fourth-order polynomial as follows

$$\beta^4 + \hat{\alpha}_1\beta^3 + \hat{\alpha}_2\beta^2 + \hat{\alpha}_3\beta + \hat{\alpha}_4 = 0. \tag{4.96}$$

According to the Ferrari's method [42], the roots of (4.96) is given by

$$\beta(3:6) = -\frac{\hat{\alpha}_1}{4} \pm_s \frac{\eta_1}{2} \pm_i \frac{\eta_2}{2}, \tag{4.97}$$

where two $\pm_s$ have the same sign, while the sign of $\pm_i$ is independent,

$$\gamma_1 = \frac{1}{3}(3\hat{\alpha}_1\hat{\alpha}_3 - 12\hat{\alpha}_4 - \hat{\alpha}_2^2), \tag{4.98a}$$

$$\gamma_2 = \frac{1}{27}(-2\hat{\alpha}_2^3 + 9\hat{\alpha}_1\hat{\alpha}_2\hat{\alpha}_3 + 72\hat{\alpha}_2\hat{\alpha}_4 - 27\hat{\alpha}_3^2 - 27\hat{\alpha}_1^2\hat{\alpha}_4), \tag{4.98b}$$

$$\gamma_3 = \frac{\hat{\alpha}_2}{3} + \sqrt[3]{-\frac{\gamma_2}{2} + \sqrt{\frac{\gamma_2^2}{4} + \frac{\gamma_1^3}{27}}} + \sqrt[3]{-\frac{\gamma_2}{2} - \sqrt{\frac{\gamma_2^2}{4} + \frac{\gamma_1^3}{27}}}, \tag{4.98c}$$

$$\eta_1 = \sqrt{\frac{\hat{\alpha}_1^2}{4} - \hat{\alpha}_2 + \gamma_3}, \tag{4.98d}$$

$$\eta_2 = \sqrt{\frac{3}{4}\hat{\alpha}_1^2 - \eta_1^2 - 2\hat{\alpha}_2 \pm_s \frac{1}{4\eta_1}(4\hat{\alpha}_1\hat{\alpha}_2 - 8\hat{\alpha}_3 - \hat{\alpha}_1^3)}. \tag{4.98e}$$

At this point, all roots of the sixth-order polynomial in (4.85) have been found completely. Then we have the set of all candidates for the optimal PA factor as

$$S_{PA} = \{\beta(1), \beta(2), \beta(3), \beta(4), \beta(5), \beta(6), 0, 1\}. \tag{4.99}$$

The set of optimal values of β is chosen from set S_{PA} with two constraints: (1) falling in the interval [0, 1]; (2) maximizing the SSR.

4.5 Simulation Results and Discussions

In this section, we make an evaluation on the performance of the proposed two transmit beamforming methods and one PA algorithm. System parameters are given as follows: $P_a = P_b = 27\text{dBm}$, $N_a = N_b = N_e = 8$, $M = 100$, $d = \lambda/2$, $\beta_1 = \beta_2 = 0.9$, $d_{ai_1} = d_{ai_2} = 30\text{m}$, $d_{ab} = d_{ae} = 80\text{m}$, $\theta_{t,ai_1} = \pi/8$, $\theta_{t,ai_2} = 7\pi/8$, $\theta_{t,ae} = 4\pi/9$, $\theta_{t,ab} = 5\pi/9$, $\sigma_a^2 = \sigma_b^2 = 2\sigma_e^2$. The path loss coefficient is defined as $g_{tr} = \frac{\alpha}{d_{tr}^c}$, where α is the path loss at reference distance d_0, d_{tr} denotes the distance between the transmitter and receiver, and c is the path loss exponent.

In what follows, three schemes will be used as performance benchmarks:

1. Case I: **No IRS**: $\boldsymbol{\Theta}_1$=$\boldsymbol{\Theta}_2$=$\mathbf{0}_{M\times M}$.
2. Case II: **IRS with random phase**: Phase of each element of both $\boldsymbol{\Theta}_1$ and $\boldsymbol{\Theta}_2$ is uniformly and independently generated from the interval [0,2π).
3. Case III: **IRS-1/IRS-2**: let us set the phase-shifting matrix of one and only one of IRS-2 and IRS-1 as zero matrix.

Figure 4.4 demonstrates the curves of SSR versus transmit power P with $P = P_a = P_b$ and no IRS as a SSR performance benchmark. It can be seen from this figure that the proposed two methods Max-SV and Max-SLNR double and triple the SSR of no IRS at $M = 100$ and $M = 500$, respectively. This means that double-IRS can bring a significant SSR improvement.

Figure 4.5 plots the curves of SSR versus the number M of IRS phase-shifting elements for $d_{ai_1} = d_{ai_2} = 40\,\text{m}$ and $N_a = N_b = N_e = 16$, where no IRS and random phase are used as performance benchmarks. Observing this figure, it is apparent that given the transmit beamforming proposed Max-SV or Max-SLNR, the proposed GPG makes a significant SSR enhancement over no IRS and random phase in terms of SSR. Fixing the IRS phase-shifting method as GPG, the proposed Max-

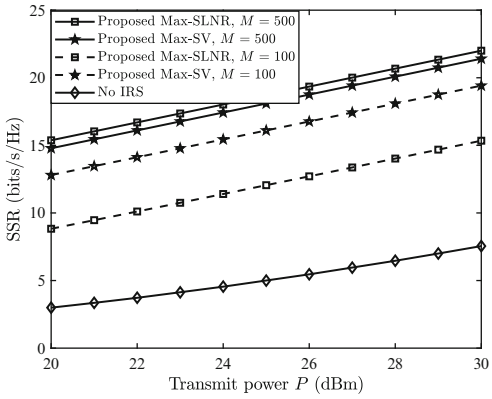


Fig. 4.4 Curves of SSR versus transmit power P for different M

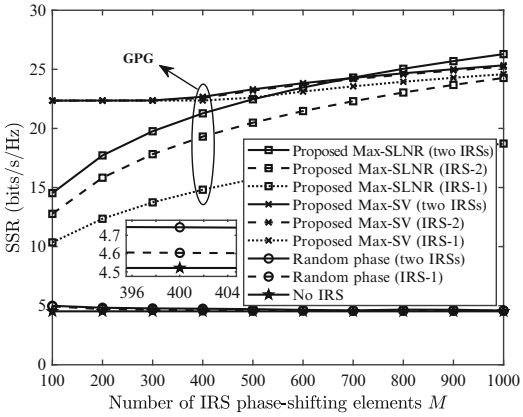


Fig. 4.5 Curves of SSR versus the number of IRS phase-shifting elements M ($d_{ab} = 70$ m)

SV outperforms the generalized Max-SLNR when the number of IRS elements is less than 700. Otherwise, there is a converse tendency. Additionally, as the number of IRS elements increases, the SSR performance of the proposed schemes grow gradually. Interestingly, even we close one of two IRSs, the performance gain achieved by two-IRS over single-IRS is also attractive.

To see the effect of distance on SSR, Fig. 4.6 plots the curves of SSR versus the number M of IRS phase-shifting elements by increasing d_{ab} from 70 to 200 m. Clearly, as d_{ab} increases, the SSR performance of all proposed methods degrades, but there is a similar performance tendency among those proposed methods.

Figure 4.7 illustrates the curved surface of SSR versus the PA factors β_1 and β_2 of the 2D-ES method where the GPG and Max-SV are used for the IRS phase-shifting and transmit beamforming method. As we can seen in the Fig. 4.7, the SSR performance first improves with increasing in PA factors and then decreases dramatically when reaching the optimal point. It seems the optimal values of β_1 and β_2 are near one.

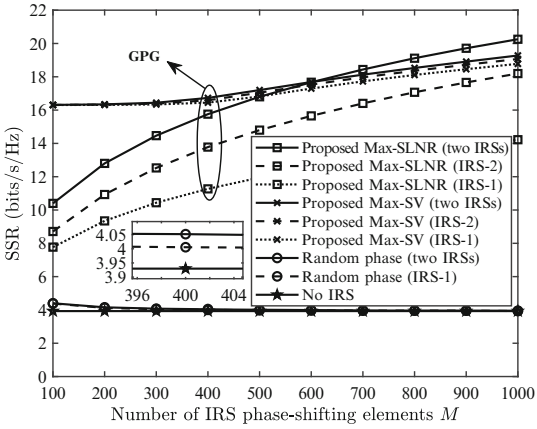


Fig. 4.6 Curves of SSR versus the number of IRS phase-shifting elements M ($d_{ab} = 200$ m)

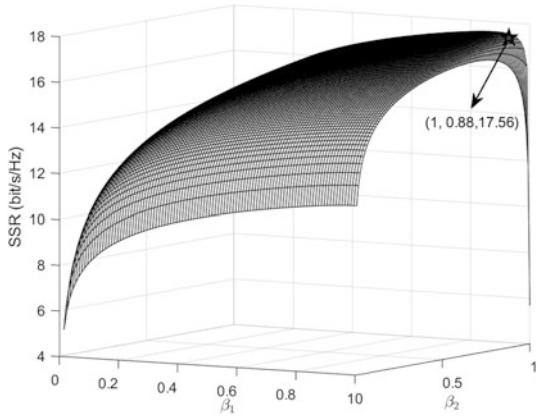


Fig. 4.7 Curved surface of SSR versus the β_1 and β_2

Figure 4.8 depicts the curves of the SSR versus the PA factor β for Max-SV method, and the equal PA is used as a benchmark. It can be seen that 1D-ES and HICF have approximate SSRs for both cases of M =128 and 1024. In particularly, observing this figure, we also find the fact that the SSR is a concave function of β. In other words, there is one unique extremum in the interval [0,1].

Figure 4.9 depicts the histograms of the SSR of the proposed HICF versus the number of IRS phase-shifting elements M for Max-SV method with 2D-ES and EPA as performance benchmarks. At M =128, the proposed HICF and 2D-ES can achieve up to 10% performance gain over EPA. As the number of IRS phase-shifting elements varies from 128 to 2048, the gain shows a slight reduction accordingly.

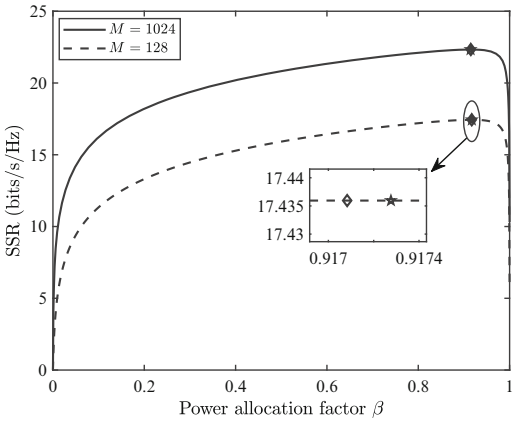


Fig. 4.8 Curves of SSR versus the PA factor β

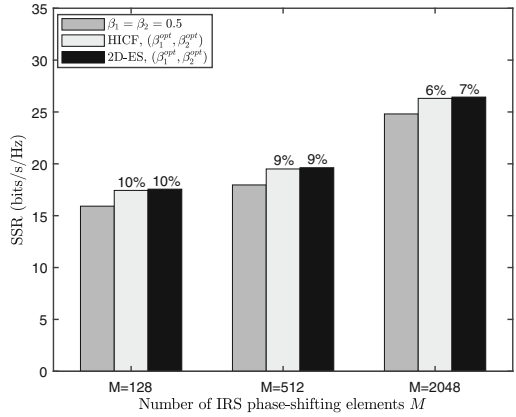


Fig. 4.9 Histograms of SSR versus the number of IRS phase-shifting elements M

4.6 Conclusion

In this book chapter, we have made an investigation of transmit beamforming and PA for a double-IRS-aided two-way DM system. With the help of two IRSs, useful controllable multipaths between Alice and Bob can be established. First, the IRS phase-shifting was designed by the GPG criterion. Then the Max-SV transmit beamforming method was proposed, and the Max-SLNR transmit beamforming method is generalized. Finally, a HICF PA algorithm is proposed to enhance the SSR performance with a reduced computational complexity compared with 1D-ES and 2D-ES. From simulation, we can find that the proposed Max-SV and generalized leakage methods approximately triple the SSRs of random phase and no IRS.

Furthermore, the proposed HICF method can provide about a 10% SSR gain over EPA and achieve the same value of SSR as 2D-ES and 1D-ES with a significant reduction in computational complexity. The proposed system and methods may be applied to the future wireless networks like marine communications, UAV network, satellite communications, even 6G.

Appendix

In Appendix, we will show how to derive (4.85) from (4.82). By a further simplification, the objective function of (4.82) can be rewritten in a new simple form

$$R(\beta) = \log_2 \frac{q_1\beta^4 + q_2\beta^3 + q_3\beta^2 + q_4\beta + q_5}{q_6\beta^4 + q_7\beta^3 + q_8\beta^2 + q_9\beta + q_{10}}, \tag{4.100}$$

where

$$q_1 = (s_1 - s_2)(s_3 - s_4)(-s_7 - s_8)^2, \tag{4.101a}$$

$$q_2 = 2(s_1 - s_2)(s_3 - s_4)(-s_7 - s_8)(s_7 + s_8 + \sigma_e^2) + \big[(s_1 - s_2)(s_4 + \sigma_b^2) + (s_3 - s_4)(s_2 + \sigma_a^2)\big](-s_7 - s_8)^2, \tag{4.101b}$$

$$q_3 = (s_1 - s_2)(s_3 - s_4)(s_7 + s_8 + \sigma_e^2)^2 + 2(-s_7 - s_8)(s_7 + s_8 + \sigma_e^2)\big[(s_1 - s_2)\cdot (s_4 + \sigma_b^2) + (s_3 - s_4)(s_2 + \sigma_a^2)\big] + (-s_7 - s_8)^2(s_2 + \sigma_a^2)(s_4 + \sigma_b^2), \tag{4.101c}$$

$$q_4 = \big[(s_1 - s_2)(s_4 + \sigma_b^2) + (s_3 - s_4)(s_2 + \sigma_a^2)\big](s_7 + s_8 + \sigma_e^2)^2 + 2(-s_7 - s_8)\cdot (s_2 + \sigma_a^2)(s_4 + \sigma_b^2)(s_7 + s_8 + \sigma_e^2), \tag{4.101d}$$

$$q_5 = (s_2 + \sigma_a^2)(s_4 + \sigma_b^2)(s_7 + s_8 + \sigma_e^2)^2, \tag{4.101e}$$

$$q_6 = s_2 s_4 (s_5 - s_7 - s_8)(s_6 - s_7 - s_8), \tag{4.101f}$$

$$q_7 = s_2 s_4 (s_5 + s_6 - 2s_7 - 2s_8)(s_7 + s_8 + \sigma_e^2) + (s_5 - s_7 - s_8)(s_6 - s_7 - s_8)\cdot \big[-s_2(s_4 + \sigma_b^2) - s_4(s_2 + \sigma_a^2)\big], \tag{4.101g}$$

$$q_8 = s_2 s_4 (s_7 + s_8 + \sigma_e^2)^2 + (s_5 + s_6 - 2s_7 - 2s_8)(s_7 + s_8 + \sigma_e^2)\big[-s_2(s_4 + \sigma_b^2) - s_4(s_2 + \sigma_a^2)\big] + (s_5 - s_7 - s_8)(s_6 - s_7 - s_8)(s_2 + \sigma_a^2)(s_4 + \sigma_b^2), \tag{4.101h}$$

$$q_9 = [-s_2(s_4 + \sigma_b^2) - s_4(s_2 + \sigma_a^2)](s_7 + s_8 + \sigma_e^2)^2 + (s_5 + s_6 - 2s_7 - 2s_8)\cdot (s_7 + s_8 + \sigma_e^2)(s_2 + \sigma_a^2)(s_4 + \sigma_b^2), \tag{4.101i}$$

$$q_{10} = (s_2 + \sigma_a^2)(s_4 + \sigma_b^2)(s_7 + s_8 + \sigma_e^2)^2. \tag{4.101j}$$

Let us define

$$\phi(\beta) = \frac{q_1\beta^4 + q_2\beta^3 + q_3\beta^2 + q_4\beta + q_5}{q_6\beta^4 + q_7\beta^3 + q_8\beta^2 + q_9\beta + q_{10}}, \tag{4.102}$$

then taking the derivative of function $R(\beta)$ with respect to β and setting it equal zero give

$$R^{'}(\beta) = \frac{\partial R(\beta)}{\partial \beta} = \frac{1}{\text{In2} \cdot \phi(\beta)} \phi^{'}(\beta) = 0. \tag{4.103}$$

Considering $\phi(\beta) \neq 0$, (4.103) reduces to

$$\phi^{'}(\beta) = 0, \tag{4.104}$$

which means that

$$\begin{aligned}&(4q_1\beta^3 + 3q_2\beta^2 + 2q_3\beta + q_4)(q_6\beta^4 + q_7\beta^3 + q_8\beta^2 + q_9\beta + q_{10}) - \\ &(q_1\beta^4 + q_2\beta^3 + q_3\beta^2 + q_4\beta + q_5)(4q_6\beta^3 + 3q_7\beta^2 + 2q_8\beta + q_9) = 0,\end{aligned} \tag{4.105}$$

which can be further simplified to

$$\begin{aligned}&(q_1q_7 - q_2q_6)\beta^6 + (2q_1q_8 - 2q_3q_6)\beta^5 + (3q_1q_9 + q_2q_8 \\ &- q_3q_7 - 3q_4q_6)\beta^4 + (4q_1q_{10} + 2q_2q_9 - 2q_4q_7 - 4q_5q_6)\beta^3 \\ &+ (3q_2q_{10} + q_3q_9 - q_4q_8 - 3q_5q_7)\beta^2 + (2q_3q_{10} - 2q_5q_8)\beta \\ &+ (q_4q_{10} - q_5q_9) = 0.\end{aligned} \tag{4.106}$$

Notice that (4.106) is a sixth-order polynomial since $q_1q_7 - q_2q_6 \neq 0$, let us define

$$\alpha_1 = (2q_1q_8 - 2q_3q_6)/(q_1q_7 - q_2q_6), \tag{4.107a}$$

$$\alpha_2 = (3q_1q_9 + q_2q_8 - q_3q_7 - 3q_4q_6)/(q_1q_7 - q_2q_6), \tag{4.107b}$$

$$\alpha_3 = (4q_1q_{10} + 2q_2q_9 - 2q_4q_7 - 4q_5q_6)/(q_1q_7 - q_2q_6), \tag{4.107c}$$

$$\alpha_4 = (3q_2q_{10} + q_3q_9 - q_4q_8 - 3q_5q_7)/(q_1q_7 - q_2q_6), \tag{4.107d}$$

$$\alpha_5 = (2q_3q_{10} - 2q_5q_8)/(q_1q_7 - q_2q_6), \tag{4.107e}$$

$$\alpha_6 = (q_4q_{10} - q_5q_9)/(q_1q_7 - q_2q_6). \tag{4.107f}$$

which means

$$f(\beta) = \beta^6 + \alpha_1\beta^5 + \alpha_2\beta^4 + \alpha_3\beta^3 + \alpha_4\beta^2 + \alpha_5\beta + \alpha_6 = 0. \tag{4.108}$$

This completes the derivation of (4.85).

References

1. Shiu, Y.S., Chang, S.Y., Wu, H.C., Huang, S.C.H., Chen, H.H.: Physical layer security in wireless networks: a tutorial. IEEE Wireless Commun. **18**(2), 66–74 (2011)
2. Larsson, E.G., Edfors, O., Tufvesson, F., Marzetta, T.L.: Massive MIMO for next generation wireless systems. IEEE Commun. Mag. **52**(2), 186–195 (2014)
3. Akdeniz, M.R., Liu, Y., Samimi, M.K., Sun, S., Rangan, S., Rappaport, T.S., Erkip, E.: Millimeter wave channel modeling and cellular capacity evaluation. IEEE J. Sel. Areas Commun. **32**(6), 1164–1179 (2014)
4. Mukherjee, A.: Physical-layer security in the internet of things: sensing and communication confidentiality under resource constraints. Proc. IEEE **103**(10), 1747–1761 (2015)
5. Ai, Y., Mathur, A., Cheffena, M., Bhatnagar, M.R., Lei, H.: Physical layer security of hybrid satellite-FSO cooperative systems. IEEE Photon. J. **11**(1), 1–15 (2019)
6. Chen, X., Ng, D.W.K., Gerstacker, W.H., Chen, H.H.: A survey on multiple-antenna techniques for physical layer security. IEEE Commun. Surv. Tutor. **19**(2), 1027–1053 (2017)
7. Wu, Y., Khisti, A., Xiao, C., Caire, G., Wong, K.K., Gao, X.: A survey of physical layer security techniques for 5G wireless networks and challenges ahead. IEEE J. Sel. Areas Commun. **36**, 679–695 (2018)
8. Zou, Y., Sun, M., Zhu, J., Guo, H.: Security-reliability tradeoff for distributed antenna systems in heterogeneous cellular networks. IEEE Trans. Wireless Commun. **17**(12), 8444–8456 (2018)
9. Babakhani, A., Rutledge, D.B., Hajimiri, A.: Transmitter architectures based on near-field direct antenna modulation. IEEE J. Solid-State Circuits. **43**(12), 2674–2692 (2008)
10. Daly, M.P., Bernhard, J.T.: Directional modulation technique for phased arrays. IEEE Trans. Antennas Propag. **57**(9), 2633–2640 (2009)
11. Daly, M.P., Daly, E.L., Bernhard, J.T.: Demonstration of directional modulation using a phased array. IEEE Trans. Antennas Propag. **58**(5), 1545–1550 (2010)
12. Daly, M.P., Bernhard, J.T.: Beamsteering in pattern reconfigurable arrays using directional modulation. IEEE Trans. Antennas Propag. **58**(5), 2259–2265 (2010)
13. Hong, T., Song, M.Z., Liu, Y.: Dual-beam directional modulation technique for physical-layer secure communication. IEEE Antennas Wireless Propag. Lett. **10**, 1417–1420 (2011)
14. Wan, S., Shu, F., Lu, J., Gui, G., Wang, J., Xia, G., Zhang, Y., Li, J., Jiangzhou, W.: Power allocation strategy of maximizing secrecy rate for secure directional modulation networks. IEEE Access. **6**, 38794–38800 (2018)
15. Teng, Y., Li, J., Huang, M., Liu, L., Xia, G., Zhou, X., Shu, F., Wang, J., You, X.: Low-complexity and high-performance receive beamforming for secure directional modulation networks against an eavesdropping-enabled full-duplex attacker. Sci China Inf. Sci. **65**(1), 119302–119302 (2022)
16. Shu, F., Qin, Y., Liu, T., Gui, L., Zhang, Y., Li, J., Han, Z.: Low-complexity and high-resolution DOA estimation for hybrid analog and digital massive MIMO receive array. IEEE Trans. Commun. **66**(6), 2487–2501 (2018)
17. Zhuang, Z., Xu, L., Li, J., Hu, J., Sun, L., Shu, F., Wang, J.: Machine-learning-based high-resolution DOA measurement and robust directional modulation for hybrid analog-digital massive MIMO transceiver. Sci. China Inf. Sci. **63**, 1–18 (2020)

18. Hu, J., Shu, F., Li, J.: Robust synthesis method for secure directional modulation with imperfect direction angle. IEEE Commun. Lett. **20**(6), 1084–1087 (2016)
19. Hu, J., Yan, S., Shu, F., Wang, J., Li, J., Zhang, Y.: Artificial-noise-aided secure transmission with directional modulation based on random frequency diverse arrays. IEEE Access. **5**, 1658–1667 (2017)
20. Shu, F., Wu, X., Hu, J., Li, J., Chen, R., Wang, J.: Secure and precise wireless transmission for random-subcarrier-selection-based directional modulation transmit antenna array. IEEE J. Sel. Area Commun. **36**(4), 890–904 (2018)
21. Qiu, B., Tao, M., Wang, L., Xie, J., Wang, Y.: Multi-beam directional modulation synthesis scheme based on frequency diverse array. IEEE Trans. Inf. Forensics Secur. **14**(10), 2593–2606 (2019)
22. Cheng, Q., Wang, S., Fusco, V., Wang, F., Zhu, J., Gu, C.: Physical-layer security for frequency diverse array-bbased directional modulation in fluctuating two-ray fading channels. IEEE Trans. Wireless Commun. **20**(7), 4190–4204 (2021)
23. Wu, Q., Zhang, R.: Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming. IEEE Trans. Wireless Commun. **18**(11), 5394–5409 (2019)
24. Pan, C., Ren, H., Wang, K., Xu, W., Elkashlan, M., Nallanathan, A., Hanzo, L.: Multicell MIMO communications relying on intelligent reflecting surfaces. IEEE Trans. Wireless Commun. **19**(8), 5218–5233 (2020)
25. Tang, W., Chen, M.Z., Chen, X., Dai, J.Y., Han, Y., Renzo, M.D., Zeng, Y., Jin, S., Cheng, Q., Cui, T.J.: Wireless communications with reconfigurable intelligent surface: path loss modeling and experimental measurement. IEEE Trans. Wireless Commun. **20**(1), 421–439 (2021)
26. Shi, W., Zhou, X., Jia, L., Wu, Y., Shu, F., Wang, J.: Enhanced secure wireless information and power transfer via intelligent refecting surface. IEEE Commun. Lett. **70**(2), 1084–1088 (2020)
27. Shen, H., Ding, T., Xu, W., Zhao, C.: Beamforming design with fast convergence for IRS-aided full-duplex communication. IEEE Commun. Lett. **24**(12), 2849–285 (2020)
28. Wang, X., Shu, F., Shi, W., Liang, X., Dong, R., Li, J., Wang, J.: Beamforming design for IRS-aided decode-and-forward relay wireless network. IEEE Trans. Green Commun. Netw. **6**(1), 198–207 (2022)
29. Zheng, B., You, C., Zhang, R.: Double-IRS assisted multi-user MIMO: cooperative passive beamforming design. IEEE Trans. Wireless Commun. **20**(7), 4513–4526 (2021)
30. Tian, G., Song, R.: Cooperative beamforming for a double-IRS-assisted wireless communication system. Eurasip J. Adv. Sig. Pr. **67**, 1–10 (2021)
31. Guan, X., Wu, Q., Zhang, R.: Intelligent reflecting surface assisted secrecy communication: is artificial noise helpful or not? IEEE Wireless Commun. Lett. **9**(6), 778–782 (2020)
32. Wang, H.M., Bai, J., Dong, L.: Intelligent reflecting surfaces assisted secure transmission without eavesdropper's CSI. IEEE Signal Process. Lett. **27**, 1300–1304 (2020)
33. Hong, S., Pan, C., Ren, H., Wang, K., Nallanathan, A.: Artificial-noise-aided secure MIMO wireless communications via intelligent reflecting surface. IEEE Trans. Commun. **68**(12), 7851–7866 (2020)
34. Shu, F., Yang, L., Jiang, X., Cai, W., Shi, W., Huang, M., Wang, J., You, X.: Beamforming and transmit power design for intelligent reconfigurable surface-aided secure spatial modulation. IEEE J-STSP. **66**(5), 933–949 (2022)
35. Zhou, G., Pan, C., Ren, H., Wang, K., Peng, Z.: Secure wireless communication in RIS-aided MISO system with hardware impairments. IEEE Wireless Commun. Lett. **10**(6), 1309–1313 (2021)
36. Shu, F., Teng, Y., Li, J., Huang, M., Shi, W., Li, J., Wu, Y., Wang, J.: Enhanced secrecy rate maximization for directional modulation networks via IRS. IEEE Trans. Commun. **69**(12), 8388–8401 (2021)
37. Lai, L., Hu, J., Cen, Y., Zheng, H., Yang, N.: Directional modulation-enabled secure transmission with intelligent reflecting surface. In: 3rd IEEE International Conference on Information Communication and Signal Processing (ICICSP 2020), pp. 450–453 (2020)

38. Tarighat, A., Sadek, M., Sayed, A.H.: A multi user beamforming scheme for downlink MIMO channels based on maximizing signal-to-leakage ratios. IEEE Int. Conf. Acoust. Speech Signal Process. **3**, 1129–1132 (2005)
39. Sadek, M., Tarighat, A., Sayed, A.H.: A leakage-based precoding scheme for downlink multi-user MIMO channels. IEEE Trans. Wireless Commun. **6**(5), 1711–1721 (2007)
40. Horn, R.A., Johnson, C.R.: Matrix Analysis. Cambridge University Press, Cambridge (1987)
41. Wasserman, L.: All of Statistics. Springer, Pittsburgh (2003)
42. Cardano, G.: The Rules of Algebra: (ARS magna). Dover, New York (2007)

Chapter 5
Beamforming and Transmit Power Design for Intelligent Reconfigurable Surface-Aided Secure Spatial Modulation

In this book chapter, an IRS-aided SSR is proposed, where the IRS perform passive beamforming and information transfer simultaneously by adjusting the on-off states of the reflecting elements. We formulate an optimization problem to maximize the average SR by jointly optimizing the passive beamforming at IRS and the transmit power at transmitter under the consideration that the direct pathes channels from transmitter to receivers are obstructed by obstacles. As the expression of SR is complex, we derive a newly fitting expression (NASR) for the expression of traditional approximate SR (TASR), which has simpler closed-form and more convenient for subsequent optimization. Based on the above two fitting expressions, three beamforming methods, called maximizing NASR via successive convex approximation (Max-NASR-SCA), maximizing NASR via dual ascent (Max-NASR-DA) and maximizing TASR via semi-definite relaxation (Max-TASR-SDR) are proposed to improve the SR performance. Additionally, two transmit power design (TPD) methods are proposed based on the above two approximate SR expressions, called Max-NASR-TPD and Max-TASR-TPD. Simulation results show that the proposed Max-NASR-DA and Max-NASR-SCA IRS beamformers harvest substantial SR performance gains over Max-TASR-SDR. For TPD, the proposed Max-NASR-TPD performs better than Max-TASR-TPD. Particularly, the Max-NASR-TPD has a closed-form solution.

5.1 Introduction

As a MIMO transmission scheme, SM exhibits a range of advantages and it has been recognized as a promising transmission option for MIMO systems [1]. The concept of SM was first proposed in [2] whose main idea was to carry additive bit information via antenna indices [3]. Different from the two typical forms of MIMO, Bell Laboratories Layer Space-Time (BLAST) [4] and space time coding (STC)

F. Shu, J. Wang, *Intelligent Reflecting Surface-Aided Physical-Layer Security*,
Wireless Networks, https://doi.org/10.1007/978-3-031-41812-9_5

[5], SM may strike a good balance between spatial multiplexing and diversity and is called the third way between BLAST and STC. Compared to BLAST and STC, SM becomes more attractive due to its advantages of no inter-channel interference (ICI), inter-antenna synchronization (IAS) [6] and the use of less active RF chains. Thus, it is also a green wireless transmission technique.

However, for such an SM system, due to the broadcast nature of wireless channel, like other MIMO systems, it is very possible that the confidential messages are intercepted by unintended receivers. As how to achieve a secure transmission is becoming a hot research topic in wireless networks, physical layer security [7, 8] in MIMO systems has been widely investigated. There are several ways to improve the performance of SM including transmit antenna selection [9–13], linear precoding [14, 15], power allocation [16, 17] and so on. In [18], the author enhanced the legitimate security by jointly precoding optimization with and without eavesdropping CSI. In [19, 20], the authors proposed a joint precoding optimization scheme which applies nonlinear energy harvesting (EH) model. Several transmitter precoding methods were proposed in [21] to increase the cut-off rate of SM systems. In [22, 23], security was enhanced by emitting the AN onto the null-space of the desired channel and the latter derived the closed-form approximated expression of ergodic secrecy rate (ESR) in perfect and imperfect CSI, respectively. In [24], the authors proposed three precoding methods and five transmit antenna subarray selection methods to improve the security performance under the hybrid SM systems. Additionally, the authors in [25] considered the malicious attacks from the eavesdropper and proposed several effective beamforming methods to eliminate the interference from eavesdropper.

As a matter of fact, the IRS has emerged as a revolutionary technology for improving the coverage and energy/spectrum efficiency of future wireless communications [26].

Specifically, IRS consists of a large number of small, low-cost, and passive elements of only reflecting the incident signal with an adjustable phase shift without complex precoding and radio frequency processing. Equipped with a smart controller, the IRS is able to intelligently adjust the phases of incident electromagnetic waves to increase the received signal energy, expand the coverage region, and alleviate interference, so as to enhance the communication quality of wireless networks.

There have been several innovative studies on the IRS-assisted wireless communication systems by jointly optimizing the beamforming vector and the phase shifts at the IRS [27–31]. An IRS-aided secure wireless information and power transfer (SWIPT) system was studied in [27], and the authors adopted the SDR and alternating optimization algorithm to maximize the harvested power. Additionally, multigroup and multicell MIMO communications were studied in [28, 31], respectively, where the former proposed to invoke an IRS at the cell boundary of multiple cells to assist the downlink transmission to cell-edge users, and the latter jointly optimized the transmit beamformer, AN vector and phase shifts at the IRS for minimizing the transmit power at Alice subject to the secrecy rate constraints as well as the unit modulus constraints of IRS phase shifts. In [29], the authors jointly

optimized the precoding matrix at the BS, covariance matrix of AN and phase shifts at the IRS for maximizing SR under the consideration of an AN-aided secure MIMO system. [31] considered the fairness among cell-edge users, and the authors aimed at maximizing the minimum achievable rate of cell-edge users by jointly optimizing the transmit beamforming at the BSs and the phase shifts at the IRS.

As mentioned above, SM is a special MIMO technology of activating one transmit antenna with one transmit antenna and exploits the index of the active antenna for information transfer. The undeniable potential of both SM and IRS based communication schemes has attracted more and more attention nowadays. The concept of IRS-assisted communications was first brought to the realm of SM in [32]. In [33], the authors applied SM principle to the IRS by adjusting the ON (active) and OFF (inactive) status of each reflecting element. Therefore, the IRS can deliver additional information by adopting SM on the index of the reflecting elements. In [32], the authors investigated the IRS-aided receive SM (RSM) technique. Inspired by [32], the authors in [34] extended its structure to combine the transmit and receive antenna indices for joint spatial modulation by shaping the reflecting beam with IRS. It is worth mentioning that conventional SM cannot combine transmit SM (TSM) and RSM at the same time, due to the limitation of a single activated transmit antenna.

Prior works on IRS-aided SM systems are mainly focused on maximizing the received signal strength, achievable rate, spectral efficiency and outage probability which also showed that the IRS-aided SM system outperforms the conventional SM system. So far, there have been no study on the SR performance of IRS-assisted SSM system, which might be a potential way to make a significant improvement in SR performance. To investigate this issue, we propose an IRS-aided SSM (IRS-SSM) system. In this system, we activate a subset of the IRS elements for reflecting a beam towards the intended destination, while exploiting the index combination of the ON-state IRS elements to implicitly convey the spatial information of the IRS. Additionally, considered that the transmit channels from transmitter to receivers are blocked by obstacles, where the IRS is necessary for communication. As there exists an illegal receiver to eavesdrop on the confidential information, we optimize the beamforming at IRS and the transmit power at transmitter jointly to maximize SR. The main contributions of this book chapter are summarized as follows:

An IRS-aided secure SM system model is established, where the direct path channels in the communication system from transmitter to receivers are obstructed by obstacles. Additionally, the transmitter is equipped with a single antenna, the desired receiver and eavesdropping receiver are equipped with multiple antennas. Since the IRS elements have been divided into multiple subsets equally, the spatial bits are carried by activating one of the subsets of IRS rather than the transmitter/receiver antenna, while the APM symbols are reflected by the active IRS subset by adjusting the activated subset to ON state. Each IRS subset reflects single bit stream by using multiple reflecting elements with secure beamforming. This will create spatial diversity and will be exploited to improve the security performance of the IRS-SSM.

To improve the secrecy performance, we first formulate the optimization problem with the aim of maximizing secrecy rate subject to constraints of transmit power limit and unit modulus of IRS phase shifts. As the objective function is different from the traditional SSM, we rederive it in Sect. 5.2. Additionally, as the objective function does not have the closed-form expression, which increases the difficulty of subsequent optimization, we review the TASR expression and propose a NASR expression. Meanwhile, the NASR fits the secrecy rate curves well and has a simple closed-form expression, which facilitates further optimization work.

To improve the secrecy performance, three IRS beamforming methods, based on the above two fitting expressions, called Max-NASR-SCA, Max-NASR-DA and TASR via Max-TASR-SDR are proposed. Due to the fact that the NASR has simpler expression than the TASR, more effective algorithms are proposed to approach the optimal solution. Simulation results show that the secrecy rate performance of the proposed Max-NASR-DA is better than the proposed Max-TASR-SDR and the proposed Max-NASR-SCA. In particular, the proposed Max-NASR-SCA has a better secrecy rate performance than Max-TASR-SDR in the medium and high SNR regions.

In order to further improve the secrecy performance, two secure TPD methods are proposed based on the NASR expression and TASR expression, respectively. Max-NASR-TPD is proposed based on the NASR expression which has the sum of ratio form. Hence, we first transform the objective function from fractions to integrations by using the quadratic transform method. Then, by solving the KKT conditions of Lagrange functions, we have a closed-form solution towards the optimization problem with low complexity. For comparison, we propose Max-TASR- TPD based on the TASR expression. As the expression is complex, we adopt the gradient ascent method to solve it. Simulation results show that the proposed Max-NASR-TPD harvests a substantial SR performance gain over the Max-TASR-TPD.

Notations Boldface lower case and upper case letters denote vectors and matrices, respectively. $(\cdot)^H$ denotes the conjugate transpose operation. $\mathbb{E}\{\cdot\}$ represents expectation operation. $\|\cdot\|$ denotes 2-norm. $\hat{[\,]}$ represents the estimation operation. $\mathbf{A}'$ represents a matrix that is different from the original matrix $\mathbf{A}$ but has a linear transformation relationship with the original matrix.

5.2 System Model

5.2.1 IRS-Aided Secure Spatial Modulation System

As shown in Fig. 5.1, we consider a system where the transmitter (Alice), the legal receiver (Bob) and the eavesdropper (Eve) are equipped with single antenna, N_b and N_e antennas respectively. We further assume that the IRS consists of N low-cost passive reflecting elements. Meanwhile, we follow the hypothesis in [32] that

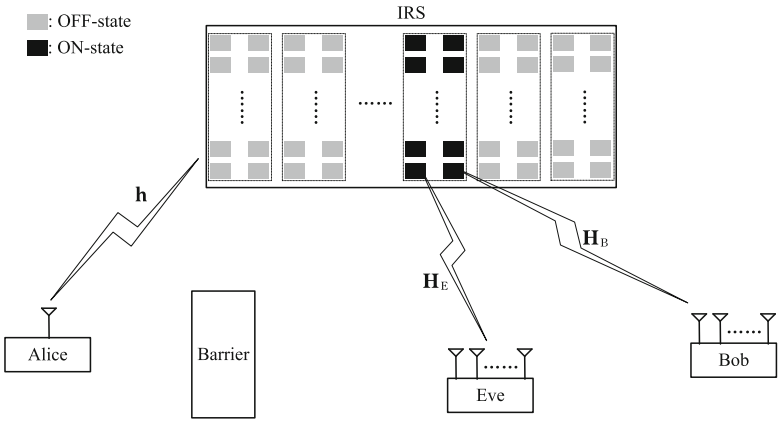


Fig. 5.1 System model for IRS-aided secure spatial modulation

the direct link between the transmitter and receiver is obstructed. In the following, the IRS reflects signal only one time.

Different from the traditional SM system, where the system adds spatial module to the transmitter or the receiver, the system in this book chapter adds spatial module to the IRS by adjusting the ON-OFF states of the reflecting elements. We adopt the IRS-elements grouping method, where a total number of N unit cell elements are divided into G groups, each of which consists of $\bar{N} = N/G$ adjacent elements and the reflection coefficient of each element in the same group is different. Specifically, for each symbol duration, one of G groups is randomly turned ON for reflecting the incident signals, and the remaining $(G-1)$ groups are deliberately turned OFF for realizing the SM scheme.

Accordingly, the transmission information is divided into two parts: the first one, denoted as $j \in \{1, 2, \cdots, M\}$, is modulated as an $\mathcal{M}$-ary quadrature amplitude modulation (QAM) or phase shifted keying (PSK) symbol, and the second one, $i \in \{1, 2, \cdots, G\}$ is used to activate the IRS subset $\mathcal{S}$. Therefore, the data rate of IRS-aided SM is expressed as

$$R = \log_2(M) + \log_2(G). \tag{5.1}$$

Additionally, the reflection coefficient vector of IRS is denoted as $\boldsymbol{\theta}_{N\times 1} \triangleq [\theta_1, \theta_2, \cdots, \theta_N]^T$, where $\theta_n = \beta_n e^{-j\phi_n}$, in which $\beta_n \in [0, 1]$ and $\phi_n \in (0, 2\pi]$ represent the common reflection amplitude and phase shift for the n-th reflection element. To ease the hardware design [32], the reflection amplitudes of the ON-state groups are set to the maximum value, i.e., $\beta_n = 1$. Meanwhile, let $\mathbf{h}_t = [\mathbf{t}_1, \mathbf{t}_2, \cdots, \mathbf{t}_G] \in \mathbb{C}^{1\times N}$, $\mathbf{H}_B = [\mathbf{B}_1, \mathbf{B}_2, \cdots, \mathbf{B}_G] \in \mathbb{C}^{N_b\times N}$, and $\mathbf{H}_E = [\mathbf{E}_1, \mathbf{E}_2, \cdots, \mathbf{E}_G] \in \mathbb{C}^{N_e\times N}$ denote the channels from Alice to IRS, IRS to Bob, and IRS to Eve, respectively, where $\mathbf{t}_g \in \mathbb{C}^{1\times \bar{N}}$, $\mathbf{B}_g \in \mathbb{C}^{N_b\times \bar{N}}$ and $\mathbf{E}_g \in \mathbb{C}^{N_e\times \bar{N}}$ denote the baseband element-wise channels from Alice to group g and from group g

to Bob and Eve, respectively. Without loss of generality, we assume that $\mathbf{h}_t$, $\mathbf{H}_B$ and $\mathbf{H}_E$ are Rayleigh flat fading channels with each element obeying the independent and identically distributed (i.i.d.) Gaussian distribution $\mathcal{CN}(0, 1)$.

Moreover, due to the severe path loss and high attenuation, the signals reflected by the IRS more than once have negligible power and hence can be ignored. Accordingly, the received signal at Bob and Eve are given by

$$\mathbf{y}_b = P_t \mathbf{H}_B \text{diag}\{\boldsymbol{\theta}\} \text{diag}\{\mathbf{s}_i\} \mathbf{h}_t b_j + \mathbf{n}_B, \tag{5.2}$$

$$\mathbf{y}_e = P_t \mathbf{H}_E \text{diag}\{\boldsymbol{\theta}\} \text{diag}\{\mathbf{s}_i\} \mathbf{h}_t b_j + \mathbf{n}_E, \tag{5.3}$$

respectively, where $\mathbf{s}_i = [\mathbf{0}, \cdots, \mathbf{0}, \mathbf{e}_i, \mathbf{0}, \cdots, \mathbf{0}]^T \in \mathbb{R}^{N\times 1}$, $\mathbf{e}_i = [1, 1, \cdots, 1]^T \in \mathbb{R}^{\tilde{N}\times 1}$, b_j is the digital symbol chosen from the $\mathcal{M}$-ary constellation for $j \in \mathbb{M} = \{1, 2, \cdots, M\}$, and satisfies $\mathbb{E}|b_j|^2 = 1$, $P_t = \beta^2 P_s$ is the transmit power with the constraint of $P_t \leq N_t$, $0 \leq \beta \leq 1$ is the transmit power factor and $P_s = N_t$ is the total transmit power at Alice. $\mathbf{n}_B \sim \mathcal{CN}(0, \sigma_b^2 \mathbf{I}_{N_b})$ and $\mathbf{n}_E \sim \mathcal{CN}(0, \sigma_e^2 \mathbf{I}_{N_e})$ denote the complex AWGN vectors at Bob and Eve, respectively.

By changing the form $\text{diag}\{\boldsymbol{\theta}\} \text{diag}\{\mathbf{s}_i\} \mathbf{h}_t$ as $\text{diag}\{\mathbf{h}_t\} \boldsymbol{\Phi} \mathbf{s}_i$, where $\boldsymbol{\Phi} = \text{diag}\{\boldsymbol{\theta}\}$, we can rewrite (5.2) and (5.3) as follows

$$\mathbf{y}_b = \beta^2 P_s \mathbf{H}'_B \boldsymbol{\Phi} \mathbf{s}_i b_j + \mathbf{n}_B, \tag{5.4}$$

$$\mathbf{y}_e = \beta^2 P_s \mathbf{H}'_E \boldsymbol{\Phi} \mathbf{s}_i b_j + \mathbf{n}_E, \tag{5.5}$$

where $\mathbf{H}'_B = \mathbf{H}_B \text{diag}\{\mathbf{h}_t\}$ and $\mathbf{H}'_E = \mathbf{H}_E \text{diag}\{\mathbf{h}_t\}$.

5.2.2 Problem Formulation

Here, we characterize the security by evaluating average SR, formulated as

$$\bar{R}_s = \mathbb{E}_{\mathbf{H}'_B, \mathbf{H}'_E}\left(\left[I(b_j, \mathbf{s}_i; \mathbf{y}_b | \mathbf{H}'_B, \mathbf{H}'_E) - I(b_j, \mathbf{s}_i; \mathbf{y}_e | \mathbf{H}'_B, \mathbf{H}'_E)\right]^+\right), \tag{5.6}$$

where $[a]^+ = \max\{a, 0\}$ and $I(b_j, \mathbf{s}_i; \mathbf{y}_b | \mathbf{H}'_B, \mathbf{H}'_E)$ $I(b_j, \mathbf{s}_i; \mathbf{y}_e | \mathbf{H}'_B, \mathbf{H}'_E)$ are the mutual information over desired and eavesdropping channels with the finite and discrete complex signal set, respectively. Similar to [22], it can be derived as follows

$$\begin{aligned} I(b_j, \mathbf{s}_i; \mathbf{y}_b | \mathbf{H}'_B, \mathbf{H}'_E) &= \int \sum_{i=1}^{G} \sum_{j=1}^{M} p(\mathbf{y}_b, \mathbf{s}_i, b_j) \log_2 \frac{p(\mathbf{y}_b, \mathbf{s}_i, b_j)}{p(\mathbf{y}_b) p(\mathbf{s}_i, b_j)} d\mathbf{y}_b \\ &= \frac{1}{GM} \sum_{i=1}^{G} \sum_{j=1}^{M} p(\mathbf{y}_b | \mathbf{s}_i, b_j) \end{aligned}$$

$$\times \log_2 \frac{GMp(\mathbf{y}_b|\mathbf{s}_i, b_j)}{\sum_{i'=1}^{G}\sum_{j'=1}^{M} p(\mathbf{y}_b|\mathbf{s}_i, b_j)} d\mathbf{y}_b$$

$$= \log_2 GM - \frac{1}{GM}\sum_{i=1}^{G}\sum_{j=1}^{M}\mathbb{E}_{\mathbf{n}_B}\left\{\log_2 \sum_{i'=1}^{G}\sum_{j'=1}^{M} \right. \tag{5.7}$$

$$\left. \exp\left[\frac{-\|\beta^2 P_s \mathbf{H}'_B \mathbf{\Phi}\left(\mathbf{s}_i b_j - \mathbf{s}_{i'} b_{j'}\right) + \mathbf{n}_B\|^2 + \|\mathbf{n}_B\|^2}{\sigma_b^2}\right]\right\}.$$

Similarly, we can derive the mutual information over eavesdropping channel as follows

$$I(b_j, \mathbf{s}_i; \mathbf{y}_e|\mathbf{H}'_B, \mathbf{H}'_E) = \log_2 GM - \frac{1}{GM}\sum_{i=1}^{G}\sum_{j=1}^{M}\mathbb{E}_{\mathbf{n}_E}\left\{\log_2 \sum_{i'=1}^{G}\sum_{j'=1}^{M} \right. \tag{5.8}$$

$$\left. \exp\left[\frac{-\|\beta^2 P_s \mathbf{H}'_E \mathbf{\Phi}\left(\mathbf{s}_i b_j - \mathbf{s}_{i'} b_{j'}\right) + \mathbf{n}_E\|^2 + \|\mathbf{n}_E\|^2}{\sigma_e^2}\right]\right\}.$$

Finally, our objective is to maximize the SR by designing the beamforming at IRS and the transmit power at Alice, which is casted as the following optimization problem

$$(\mathbf{P1}): \quad \max \quad R_s \tag{5.9}$$

$$\text{s.t.} \quad |\mathbf{\Phi}_{\mathbf{n},\mathbf{n}}| = 1,$$

$$\beta^2 \leq 1. \tag{5.10}$$

5.3 Approximation of the Ergodic Mutual Information

5.3.1 Traditional Approximate Secrecy Rate Expression

In accordance with the definition of the cut-off rate for traditional MIMO systems in [35], we have the cut-off rate for Bob and Eve as follows

$$I_0^B = 2\log_2 GM - \log_2 \sum_{i=1}^{GM}\sum_{j=1}^{GM} \exp\left(\frac{-\beta^2 P_s \mathbf{d}_{ij}^H \mathbf{\Phi}^H \mathbf{H}'^H_B \mathbf{\Omega}_{\mathrm{B}}^{-1} \mathbf{H}'_B \mathbf{\Phi} \mathbf{d}_{ij}}{4}\right), \tag{5.11}$$

which can be derived similarly to Appendix A in [35] with a slight modification as $\mathbf{d}_{i,j} = \mathbf{x}_i - \mathbf{x}_j$ and $\mathbf{x} = \mathbf{s}_i b_j$. Similarly, the cut-off rate for Eve is given by

$$I_0^E = 2\log_2 GM - \log_2 \sum_{i=1}^{GM}\sum_{j=1}^{GM} \exp\left(\frac{-\beta^2 P_s \mathbf{d}_{ij}^H \mathbf{\Phi}^H \mathbf{H}_E'^H \mathbf{\Omega}_{\mathrm{E}}^{-1} \mathbf{H}_E' \mathbf{\Phi} \mathbf{d}_{ij}}{4}\right), \tag{5.12}$$

where $\mathbf{\Omega}_{\mathrm{B}} = \sigma_b^2 \mathbf{I}_{N_b}$ and $\mathbf{\Omega}_{\mathrm{E}} = \sigma_e^2 \mathbf{I}_{N_e}$. Therefore, the TASR can be expressed as

$$R_s^a = I_0^B - I_0^E. \tag{5.13}$$

5.3.2 *Proposed Newly Approximate Secrecy Rate Expression*

As previously stated, (5.7) and (5.8) can be applied to evaluate the ergodic mutual information (EMI). With this equation, we know that the mutual information is decided by the four variables, $\mathbf{s}_i$, b_j, $\mathbf{H}$ and $\mathbf{n}$, and its expression is complex and does not have a closed-form expression. Authors in [36, 37] tried to replace the above four variables with one variable SNR and they used the 1stOpt software to get a fitting expression which is simpler and has the closed-form expression. Here, we first try to fit the EMI in the same way as the authors in [36]. However, we found that if we choose the expression of the same independent variable as [36, 37], the SR does not fit well. Therefore, we try to find another expression of independent variable which is derived from (5.8) and (5.9) directly.

Inspired by the formula given in [[6], Eq. (4.3.34)], (11) can be rewritten as

$$I_0^B = -\log_2 \sum_{i=1}^{GM}\sum_{j=1}^{GM} \frac{1}{(N_t M)^2} \int p(\mathbf{y}_b|\mathbf{x}_i)^{1/2} p(\mathbf{y}_b|\mathbf{x}_j)^{1/2} d\mathbf{y}_b, \tag{5.14}$$

where $\mathbf{x}_i = \mathbf{s}_i b_j$. For a given channel $\mathbf{H}$, assuming the decoded received signal $\mathbf{y}_b$ is a complex Gaussian distribution, the corresponding conditional probability is

$$p(\mathbf{y}_b'|\mathbf{x}_i) = \frac{1}{(\pi\sigma_b^2)^{N_b}} \exp\left(\|(\mathbf{y}_b' - \beta^2 P_s \mathbf{H}_B \mathbf{\Phi} \mathbf{x}_i)\|^2\right). \tag{5.15}$$

By plugging $p(\mathbf{y}_b'|\mathbf{x}_i)$ and $p(\mathbf{y}_b'|\mathbf{x}_j)$ into (5.14), we get

$$\begin{aligned} I_0^B = 2\log_2 GM - \log_2 \sum_{j=1}^{GM}\sum_{j=1}^{GM} \int \left[\frac{1}{(\pi\sigma_b^2)^{N_r}} \exp\left(\|(\mathbf{y}_b' - \beta^2 P_s \mathbf{H}_B \mathbf{\Phi} \mathbf{x}_i)\|^2\right)\right]^{\frac{1}{2}} \\ \times \left[\frac{1}{(\pi\sigma_b^2)^{N_r}} \exp\left(\|(\mathbf{y}_b' - \beta^2 P_s \mathbf{H}_B \mathbf{\Phi} \mathbf{x}_j)\|^2\right)\right]^{\frac{1}{2}} d\mathbf{y}_b, \end{aligned} \tag{5.16}$$

where the integrand can be simplified as

$$\mathbf{I}_1 = \frac{1}{(\pi\sigma_b^2)^{N_b}} \exp\Big(-\|\mathbf{y}_b'\|^2 - \frac{1}{2}\|\beta^2 P_s \mathbf{H}_B \mathbf{\Phi}\mathbf{x}_i\|^2 \tag{5.17}$$
$$-\frac{1}{2}\|\beta^2 P_s \mathbf{H}_B \mathbf{\Phi}\mathbf{x}_j\|^2 + R_e\left\{\left(\beta^2 P_s \mathbf{H}_B \mathbf{\Phi}\mathbf{x}_i\right) * \mathbf{y}_b'\right\} + R_e\left\{\left(\beta^2 P_s \mathbf{H}_B \mathbf{\Phi}\mathbf{x}_j\right) * \mathbf{y}_b'\right\}\Big).$$

Then, substituting $\mathbf{I}_1$ into (5.16) yields

$$I_0^B = 2\log_2 GM - \log_2 \sum_{j=1}^{GM}\sum_{j=1}^{GM} \exp\left(-\frac{\|\mathbf{H}_B \mathbf{\Phi}\left(\frac{\mathbf{x}_i - \mathbf{x}_j}{2}\right)\|^2}{\sigma_b^2}\right) \tag{5.18}$$
$$-\log_2 \sum_{j=1}^{GM}\sum_{j=1}^{GM} \int \left[\exp\left(-\frac{\|\mathbf{y}_b' - \mathbf{H}_B \mathbf{\Phi}\left(\frac{\mathbf{x}_i + \mathbf{x}_j}{2}\right)\|^2}{\sigma^2}\right) \times \frac{1}{(\pi\sigma_b^2)^{N_b}}\right] d\mathbf{y}_b',$$

where the third item integral is equal to 1 since the integrand is a multi-variate Gaussian probability density function. Moreover, we can simplify the second item by the Jensen's inequality as follows

$$I_0^B(\gamma) = 2\log_2 GM - \log_2 \exp\left(-\underbrace{\sum_{j=1}^{GM}\sum_{j=1}^{GM} \frac{\|\mathbf{H}_B \mathbf{\Phi}(\mathbf{x}_i - \mathbf{x}_j)\|^2}{4\sigma^2}}_{\gamma}\right). \tag{5.19}$$

For the sake of improving the accuracy of the fitting expression, we choose γ in the above as the independent variable. We plot the mutual information with respect to SNR for various values of G in Fig. 5.2, and we find that the sum of ratio term(s)

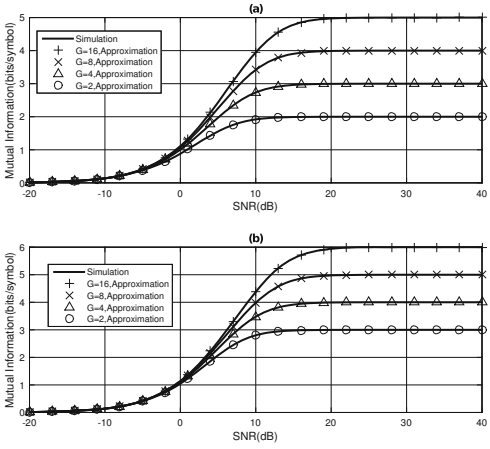


Fig. 5.2 Simulated (denoted by lines) and approximated mutual information of M-PSK (a.BPSK, b.QPSK) over Rayleigh fading channels

curve fitting based expression can be applied to accurately fit $I(b_j, \mathbf{s}_i; \mathbf{y}_b|\mathbf{H}'_B, \mathbf{H}'_E)$, which is expressed by

$$I(b_j, \mathbf{s}_i; \mathbf{y}_b|\mathbf{H}'_B, \mathbf{H}'_E) \approx \hat{I}_B^{(M,G)}(\gamma_b) = \sum_{i=1}^{k_G} \frac{\zeta_i^{(G)}\gamma_b}{\xi_i^{(G)} + \gamma_b}. \tag{5.20}$$

By using the open-source fitting software package 1stOpt, the fitting parameters k_M, k_G, $\left\{\zeta_i^{(M)}\right\}$ and $\left\{\xi_j^{(G)}\right\}$ can be found, which are listed in Table 5.1. The values of the SR and γ_b used for fitting are obtained by the corresponding expectations of the SR and γ_b when 1000 channel realizations are randomly given. Notice that the mutual information will tend to $\log_2 GM$ or 0 when γ tends to $+\infty$ or $-\infty$. In this table, RMSE is short for means root mean square error, standing for the gap between the exact and approximated value.

To further investigate the precision of (5.20), we compare the approximated and exact mutual information in Fig. 5.2, which is shown in the simulation part for different modulation schemes and different number of G. It can be seen from the figure that the approximation results are very close to the simulation results, which verifies the precision of (5.20).

Similarly, we can get the approximate expression of the mutual information over wiretap channel as follows

$$I(b_j, \mathbf{s}_i; \mathbf{y}_e|\mathbf{H}'_B, \mathbf{H}'_E) \approx \hat{I}_E^{(M,G)}(\gamma_e) = \sum_{i=1}^{k_G} \frac{\zeta_i^{(G)}\gamma_e}{\xi_i^{(G)} + \gamma_e}. \tag{5.21}$$

Therefore, the optimization problem (**P1**) can be rewritten as follows

$$\begin{aligned} (\mathbf{P2}): \max_{\beta, \mathbf{\Phi}} \quad & \sum_{i=1}^{k_G} \frac{\zeta_i^{(G)}\gamma_b}{\xi_i^{(G)} + \gamma_b} - \sum_{i=1}^{k_G} \frac{\zeta_i^{(G)}\gamma_e}{\xi_i^{(G)} + \gamma_e} \\ \text{s.t.} \quad & |\mathbf{\Phi}_{\mathbf{n},\mathbf{n}}| = 1, \\ & \beta^2 \le 1, \end{aligned} \tag{5.22}$$

where the expressions of γ_b and γ_e can be further simplified from the original form in (5.19) as follows

$$\gamma_b = \sum_{i=1}^{GM}\sum_{j=1}^{GM} \frac{\|\mathbf{H}'_B \mathbf{\Phi}(\mathbf{x}_i - \mathbf{x}_j)\|^2}{4\sigma^2} \tag{5.23}$$

$$= \sum_{j=1}^{GM}\sum_{j=1}^{GM} \frac{\mathrm{tr}\left(\mathbf{H}'_B \mathbf{\Phi} \mathbf{d}_{i,j} \mathbf{d}_{i,j}^H \mathbf{\Phi}^H \mathbf{H}_B'^H\right)}{4\sigma^2} \tag{5.24}$$

Table 5.1 Fitting coefficients for M-PSK with different G in (5.20)

M	G	k_M	k_G	$\zeta_1^{(M)}$	$\zeta_2^{(M)}$	$\zeta_3^{(M)}$	$\xi_1^{(G)}$	$\xi_2^{(G)}$	$\xi_3^{(G)}$	RMSE
8	16	2	4	2.007602	−1.83073	4.78618	16.48645	1.90012	11.89605	1.298E-3
	8			3.22453	4.62917	-0.85445	2.89612	13.98985	88.82823	2.7413E-3
	4		3	4.67308	−1.41513	2.74124	11.89605	45.76453	2.55830	2.4591E-4
	2			−61.65283	2.007602	64.640742	16.48645	1.90012	15.62086	4.1167E-4
4	16	2	4	−69.79872	73.46507	2.33084	14.87082	14.01141	2.57772	1.298E-3
	8			1.96523	42.82407	−39.79035	1.13629	5.11235	5.57396	1.081E-3
	4		3	−24.41596	27.36585	1.05006	3.74558	3.30759	0.84914	8.808E-4
	2			0.044593	−1.83073	4.78618	0.247079	4.14794	1.57405	6.613E-4
2	16	2	4	62.5582	−58.9554	1.39777	9.93359	10.61559	1.97674	9.612E-4
	8			0.37940	60.51929	−56.90064	1.02712	6.658413	7.10888	8.234E-4
	4	1	3	0.08038	58.8141	−55.8964	0.39127	4.63607	4.89234	8.312E-4
	2			14.6211	−15.6089	2.9887	13.1342	12.6401	1.9804	9.087E-4

M represents the modulation order of M-PSK. RMSE denotes the root mean square error

$$= \frac{1}{4\sigma^2}\mathrm{tr}\left(\sum_{j=1}^{GM}\sum_{j=1}^{GM}\mathbf{H}'_B\boldsymbol{\Phi}\mathbf{d}_{i,j}\mathbf{d}_{i,j}^H\boldsymbol{\Phi}^H\mathbf{H}_B'^H\right) \tag{5.25}$$

$$= \frac{1}{4\sigma^2}\mathrm{tr}\left(\mathbf{H}'_B\boldsymbol{\Phi}\mathbf{D}_{ij}\boldsymbol{\Phi}^H\mathbf{H}_B'^H\right) \tag{5.26}$$

$$= \frac{1}{4\sigma^2}\mathrm{tr}\left(\mathbf{D}_{ij}\boldsymbol{\Phi}^H\mathbf{H}_B'^H\mathbf{H}'_B\boldsymbol{\Phi}\right). \tag{5.27}$$

The derivation from (5.23) to (5.24) is achieved by denoting $\mathbf{d}_{i,j} = \mathbf{x}_i - \mathbf{x}_j$, and the derivation from (5.24) to (5.25) and (5.26) to (5.27) is achieved by utilizing the trace property, i.e., $\mathrm{tr}(\mathbf{A}+\mathbf{B}) = \mathrm{tr}(\mathbf{A})+\mathrm{tr}(\mathbf{B})$ and $\mathrm{tr}(\mathbf{ABC}) = \mathrm{tr}(\mathbf{BCA})$, respectively. Similarly, we can get the expression of γ_e as follows

$$\gamma_e = \frac{\mathrm{tr}(\mathbf{D}_{ij}\boldsymbol{\Phi}^H\mathbf{H}_E'^H\mathbf{H}'_E\boldsymbol{\Phi})}{G\sigma_e^2}. \tag{5.28}$$

P2 is difficult to solve due to the non-concave objective function as well as the coupled optimization variables. However, we observe that the resultant problems can be efficiently solved when one of $\boldsymbol{\Phi}$ and P_t is fixed. This thus motivates us to propose an alternating optimization based algorithm to solve **P2** sub-optimally, by iteratively optimizing $\boldsymbol{\Phi}$ (**P2-1**) and P_t (**P2-2**) with the other being fixed at each iteration until convergence is reached, as detailed in the next sections.

5.4 Beamforming Design for Given Transmit Power Based on Approximate Expression of SR

For IRS-aided SM systems, the design of beamformer at IRS is necessary to improve the system performance. In this section, two beamformers at IRS, called Max-NASR-SCA and Max-NASR-DA, are proposed based on the proposed NASR to enhance the security of IRS-aided SM systems. Additionally, the Max-TASR-SDR based on the traditional ASR is proposed and used as a performance reference.

5.4.1 Proposed Max-NASR-SCA

Observing the optimization problem in (**P2**), we find it is the fractional programming problem actually. However, the conventional FP techniques mostly can only deal with the single-ratio or the max-min-ratio case rather than the multiple-ratio FP problems like (**P2**). Thus we propose the Max-NASR-SCA method which first decouples the numerator and the denominator of each ratio term, and then utilizes the SCA method based on SDR to solve the problem. First we rewrite optimization problems with P_t fixed as follows

$$\begin{aligned}(\mathbf{P2\text{-}1}): \min_{\mathbf{\Phi}} \ & \sum_{i=1}^{k_G} \frac{\zeta_i^{(G)} P_t \mathrm{tr}(\mathbf{D}_{ij}\mathbf{\Phi}^H \mathbf{H}_E'^H \mathbf{H}_E' \mathbf{\Phi})}{4\xi_i^{(G)}\sigma_e^2 + P_t \mathrm{tr}(\mathbf{D}_{ij}\mathbf{\Phi}^H \mathbf{H}_E'^H \mathbf{H}_E' \mathbf{\Phi})} \\ & - \sum_{j=1}^{k_G} \frac{\zeta_j^{(G)} P_t \mathrm{tr}(\mathbf{D}_{ij}\mathbf{\Phi}^H \mathbf{H}_B'^H \mathbf{H}_B' \mathbf{\Phi})}{4\xi_j^{(G)}\sigma_b^2 + P_t \mathrm{tr}(\mathbf{D}_{ij}\mathbf{\Phi}^H \mathbf{H}_B'^H \mathbf{H}_B' \mathbf{\Phi})} \\ \text{s.t.} \ & |\mathbf{\Phi}_{n,n}| = 1. \end{aligned} \tag{5.29}$$

It is easy to see that the problem **P2-1** is equivalent to the following problem

$$\begin{aligned}(\mathbf{P2\text{-}1\text{-}1}): \min_{\mathbf{\Phi}} \quad & \sum_{i=1}^{2k_G} \alpha_i \\ \text{s.t.} \quad & \frac{h_i(\mathbf{\Phi})}{g_i(\mathbf{\Phi})} \le \alpha_i, i = 1, \cdots, 2k_G, \\ & |\mathbf{\Phi}_{n,n}| = 1, \end{aligned} \tag{5.30}$$

where $\boldsymbol{\alpha}$ refers to a collection of variables $\{\alpha_1, \cdots, \alpha_{2k_G}\}$, and when $\mathbf{\Phi}$ is fixed, the optimal α_i can be found in closed form expression as

$$\alpha_i^* = \frac{h_i(\mathbf{\Phi})}{g_i(\mathbf{\Phi})}, \ \ \forall i = 1, \cdots, 2k_G \tag{5.31}$$

where

$$h_i(\mathbf{\Phi}) = U_i P_t \mathrm{tr}(\mathbf{D}_{ij}\mathbf{\Phi}^H \mathbf{H}_g'^H \mathbf{H}_g' \mathbf{\Phi}), \tag{5.32}$$

and

$$g_i(\mathbf{\Phi}) = 4Q_i\sigma_g^2 + P_t \mathrm{tr}(\mathbf{D}_{ij}\mathbf{\Phi}^H \mathbf{H}_g'^H \mathbf{H}_g' \mathbf{\Phi}), \tag{5.33}$$

where g stands for B (Bob) or E (Eve), $U_i \in \{\zeta_i^{(G)}, -\zeta_j^{(G)}\}$, $Q_i \in \{\xi_i^{(G)}, \xi_j^{(G)}\}$. Combined with Table 5.1, we can see that U_i could be positive or it could be negative and Q_i is all positive. Additionally, it is easy for us to see that α_i always has the same sign as U_i. Therefore, we can rewrite (**P2-1-1**) as follows with the condition $g_i(\mathbf{\Phi}) > 0$.

$$(\mathbf{P2\text{-}1\text{-}2}): \min_{\mathbf{\Phi}} \quad \sum_{i=1}^{2k_G} \alpha_i \tag{5.34a}$$

$$\text{s.t.} \quad f_i(\mathbf{\Phi}) \le 0, \ \ i = 1, \cdots, 2k_G, \tag{5.34b}$$

$$|\mathbf{\Phi}_{n,n}| = 1, \tag{5.34c}$$

where

$$\begin{aligned} f_i(\mathbf{\Phi}) &= h_i(\mathbf{\Phi}) - \alpha_i g_i(\mathbf{\Phi}) \\ &= (U_i - \alpha_i) P_t \mathrm{tr}(\mathbf{D}_{ij} \mathbf{\Phi}^H \mathbf{H}_g'^H \mathbf{H}_g' \mathbf{\Phi}) - 4\alpha_i Q_i \sigma_g^2. \end{aligned} \tag{5.35}$$

Next, we aim to transform the constraints (5.34b) and (5.34c) to the convex constraints. First, we derive the first order and second order Hessian matrices of (5.34b) with respect to $\mathbf{\Phi}$ as follows

$$\nabla f_i(\mathbf{\Phi}) = (U_i - \alpha_i) P_t \mathbf{H}^H \mathbf{H} \mathbf{\Phi} \left(\mathbf{D}_{ij} + \mathbf{D}_{ij}^H \right), \tag{5.36}$$

$$\nabla^2 f_i(\mathbf{\Phi}) = (U_i - \alpha_i) P_t \mathbf{H}^H \mathbf{H} \left(\mathbf{D}_{ij} + \mathbf{D}_{ij}^H \right), \tag{5.37}$$

which hold due to the fact that

$$\frac{\partial \mathrm{tr}(\mathbf{W} \mathbf{A}^H \mathbf{W}^H \mathbf{B})}{\partial \mathbf{W}} = \mathbf{B} \mathbf{W} \mathbf{A} + \mathbf{B}^H \mathbf{W} \mathbf{A}^H, \tag{5.38}$$

$$\frac{\partial \mathbf{A} \mathbf{W} \mathbf{B}}{\partial \mathbf{B}} = \mathbf{A}^H \mathbf{B}. \tag{5.39}$$

From (5.36) and (5.37) we can see that the convexity of constraint (5.34b) is determined by the positive and negative properties of $(U_i - \alpha_i)$, which is not sure as U_i always has the same sign as α_i. Notice that linear functions can be considered either convex or concave and we use SCA method to solve the above problem when $(U_i - \alpha_i) < 0$ as follows

$$f_i(\mathbf{\Phi}) \geq f_i(\mathbf{\Phi}_0) + \mathrm{tr}\left[\nabla f_i(\mathbf{\Phi}_0)(\mathbf{\Phi} - \mathbf{\Phi}_0) \right]. \tag{5.40}$$

Accordingly, the constraint (5.34b) can be rewritten as follows

$$f_i(\mathbf{\Phi}) = \begin{cases} (U_i - \alpha_i) P_t \mathrm{tr}(\mathbf{D}_{ij} \mathbf{\Phi}^H \mathbf{H}_g'^H \mathbf{H}_g' \mathbf{\Phi}) - 4\alpha_i Q_i \sigma_g^2, & (U_i - \alpha_i) > 0 \\ (U_i - \alpha_i) P_t \mathrm{tr}(\mathbf{D}_{ij} \mathbf{\Phi}_0^H \mathbf{H}_g'^H \mathbf{H}_g' \mathbf{\Phi}_0) + (U_i - \alpha_i) \\ P_t \mathrm{tr}\left(\mathbf{H}^H \mathbf{H} \mathbf{\Phi} \left(\mathbf{D}_{ij} + \mathbf{D}_{ij}^H \right) (\mathbf{\Phi} - \mathbf{\Phi}_0) \right) - 4\alpha_i & (U_i - \alpha_i) < 0 \\ \times Q_i \sigma_g^2 \end{cases} \tag{5.41}$$

And the constraint (5.34c) can be transformed to convex by relaxing (5.34c) as follows

$$|\mathbf{\Phi}_{n,n}| \leq 1. \tag{5.42}$$

Hence, the optimization problem (**P2-1-2**) can be transformed to (**P2-1-3**) as follows

$$(\mathbf{P2\text{-}1\text{-}3}) : \min_{\mathbf{\Phi}} \quad \sum_{i=1}^{2k_G} \alpha_i \tag{5.43}$$

$$\text{s.t.} \quad (5.41), (5.42)$$

which can be solved by using convex optimizing toolbox such as CVX. Then, we can get the beamformer at IRS as follows

$$\mathbf{\Phi}_{n,n} = e^{j\text{angle}(\mathbf{\Phi}_{n,n})}, \quad \forall n = 1, 2, \cdots, N. \tag{5.44}$$

Additionally, a step-by-step summary is provided as follows: Algorithm 1.

Algorithm 1: Proposed Max-NASR-SCA beamformer

Input: the channel matrix $\mathbf{H}'_B$ and $\mathbf{H}'_E$, P_t, the $\mathcal{M}$-ary constellation
Output: $\mathbf{\Phi}$

1: Initialize $\mathbf{\Phi}_0$ to a feasible value.
2: Initialize $\alpha_i^0 = \frac{h_i(\mathbf{\Phi}_0)}{g_i(\mathbf{\Phi}_0)}$, step $k = 0$.
3: Reformulate the problem by the SCA method to get **P2-1-3**
4: **repeat**
5: Let $k = k + 1$
6: Update $\boldsymbol{\alpha}_k$ by (5.31)
7: Update the beamforming matrix $\mathbf{\Phi}_k$ by solving the reformulated convex optimization problem (5.43) over $\mathbf{\Phi}_k$ for fixed $\boldsymbol{\alpha}_k$
8: **until** $\|\mathbf{\Phi}_k - \mathbf{\Phi}_{k-1}\|_2 \leq 0.01$
9: Compute $\mathbf{\Phi}$ as the beamformer at IRS according to (5.44).
10: **return** $\mathbf{\Phi}$

5.4.2 *Proposed Max-NASR-DA*

In the previous section, the Max-NASR-SCA algorithm was presented to optimize the secure IRS beamforming matrices. For the comparison of the secrecy performance and to offer a new solution to this non-convex optimization problem, we propose another secure IRS beamforming method with better performance, namely Max-NASR-DA, in what follows.

Observe the objective function below

$$(\mathbf{P2\text{-}1}) : \max_{\mathbf{\Phi}} \quad \sum_{i=1}^{k_G} \frac{h_i(\mathbf{\Phi})}{g_i(\mathbf{\Phi})} \tag{5.45}$$

$$\text{s.t.} \quad |\mathbf{\Phi}_{n,n}| = 1,$$

it is easy to see that in each of the ratios, the denominator $g_i(\mathbf{\Phi}) > 0, \forall i = 1, 2, \cdots, 2k_G$, and the numerator $h_i(\mathbf{\Phi})$ can be negative which makes it difficult for us to realize quadratic transform. Therefore, we first realize the equivalent transform as follows

$$\begin{aligned}(\mathbf{P2\text{-}1\text{-}4}): \max_{\mathbf{\Phi}} \ & \sum_{i=1}^{2k_G} \frac{h_i(\mathbf{\Phi}) + M_i g_i(\mathbf{\Phi})}{g_i(\mathbf{\Phi})} - \sum_{i=1}^{2k_G} M_i \\ \text{s.t.} \quad & |\mathbf{\Phi}_{n,n}| = 1,\end{aligned} \tag{5.46}$$

where $M_i > \max |U_i|, i = 1, 2 \cdots, 2k_G$ and the numerator can be written as

$$\begin{aligned}u_i(\mathbf{\Phi}) &= h_i(\mathbf{\Phi}) + M_i g_i(\mathbf{\Phi}) \\ &= \underbrace{(U_i + M_i)\, P_t \mathrm{tr}\left(\mathbf{H}_g' \mathbf{\Phi} \mathbf{D}_{ij} \mathbf{\Phi}^H \mathbf{H}_g'^H\right)}_{a_1 \geq 0} + \underbrace{4 M_i Q_i \sigma^2}_{a_2 > 0}.\end{aligned} \tag{5.47}$$

According to (5.47), we can rearrange (5.46) as follows

$$\begin{aligned}(\mathbf{P2\text{-}1\text{-}4}): \max_{\mathbf{\Phi}} \ & \sum_{i=1}^{k_G} \frac{(U_i + M_i)\, P_t \mathrm{tr}\left(\mathbf{H}_g' \mathbf{\Phi} \mathbf{D}_{ij} \mathbf{\Phi}^H \mathbf{H}_g'^H\right)}{4 Q_i \sigma_g^2 + P_t \mathrm{tr}\left(\mathbf{H}_g' \mathbf{\Phi} \mathbf{D}_{ij} \mathbf{\Phi}^H \mathbf{H}_g'^H\right)} \\ & + \sum_{i=1}^{2k_G} \frac{4 M_i Q_i \sigma^2}{4 Q_i \sigma_g^2 + P_t \mathrm{tr}\left(\mathbf{H}_g' \mathbf{\Phi} \mathbf{D}_{ij} \mathbf{\Phi}^H \mathbf{H}_g'^H\right)} - \sum_{i=1}^{2k_G} M_i \\ \text{s.t.} \quad & |\mathbf{\Phi}_{n,n}| = 1,\end{aligned} \tag{5.48}$$

where each numerator and denominator are positive. Using quadratic transform proposed in [38, 39], (**P2-1-4**) can be reformulated as an equivalent optimization problem with a new objective function:

$$\begin{aligned}f(\mathbf{\Phi}) = & \sum_{i=1}^{2k_G} 2 y_i \sqrt{(U_i + M_i)\, P_t} \mathbf{H}_g' \mathbf{\Phi} \mathbf{D}_{ij}^{-1/2} + \sum_{i=1}^{2k_G} 2 y_i \sqrt{4 M_i Q_i \sigma^2} - \sum_{i=1}^{2k_G} M_i \\ & - \sum_{i=1}^{2k_G} 2 y_i^2 \left[4 Q_i \sigma_g^2 + P_t \mathrm{tr}\left(\mathbf{H}_g' \mathbf{\Phi} \mathbf{D}_{ij} \mathbf{\Phi}^H \mathbf{H}_g'^H\right)\right],\end{aligned} \tag{5.49}$$

where the auxiliary variables y_i can be found in a closed-form expression as follows

$$y_i^* = \frac{\sqrt{u_i(\mathbf{\Phi})}}{g_i(\mathbf{\Phi})}, \ \forall i = 1, \cdots, 2k_G, \tag{5.50}$$

when $\boldsymbol{\Phi}$ is fixed. (**P2-1-4**) has been transformed as a non-convex optimization problem with convex objective function and non-convex equality constraint. According to the equality constraint, we adopt the dual ascent (DA) algorithm to solve (**P2-1-4**).

The key idea of the non-convex DA is to introduce an auxiliary vector $\boldsymbol{\varphi} = \boldsymbol{\Phi}$, as well as a penalty term for $\boldsymbol{\varphi} \neq \boldsymbol{\Phi}$. Then, (**P2-1-4**) is equivalently represented as

$$\begin{aligned} (\mathbf{P2\text{-}1\text{-}5}): \max_{\boldsymbol{\Phi}} \ & f(\boldsymbol{\varphi}) + \frac{\rho}{2}\|\boldsymbol{\varphi} - \boldsymbol{\Phi}\|_2^2 \\ \text{s.t.} \ & |\boldsymbol{\varphi}_{n,n}| = 1, \\ & \boldsymbol{\varphi} = \boldsymbol{\Phi}, \end{aligned} \tag{5.51}$$

where $\rho > 0$ is the penalty parameter. Then, we have the Lagrangian function of (**P1.5**):

$$\begin{aligned} \mathcal{G}(\boldsymbol{\varphi}, \boldsymbol{\Phi}, \boldsymbol{\lambda}) = & \sum_{i=1}^{2k_G} 2y_i^2 \left[-4Q_i\sigma_g^2 - P_t \mathrm{tr}\left(\mathbf{H}_g' \boldsymbol{\varphi} \mathbf{D}_{ij} \boldsymbol{\varphi}^H \mathbf{H}_g'^H \right) \right] \\ & + \sum_{i=1}^{2k_G} 2y_i \sqrt{(U_i + M_i)\, P_t} \mathbf{H}_g' \boldsymbol{\varphi} \mathbf{D}_{ij}^{-1/2} - \sum_{i=1}^{2k_G} M_i \\ & + \sum_{i=1}^{2k_G} 2y_i \sqrt{4M_i Q_i \sigma^2} + \boldsymbol{\lambda}(\boldsymbol{\varphi} - \boldsymbol{\Phi}) + \frac{\rho}{2}\|\boldsymbol{\varphi} - \boldsymbol{\Phi}\|_2^2, \end{aligned} \tag{5.52}$$

where $\boldsymbol{\lambda}$ is the dual variable for $\mathrm{Re}\{\boldsymbol{\varphi} - \boldsymbol{\Phi}\} = 0$ and $\mathrm{Im}\{\boldsymbol{\varphi} - \boldsymbol{\Phi}\} = 0$, respectively. The alternating iterative process of DA includes three main expressions:

$$\boldsymbol{\Phi}^{t+1} = \arg\max_{\boldsymbol{\Phi}} \mathcal{G}(\boldsymbol{\varphi}^t, \boldsymbol{\Phi}, \boldsymbol{\lambda}^t), \tag{5.53}$$

$$\boldsymbol{\varphi}^{t+1} = \arg\max_{\boldsymbol{\varphi}} \mathcal{G}(\boldsymbol{\varphi}, \boldsymbol{\Phi}^t, \boldsymbol{\lambda}^t), \tag{5.54}$$

$$\boldsymbol{\lambda}^{t+1} = \boldsymbol{\lambda}^t + \rho(\boldsymbol{\varphi}^{t+1} - \boldsymbol{\Phi}^{t+1}), \tag{5.55}$$

where t is the iteration index.

5.4.2.1 Optimizing $\boldsymbol{\Phi}$

In (5.53), the optimal $\boldsymbol{\Phi}$ for fixed $\boldsymbol{\varphi}^t$ and $\boldsymbol{\lambda}^t$ is

$$\boldsymbol{\Phi}^{t+1} = e^{j\mathrm{angle}\left(\boldsymbol{\varphi}^t - \frac{1}{\rho}\boldsymbol{\lambda}^t\right)}. \tag{5.56}$$

5.4.2.2 Optimizing $\boldsymbol{\varphi}$

In (5.54), $\boldsymbol{\varphi}$ is optimized for fixed $\boldsymbol{\Phi}^t$ and $\boldsymbol{\lambda}^t$, and we have

$$\boldsymbol{\varphi}^{t+1} = \left[\rho \mathbf{I}_N - \sum_{i=1}^{2k_G} 2y_i^2 P_t \mathbf{H}_g'^H \mathbf{H}_g' \left(\mathbf{D}_{ij} + \mathbf{D}_{ij}^H\right)\right]^{-1} \times \left(-\boldsymbol{\lambda}^{t\,H} - \sum_{i=1}^{2k_G} 2y_i \sqrt{(U_i + M_i)\, P_t} \mathbf{H}_g' \boldsymbol{\varphi} \mathbf{D}_{ij}^{-1/2} + \rho \boldsymbol{\Phi}^{t+1}\right). \tag{5.57}$$

Additionally, a step-by-step summary is provided as follows: Algorithm 2.

Algorithm 2: Proposed Max-NASR-DA beamformer

Input: the channel matrix $\mathbf{H}_B'$ and $\mathbf{H}_E'$, P_t, the $\mathcal{M}$-ary constellation
Output: $\boldsymbol{\Phi}$

```
Initialize Φ_0, φ_0 and λ_0 to a feasible value.
Initialize y_i^0 = h_i(Φ_0) / g_i(Φ_0), step t = 0 and ρ = 0.5.
Reformulate the problem by the DA method to get P1.5
repeat
    Let t = t + 1
    Update y_i^t by (5.50)
    repeat
        Update the beamforming matrix Φ_{t+1} according to (5.56)
        Update the auxiliary matrix φ_{t+1} according to (5.57)
        Update the dual matrix λ_{t+1} according to (5.58)
    until ‖Φ_k − Φ_{k−1}‖_2 ≤ 0.01
until R_s(Φ_{t+1}) − R_s(Φ_t) ≤ 10^{−4}
return Φ
```

5.4.3 *Proposed Max-TASR-SDR Method*

Based on the traditional approximate expression, we propose the Max-TASR-SDR method in this subsection. The expression of SR is given by

$$R_s^a = I_0^B - I_0^E, \tag{5.58}$$

where I_0^B and I_0^E are shown in (5.12) and (5.12). By using the Jensen's inequality and changing variables as $\boldsymbol{\Phi}\mathbf{d}_{ij} = \text{diag}\left\{\mathbf{d}_{ij}\right\}\boldsymbol{\varphi}$, the lower bound of R_s^a is

$$R_s^{a'} = \log_2 \exp \sum_{i=1}^{GM} \sum_{j=1}^{GM} \left(\frac{-\boldsymbol{\varphi}^H \operatorname{diag}\left\{\mathbf{d}_{ij}\right\}^H \mathbf{H}_E'^H \mathbf{H}_E' \operatorname{diag}\left\{\mathbf{d}_{ij}\right\} \boldsymbol{\varphi}}{4} \right)$$
$$- \log_2 \exp \sum_{i=1}^{GM} \sum_{j=1}^{GM} \left(\frac{-\boldsymbol{\varphi}^H \operatorname{diag}\left\{\mathbf{d}_{ij}\right\}^H \mathbf{H}_B'^H \mathbf{H}_B' \operatorname{diag}\left\{\mathbf{d}_{ij}\right\} \boldsymbol{\varphi}}{4} \right) \tag{5.59}$$

$$= \log_2 e \cdot \left[\sum_{i=1}^{GM} \sum_{j=1}^{GM} \left(\frac{-\boldsymbol{\varphi}^H \operatorname{diag}\left\{\mathbf{d}_{ij}\right\}^H \mathbf{H}_E'^H \mathbf{H}_E' \operatorname{diag}\left\{\mathbf{d}_{ij}\right\} \boldsymbol{\varphi}}{4} \right) \right.$$
$$\left. - \sum_{i=1}^{GM} \sum_{j=1}^{GM} \left(\frac{-\boldsymbol{\varphi}^H \operatorname{diag}\left\{\mathbf{d}_{ij}\right\}^H \mathbf{H}_E'^H \mathbf{H}_E' \operatorname{diag}\left\{\mathbf{d}_{ij}\right\} \boldsymbol{\varphi}}{4} \right) \right]. \tag{5.60}$$

Hence, Problem (**P2-1-6**) can be rewritten as follows

$$(\mathbf{P2\text{-}1\text{-}6}): \quad \max \ \frac{\log_2 e}{4} \cdot \boldsymbol{\varphi}^H \boldsymbol{\Omega} \boldsymbol{\varphi} \tag{5.61}$$
$$\text{s.t.} \quad |\boldsymbol{\varphi}_{\mathbf{n}}| = 1,$$

where

$$\boldsymbol{\Omega} = \sum_{i=1}^{GM} \sum_{j=1}^{GM} \left(-\operatorname{diag}\left\{\mathbf{d}_{ij}\right\}^H \mathbf{H}_E'^H \mathbf{H}_E' \operatorname{diag}\left\{\mathbf{d}_{ij}\right\} \right)$$
$$- \sum_{i=1}^{GM} \sum_{j=1}^{GM} \left(-\operatorname{diag}\left\{\mathbf{d}_{ij}\right\}^H \mathbf{H}_B'^H \mathbf{H}_B' \operatorname{diag}\left\{\mathbf{d}_{ij}\right\} \right). \tag{5.62}$$

The objective function of (5.61) can be rewritten as $\boldsymbol{\varphi}^{\mathbf{H}} \boldsymbol{\Omega} \boldsymbol{\varphi} = \operatorname{tr}(\boldsymbol{\Omega}\mathbf{Q})$ with $\mathbf{Q} = \boldsymbol{\varphi}\boldsymbol{\varphi}^{\mathbf{H}}$. In particular, $\mathbf{Q}$ is a positive semidefinite matrix with $\operatorname{rank}(\mathbf{Q}) = 1$. However, as the rank-one constraint is non-convex, we apply the semi-definite relaxation (SDR) method to relax this constraint and reformulate (**P2-1-6**) as

$$(\mathbf{P2\text{-}1\text{-}7}): \quad \max \ \frac{\log_2 e}{4} \cdot \operatorname{tr}(\boldsymbol{\Omega}\mathbf{Q}) \tag{5.63}$$
$$\text{s.t.} \quad \mathbf{Q}_{n,n} = 1,$$
$$\mathbf{Q} \succeq 0,$$

which is a standard convex semi-definite programming (SDP) problem and can be solved via existing convex optimization solvers such as CVX [40]. It is worth

pointing out that after the relaxation, the optimal solution $\mathbf{Q}^*$ to problem (**P2-1-7**) may not be a rank-one solution and we can solve it by the method of Gaussian randomization.

5.5 Transmit Power Design for Given Beamforming Based on Approximate Expression of SR

In IRS-aided SM systems, transmit power design is an important technique to improve the system performance. In this section, two transmit power design methods are proposed based on the TASR and proposed NASR expression respectively, for secure IRS-aided SM systems: Max-NASR-TPD and Max-TASR-TPD.

5.5.1 Transmit Power Design Based on Proposed NASR

As the beamformer is fixed, we can write the optimization problem as follows

$$(\mathbf{P2\text{-}2}): \max_{\beta} \quad \sum_{i=1}^{2k_G} \frac{h_i(\beta)}{g_i(\beta)} \quad \text{s.t.} \quad \beta^2 \leq 1, \tag{5.64}$$

where

$$h_i(\beta) = U_i \beta^2 \mathrm{tr}(\mathbf{D}_{ij} \mathbf{\Phi}^H \mathbf{H}_g'^H \mathbf{H}_g' \mathbf{\Phi}), \tag{5.65}$$

and

$$g_i(\beta) = 4Q_i \sigma_g^2 + \beta^2 \mathrm{tr}(\mathbf{D}_{ij} \mathbf{\Phi}^H \mathbf{H}_g'^H \mathbf{H}_g' \mathbf{\Phi}), \tag{5.66}$$

where g stands for B (Bob) or E (Eve), $U_i \in \left\{\zeta_i^{(G)}, -\zeta_j^{(G)}\right\}$, $Q_i \in \left\{\xi_i^{(G)}, \xi_j^{(G)}\right\}$. Similarly, to ensure the denominator and the numerator are all positive, we transform the optimization problem as follows equally

$$(\mathbf{P2\text{-}2\text{-}1}): \max_{\beta} \quad \sum_{i=1}^{2k_G} \frac{h_i(\beta) + M_i g_i(\beta)}{g_i(\beta)} - \sum_{i=1}^{2k_G} M_i \quad \text{s.t.} \quad \beta^2 \leq 1, \tag{5.67}$$

where $M_i > \max|U_i|, i = 1, 2, \cdots, 2k_G$ and therefore the numerator and the denominator in each ratio are positive. Similarly, we can rearrange (5.67) as follows

$$\begin{aligned}(\mathbf{P2\text{-}2\text{-}1}): \max_{\beta} \quad & \sum_{i=1}^{k_G} \frac{(U_i + M_i)\,\beta^2 P_s \mathrm{tr}\left(\mathbf{H}_g' \mathbf{\Phi} \mathbf{D}_{ij} \mathbf{\Phi}^H \mathbf{H}_g'^H\right)}{4Q_i\sigma_g^2 + \beta^2 P_s \mathrm{tr}\left(\mathbf{H}_g' \mathbf{\Phi} \mathbf{D}_{ij} \mathbf{\Phi}^H \mathbf{H}_g'^H\right)} \\ & + \sum_{i=1}^{2k_G} \frac{4M_i Q_i \sigma^2}{4Q_i\sigma_g^2 + \beta^2 P_s \mathrm{tr}\left(\mathbf{H}_g' \mathbf{\Phi} \mathbf{D}_{ij} \mathbf{\Phi}^H \mathbf{H}_g'^H\right)} - \sum_{i=1}^{2k_G} M_i \\ \text{s.t.} \quad & \beta^2 \le 1,\end{aligned} \tag{5.68}$$

Using quadratic transform proposed in [38], (**P2**) can be reformulated as an equivalent optimization problem with a new objective function:

$$\begin{aligned}f(\beta) = & \sum_{i=1}^{2k_G} 2y_i \sqrt{(U_i + M_i)\,\mathrm{tr}\left(\mathbf{H}_g' \mathbf{\Phi} \mathbf{D}_{ij} \mathbf{\Phi}^H \mathbf{H}_g'^H\right)} \beta^2 P_s \\ & + \sum_{i=1}^{2k_G} 2y_i \sqrt{4M_i Q_i \sigma^2} - \sum_{i=1}^{2k_G} M_i \\ & - \sum_{i=1}^{2k_G} 2y_i^2 \left[4Q_i\sigma_g^2 + \beta^2 P_s \mathrm{tr}\left(\mathbf{H}_g' \mathbf{\Phi} \mathbf{D}_{ij} \mathbf{\Phi}^H \mathbf{H}_g'^H\right)\right],\end{aligned} \tag{5.69}$$

where the auxiliary variables y_i can be found in a closed-form expression as follows

$$y_i^* = \frac{\sqrt{h_i(\beta) + M_i g_i(\beta)}}{g_i(\beta)}, \ \forall i = 1, \cdots, 2k_G, \tag{5.70}$$

when $P_t = \beta^2 P_s$ is fixed.

Then, we have the Lagrangian function of (**P2-2-1**):

$$\begin{aligned}\mathcal{L}(\beta, \lambda) = & \sum_{i=1}^{2k_G} 2y_i \sqrt{(U_i + M_i)\,\mathrm{tr}\left(\mathbf{H}_g' \mathbf{\Phi} \mathbf{D}_{ij} \mathbf{\Phi}^H \mathbf{H}_g'^H\right)} \beta \\ & + \sum_{i=1}^{2k_G} 2y_i \sqrt{4M_i Q_i \sigma^2} - \sum_{i=1}^{2k_G} M_i - \lambda\left(\beta^2 P_s - 1\right) \\ & - \sum_{i=1}^{2k_G} 2y_i^2 \left[4Q_i\sigma_g^2 + \beta^2 P_s \mathrm{tr}\left(\mathbf{H}_g' \mathbf{\Phi} \mathbf{D}_{ij} \mathbf{\Phi}^H \mathbf{H}_g'^H\right)\right].\end{aligned} \tag{5.71}$$

And we get the KKT condition equations as follows

$$\begin{cases} \nabla_{\beta}\mathcal{L}(\beta,\lambda)=0, \\ \beta^2 P_s - 1 \geq 0, \\ \lambda(\beta^2 P_s - 1) = 0, \\ \lambda \geq 0. \end{cases} \tag{5.72}$$

which yields the solution

$$\begin{cases} \beta = \dfrac{\sum_{i=1}^{2k_G} y_i \sqrt{(U_i + M_i)\, P_s \mathrm{tr}\left(\mathbf{H}'_g \mathbf{\Phi} \mathbf{D}_{ij} \mathbf{\Phi}^H \mathbf{H}'^H_g\right)}}{\lambda + \sum_{i=1}^{2k_G} y_i^2 P_s \mathrm{tr}\left(\mathbf{H}'_g \mathbf{\Phi} \mathbf{D}_{ij} \mathbf{\Phi}^H \mathbf{H}'^H_g\right)}, \\ \lambda = 0. \end{cases} \tag{5.73}$$

Additionally, a step-by-step summary is provided as follows: Algorithm 3

Algorithm 3: Proposed Max-NASR-TPD transmit power method

Input: the channel matrix $\mathbf{H}'_B$ and $\mathbf{H}'_E$, $\mathbf{\Phi}$, P_s, the $\mathcal{M}$-ary constellation
Output: β

1: Initialize β^0 to a feasible value.
2: Initialize y_i^0 according to (5.70), step $k = 0$.
3: Reformulate the problem by the quadratic transform to get (5.68).
4: **repeat**
5: Update $k = k + 1$
6: Update y_i^k according to (5.70)
7: Update β^k by (5.73)
8: **until** $R_s(\beta^k) - R_s(\beta^{k-1}) \leq 10^{-4}$
9: **return** P_t

5.5.2 *Transmit Power Design Based on TASR*

In the previous section, the Max-NASR-TPD algorithm was presented to optimize the transmit power for higher SR. For the comparison of the secrecy performance and to offer a new solution to this non-convex optimization problem, we propose another secure transmit power scheme, namely Max-TASR-TPD based on the TASR expression, in what follows. To maximize $R_s^a(P_t)$, the Max-TASR-TPD method can be employed to directly optimize the transmit power P_t. We derive the gradient of $R_s^a(P_t)$ with respect to P_t applying $P_t = \beta^2 P_s$ as

$$\nabla_\beta R_s^a(\beta) = \frac{-\beta\sqrt{P_s}}{2\sigma^2 \ln 2} \times \left[\frac{1}{\kappa_E} \sum_{i=1}^{GM} \sum_{j=1}^{GM} \exp\left(\beta^2 P_s \alpha_{i,j}^e\right) \cdot \alpha_{i,j}^e \right.$$
$$\left. - \frac{1}{\kappa_B} \sum_{i=1}^{GM} \sum_{j=1}^{GM} \exp\left(\beta^2 P_s \alpha_{i,j}^b\right) \cdot \alpha_{i,j}^b \right], \tag{5.74}$$

where

$$\alpha_{i,j}^b = -\frac{\mathbf{d}_{i,j}^H \mathbf{H}_B'^H \mathbf{\Phi}^H \mathbf{\Phi} \mathbf{H}_B \mathbf{d}_{i,j}}{4\sigma^2}, \tag{5.75}$$

$$\alpha_{i,j}^e = -\frac{\mathbf{d}_{i,j}^H \mathbf{H}_E'^H \mathbf{\Phi}^H \mathbf{\Phi} \mathbf{H}_E \mathbf{d}_{i,j}}{4\sigma^2}, \tag{5.76}$$

$$\kappa_B = \log_2 \sum_{i}^{GM} \sum_{j}^{GM} \exp\left(\beta^2 P_s \alpha_{i,j}^B\right), \tag{5.77}$$

$$\kappa_E = \log_2 \sum_{i}^{GM} \sum_{j}^{GM} \exp\left(\beta^2 P_s \alpha_{i,j}^E\right). \tag{5.78}$$

In order to find a locally optimal β, we first initialize β and R_s^a, solve the gradient $\nabla_\beta R_s^a(\beta)$, and adjust P_t according to $\nabla_\beta R_s^a(\beta)$. The value of β is updated according to the following iterative formula

$$\beta_{k+1} = \beta_k + \mu \nabla_\beta R_s^a(\beta_k). \tag{5.79}$$

Then, obtain R_s^a, update β or step size μ according to the difference between before and after R_s^a, and repeat the above steps until the termination condition is reached.

5.6 Complexity Analysis

The unit of computational complexity is floating-point operations (FLOPs), which is omitted for convenience in what follows.

For the proposed Max-NASR-SCA method, the computational complexity is divided into three parts: (a) the computation of (5.31), (b) the computation of the function (5.43) using CVX, (c) the computation of NASR. For part (a), the computational complexity of $h_i(\mathbf{\Phi})$ is $M^2G^2(N^2N_b + 2N\overline{N})$, hence, α_i requires $C_{\alpha_i} = 2k_G(2N^2 + C_{h_i(\mathbf{\Phi})}) = 2k_G M^2 G^2 (N^2 N_b + 2N\overline{N}) + 4k_G N^2$. The highest-order computational complexity per iteration in part (b) is $O(N^3)$. We can easily get the computational complexity of part (c) from (5.20) and (5.21),

$$C_{NASR} = 2k_G(2N^2 + C_{h_i(\mathbf{\Phi})}). \tag{5.80}$$

Therefore, the computational complexity of Max-NASR-SCA method is:

$$C_{NASR-SCA} = D_{SCA}\Big(4k_G M^2 G^2 (N^2 N_b + 2N\overline{N}) + 8k_G N^2\Big), \tag{5.81}$$

where D_{SCA} denotes the iteration time of the SCA algorithm.

For the proposed Max-NASR-DA method, the computational complexity is composed of three parts: (a) the computation of auxiliary variables $h_i(\mathbf{\Phi})$ and y_i in Eqs. (5.48) and (5.50), (b) the computation of the Lagrangian function (5.52), (c) the computation of NASR. The computational complexity of $h_i(\mathbf{\Phi})$ requires $C_{h_i(\mathbf{\Phi})} = M^2 G^2 (N^2 N_b + 2N\overline{N})$, therefore, the complexity of part (a) is expressed:

$$\begin{aligned} C_a &= 2k_G(2N^2 + C_{h_i(\mathbf{\Phi})}) \\ &= 2k_G M^2 G^2 (N^2 N_b + 2N\overline{N}) + 4N^2 k_G. \end{aligned} \tag{5.82}$$

According to [41], the complexity of the Lagrangian function (5.52) is $2(N^3 + N^2(N + M))$, where N shows the dimension of the problem. The calculation of NASR is omitted here because it has been described previously.

Consequently, the computational complexity of Max-NASR-DA method is:

$$\begin{aligned} C_{NASR-DA} = D_{DA}\Big(&4k_G M^2 G^2 (N^2 N_b + 2N\overline{N}) \\ &+ 2\big(N^3 + N^2(N + M)\big) + 8N^2 k_G\Big), \end{aligned} \tag{5.83}$$

where D_{DA} stands for the iteration time of the DA method.

For the proposed Max-TASR-SDR, the computational complexity is partitioned into three parts: (a) the computation of the objective function in (5.63), (b) the computation of the SDP problem (5.63) using CVX, (c) the computation of TASR. For part (a), the computational complexity of the objective function in (5.63) requires $C_a = 2M^2 G^2 (2N^2 N_b + 3N\overline{N})$, The complexity of SDP problem (5.63) using CVX is $C_{SDP} = O\big(N^{4.5}\log(\frac{1}{\varsigma})\big) + 2M^2 G^2 (3N^2 N_b + 4N\overline{N})$, where ς denotes the accuracy of solution. For part (c), we have

$$C_{TASR} = 2M^2 G^2 (4N^2 + N_b + N_e). \tag{5.84}$$

As a result, the computational complexity of Max-TASR-SDR method is:

$$\begin{aligned} C_{TASR-SDR} = D_{SDR}\Big(&\big(N^{4.5}\log(\frac{1}{\varsigma})\big) + 2M^2 G^2 (3N^2 N_b + 4N\overline{N} \\ &+ 2N^2 N_b + 3N\overline{N} + 4N^2 + N_b + N_e)\Big), \end{aligned} \tag{5.85}$$

where D_{SDR} represents the iteration of SDR method.

As a contrast method, the computational complexity of gradient-based optimization in [42] is

$$C_{GA} = 2D_{GA}M^2G^2(11N^2 + N_b + N_e), \tag{5.86}$$

where D_{GA} denotes the iteration time of GA algorithm.

The complexity of Max-NASR-TPD is $2k_G D_{NASR-TPD}[M^2G^2(N^2+2N\overline{N})+4N^2]$, where $D_{NASR-TPD}$ indicates the iteration time. The complexity of MAX-TASR-TPD is $2k_G D_{TASR-TPD}M^2G^2(4N^2 + N_b + N_e)$, where $D_{TASR-TPD}$ expresses the iteration time.

The above analytical results show that, the computational complexities of the three proposed IRS optimizations and the gradient-based method are listed in an ascending order: GA, NASR-SCA, NASR-DA, and TASR-SDR.

Concerning the TPD, as the number of electromagnetic units N is the main impact factor, we can see that the proposed two TPD methods have the same highest order of computational complexity.

The complexity of the three combinations for the beamformer and TPD mentioned in Sect. 5.7, are detailed as follows,

$$\begin{aligned} C_{C1} &= D_{C1}(C_{NASR-DA} + C_{NASR-TPD}) \\ &= D_{C1}\{2D_{DA}\left(N^3 + N^2(N+M)\right) \\ &\quad + (4k_G D_{DA} + 2k_G D_{NASR-TPD})\left(M^2G^2(N^2+2N\overline{N})\right) \\ &\quad + 8k_G(D_{DA} + D_{NASR-TPD})\}, \end{aligned} \tag{5.87}$$

$$\begin{aligned} C_{C2} &= D_{C2}(C_{NASR-SCA} + C_{NASR-TPD}) \\ &= D_{C1}\{2D_{SCA}N^3 + (4k_G D_{DA} + 2k_G D_{NASR-TPD})\left(M^2G^2(N^2+2N\overline{N})\right) \\ &\quad + 8k_G(D_{DA} + D_{NASR-TPD})\}, \end{aligned} \tag{5.88}$$

and

$$\begin{aligned} C_{C3} &= D_{C3}(C_{TASR-SDR} + C_{TASR-TPD}) \\ &= D_{C3}\{D_{SDR}\Big(\big(N^{4.5}\log(\frac{1}{\varsigma})\big) + 2M^2G^2(3N^2N_b + 4N\overline{N} + 2N^2N_b + 3N\overline{N})\Big) \\ &\quad + 2(D_{SDR} + D_{TASR-TPD})M^2G^2(4N^2 + N_b + N_e)\}, \end{aligned} \tag{5.89}$$

where D_{C1}, D_{C2} and D_{C3} represent the number of outer layer iterations of each combination.

5.7 Simulation Results and Analysis

5.7.1 Rayleigh Fading Channel

In this section, we evaluate the performance of these beamformers and these transmit power methods. The system parameters are set as follows: $G = 4$, $N = 100$, $N_t = 1$, $P_s = N_t$W and quadrature phase shift keying (QPSK) modulation[43, 44]. For the convenience of simulation, it is assumed that the total transmit power $P = N_t$ W. For the sake of fairness of Bob and Eve, it is assumed that all noise variances in channels are identical, i.e., $\sigma_b^2 = \sigma_e^2$ and $N_b = N_e = 2$.

We compare our proposed algorithms to the following benchmark schemes:

(1) Case I: **IRS with no beamforming:** Obtain the maximum SR by optimizing beamforming vectors with the IRS phase-shift matrix set to zero with the magnitude set to one, i.e., $\mathbf{\Phi} = \mathbf{I}_{N\times N}$.

(2) Case II: **IRS with Random beamforming:** Obtain the maximum SR by optimizing the beamforming vectors with all the phase for each reflection element uniformly and independently generated from $[0,2\pi)$.

Figure 5.2 demonstrates the mutual information fitting results for the NASR which is proposed in Sect. 5.3 with BPSK and QPSK employed. For BPSK (Fig. 5.2a), the simulation results of NASR fits the curves of practical simulation results well with different number of IRS subsets in all SNR regions. As for QPSK (Fig. 5.2b), we have the same the conclusion about the accuracy of fitness.

When the Max-NASR-TPD transmit power strategy is adopted in IRS-aided SM, Fig. 5.3 demonstrates the curves of average SR versus SNR of the proposed Max-NASR-DA, proposed Max-NASR-SCA and proposed Max-TASR-SDR for $G = 4$ with the above Case I and Case II as the performance benchmarks. It is seen that the SR of the proposed Max-NASR-DA algorithm is much better than that of Max-NASR-SCA and Max-TASR-SDR in all average SNR regions. As the average

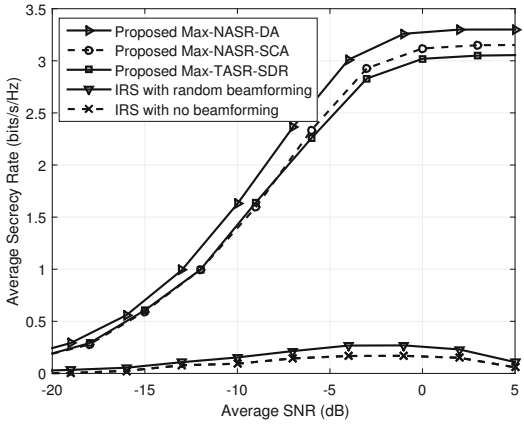


Fig. 5.3 Curves of average SR versus average SNR for different IRS beamforming algorithms with transmit power fixed with $G = 4$

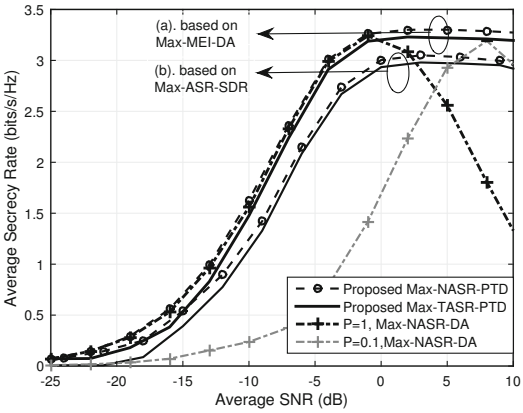


Fig. 5.4 Curves of average SR versus average SNR for different TPD methods with IRS beamformer fixed with $G = 4$

SNR increases, the Max-NASR-DA algorithm can approach the rate ceil of the achievable SR with a more rapid rate than Max-NASR-SCA and Max-TASR-SDR. This tendency implies that the SR performance of the proposed Max-NASR-DA beamformer is better than that of Max-TASR-SDR and Max-NASR-SCA. The SR performance of the proposed Max-NASR-SCA method is in a region between the proposed Max-TASR-SDR and Max-NASR-DA in the medium and high average SNR regions, and only slightly higher than the Max-TASR-SDR algorithm in the low average SNR region.

Now, we fix the IRS beamforming method, and make a performance comparison of two TPD strategies. Fig. 5.4 demonstrates the average SR versus average SNR of two TPD methods when $G = 4$ and $N = 100$. Figure 5.4a, we adopt the Max-NASR-DA method as IRS beamformer, it can be clearly seen that the proposed Max-NASR-TPD strategy has higher security performance than Max-TASR-TPD nearly in all average SNR regions. Meanwhile, Fig. 5.4b which adopt Max-TASR-SDR method as the fixed IRS beamformer, the tendency of the curves is the same as those in Fig. 5.4a. However, in all SNR regions, the proposed two methods outperform two fixed transmit power strategies in terms of SR. This confirms that TPD can improve the SR performance. Observing Fig. 5.4, we find the SRs of Max-NASR-TPD and Max-TASR-TPD increase as SNR increases. For the three fixed TPD strategies, their SRs first increase up to the corresponding maximum values, and then reduce gradually as SNR increases. The main reason is that their transmit power are fixed and independent of the change of SNR while the remaining two schemes adaptively adjust their transmit power in accordance with the exact value of SNR in the channel.

Figure 5.5 plots the maximum achievable SR versus transmit power with different SNR. From this figure, we can see that for all fixed SNR, the Max-NASR-TPD always approaches the value got from optimal ES better, where the configurations are the same as Fig. 5.4. Additionally, it can be observed that when SNR=0dB, the change of SR versus transmit power is generally gentle, while there is a slightly big difference between the transmit power solved by different algorithms, but the

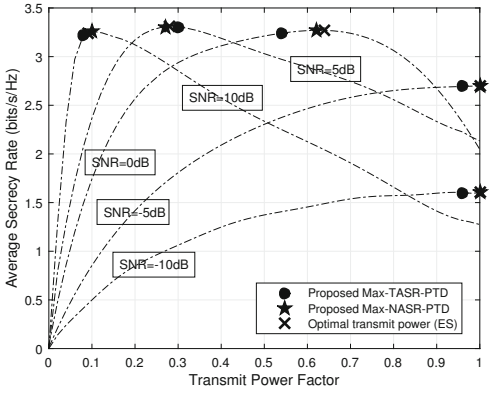


Fig. 5.5 Curves of average SR versus average β for different IRS beamforming algorithms with different SNR and $G = 4$

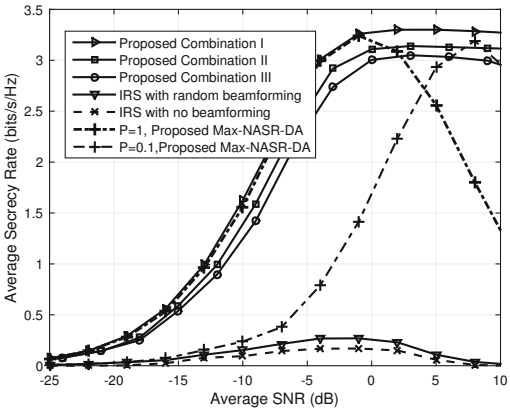


Fig. 5.6 Curves of average SR versus average SNR for different IRS beamforming algorithms and TPD algorithms with $G = 4$

corresponding SR value does not change much. As for under the other values of SNR, it can be observed that the change of SR versus transmit power becomes steeper, and the solutions obtained by the three different algorithms are relatively close.

Figure 5.6 plots the curves of the average SR versus average SNR for jointly optimizing IRS beamformer and transmit power with the previous Case I and Case II as the performance benchmarks. There are three combinations for the beamformer and TPD: (1) Combination I:Max-NASR-DA plus Max-NASR-TPD; (2) Combination II:Max-NASR-SCA plus Max-NASR-TPD; (3) Combination III:Max-TASR-SDR plus Max-TASR-TPD. From Fig. 5.6, it is obviously seen that the SR performance of Combination I performs much better than those of other combinations as Max-NASR-DA and Max-NASR-TPD both have the best security performance. Compared with Combination III, Combination I and Combination II harvest more SR performance gains in all SNR regions. And Combination II is between the proposed Combination I and Combination III in most SNR regions.

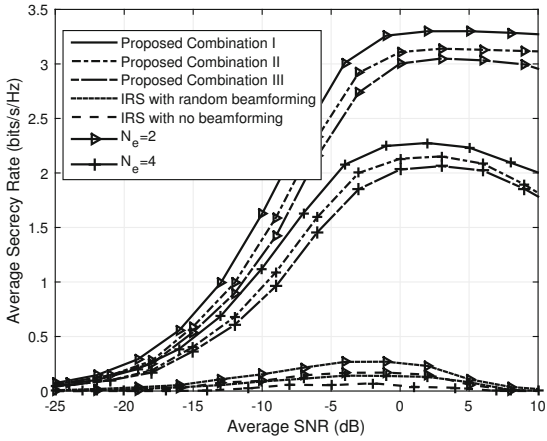


Fig. 5.7 Curves of average SR versus average SNR for different IRS beamforming algorithms and TPD algorithms with $G = 4$ and different N_e

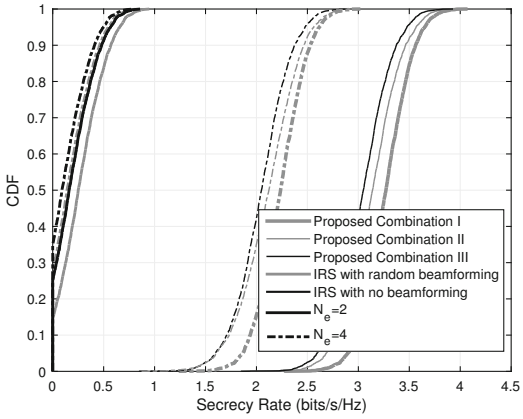


Fig. 5.8 CDF curves versus SR with $G = 4$ and different N_e

Figure 5.7 plots the average SR performance achieved by the above three combinations by fixing $G = 4$ and $N_b = 2$, and only changing N_e. When $N_b = N_e = 2$, as the average SNR increases, the SR curves increase until it reaches a certain average SNR, and then the curves will descend slightly. However, when N_e is larger than N_b, the SR will descend much when the average SNR is beyond some thresholds. As N_e increases, the SR curves can achieve the corresponding maximum SRs, and then decreases. This is because when the average SNR is very high, both Bob and Eve have a very good quality of channels, while Eve has a larger number of receive antennas than Bob, which is the worst situation, so the SR performance begins to decline.

Figure 5.8 shows the cumulative distribution function (CDF) curves of the three combinations for the different numbers of eavesdropper's antennas when average SNR = 5 dB. In this situation, Fig. 5.8 has the same descending trend in SR performance as Fig. 5.7: Combination I, Combination II and Combination III.

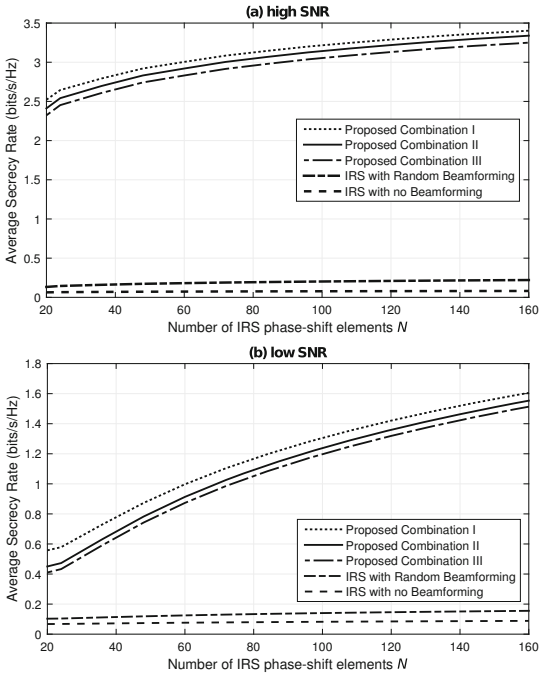


Fig. 5.9 Curves of average SR versus number of IRS phase-shift elements for different IRS beamforming algorithms and TPD algorithms with $G = 4$ and different N_e

In Fig. 5.9, we investigate the impact of the numbers of IRS phase-shift elements on SR performance under (a).low-SNR region and (b).high-SNR region, respectively. From Fig. 5.9a, b, it can be seen that the proposed three combinations improve the SR performance whether in the low-SNR regime or the high-SNR regime. As the number of IRS elements increases, the SR gains achieved by Combination I and Combination II over IRS with no beamforming and random phase grow gradually and become more significant. Compared with IRS with no beamforming and random phase scheme, the IRS phase-shift-optimization schemes and transmit power design performs much better, especially with a large value of N. This is explicit about the importance of the optimization of the phase-shift design. Even with a value of $N = 30$, our proposed scheme can also perform better than that scheme without the IRS phase-shift-optimization.

5.7.2 Rayleigh Fading Channel Considering Path Loss

A three-dimension coordinate system shown in Fig. 5.10 is considered, where the positions of Alice, IRS, Bob, and Eve are located at (d_{xa}m, 0m, 2m), (0m, d_ym, 2m), (d_{xb}m, d_{yb}m, 0m), (d_{xe}m, and d_{ye}m, 0m) respectively. All channels are assumed to follow the Rayleigh fading model and the path loss at the distance d is modeled as:

$$PL(d) = PL_0 - 10\alpha \log_{10}(\frac{d}{d_0}), \tag{5.90}$$

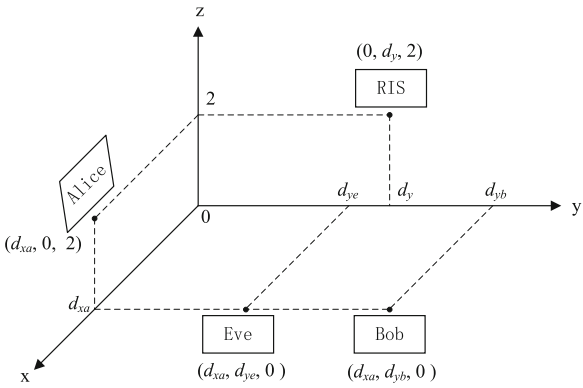


Fig. 5.10 3D coordinate diagram of IRS-SSM system

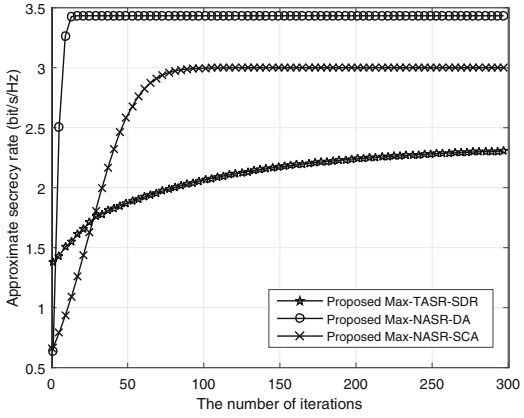


Fig. 5.11 Curves of average SR versus number of iterations for different IRS beamforming algorithms

where $PL_0 = -30\,\text{dB}$ represents the path loss when $d_0 = 1\text{m}$ and α denotes path loss exponent. In an IRS aided communication scenario [45], it is reasonable to place IRS near Alice or Bob to improve system performance. Thus, we place IRS near receiver and the parameters are set as $d_{xa} = d_{xb} = d_{xe} = 10, d_{yb} = 136$ and $d_{ye} = 115$. To investigate the impact of the IRS position on the safety performance when the IRS moves on the receiver side, $d_y \in [100, 145]$ is set. The path loss exponents of the Alice-IRS and IRS-Bob/Eve are set to be $\alpha_0 = 2.2$ and $\alpha_1 = 2.5$, respectively. Unless specified otherwise later, the other simulation parameters are set as: $G = 4$, $N = 16$, $N_t = 1$, $P_s = N_t\text{W}$ and quadrature phase shift keying (QPSK) modulation. For the convenience of simulation, it is assumed that the total transmit power $P = N_t$ W. For the sake of fairness of Bob and Eve, it is assumed that all noise variances in channels are identical, i.e., $\sigma_b^2 = \sigma_e^2$ and $N_b = N_e = 2$.

It is shown clearly in Fig. 5.11 that the approximate SRs of the three IRS beamformer designs change as the number of iterations increases. It can be seen from the figure that at the beginning of the iteration, the approximate SR value increases significantly, and as the iteration continues, the approximate SR value increases gradually until the convergence tolerance is reached. Moreover, from Fig. 5.11, we

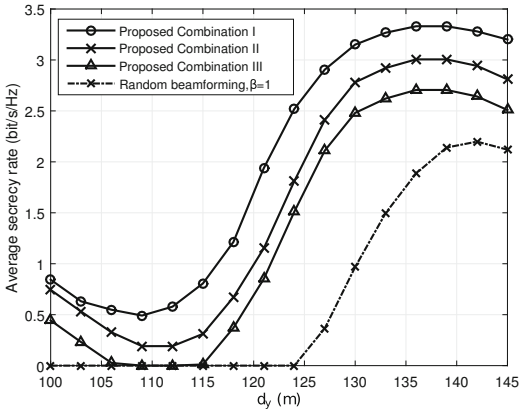


Fig. 5.12 Curves of average SR versus IRS position d_y for different IRS beamforming algorithms and TPD algorithms with G=4

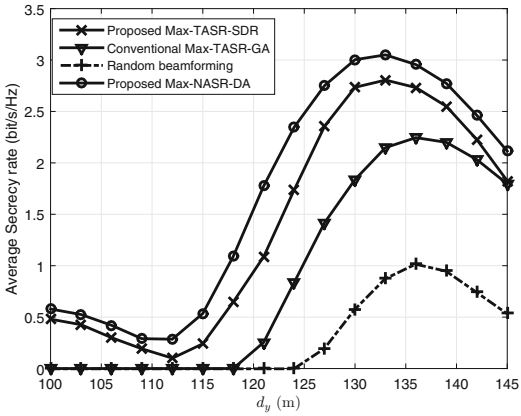


Fig. 5.13 Curves of average SR versus IRS position d_y for different IRS beamforming algorithms with β=0.5

can know that the convergence speeds of these methods have an ascending order: Max-NASR-DA, Max-NASR-SCA, and Max-TASR-SDR. In accordance with the complexity analysis mentioned, we can see that the computational complexity of the Max-NASR-DA scheme is the highest, which means that the optimization cost of the Max-NASR-DA scheme is higher, but the number of iterations is less. The Max-NASR-SCA scheme sacrifices a certain number of iterations in exchange for lower optimization complexity, while the Max-TASR-SDR scheme has the lowest optimization complexity, but also requires the highest number of iterations.

The impact of free-space path loss (FSPL) on secrecy performance of IRS-SSM is shown in Fig. 5.12. From this figure, it is observed that all curves have a similar trend. It is clearly shown that when IRS getting near the Eve, the average SR decreases. And with IRS getting close to Bob, the average SR increases rapidly. Moreover, when IRS moves away from Bob, the average SR declines as both Bob and Eve receive lower signal energy.

Figure 5.13 plots the average SR versus IRS position d_y for different IRS beamforming algorithms when the transmit power factor β is fixed at 0.5. The con-

ventional Max-TASR-GA IRS optimization and random beamforming are presented in Fig. 5.13 as performance benchhmarks. It is clearly shown in this figure that the security performances of the two proposed algorithms and the conventional TASR-GA algorithm are better than random beamforming, which shows the importance of IRS beamforming design. Besides, the performances of these three algorithms are listed in an ascending order: TASR-GA, TASR-SDR, NASR-DA. It is worth noting that when the IRS gets close to the Eve, the SR of the TASR-GA is 0, but the two proposed algorithms can still guarantee the secrecy performance of the system. Thus, compared with the traditional TASR-GA, the two algorithms proposed are more suitable for harsh communication environments.

5.8 Conclusion

In this book chapter, we have made a comprehensive investigation of IRS beamforming and transmit power design concerning IRS-SSM. In such an architecture, the first part of bitstream is transmitted by APM symbol, and the second part of bitstream is carried by selecting a subset in the IRS rather than a single transmit/receiver antenna. Considering the physical-layer security, a simple approximated SR expression was proposed. Based on the NASR and TASR, three IRS beamformers, Max-NASR-DA, Max-NASR-SCA and Max-TASR-SDR, were proposed. Simulation results showed that the proposed beamforming methods have an ascending order in SR: IRS with no beamforming, IRS with random beamforming, Max-TASR-SDR, Max-NASR-SCA and Max-NASR-DA. Particularly, two TPD methods were also proposed: Max-NASR-TPD and Max-TASR-TPD. Simulation results showed that the proposed TPD strategies have an ascending order in SR: fixed transmit power, Max-TASR-TPD and Max-NASR-TPD. Accordingly, either the IRS beamforming or the TPD algorithms based on the NASR performs better than those based on the TASR.

References

1. Wen, M., Zheng, B., Kim, K.J., Di Renzo, M., Tsiftsis, T.A., Chen, K.C., Al-Dhahir, N.: A survey on spatial modulation in emerging wireless systems: research progresses and applications. IEEE J. Sel. Areas Commun. **37**(9), 1949–1972 (2019)
2. Chau, Y., Yu, S.H.: Space modulation on wireless fading channels. In: IEEE 54th Vehicular Technology Conference. VTC Fall 2001. Proceedings (Cat. No.01CH37211). vol. 3, pp. 1668–1671 (2021)
3. Mesleh, R.Y., Haas, H., Sinanovic, S., Ahn, C.W., Yun, S.: Spatial modulation. IEEE Trans. Veh. Technol. **57**(4), 2228–2241 (2008)
4. Foschini, G.J.: Layered space-time architecture for wireless communication in a fading environment when using multi-element antennas. Bell Labs Tech. J. **1**(2), 41–59 (1996)
5. Yu, X., Leung, S.H., Wu, B., Rui, Y.: Power control for space-time-coded MIMO systems with imperfect feedback over joint transmit-receive-correlated channel. IEEE Trans. Veh. Technol. **64**(6), 2489–2501 (2015)

6. Renzo, M.D., Haas, H., Grant, P.M.: Spatial modulation for multiple-antenna wireless systems: a survey. IEEE Commun. Mag. **49**(12), 182–191 (2011)
7. Chen, X., Zhang, Y.: Mode selection in MU-MIMO downlink networks: a physical-layer security perspective. IEEE Syst. J. **11**(2), 1128–1136 (2017)
8. Trappe, W.: The challenges facing physical layer security. IEEE Commun. Mag. **53**(6), 16–20 (2015)
9. Shu, F., Wang, Z., Chen, R., Wu, Y., Wang, J.: Two high-performance schemes of transmit antenna selection for secure spatial modulation. IEEE Trans. Veh. Technol. **67**(9), 8969–8973 (2018)
10. Rajashekar, R., Hari, K.V.S., Hanzo, L.: Antenna selection in spatial modulation systems. IEEE Commun. Lett. **17**(3), 521–524 (2013)
11. Xia, G., Shu, F., Zhang, Y., Wang, J., ten Brink, S., Speidel, J.: Antenna selection method of maximizing secrecy rate for green secure spatial modulation. IEEE Trans. Green Commun. Netw. **3**(2), 288–301 (2019)
12. Xia, G., Lin, Y., Liu, T., Shu, F., Hanzo, L.: Transmit antenna selection and beamformer design for secure spatial modulation with rough CSI of Eve. IEEE Trans. Wireless Commun. **19**(7), 4643–4656 (2020)
13. Wang, Y., Xiong, W., Xiao, Y., Fang, S., Li, Y.: Transmit antenna selection in offset spatial modulation systems. IEEE Commun. Lett. **24**(7), 1572–1576 (2020)
14. Jin, S.R., Choi, W.C., Park, J.H., Park, D.J.: Linear precoding design for mutual information maximization in generalized spatial modulation with finite alphabet inputs. IEEE Commun. Lett. **19**(8), 1323–1326 (2015)
15. Yang, L.L.: Transmitter preprocessing aided spatial modulation for multiple-input multiple-output systems. In: Proceedings of IEEE Vehicular Technology Conference, pp. 1–5 (2011)
16. Shu, F., Liu, X., Xia, G., Xu, T., Li, J., Wang, J.: High-performance power allocation strategies for secure spatial modulation. Proc. IEEE Trans. Veh. Technol. **68**(5), 5164–5168 (2019)
17. Xia, G., Jia, L., Qian, Y., Shu, F., Zhuang, Z., Wang, J.: Power allocation strategies for secure spatial modulation. IEEE Syst. J. **13**(4), 3869–3872 (2019)
18. Zhao, N., Li, D., Liu, M., Cao, Y., Chen, Y., Ding, Z., Wang, X.: Secure transmission via joint precoding optimization for downlink MISO NOMA. IEEE Trans. Veh. Technol. **68**(9), 7603–7615 (2019)
19. Wang, W., Tang, J., Zhao, N., Liu, X., Zhang, X.Y., Chen, Y., Qian, Y.: Joint precoding optimization for secure SWIPT in UAV-aided NOMA networks. IEEE Trans. Commun. **68**(8), 5028–5040 (2020)
20. Zhao, N., Li, Y., Zhang, S., Chen, Y., Lu, W., Wang, J., Wang, X.: Security enhancement for NOMA-UAV networks. IEEE Trans. Veh Technol. **69**(4), 3994–4005 (2020)
21. Perovi, N.S., Liu, P., Blumenstein, J., Di Renzo, M., Springer, A.: Optimization of the cut-off rate of generalized spatial modulation with transmit precoding. IEEE Trans. Commun. **66**(10), 4578–4595 (2018)
22. Wang, L., Bashar, S., Wei, Y., Li, R.: Secrecy enhancement analysis against unknown eavesdropping in spatial modulation. IEEE Commun. Lett. **19**(8), 1351–1354 (2015)
23. Yu, X., Hu, Y., Pan, Q., Dang, X., Li, N., Shan, M.H.: Secrecy performance analysis of artificial-noise-aided spatial modulation in the presence of imperfect CSI. IEEE Access. **6**, 41060–41067 (2018)
24. Shu, F., Jiang, X., Liu, X., Xu, L., Xia, G., Wang, J.: Precoding and transmit antenna subarray selection for secure hybrid spatial modulation. IEEE Trans. Wireless Commun. **20**(3), 1903–1917 (2021)
25. Jiang, X., Liu, X., Chen, R., Wang, Y., Shu, F., Wang, J.: Precoding and transmit antenna subarray selection for secure hybrid spatial modulation. IEEE Trans. Veh. Technol. **70**(2), 1962–1966 (2021)
26. Wu, Q., Zhang, S., Zheng, B., You, C., Zhang, R.: Intelligent reflecting surface-aided wireless communications: a tutorial. IEEE Trans. Veh. Technol. **69**(5), 3313–3351 (2021)
27. Shi, W., Zhou, X., Jia, L., Wu, Y., Shu, F., Wang, J.: Enhanced secure wireless information and power transfer via intelligent reflecting surface. IEEE Commun. Lett. **25**(4), 1084–1088 (2021)

28. Shi, W., Li, J., Xia, G., Wang, Y., Zhou, X., Zhang, Y., Shu, F.: Secure multigroup multicast communication systems via intelligent reflecting surface. China Commun. **18**(3), 39–51 (2021)
29. Hong, S., Pan, C., Ren, H., Wang, K., Nallanathan, A.: Artificial-noise-aided secure MIMO wireless communications via intelligent reflecting surface. IEEE Trans. Commun. **68**(12), 7851–7866 (2020)
30. Pan, C., Ren, H., Wang, K., Xu, W., Elkashlan, M., Nallanathan, A., Hanzo, L.: Multicell MIMO communications relying on intelligent reflecting surfaces. IEEE Trans. Wireless Commun. **19**(8), 5218–5233 (2020)
31. Hua, M., Wu, Q., Ng, D.W.K., Zhao, J., Yang, Intelligent reflecting surface-aided joint processing coordinated multipoint transmission. IEEE Trans. Commun. **69**(3), 1650–1665 (2021)
32. Basar, E.: Reconfigurable intelligent surface-based index modulation: a new beyond MIMO paradigm for 6G. IEEE Trans. Commun. **68**(5), 3187–3196 (2020)
33. Yan, W., Yuan, X., He, Z.Q., Kuai, X.: Passive beamforming and information transfer design for reconfigurable intelligent surfaces aided multiuser MIMO systems. IEEE J. Sel. Areas Commun. **38**(8), 1793–1808 (2020)
34. Ma, T., Xiao, Y., Lei, X., Yang, P., Lei, X., Dobre, O.A.: Passive beamforming and information transfer design for large large intelligent surface assisted wireless communications with spatial modulation and antenna selection. IEEE J. Sel. Areas Commun. **38**(11), 2562–2574 (2020)
35. Yu, X., Shen, J.C., Zhang, J., Letaief, K.B.: Alternating minimization algorithms for hybrid precoding in millimeter wave MIMO systems. IEEE J. Sel. Topics Signal Process. **10**(3), 485–500 (2016)
36. Ouyang, C., Wu, S., Jiang, C., Cheng, J., Xiao, A., Yang, H.: Security enhancement via antenna selection in MIMOME channels with discrete inputs. IEEE Trans. Commun. **68**(8), 5041–5055 (2020)
37. Ouyang, C., Wu, S., Jiang, C., Ng, D.W.K., Yang, H.: Receive antenna selection under discrete inputs: approximation and applications. IEEE Trans. Commun. **68**(4), 2634–2647 (2020)
38. Shen, K., Yu, W.: Fractional programming for communication systems - part i: power control and beamforming. IEEE Trans. Signal Proc. **66**(10), 2616–2630 (2018)
39. Shen, K., Yu, W.: Fractional programming for communication systems - part ii: uplink scheduling via matching. IEEE Trans. Signal Proc. **66**(10), 2631–2644 (2018)
40. Grant, M., Boyd, S.: CVX: matlab software for disciplined convex programming (2016). http://cvxr.com/cvx
41. Lee, M.C., Chung, W.H., Lee, T.S.: Generalized precoder design formulation and iterative algorithm for spatial modulation in MIMO systems with CSIT. IEEE Trans. Commun. **63**(4), 1230–1244 (2015)
42. Perović, N.S., Tran, L.N., Renzo, M.D., Flanagan, M.F.: Optimization of RIS-aided MIMO systems via the cutoff rate. IEEE Wireless Commun. Lett. **10**(8), 1692–1696 (2021)
43. Zhu, H., Wang, J.: Chunk-based resource allocation in OFDMA systems - part I: chunk allocation. IEEE Trans. Commun. **57**(9), 2734–2744 (2009)
44. Zhu, H., Wang, J.: Chunk-based resource allocation in OFDMA systems - part II: joint chunk, power and bit allocation. IEEE Trans. Commun. **60**(2) 499–509 (2012)
45. Shu, F., Teng, Y., Li, J., Huang, M., Shi, W., Li, J., Wu, Y., Wang, J.: Enhanced secrecy rate maximization for directional modulation networks via IRS. IEEE Trans. Commun. **69**(12), 8388–8401 (2021)

Chapter 6
IRS-Aided Covert Wireless Communications with Delay Constraint

In this chapter, we examine the performance gain achieved by deploying an IRS in covert communications. To this end, we formulate the joint design of the transmit power and the IRS reflection coefficients by taking into account the communication covertness for the cases with global CSI and without a warden's instantaneous CSI. For the case of global CSI, we first prove that perfect covertness is achievable with the aid of the IRS even for a single-antenna transmitter, which is impossible without an IRS. Then, we develop a penalty successive convex approximation (PSCA) algorithm to tackle the design problem. Considering the high complexity of the PSCA algorithm, we further propose a low-complexity two-stage algorithm, where analytical expressions for the transmit power and the IRS's reflection coefficients are derived. For the case without the warden's instantaneous CSI, we first derive the covertness constraint analytically facilitating the optimal phase shift design. Then, we consider three hardware-related constraints on the IRS's reflection amplitudes and determine their optimal designs together with the optimal transmit power. Our examination shows that significant performance gain can be achieved by deploying an IRS into covert communications.

6.1 Introduction

To meet the ever-increasing demand for high-data rate applications and massive connections in wireless networks, multiple advanced technologies, such as massive MIMO, mmWave, and ultra-dense network (UDN), have been advocated [1, 2]. However, these technologies generally suffer from high energy consumption or high hardware complexity, due to the use of a large number of power-hungry RF chains. As a remedy, IRS is emerging as a promising solution to improving the spectral and energy efficiency effectively [3]. Specifically, IRS is a planar surface consisting of a large number of re-configurable and low-cost passive reflecting elements, each of

F. Shu, J. Wang, *Intelligent Reflecting Surface-Aided Physical-Layer Security*,
Wireless Networks, https://doi.org/10.1007/978-3-031-41812-9_6

which is able to reflect the incident signals with controllable amplitudes and phase shifts. Thus, IRS can customize the propagation environment from the transmitter to receiver to achieve various design objectives (e.g., signal enhancement, interference suppression).

Due to the aforementioned advantages, IRS has been investigated in various application scenarios, e.g., single-user systems [4, 5], multi-user systems [6–11], and wireless information and power transfer systems [12, 13], and it has been considered as a promising technology for enabling the 6G wireless networks [14, 15].

Recently, considering the increasing concerns on security issues in wireless communications, several recent works addressed communication security in the context of IRS-assisted wireless networks from the perspective of physical layer security, e.g., [16–23]. In general, the secrecy performance of IRS-assisted networks can be improved by properly designing the IRS reflection coefficients to simultaneously enhance the received signal strength at desired users and weaken them at eavesdroppers. For example, as shown in [16], by jointly optimizing the transmit beamforming together with the reflect beamforming, physical layer security is guaranteed in IRS-assisted network, even if the eavesdropping channel quality is higher than that of the legitimate channel. Along this direction, an alternative optimization algorithm based on SDP relaxation technique was proposed to determine the secure transmit beamforming and reflecting phase shifts in [17]. In addition, the authors of [18] tackled the question whether and when AN is beneficial to the physical layer security in IRS-assisted wireless communication systems. Meanwhile, MIMO wiretap channels were considered in [19–21] for optimizing the transmit covariance matrix and IRS phase shifts, and the channel imperfectness on multiuser MISO and MIMO wireless secure communications were considered in [22] and [23], respectively.

The aforementioned physical layer security technologies focus on protecting the content of the transmitted message against eavesdropping. However, these technologies cannot alleviate privacy issues posed by discovering the presence of the transmitter or transmissions. Fortunately, the emerging and cutting-edge covert communication technology, which aims at hiding the existence of a wireless transmission, is able to preserve such a high-level security and privacy [24]. In general, a positive covert transmission rate can be achieved when the warden (Willie) has various uncertainties, e.g., noise uncertainty [25] and channel uncertainty [26]. In particular, the fundamental limits of covert communication in AWGN channels was established in [27], where the authors proved that at most $O(\sqrt{n})$ bits of information can be covertly and reliably conveyed to from a transmitter (Alice) to a desired receiver (Bob) over n channel uses. In addition, covert communication with the help of a FD receiver was examined in [28], where a FD receiver generates AN with a random transmit power to deliberately confuse Willie's detection. Inspired by this, the authors of [29] introduced an uninformed jammer to impose artificial uncertainty on Willie. It was revealed that, under the average covertness constraint, the optimal transmit power strategy is in the form of truncated channel inversion. Meanwhile, covert communication in relaying networks and UAV networks was examined

in [30] and [31, 32], respectively. Furthermore, the conditions for guaranteeing the optimality of Gaussian signalling for covert communication was addressed in [33]. Most recently, covert communication in random wireless networks and covert communication with delay constraints were investigated in [34, 35] and [36], respectively.

Although the aforementioned works on covert communication, i.e., [24–36], have studied various strategies to improve its performance, the achievable covert communication rate is still in a low regime due to the stringent covertness requirement (e.g., a low transmit power). We note that the IRS has the capability of simultaneously enhancing the received signals at a legitimate receiver and deteriorating them at a warden. Therefore, the IRS technique is practically appealing in improving covert communication performance, which has been pointed out in a recently published magazine article [37]. In addition, the impact of a warden's noise uncertainty on IRS-assisted covert communication was examined under the assumption of infinite number of channel uses (i.e., without delay constraints) in [38], where the reflection beamforming was optimized with fixed IRS reflection amplitudes. We note that the communication delay from a transmitter to a receiver generally increases as the number of channel uses increases. In order to meet the requirement in some low-latency applications (e.g., real-time video processing, connected vehicles), a short packet (i.e., a finite blocklength) should be considered. We also note that the finite blocklength implies that the transmission should occur within the available channel uses, which is essentially a delay constraint. In addition, covert communications with a finite blocklength is fundamentally different from that with an infinite blocklength, which is due to that the decoding error probability is not negligible in short-packet communications. As such, the main challenge of the covert communications with a finite blocklength arises from that the coding strategy needs to balance between the receiver's decoding error probability and the warden's detection error rate. Furthermore, in the context of covert communication, fixing the IRS reflection amplitudes to 1 may limit its performance and thus may not be optimal. Against this background, this work considers the delay-constrained IRS-assisted covert communication, where Alice wants to transmit information to Bob covertly in a finite blocklength with the aid of an IRS, while Willie intends to detect the existence of this transmission. We jointly design Alice's transmit power, the IRS reflection amplitudes and phase shifts to enhance covert communication performance. The main contributions of this work are summarized as below.

- Considering global CSI being available, we prove that perfect covertness (i.e., Willie's detection is equivalent to a random guess) with non-zero transmit power is achievable for a single-antenna Alice in the IRS-assisted covert communication system. Specifically, our analysis reveals that the condition for achieving the perfect communication covertness is that the quality of the channel of Alice-IRS-Willie is better than that of the channel Alice-Willie. Intuitively, this is due to that the reflected signals from the IRS is able to cancel the signals transmitted from Alice directly to Willie. It is found that without the deployment of an IRS, it is impossible to achieve such perfect covertness for a single-antenna Alice,

due to the lack of a null space in the channel from Alice to Willie. This result demonstrates the importance of IRS for covert communication.

- With the global CSI, we first prove that the covertness constraint is convex. We then transform the optimization problem into a generalized nonlinear convex programming (GNCP) and develop a PSCA algorithm to jointly optimize Alice's transmit power together with the reflection amplitudes and phase shifts at the IRS. In order to reduce the computational complexity, we further develop a low-complexity two-stage algorithm, where we derive analytical expressions for Alice's transmit power and the IRS's reflection coefficients.
- Considering the case without Willie's instantaneous CSI, we first prove that the Kullback-Leibler (KL) divergence adopted in the covertness constraint is a monotonically increasing function of the received power at Willie, based on which we derive a closed-form expression for the covertness constraint in this case. Our analysis reveals that the covertness constraint is independent of the phase shift of each IRS element, which only affects the signal-to-noise ratio (SNR) at Bob. This observation facilitates the design of the optimal IRS phase shifts. Then, we consider three different practical constraints on the IRS's reflection amplitudes ρ_n, i.e., $\rho_n = 1, \forall n$, $\rho_n = \rho_0, \forall n$, and $0 \leq \rho_n \leq 1, \forall n$, under which the IRS's reflection amplitudes and Alice's transmit power are determined. Our examination shows that the considered IRS-assisted system can significantly outperform the system without an IRS in the context of covert communications in both the considered CSI scenarios.

The remainder of this work is organized as follows. Section 6.2 presents the considered system model. Sections 6.3 and 6.4 respectively present the covert communication design for the cases with global CSI and without Willie's instantaneous CSI. Section 6.5 provides our numerical results, where the impact of the IRS's location is also examined. This book chapter is concluded in Sect. 6.6.

Notation Vectors and matrices are denoted by Boldface lowercase and uppercase letters, respectively. $\mathbf{A}^T$, $\mathbf{A}^H$, represent transpose, conjugate transpose, respectively, while $\mathbf{A} \succeq \mathbf{0}$ denotes semidefiniteness of matrix $\mathbf{A}$. $\mathbb{E}_x[\cdot]$, $\arg(\cdot)$, $\|\cdot\|$, $\|\cdot\|_1$, and $|\cdot|$ denote the statistical expectation of x, phase, ℓ_2-norm, ℓ_1-norm, and the absolute value, respectively. $\Pr\{\cdot\}$ and $\mathcal{CN}(\mu, \sigma^2)$ denote the probability of an event and Gaussian distribution with mean μ and variance σ^2, respectively.

6.2 System Model

6.2.1 Considered Scenario and Assumptions

As shown in Fig. 6.1, we consider an IRS-assisted covert communication system, where Alice intends to transmit information to Bob covertly with the aid of an IRS, while a warden Willie seeks to detect the existence of this transmission. We assume

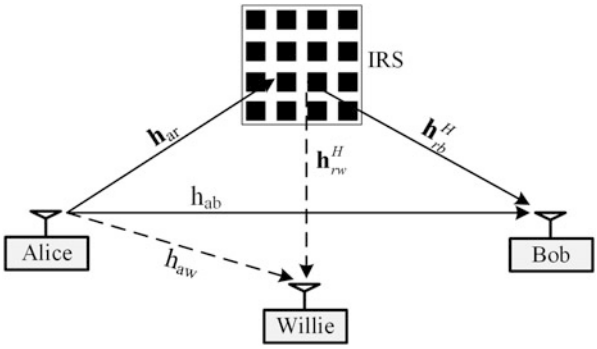


Fig. 6.1 IRS-assisted wireless covert communications

that each of Alice, Bob, and Willie is equipped with a single antenna. The IRS is equipped with N passive reflecting elements and the reflection coefficient (including phase shift and reflection amplitude) of each reflecting element can be dynamically adjusted based on the propagation environment. In addition, it is assumed that the signals reflected by the IRS twice or more are ignored due to the significant path loss [8]. All channels in the considered system are subject to quasi-static flat-fading. Specifically, the baseband equivalent channels from Alice to IRS, Bob and Willie are denoted by $\mathbf{h}_{ar} = \sqrt{\chi_{ar}}\bar{\mathbf{h}}_{ar}$, $h_{ab} = \sqrt{\chi_{ab}}\bar{h}_{ab}$, and $h_{aw} = \sqrt{\chi_{aw}}\bar{h}_{aw}$, respectively, while the channels from IRS to Bob and to Willie are denoted by $\mathbf{h}_{rb}^{H} = \sqrt{\chi_{rb}}\bar{\mathbf{h}}_{rb}^{H}$ and $\mathbf{h}_{rw}^{H} = \sqrt{\chi_{rw}}\bar{\mathbf{h}}_{rw}^{H}$, respectively. In addition, χ_{ij} denotes the large-scale path loss, where $ij \in \{ar, ab, aw, rb, rw\}$ corresponding to different channels, while $\bar{\mathbf{h}}_{ar}$, $\bar{h}_{ab}$, $\bar{h}_{aw}$, $\bar{\mathbf{h}}_{rb}^{H}$, and $\bar{\mathbf{h}}_{rw}^{H}$ are the corresponding small-scale fading coefficients. We denote $\boldsymbol{\Theta} = \text{diag}\left(\rho_1 e^{j\theta_1}, \rho_2 e^{j\theta_2}, \cdots, \rho_N e^{j\theta_N}\right)$ as the diagonal reflecting matrix of IRS, where $\theta_n \in [0, 2\pi)$ and $\rho_n \in [0, 1]$, $n = 1, 2, \cdots, N$, represent the phase shift and reflection amplitude on the combined incident signal at the n-th element, respectively. Furthermore, we assume that the signal transmitted by Alice in the i-th channel use is denoted by $x[i], \forall i \in \{1, 2, \cdots, L\}$, where $x[i] \sim \mathcal{CN}(0, 1)$ and L is the total number of channel uses, which is the total number of symbols transmitted over the considered fading block.

6.2.2 Binary Hypothesis Testing at Willie

In this work, we focus on delay-constrained covert communications, i.e., the number of channel uses L is finite. In order to detect the existence of the transmission, Willie is required to distinguish between the following two hypotheses:

$$y_w[i] = \begin{cases} n_w[i], & \mathcal{H}_0, \\ \sqrt{P_a}\left(\mathbf{h}_{rw}^H \boldsymbol{\Theta} \mathbf{h}_{ar} + h_{aw}\right) x[i] + n_w[i], & \mathcal{H}_1, \end{cases} \tag{6.1}$$

where $y_w[i]$ is the received signal at Willie for the i-th channel use, $\mathcal{H}_0$ denotes the null hypothesis in which Alice does not transmit, and $\mathcal{H}_1$ denotes alternative hypothesis in which Alice transmits information to Bob. In addition, P_a is the transmit power of Alice and $n_w[i]$ is the AWGN at Willie with zero mean and variance σ_w^2. Following (6.1), the false alarm rate and miss detection rate at Willie are given by $\Pr\{\mathcal{D}_1|\mathcal{H}_0\}$ and $\Pr\{\mathcal{D}_0|\mathcal{H}_1\}$, respectively, where $\mathcal{D}_1$ and $\mathcal{D}_0$ are the binary decisions that infer whether Alice's transmission occurred or not. Then, the total detection error rate at Willie is given by

$$\xi = \pi_0 \Pr\{\mathcal{D}_1|\mathcal{H}_0\} + \pi_1 \Pr\{\mathcal{D}_0|\mathcal{H}_1\}, \tag{6.2}$$

where π_0 and $\pi_1 = 1 - \pi_0$ denote the *priori* probabilities of hypotheses $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively. We note that the knowledge of the *priori* probabilities is beneficial to improving Willie's detection performance. In this work, we assume $\pi_0 = \pi_1 = 0.5$ (i.e., equal *priori* probabilities), which has been widely adopted in covert communications (e.g., [32, 35]).

In covert communications, Willie wishes to minimize its total detection error rate ξ to detect the presence of the transmission. The optimal test that minimizes ξ is the likelihood ratio test, which is given by

$$\frac{\mathbb{P}_1 \triangleq \prod_{i=1}^{L} f(y_w[i]|\mathcal{H}_1)}{\mathbb{P}_0 \triangleq \prod_{i=1}^{L} f(y_w[i]|\mathcal{H}_0)} \underset{\mathcal{D}_0}{\overset{\mathcal{D}_1}{\gtrless}} 1, \tag{6.3}$$

where $\mathbb{P}_0$ and $\mathbb{P}_1$ are the likelihood functions of Willie's observation vector over L independent channel uses under $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively. We have $f(y_w[i]|\mathcal{H}_0) = \mathcal{CN}(0, \sigma_w^2)$ and $f(y_w[i]|\mathcal{H}_1) = \mathcal{CN}(0, P_a|\mathbf{h}_{rw}^H \boldsymbol{\Theta} \mathbf{h}_{ar} + h_{aw}|^2 + \sigma_w^2)$ as the likelihood function of $y_w[i]$ under $\mathcal{H}_0$ and $\mathcal{H}_1$, respectively. We note that the optimal detection threshold and the corresponding minimum detection error rate ξ^* at Willie can be derived based on (6.3) [36]. However, the resultant expression for ξ^* involves incomplete gamma functions, which is not tractable for subsequent analysis and design. To overcome this difficulty, we present a lower bound on ξ^*, which is given by Bash et al. [27]

$$\xi^* \geq 1 - \sqrt{\frac{1}{2}\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1)}, \tag{6.4}$$

where $\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1)$ is the KL divergence from $\mathbb{P}_0$ to $\mathbb{P}_1$, and given by Yan et al. [36]

$$\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1) = L\left[\ln\left(1+\frac{P_a|\mathbf{h}_{rw}^H\boldsymbol{\Theta}\mathbf{h}_{ar}+h_{aw}|^2}{\sigma_w^2}\right)-\frac{P_a|\mathbf{h}_{rw}^H\boldsymbol{\Theta}\mathbf{h}_{ar}+h_{aw}|^2}{P_a|\mathbf{h}_{rw}^H\boldsymbol{\Theta}\mathbf{h}_{ar}+h_{aw}|^2+\sigma_w^2}\right]. \tag{6.5}$$

Following the fact that $\mathbf{h}_{rw}^H\boldsymbol{\Theta}\mathbf{h}_{ar} = \mathbf{v}^H\text{diag}(\mathbf{h}_{rw}^H)\mathbf{h}_{ar}$, $|\mathbf{h}_{rw}^H\boldsymbol{\Theta}\mathbf{h}_{ar}+h_{aw}|^2$ can be equivalently rewritten as $|\mathbf{v}^H\mathbf{a}+h_{aw}|^2$, where $\mathbf{v} = [v_1, v_2, \cdots, v_N]^T$, $\mathbf{a} = \text{diag}(\mathbf{h}_{rw}^H)\mathbf{h}_{ar}$ and $v_n = \rho_n e^{-j\theta_n}, \forall n$.

In covert communications, $\xi^* \geq 1-\epsilon$ is generally adopted as the covertness constraint, where ϵ is a small value to determine the required covertness level. As per (6.4), we note that $\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1) \leq 2\epsilon^2$ is a more stringent constraint than the constraint $\xi^* \geq 1-\epsilon$. As such, in this work we adopt $\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1) \leq 2\epsilon^2$ as the required covertness constraint.

6.2.3 *Transmission from Alice to Bob*

When Alice transmits information, the received signal at Bob for the i-th channel use can be expressed as

$$y_b[i] = \sqrt{P_a}\left(\mathbf{h}_{rb}^H\boldsymbol{\Theta}\mathbf{h}_{ar}+h_{ab}\right)x[i]+n_b[i], \tag{6.6}$$

where $n_b[i]$ is the AWGN at Bob with zero mean and variance σ_b^2. The corresponding SNR at Bob is given by

$$\gamma_b = \frac{P_a}{\sigma_b^2}|\mathbf{h}_{rb}^H\boldsymbol{\Theta}\mathbf{h}_{ar}+h_{ab}|^2 = \frac{P_a}{\sigma_b^2}|\mathbf{v}^H\mathbf{b}+h_{ab}|^2, \tag{6.7}$$

where $\mathbf{b} = \text{diag}(\mathbf{h}_{rb}^H)\mathbf{h}_{ar}$.

We should point out that the decoding error probability δ at Bob is not negligible for a fixed transmission rate R, when the number of channel uses L is finite. As such, the effective throughput, i.e., $LR(1-\delta)$, can be employed to quantify the covert transmission performance of the considered delay-constrained scenario. We note that the effective throughput increases with L. However, Willie would have more observations to detect the covert communication as L increases, which improves his detection performance. We also note that $\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1)$ is a monotonicity increasing function of $P_a|\mathbf{h}_{rw}^H\boldsymbol{\Theta}\mathbf{h}_{ar}+h_{aw}|^2$. As such, we can reduce the value of $P_a|\mathbf{h}_{rb}^H\boldsymbol{\Theta}\mathbf{h}_{ar}+h_{ab}|^2$ by properly designing the transmit power P_a and IRS reflection beamforming in order to limit the value of $\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1)$ when L increases, in order to satisfy the covertness constraint. The recent works [36] and [39] revealed that the optimal number of channel uses in the delay-constraint covert communications is the maximum allowable number of channel uses and the effective throughput is an increasing function of γ_b for a fixed transmission rate R. As such, in this work

we use γ_b to evaluate the communication quality from Alice to Bob, and then we aim to maximize γ_b subject to the covertness constraint $\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1) \leq 2\epsilon^2$ and other practical constraints.

6.3 Covert Communication Design with Global Channel State Information

In this section, we assume that the CSI of all channels in the considered system is publicly available, which enables us to obtain an upper bound on the performance gain achieved by introducing IRS into covert communications. We note that the acquisition of accurate CSI in IRS-aided communication systems is practically challenging, since the total number of channel coefficients that need to be estimated are significantly increased compared with the case without IRS, while IRS is generally without active transmit RF chains. This challenge was addressed in the literature. For example, the recent works [40] and [41] respectively proposed a matrix-calibration based cascaded channel estimation method and a parallel factor decomposition based framework, which can accurately estimate the involved channels in IRS-aided systems.

6.3.1 Optimization Problem and Perfect Covertness Condition

Our goal is to maximize the received SNR at Bob by jointly designing the transmit power at Alice and reflect beamforming vector $\mathbf{v}$ (i.e., the phase shifts and reflection amplitudes) at the IRS, subject to the covertness constraint and the maximum transmit power constraint at Alice together with the IRS reflection coefficients constraint. The formulated optimization problem can be written as

$$(\text{P1}): \max_{P_a, \mathbf{v}} \; P_a |\mathbf{v}^H \mathbf{b} + h_{ab}|^2 \tag{6.8a}$$

$$\text{s.t.} \quad \mathcal{D}(\mathbb{P}_0|\mathbb{P}_1) \leq 2\epsilon^2, \tag{6.8b}$$

$$P_a \leq P_{\max}, \tag{6.8c}$$

$$|v_n| \leq 1, \forall n = 1, 2, \cdots, N, \tag{6.8d}$$

where σ_b^2 is omitted in the objective function (6.8a), since it is a constant term. In addition, (6.8b) is the covertness constraint and (6.8d) is due to $\rho_n \in [0, 1]$, since the IRS cannot amplify signals. We note that, following [42] and [43], constraint (6.8d) implies that the reflection amplitude and phase shift of each IRS element can be independently adjusted over $[0, 1]$ and $[0, 2\pi)$, respectively.

We should point out that for some specific hardware implementations, IRS reflection amplitudes may depend on its phase shifts, which leads to that the reflection amplitudes and phase shifts are coupled [44]. As such, the independent design of IRS reflection amplitudes and phase shifts may suffer from a certain performance degradation caused by this coupling impact. Meanwhile, some existing works (e.g., [42, 43]) expected that near future hardware improvement may support the feasibility that the IRS reflection amplitudes and phase shifts can be adjusted independently. On the other hand, the formulated optimization problem (P1) jointly designs the reflection amplitudes and phase shifts of the IRS, where only designing the phase shifts of the IRS serves as a special case. In addition, the considered joint design can help us obtain an upper bound on the performance gain achieved by introducing an IRS into covert communications. Furthermore, it can also help us determine the impact of IRS amplitude control on delay-constraint covert communications.

We note that the considered representative single-antenna setup enables us to identify the fundamental reasons why IRS is beneficial to covert communications and to facilitate us to draw useful insights regarding the impacts of different system parameters on the system performance. The extension of the considered setup to the one with multi-antenna transceivers (e.g., Alice, Bob, and Willie) requires the joint optimization of transmit beamforming and IRS's reflection coefficients. For this joint optimization, the number of data streams transmitted from Alice to Bob and the observation correlation at different antennas should be considered. In addition, the number of antennas at Alice and Willie could significantly affect the optimal design together with the achievable communication covertness of such a multi-antenna system, e.g., the conditions for achieving perfect communication covertness. This is beyond the scope of the chapter and such an extension is left for future work.

Before solving the problem (P1), in the following theorem, we first identify the conditions for achieving perfect covertness (i.e., $\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1) = 0$) with non-zero transmit power in the considered IRS-assisted covert communication system. We note that when the blocklength is finite, perfect covertness is not achievable in covert communication systems without an IRS (e.g., [36]).

Theorem 6.1 *Perfect covertness can be achieved with non-zero transmit power, i.e., the below optimization problem*

$$(\mathrm{P1}') \max_{P_a, \mathbf{v}} \; P_a |\mathbf{v}^H \mathbf{b} + h_{ab}|^2 \tag{6.9a}$$

$$\text{s.t.} \quad P_a |\mathbf{v}^H \mathbf{a} + h_{aw}|^2 = 0, \tag{6.9b}$$

$$P_a \le P_{\max}, \tag{6.9c}$$

$$|v_n| \le 1, \forall n = 1, 2, \cdots, N. \tag{6.9d}$$

is feasible, if and only if $\sum_{n=1}^{N} |a_n| \ge |h_{aw}|$, *where* a_n *is the n-th element of* $\mathbf{a} = \mathrm{diag}(\mathbf{h}_{rw}^H)\mathbf{h}_{ar}$.

Proof The detailed proof is provided in Appendix. □

We note that $\mathbf{v}^H\mathbf{a}$ is the equivalent channel coefficient of reflect-path from Alice to Willie through the IRS. We also note that $\sum_{n=1}^{N}|a_n| = ||\mathbf{a}||_1$, which can be equivalently written as $||\mathbf{a}||_1 = |\mathbf{v}^H\mathbf{a}|_1$ when $\rho_n = 1, \forall n$. In addition, h_{aw} is the channel coefficient of direct-path from Alice to Willie. Thus, Theorem 6.1 implies that when the channel quality of the reflect-path is higher than that of the direct-path, perfect covertness can be achieved. Interestingly, Theorem 6.1 also reveals that the additional reflect-path can deteriorate Willie's detection performance (i.e., Willie receives less covert information energy transmitted by Alice), when the reflect beamforming is properly designed. This essentially shows that the IRS is capable of effectively improving the communication covertness, which will be explicitly examined through solving the optimization problem (P1). We should point out that under the condition of achieving perfect covertness as given in Theorem 1, an eavesdropper is not able to wiretap any information from the legitimate transmission, since the eavesdropper cannot receive any useful signal for decoding the confidential information, which indicates that this condition can also be applied to guarantee the physical layer security [45].

It should be emphasized that problem (P1′) given in (6.9) is a special case of the problem (P1), where (P1) is non-convex due to the non-concave objective function and the non-convex covertness constraint (6.8b). In the following, we first propose a joint design based on PSCA algorithm to solve (P1) and then we develop a low-complexity solution to balance the computational complexity and the achievable covert communication performance.

6.3.2 *Joint Transmit Power and Reflect Beamforming Design*

In this subsection, we first transform problem (P1) into a GNCP problem. Then, a PSCA algorithm is developed to solve the resultant problem. To proceed, we first note that $P_a|\mathbf{v}^H\mathbf{b} + h_{ab}|^2$ in the objective function (6.8a) and the term $P_a|\mathbf{v}^H\mathbf{a} + h_{aw}|^2$ in the covertness constraint (6.8b) can be equivalently rewritten as

$$P_a\left(\mathbf{v}^H\mathbf{b}\mathbf{b}^H\mathbf{v} + 2\mathrm{Re}(\mathbf{v}^H\mathbf{b}h_{ab}^*t) + |h_{ab}|^2|t|^2\right), \tag{6.10}$$

$$P_a\left(\mathbf{v}^H\mathbf{a}\mathbf{a}^H\mathbf{v} + 2\mathrm{Re}(\mathbf{v}^H\mathbf{a}h_{aw}^*t) + |h_{aw}|^2|t|^2\right), \tag{6.11}$$

respectively, where the newly introduced slack variable t satisfies $|t|^2 = 1$. In fact, (6.10) and (6.11) can be further rewritten into a quadratic forms $P_a\mathbf{u}^H\mathbf{B}\mathbf{u}$ and $P_a\mathbf{u}^H\mathbf{A}\mathbf{u}$, respectively, where

$$\mathbf{u}=\begin{bmatrix}\mathbf{v}\\ t\end{bmatrix}, \mathbf{B}=\begin{bmatrix}\mathbf{b}\mathbf{b}^H & \mathbf{b}h_{ab}^*\\ h_{ab}\mathbf{b}^H & |h_{ab}|^2\end{bmatrix}, \mathbf{A}=\begin{bmatrix}\mathbf{a}\mathbf{a}^H & \mathbf{a}h_{aw}^*\\ h_{aw}\mathbf{a}^H & |h_{aw}|^2\end{bmatrix}. \tag{6.12}$$

Following the above transformations, (P1) can be equivalently rewritten as

$$(\text{P1.1}): \max_{P_a,\mathbf{u}} \ P_a\mathbf{u}^H\mathbf{B}\mathbf{u} \tag{6.13a}$$

$$\text{s.t.} \ \ln\left(1+\frac{P_a\mathbf{u}^H\mathbf{A}\mathbf{u}}{\sigma_w^2}\right)-\frac{P_a\mathbf{u}^H\mathbf{A}\mathbf{u}}{P_a\mathbf{u}^H\mathbf{A}\mathbf{u}+\sigma_w^2}\le\frac{2\epsilon^2}{L}, \tag{6.13b}$$

$$P_a \le P_{\max}, \tag{6.13c}$$

$$|u_n| \le 1, \forall n = 1, 2, \cdots, N, \tag{6.13d}$$

$$|u_{N+1}| = 1, \tag{6.13e}$$

where (6.13d) is due to $\rho_n \in [0, 1]$, while (6.13e) is to guarantee $|t| = 1$. We note that if $\mathbf{u}$ is an optimal solution to the optimization problem (P1.1), $\frac{\mathbf{v}}{t}$ is an optimal solution to the original optimization problem (P1). However, (P1.1) is still difficult to tackle due to the fact that the transmit power variable P_a and the reflect beamforming vector $\mathbf{u}$ are coupled in the objective function (6.13a) and the covertness constraint (6.13b). Fortunately, P_a is a scale variable and it is constrained by (6.13c), which allows us to simplify (P1.1) as

$$(\text{P1.2}): \max_{P_a,\mathbf{w}} \ \mathbf{w}^H\mathbf{B}\mathbf{w} \tag{6.14a}$$

$$\text{s.t.} \ \ln\left(\frac{\mathbf{w}^H\mathbf{A}\mathbf{w}+\sigma_w^2}{\sigma_w^2}\right)-\frac{\mathbf{w}^H\mathbf{A}\mathbf{w}}{\mathbf{w}^H\mathbf{A}\mathbf{w}+\sigma_w^2}\le\frac{2\epsilon^2}{L}, \tag{6.14b}$$

$$P_a \le P_{\max}, \tag{6.14c}$$

$$|w_n| \le \sqrt{P_a}, \forall n = 1, 2, \cdots, N, \tag{6.14d}$$

$$|w_{N+1}| = \sqrt{P_a}, \tag{6.14e}$$

where $\mathbf{w} = \sqrt{P_a}\mathbf{u}$. We note that (P1.2) is NP-hard due to the non-convex constraints (6.14b) and (6.14e), which generally difficult to tackle directly. To facilitate the develepment of problem, we first define $\mathbf{W} = \mathbf{w}\mathbf{w}^H$. Then, problem (P1.2) can be recast as

$$(\text{P1.3}): \max_{P_a,\mathbf{W}} \ \text{Tr}(\mathbf{B}\mathbf{W}) \tag{6.15a}$$

$$\text{s.t.} \ \ln\left(1+\frac{\text{Tr}(\mathbf{A}\mathbf{W})}{\sigma_w^2}\right)-\frac{\text{Tr}(\mathbf{A}\mathbf{W})}{\text{Tr}(\mathbf{A}\mathbf{W})+\sigma_w^2}\le\frac{2\epsilon^2}{L}, \tag{6.15b}$$

$$P_a \le P_{\max}, \tag{6.15c}$$

$$\mathbf{W}_{n,n} \le P_a, \forall n = 1, 2, \cdots, N, \tag{6.15d}$$

$$\mathbf{W}_{N+1,N+1} = P_a, \tag{6.15e}$$

$$\mathbf{W} \succeq \mathbf{0}, \tag{6.15f}$$

$$\text{rank}(\mathbf{W}) = 1, \tag{6.15g}$$

where (6.15f) and (6.15g) are in (P1.3) to guarantee that $\mathbf{W} = \mathbf{w}\mathbf{w}^H$ holds after the optimization. We note that the objective function (6.15a) is linear, while (6.15c) and (6.15d) together with (6.15e) are linear constraints. In addition, (6.15f) is a linear matrix inequality (LMI), which are convex with respect to the corresponding optimization variables. In the following, we first present a lemma to determine the convexity of the covertness constraint (6.15b), and then we tackle the non-convex rank-one constraint (6.15g).

Lemma 6.1 *The constraint* (6.15b) *can be rearranged as*

$$\left(1+\frac{\text{Tr}(\mathbf{AW})}{\sigma_w^2}\right)\ln\left(1+\frac{\text{Tr}(\mathbf{AW})}{\sigma_w^2}\right)-\left(1+\frac{2\epsilon^2}{L}\right)\frac{\text{Tr}(\mathbf{AW})}{\sigma_w^2} \le \frac{2\epsilon^2}{L}, \tag{6.16}$$

which is a convex constraint with respect to $\mathbf{W}$.

Proof The detailed proof is provided in Appendix. □

In the following, we focus on tackling the non-convex rank-one constraint (6.15g). In general, problem (P1.3) can be transformed into a convex optimization problem by relaxing the rank-one constraint (6.15g) and the constraint-relaxed problem can be solved by convex optimization tools, such as CVX [46]. However, the optimal $\mathbf{W}$ of the resultant problem may not be rank-one and the corresponding optimal objective value serves as an upper bound on that of problem (P1.3).

In the following, we develop a PSCA iterative algorithm to solve (P1.3), which guarantees that the ultimate convergence solution is a locally optimal solution. To proceed, we first note that the rank-one constraint (6.15g) is equivalent to

$$\text{Tr}(\mathbf{W}) - \lambda_{\max}(\mathbf{W}) \le 0, \tag{6.17}$$

where $\lambda_{\max}(\mathbf{W})$ is the maximal eigenvalue of $\mathbf{W}$. This follows from the fact that $\text{Tr}(\mathbf{W}) - \lambda_{\max}(\mathbf{W}) \ge 0$ must hold when $\mathbf{W} \succeq \mathbf{0}$. As such, constraint (6.17) is equivalent to $\text{Tr}(\mathbf{W}) = \lambda_{\max}(\mathbf{W})$, which implies that $\mathbf{W}$ has only one non-zero eigenvalue. It should be emphasized that $\lambda_{\max}(\mathbf{W})$ is a spectral function and is convex with respect to $\mathbf{W}$. Following this fact, the left-hand side (LHS) of the constraint (6.17) is in the form of a linear function minus a convex function. We note that any convex function is lower-bounded by its first-order approximation at any given point [46]. As a result, the non-convex constraint (6.17) can be transformed into a more stringent convex constraint for given any feasible solution $\tilde{\mathbf{W}}$. Then, the successive convex approximation (SCA) method can be employed to solve the resultant convex optimization problem iteratively.

In applying SCA method, it is difficult to identify an initial feasible $\tilde{\mathbf{W}}$ to the resultant optimization problem, due to the existence of implicit constraint $\mathrm{Tr}(\mathbf{W}) - \lambda_{\max}(\mathbf{W}) \geq 0$. To overcome this difficulty, we resort to the exact penalty method. Specifically, we first introduce a slack variable $\eta \geq 0$ to enlarge the size of the feasible solution set spanned by constraint (6.17). Then we develop a penalty method by adding a slack variable into the objective function. Following the above discussions, we rewrite problem (P1.3) as

$$
\begin{aligned}
(\text{P1.4}): \max_{P_a, \mathbf{W}, \eta} \quad & \mathrm{Tr}(\mathbf{BW}) - \tau\eta && \text{(6.18a)}\\
\text{s.t.} \quad & \text{(6.15c), (6.15d), (6.15e), (6.15f), (6.16),} && \text{(6.18b)}\\
& \mathrm{Tr}(\mathbf{W}) - \lambda_{\max}(\mathbf{W}) \leq \eta, && \text{(6.18c)}\\
& \eta \geq 0, && \text{(6.18d)}
\end{aligned}
$$

where $\tau > 0$ is a penalty parameter. We note that (P1.3) and (P1.4) are equivalent when $\tau > \tau_0$, and thus (P1.4) provides the exact penalty optimization solution to (P1.3).

Now, we turn to address the non-convex constraint (6.18c). Since the spectral function $\lambda_{\max}(\mathbf{W})$ is non-smooth (i.e., not differentiable), we adopt its sub-gradient given by $\mathbf{w}_{\max}\mathbf{w}_{\max}^H$ [47], where $\mathbf{w}_{\max}$ is the eigenvector associated to the maximum eigenvalue of $\lambda_{\max}(\mathbf{W})$. As such, the first-order restrictive approximation of $\lambda_{\max}(\mathbf{W})$ is replaced by

$$
\lambda_{\max}(\mathbf{W}) \geq \lambda_{\max}(\tilde{\mathbf{W}}) + \mathrm{Tr}\left(\tilde{\mathbf{w}}_{\max}\tilde{\mathbf{w}}_{\max}^H(\mathbf{W} - \tilde{\mathbf{W}})\right), \tag{6.19}
$$

where $\tilde{\mathbf{W}}$ is a given feasible point and $\tilde{\mathbf{w}}_{\max}$ is the unit-norm eigenvector corresponding to the maximum eigenvalue $\lambda_{\max}(\tilde{\mathbf{W}})$ of the matrix $\tilde{\mathbf{W}}$. As such, the constraint (6.18c) can be rewritten as

$$
\mathrm{Tr}(\mathbf{W}) - \lambda_{\max}(\tilde{\mathbf{W}}) - \mathrm{Tr}\left(\tilde{\mathbf{w}}_{\max}\tilde{\mathbf{w}}_{\max}^H(\mathbf{W} - \tilde{\mathbf{W}})\right) \leq \eta. \tag{6.20}
$$

We should point out that the value of the aforementioned τ_0 can be chosen to be greater than the largest optimal dual variable related to constraint (6.20) with $\eta = 0$ [48]. As per (6.20), the optimization problem (P1.4) can be rewritten as

$$
\begin{aligned}
(\text{P1.5}): \max_{P_a, \mathbf{W}, \eta} \quad & \mathrm{Tr}(\mathbf{BW}) - \tau\eta\\
\text{s.t.} \quad & \text{(6.15c), (6.15d), (6.15e), (6.15f), (6.16), (6.18d), (6.20).}
\end{aligned} \tag{6.21a}
$$

We note that the problem (P1.5) is a GNCP problem due to the exponential cone constraint involved in the covertness constraint (6.16). For a given penalty parameter

Algorithm 1 PSCA algorithm for Solving (P1.2)

1. Given an initial feasible solution $\tilde{\mathbf{W}}^0$ and an initial penalty parameter τ^0; Given $c > 1$ and $\tau_{\max}$; Set $r = 0$.
2. **repeat**
3. Solve (P1.5) with given a feasible solution $\tilde{\mathbf{W}}^r$ and obtain the current optimal solution $\{\mathbf{W}^{r+1}, P_a^{r+1}, \eta^{r+1}\}$.
4. Update $\tau^{r+1} = \min\{c\tau^r, \tau_{\max}\}$ and set $\tilde{\mathbf{W}}^{r+1} = \mathbf{W}^{r+1}$; Set the iteration number $r = r + 1$.
5. **until**
6. Convergence.

τ and an initial feasible solution $\tilde{\mathbf{W}}$, it can be solved by convex optimization solvers such as CVX [46]. The optimal solution to (P1.5) is also a feasible solution to (P1.4), since the feasible set of (P1.5) is smaller than that of (P1.4). In addition, problem (P1.2) can be tackled by solving (P1.5) iteratively. The detailed iterative algorithm is presented in Algorithm 1. We note that Algorithm 1 starts with a small value of the penalty parameter τ^0 to put a less emphasis in forcing the rank-one constraint. Then, the penalty parameter τ is gradually increased by a constant $c > 1$ at each iteration until a large upper bound $\tau_{\max}$ is achieved to guarantee $\eta = 0$. We note that Algorithm 1 does not guarantee that the value of objective function always increases with the iteration number, but the objective value will converge. The former is due to the disturbance of the penalty term in the objective function, while the latter is due to the fact that Algorithm 1 is reduced to a standard SCA algorithm when τ reaches its upper bound $\tau_{\max}$. We note that the convergence of the standard SCA algorithm has been proven in [49]. We note that solving a GNCP problem requires a high computational complexity compared to solving other standard convex programs such as SDP [50]. We also note that the complexity of solving a SDP problem with the same size as the problem (P1.5) is $O\left((N+1)^{6.5})\right)$ [17]. As such, the complexity of the proposed Algorithm 1 is at least on the order of $O\left(K_1(N+1)^{6.5})\right)$, where K_1 is the number of iterations.

6.3.3 Low-Complexity Algorithm

In this subsection, we develop a low-complexity two-stage algorithm to strike a balance between the covert transmission performance and computational complexity. Specifically, the IRS's reflection beamforming is designed in the first stage, while Alice's transmit power is determined in the second stage.

6.3.3.1 IRS Beamforming Design

In order to develop a low-complexity IRS beamforming design, as per (P1.1) we note that $\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1)$ in the covertness constraint (6.13b) is a monotonically increas-

ing function of $P_a\mathbf{u}^H\mathbf{A}\mathbf{u}$, which implies that the covertness level is dominated by the received energy at Willie. Following this fact, we adopt the ratio from the received energy at Bob to the received energy at Willie, i.e., $\frac{P_a\mathbf{u}^H\mathbf{B}\mathbf{u}}{P_a\mathbf{u}^H\mathbf{A}\mathbf{u}}$, as our performance metric to design the reflection beamforming, yielding the following optimization problem

$$(\text{P2}): \max_{\mathbf{u}} \frac{\mathbf{u}^H\mathbf{B}\mathbf{u}}{\mathbf{u}^H\mathbf{A}\mathbf{u}} \tag{6.22a}$$

$$\text{s.t.} \quad |u_n| \leq 1, \forall n = 1, 2, \cdots, N, \tag{6.22b}$$

$$|u_{N+1}| = 1. \tag{6.22c}$$

We note that the optimization problem (P2) is difficult to tackle directly, since the objective function (6.22a) is highly non-concave and the unit modules constraint (6.22c) is non-convex. Furthermore, this problem is quite different from the generalized Rayleigh quotient problem, due to the multiple reflection coefficient constraints that characterize the phase shift and reflection amplitude limits. In the following, we first derive a lower bound on the objective function (6.22a), and then we develop a SCA algorithm to solve (P2) iteratively. Based on [51], a lower bound on (6.22a) is given by

$$\frac{\mathbf{u}^H\mathbf{B}\mathbf{u}}{\mathbf{u}^H\mathbf{A}\mathbf{u}} \geq \frac{2\text{Re}(\tilde{\mathbf{u}}^H\mathbf{B}\mathbf{u})}{\tilde{\mathbf{u}}^H\mathbf{A}\tilde{\mathbf{u}}} - \frac{\tilde{\mathbf{u}}^H\mathbf{B}\tilde{\mathbf{u}}}{(\tilde{\mathbf{u}}^H\mathbf{A}\tilde{\mathbf{u}})^2}\mathbf{u}^H\mathbf{A}\mathbf{u}, \tag{6.23}$$

where $\tilde{\mathbf{u}}$ is a given feasible point. We note that although the lower bound detailed in (6.23) is a concave function of $\mathbf{u}$, it is not conducive to derive a low-complexity analytic expression for $\mathbf{u}$, as such, we further establish an upper bound on $\mathbf{u}^H\mathbf{A}\mathbf{u}$ [10], as below:

$$\mathbf{u}^H\mathbf{A}\mathbf{u} \leq \mathbf{u}^H\mathbf{M}\mathbf{u} + 2\text{Re}\left(\mathbf{u}^H(\mathbf{A}-\mathbf{M})\tilde{\mathbf{u}}\right) + \tilde{\mathbf{u}}^H(\mathbf{M}-\mathbf{A})\tilde{\mathbf{u}}, \tag{6.24}$$

where $\mathbf{M} = \lambda_{\max}(\mathbf{A})\mathbf{I}_{N+1}$. We recall that $\mathbf{A}$ is a rank-one matrix, it follows that $\lambda_{\max}(\mathbf{A}) = \bar{\mathbf{a}}^H\bar{\mathbf{a}}$, where $\bar{\mathbf{a}} = [\mathbf{a}^H \; h_{aw}^*]^H$. Then, substituting (6.24) into (6.23) and considering that the values of $||\mathbf{u}||^2$ and $||\tilde{\mathbf{u}}||^2$ are less than or equal to $N+1$, we have

$$\frac{\mathbf{u}^H\mathbf{B}\mathbf{u}}{\mathbf{u}^H\mathbf{A}\mathbf{u}} \geq 2\text{Re}\left(\mathbf{f}^H\mathbf{u}\right) + \varsigma, \tag{6.25}$$

where

$$\mathbf{f} = \left(\frac{\mathbf{B}}{\tilde{\mathbf{u}}^H\mathbf{A}\tilde{\mathbf{u}}} - \frac{\left(\mathbf{A} - \bar{\mathbf{a}}^H\bar{\mathbf{a}}\mathbf{I}_{N+1}\right)\tilde{\mathbf{u}}^H\mathbf{B}\tilde{\mathbf{u}}}{(\tilde{\mathbf{u}}^H\mathbf{A}\tilde{\mathbf{u}})^2}\right)\tilde{\mathbf{u}}, \tag{6.26}$$

$$\varsigma = \frac{\tilde{\mathbf{u}}^H \mathbf{B}\tilde{\mathbf{u}}}{\tilde{\mathbf{u}}^H \mathbf{A}\tilde{\mathbf{u}}} - \frac{2\bar{\mathbf{a}}^H \bar{\mathbf{a}}(N+1)\tilde{\mathbf{u}}^H \mathbf{B}\tilde{\mathbf{u}}}{(\tilde{\mathbf{u}}^H \mathbf{A}\tilde{\mathbf{u}})^2}. \tag{6.27}$$

Then, a lower bound value of optimization problem (P2) can be obtained by solving

$$(\text{P2.1}): \max_{\mathbf{u}} \ 2\text{Re}\left(\mathbf{f}^H \mathbf{u}\right) + \varsigma \tag{6.28a}$$

$$\text{s.t.} \quad |u_n| \le 1, \forall n = 1, 2, \cdots, N, \tag{6.28b}$$

$$|u_{N+1}| = 1. \tag{6.28c}$$

In order to tackle the optimal solution to the optimization problem (P2.1), we first equivalently rewrite the objective function (6.28a) as

$$2\text{Re}\left(\sum_{n=1}^{N+1}\left(|f_n||u_n|e^{j(\arg(u_n)-\arg(f_n))}\right)\right) + \varsigma, \tag{6.29}$$

where f_n is the n-th element of $\mathbf{f}$. As a result, for a given feasible solution $\tilde{\mathbf{u}}$, the optimal solution to (P2.1) is given by $\arg(u_n) = \arg(f_n)$ and $|u_n| = 1, \forall n$. It follows that $\mathbf{u} = e^{j\arg(\mathbf{f})}$. We note that we always have $|u_n| = 1, \forall n$, in this low-complexity design, since otherwise we can always increase the value of $|u_n|$ to further increase the objective function. This also shows the sub-optimality of this design, which will be thoroughly investigated in Sect. 6.5.

6.3.3.2 Transmit Power Design

For a given $\mathbf{u}$, the optimization problem (P1.1) is simplified to

$$(\text{P3}): \max_{P_a} \ P_a \mathbf{u}^H \mathbf{B}\mathbf{u} \tag{6.30a}$$

$$\text{s.t.} \quad \ln\left(1 + \frac{P_a \mathbf{u}^H \mathbf{A}\mathbf{u}}{\sigma_w^2}\right) - \frac{P_a \mathbf{u}^H \mathbf{A}\mathbf{u}}{P_a \mathbf{u}^H \mathbf{A}\mathbf{u} + \sigma_w^2} \le \frac{2\epsilon^2}{L}, \tag{6.30b}$$

$$P_a \le P_{\max}. \tag{6.30c}$$

We note that $\frac{2\epsilon^2}{L}$ generally is a small value in covert communications. As per $\ln(1+x) \le x$ for $x > -1$, a conservative approximation of the covertness constraint (6.30b) is given by

$$\frac{P_a \mathbf{u}^H \mathbf{A}\mathbf{u}}{\sigma_w^2} - \frac{P_a \mathbf{u}^H \mathbf{A}\mathbf{u}}{P_a \mathbf{u}^H \mathbf{A}\mathbf{u} + \sigma_w^2} \le \frac{2\epsilon^2}{L}. \tag{6.31}$$

Then, the optimization problem (P3) can be recast as

$$\begin{aligned}(\text{P3.1}): \ &\max_{P_a} \ P_a \mathbf{u}^H \mathbf{B}\mathbf{u} \\ &\text{s.t.} \quad (6.30b),\ (6.30c),\ (6.31). \end{aligned} \tag{6.32}$$

One can verify that the LHS of constraint (6.31) is a monotonically increasing function of P_a, and the objective function in (P3.1) also monotonically increases with P_a. Thus, in the optimal solution to (P3.1) the covertness constraint (6.31) holds with equality, which lead to $P_a = \frac{\sigma_w^2\left(\epsilon^2 \pm \sqrt{\epsilon^4+2\epsilon^2 L}\right)}{L\mathbf{u}^H\mathbf{A}\mathbf{u}}$. Considering that $\epsilon^2 \le \sqrt{\epsilon^4+2\epsilon^2 L}$ and $0 \le P_a \le P_{\max}$, the optimal transmit power is given by

$$P_a^* = \min\left\{\frac{\sigma_w^2\left(\epsilon^2+\sqrt{\epsilon^4+2\epsilon^2 L}\right)}{L\mathbf{u}^H\mathbf{A}\mathbf{u}}, P_{\max}\right\}. \tag{6.33}$$

We should point out that the adopted approximation in (6.31) is to find a low-complexity solution to (P3). In fact, the optimal P_a to (P3) can be achieved by solving equation (6.30b) with equality. However, it is a transcendental equation with respect to P_a, which does not facilitate the derivation of an analytical expression for P_a. We note that the approximation solution shown in (6.33) is a high-quality solution to (P3), which is mainly due to the fact that the LHS of constraint (6.30b) is a monotonicity increasing function of P_a and the value of $\frac{2\epsilon^2}{L}$ is small. We note that P_a^* in (6.33) decreases as $\mathbf{u}^H\mathbf{A}\mathbf{u}$ increases, which verifies the effectiveness of the adopted performance metric in (P2), since it guarantees a relatively small value of $\mathbf{u}^H\mathbf{A}\mathbf{u}$. We also note that P_a^* decreases as the required covertness level ϵ decreases, which is consistent with our intuition.

The proposed low-complexity two-stage algorithm is summarized in Algorithm 2. We note that in the first stage we design the reflection beamforming without considering the covertness constraint, i.e., the covertness constraint is not involved in the optimization problem (P2). In the second stage, Alice's transmit power is determined to explicitly ensure the covertness constraint. We note that the main computational complexity of Algorithm 2 comes from calculating $\mathbf{f}$ in step 3 and P_a in step 6. We observe from (6.24) and (6.33) that the complexity of calculating $\mathbf{f}$ and P_a mainly depends on the calculation of the quadratic form, which is on the order of $O\left((N+1)^2\right)$. As such, the total computational complexity of Algorithm 2 is given by $O\left(K_2(N+1)^2\right)$, where K_2 is the number of iterations at the first stage. We note that the complexity of the proposed Algorithm 2 is much lower than that of the proposed Algorithm 1.

We should point out that the aforementioned low-complexity two-stage algorithm cannot obtain the perfect covertness with non-zero transmit power detailed in the optimization problem P1′. This is due to the fact that we have performed multiple lower bound approximation operations on the objective function (6.22a)

and Alice's transmit power approaches to 0 as $\epsilon \to 0$. As such, in the following we develop a low-complexity solution to (P1′). To this end, we first recall that, as per Theorem 6.1, the perfect covertness can be achieved when $\sum_{n=1}^{N} |a_n| \geq |h_{aw}|$. Following this fact, we can equivalently rewrite $\sum_{n=1}^{N} |a_n| \geq |h_{aw}|$ as $\sum_{n=1}^{N} |a_n| = \kappa |h_{aw}|$, where $\kappa \geq 1$ is a scale factor. Then, we can see that $\{v_n = e^{j(\arg(a_n)-\pi-\arg(h_{aw}))}, \forall n, P_a = P_{\max}\}$ is the optimal solution to (P1′) when $\kappa = 1$ and $\{v_n = \frac{1}{\kappa} e^{j(\arg(a_n)-\pi-\arg(h_{aw}))}, \forall n, P_a = P_{\max}\}$ is a feasible solution to (P1′) for $\kappa > 1$.

Algorithm 2 Proposed Low-Complexity Algorithm

1. Given an initial feasible solution $\tilde{\mathbf{u}}^0$ and set iteration index $r = 0$.
2. **repeat**
3. Compute $\mathbf{u} = e^{j\arg(\mathbf{f})}$ to obtain the current optimal solution of problem (P2.1).
4. Update $\tilde{\mathbf{u}}^r = \mathbf{u}$ and set $r = r + 1$.
5. **until**
6. Convergence.
7. Compute P_a according to (6.33).

6.4 Covert Communication Design Without Willie's Instantaneous CSI

If Willie is not a legitimate user in the considered system for other service, it may be difficult to obtain his instantaneous CSI. As such, in this section we consider that Alice and the IRS only know that $h_{aw} \sim \mathcal{CN}(0, \chi_{aw})$ and $h_{rw_n} \sim \mathcal{CN}(0, \chi_{rw})$, where h_{rw_n} is the n-th element of $\mathbf{h}_{rw}$, but they do not know the instantaneous realizations of h_{aw} or $\mathbf{h}_{rw}$. From a conservative point of view, we assume that Willie knows the instantaneous h_{aw} and $\mathbf{h}_{rw}$.

6.4.1 Expression for Covertness Constraint

As per (6.5), the covertness constraint $\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1) \leq 2\epsilon^2$ depends on h_{aw} and $\mathbf{h}_{rw}$. As such, we consider the expected value of $\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1)$ over all realizations of h_{aw} and $\mathbf{h}_{rw}$ as the measure of covertness. Then, the covertness constraint can be rewritten as $\mathbb{E}_X[\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1)] \leq 2\epsilon^2$, where

$$\mathbb{E}_X[\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1)] = \mathbb{E}_X\left\{L\left[\ln\left(1+\frac{P_a X}{\sigma_w^2}\right) - \frac{P_a X}{P_a X + \sigma_w^2}\right]\right\}, \tag{6.34}$$

and $X \triangleq |\mathbf{h}_{rw}^H \boldsymbol{\Theta} \mathbf{h}_{ar} + h_{aw}|^2$. We note that the use of $\mathbb{E}_X[\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1)] \leq 2\epsilon^2$ as the covertness constraint lies in the fact that Willie knows the instantaneous h_{aw} and $\mathbf{h}_{rw}$. This fact enables Willie to vary his detection threshold for each instantaneous realization of h_{aw} or $\mathbf{h}_{rw}$, such that $\mathbb{E}_X[\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1)]$ can be used to provide a lower bound on Willie's minimum detection error rate ξ^*. We note that, if Willie uses a fixed detection threshold for all the realizations of h_{aw} and $\mathbf{h}_{rw}$, $\mathbb{E}_X[\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1)] \leq 2\epsilon^2$ should not be used as the covertness constraint. Since the expression of $\mathbb{E}_X[\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1)]$ is very complex, an exact analytical expression of $\mathbb{E}_X[\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1)]$ is difficult to obtain directly. In the following, we present a theorem to determine the analytical expression of $\mathbb{E}_X[\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1)] \leq 2\epsilon^2$.

Theorem 6.2 *The covertness constraint $\mathbb{E}_X[\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1)] \leq 2\epsilon^2$ can be equivalently rewritten as*

$$\frac{P_a}{\sigma_w^2}\left(\chi_{rw}\sum_{n=1}^{N}\rho_n^2|h_{ar_n}|^2 + \chi_{aw}\right) \leq \bar{\epsilon}, \tag{6.35}$$

where $\bar{\epsilon}$ is the solution to

$$\left(1+\frac{1}{\bar{\epsilon}}\right)e^{\frac{1}{\bar{\epsilon}}}E_1\left(\frac{1}{\bar{\epsilon}}\right) - 1 - \frac{2\epsilon^2}{L} = 0, \tag{6.36}$$

which can be obtained via the bisection method [46], where $E_1(x) = \int_x^\infty \frac{e^{-t}}{t}dt$ is an exponential integral function.

Proof The detailed proof is provided in Appendix. □

We note that $\mathbb{E}_X[\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1)] \leq 2\epsilon^2$ is a new covertness constraint in the context of covert communications when Willie's instantaneous CSI is not available. Theorem 6.2 equivalently transforms the mathematically intractable covertness constraint $\mathbb{E}_X[\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1)] \leq 2\epsilon^2$ into the constraint (6.35), which facilitates us determine the optimal IRS's reflection beamforming and Alice's transmit power in the next subsection.

6.4.2 Optimal Design Without Willie's Instantaneous CSI

Following Theorem 6.2, when Willie's instantaneous CSI is not available, the optimal design of the IRS's reflection beamforming and Alice's transmit power is formulated as

$$(\text{P5}): \max_{P_a,\boldsymbol{\rho},\boldsymbol{\theta}} P_a\left|\sum_{n=1}^{N}\rho_n|b_n|e^{j(\theta_n+\arg(b_n))} + h_{ab}\right|^2 \tag{6.37a}$$

$$\text{s.t.} \quad P_a \left(\chi_{rw} \sum_{n=1}^{N} \rho_n^2 |h_{ar_n}|^2 + \chi_{aw} \right) \leq \bar{\epsilon} \sigma_w^2, \tag{6.37b}$$

$$P_a \leq P_{\max}, \tag{6.37c}$$

$$0 \leq \rho_n \leq 1, \forall n = 1, 2, \cdots, N, \tag{6.37d}$$

$$0 \leq \theta_n < 2\pi, \forall n = 1, 2, \cdots, N, \tag{6.37e}$$

where b_n is the n-th element of $\mathbf{b}$, $\boldsymbol{\rho} = [\rho_1, \rho_2, \cdots, \rho_N]^T$ and $\boldsymbol{\theta} = [\theta_1, \theta_2, \cdots, \theta_N]^T$. Interestingly, we find that covertness constraint (6.37b) is independent of the phase shift $\boldsymbol{\theta}$, which implies that the optimal phase shift strategy at the IRS is to maximize Bob's SNR when IRS does not know Willie's instantaneous CSI. Following the fact that

$$\left| \sum_{n=1}^{N} \rho_n |b_n| e^{j(\theta_n + \arg(b_n))} + h_{ab} \right| \leq \sum_{n=1}^{N} \left| \rho_n |b_n| e^{j(\theta_n + \arg(b_n))} \right| + |h_{ab} e^{j \arg(h_{ab})}|, \tag{6.38}$$

where the equality holds when $\theta_n + \arg(b_n) = \arg(h_{ab}), \forall n$, we can conclude that the optimal $\boldsymbol{\theta}$ to the optimization problem in (P5) is given by

$$\theta_n^* = \arg(h_{ab}) - \arg(b_n), \forall n. \tag{6.39}$$

Substituting (6.39) into (P5) and performing the root operation on the objective function (6.37a), we have

$$\begin{aligned} (\text{P5.1}): \max_{P_a, \boldsymbol{\rho}} \sqrt{P_a} \left(\sum_{n=1}^{N} \rho_n |b_n| + |h_{ab}| \right) \\ \text{s.t.} \quad (6.37b), (6.37c), (6.37d). \end{aligned} \tag{6.40}$$

In the following, we present the optimal solution to the optimization problem (P5.1) by considering three possible types of the amplitude regulator to be adapted in the IRS, i.e., different constraints on the IRS's amplitude coefficients in three practical scenarios.

1. $\rho_n = 1, \forall n$ In this scenarios, $\boldsymbol{\rho}$ is fixed to be 1, which means that only the phase shifts in the IRS can be controlled. Then, in the problem (P5.1), only Alice's transmit power need to be determined, of which the optimal value is given by

$$P_a^* = \min \left\{ \frac{\bar{\epsilon} \sigma_w^2}{\chi_{rw} ||\mathbf{h}_{ar}||^2 + \chi_{aw}}, P_{\max} \right\}. \tag{6.41}$$

2. $\rho_n = \rho_0, \forall n$ In this scenario, all the elements of the IRS share a common amplitude coefficient controller due to hardware limitations. As such, we need to jointly design ρ_0 and P_a in the optimization problem (P5.1). To this end, we first rewrite (P5.1) as

$$\text{(P5.2)}: \max_{P_a, \rho_0} \sqrt{P_a}\,(\rho_0 ||\mathbf{b}||_1 + |h_{ab}|) \tag{6.42a}$$

$$\text{s.t.} \quad P_a \left(\chi_{rw}\rho_0^2 ||\mathbf{h}_{ar}||^2 + \chi_{aw}\right) \leq \bar{\epsilon}\sigma_w^2, \tag{6.42b}$$

$$P_a \leq P_{\max}, \tag{6.42c}$$

$$0 \leq \rho_0 \leq 1. \tag{6.42d}$$

We note that constraint (6.42b) must hold with equality at the optimal solution, otherwise we can always increase P_a or ρ_0 to further improve the objective function. As such, the optimal value of the transmit power P_a can be expressed as

$$P_a^* = \begin{cases} P_{\max}, & \frac{\bar{\epsilon}\sigma_w^2}{(\chi_{rw}\rho_0^2 ||\mathbf{h}_{ar}||^2 + \chi_{aw})} > P_{\max}, \\ \frac{\bar{\epsilon}\sigma_w^2}{(\chi_{rw}\rho_0^2 ||\mathbf{h}_{ar}||^2 + \chi_{aw})}, & \frac{\bar{\epsilon}\sigma_w^2}{(\chi_{rw}\rho_0^2 ||\mathbf{h}_{ar}||^2 + \chi_{aw})} \leq P_{\max}. \end{cases} \tag{6.43}$$

We should point out that increasing the values of P_a and ρ_0 can improve the communication quality from Alice to Bob, but may decrease the achievable communication covertness. In addition, we observe from (6.43) that P_a decreases with ρ_0 when $\frac{\bar{\epsilon}\sigma_w^2}{(\chi_{rw}\rho_0^2 ||\mathbf{h}_{ar}||^2 + \chi_{aw})} \leq P_{\max}$ holds. As such, the transmit power P_a and the IRS amplitude coefficient ρ_0 should be carefully designed to balance the communication quality and communication covertness. As per (6.43), we consider the following two cases.

(a) $P_a^* = P_{\max}$ In this case, (P5.2) can be recast as

$$\text{(P5.3)}: \max_{\rho_0} \sqrt{P_{\max}}\,(\rho_0 ||\mathbf{b}||_1 + |h_{ab}|) \tag{6.44a}$$

$$\text{s.t.} \quad 0 \leq \rho_0 \leq 1, \ \rho_0^2 \leq \frac{\frac{\bar{\epsilon}\sigma_w^2}{P_{\max}} - \chi_{aw}}{\chi_{rw}||\mathbf{h}_{ar}||^2}. \tag{6.44b}$$

Since the objective function (6.44a) is a linear function of ρ_0, the optimal ρ_0 must be on the boundary of (6.44b). Thus, the optimal ρ_0 is given by

$$\rho_0^* = \min\left\{1, \sqrt{\frac{\frac{\bar{\epsilon}\sigma_w^2}{P_{\max}} - \chi_{aw}}{\chi_{rw}||\mathbf{h}_{ar}||^2}}\right\}. \tag{6.45}$$

We observe from (6.45) that the optimal ρ_0 decreases as χ_{aw} or χ_{rw} increases, since as the channel quality from Alice or IRS to Willie is

improved, it becomes easier for Willie to make correct decisions on the detection of Alice's transmission. As such, IRS will reduce its amplitudes to maintain the same level of covertness.

(b) $P_a^* = \frac{\bar{\epsilon}\sigma_w^2}{\chi_{rw}\rho_0^2||\mathbf{h}_{ar}||^2+\chi_{aw}}$ In this case, (P5.2) can be rewritten as

$$(\text{P5.4}): \max_{\rho_0} \frac{\sqrt{\bar{\epsilon}\sigma_w^2}\,(\rho_0||\mathbf{b}||_1 + |h_{ab}|)}{\sqrt{\chi_{rw}\rho_0^2||\mathbf{h}_{ar}||^2 + \chi_{aw}}} \tag{6.46a}$$

$$\text{s.t.} \quad 0 \le \rho_0 \le 1, \rho_0^2 \ge \frac{\frac{\bar{\epsilon}\sigma_w^2}{P_{\max}} - \chi_{aw}}{\chi_{rw}||\mathbf{h}_{ar}||^2}. \tag{6.46b}$$

Since (P5.4) is a univariate optimization problem, its optimal solution must be attained either at the stationary point of the objective function or on the boundary of the feasible set, where the stationary point of (6.46a) is given by

$$\rho_0^s = \frac{\chi_{aw}||\mathbf{b}||_1}{\chi_{rw}|h_{ab}|||\mathbf{h}_{ar}||^2}. \tag{6.47}$$

Thus, the optimal ρ_0 to problem (P5.4) can be obtained by checking the objective values of the feasible stationary point and endpoints of the constraint (6.46b).

Finally, to determine the solution to (P5.2) in this scenario, we compare the achieved objective function values in the aforementioned two cases and choose the candidate optimal solution with the higher objective function value as the optimal ρ_0. Then, the optimal P_a can be obtained as per (6.43).

3. $0 \le \rho_n \le 1, \forall n$ In this scenario, we have the general case of jointly optimizing P_a and $\boldsymbol{\rho}$. We note that the optimization problem (P5.1) is non-convex due to the non-concave objective function and the non-convex constraint (6.37b). Fortunately, it can be equivalently transformed into the following convex form:

$$(\text{P5.5}): \max_{P_a, \bar{\boldsymbol{\rho}}} \bar{\boldsymbol{\rho}}^T\bar{\mathbf{b}} + \sqrt{P_a}|h_{ab}| \tag{6.48a}$$

$$\text{s.t.} \quad \chi_{rw}\bar{\boldsymbol{\rho}}^T\mathbf{H}_{ar}\bar{\boldsymbol{\rho}} + P_a\chi_{aw} \le \bar{\epsilon}\sigma_w^2, \tag{6.48b}$$

$$P_a \le P_{\max}, \tag{6.48c}$$

$$0 \le \bar{\rho}_n \le \sqrt{P_a}, \forall n = 1, 2, \cdots, N. \tag{6.48d}$$

where $\bar{\boldsymbol{\rho}} = \sqrt{P_a}\boldsymbol{\rho}$, $\bar{\mathbf{b}} = [|b_1|, |b_2|, \cdots, |b_N|]^T$, $\bar{\rho}_n$ is the n-th element of $\bar{\boldsymbol{\rho}}$, and $\mathbf{H}_{ar} = \text{diag}\big(|h_{ar_1}|^2, |h_{ar_2}|^2, \cdots, |h_{ar_N}|^2\big)$. We note that (P5.5) is a convex optimization problem, which can be efficiently solved by the current convex optimization solver CVX [46]. Then, the optimal $\boldsymbol{\rho}$ to the problem (P5.1) can be recovered by $\frac{\bar{\boldsymbol{\rho}}}{\sqrt{P_a}}$.

6.5 Numerical Results

In this section, we provide numerical results to evaluate the performance of the IRS-assisted covert communication system with our proposed designs. We consider a three-dimensional coordinate system, Alice, IRS, Bob, and Willie are respectively located at (0, 5, 5) meter (m), (100, 0, 5) m, (70, 10, 0) m, and (100, 10, 0) m. In addition, we assume that IRS is equipped with a uniform rectangular array (URA) with $N = N_x N_z$, where N_x and N_z are the number of reflecting elements along the x-axis and z-axis, respectively. Note that all results presented below are averaged over 1000 independent channel realizations. Considering that IRS is deployed generally with the knowledge of Alice's location, the channel realizations from Alice to IRS are randomly drawn from Rician fading with a Rician factor of 5 dB, while all other channel realizations are drawn from Rayleigh fading. The large-scale path loss from node i to node j is denoted as $\chi_{ij} = \beta_0 \left(\frac{d_{ij}}{d_0}\right)^{-\alpha_{ij}}$, where β_0 is the channel power gain at the reference distance 1 m, d_{ij} is the distance between node i and node j, and α_{ij} is the corresponding path loss exponent. Specifically, the path loss exponents are set as $\alpha_{ar} = 2.4$, $\alpha_{ab} = 4.2$, $\alpha_{aw} = 4.2$, $\alpha_{rb} = 3$, and $\alpha_{rw} = 3$. Unless stated otherwise, the remaining system parameters are set as follows: $\beta_0 = -30$ dB, $P_{\max} = 36$ dBm, $L = 100$, $\sigma_b^2 = \sigma_w^2 = -80$ dBm, and $N_x = 5$.

6.5.1 With Global CSI

In this subsection, we present numerical results to evaluate the Bob's SNR achieved by our proposed PSCA algorithm and low-complexity algorithm. The proposed design algorithms and the corresponding benchmark schemes are denoted as follows.

- Upper bound: Achieved by solving problem (P1.3) by relaxing the rank-one constraint.
- PSCA algorithm ($\rho_n \leq 1, \forall n$): Jointly design Alice's transmit power as well as phase shift and reflection amplitude of each IRS reflecting element.
- PSCA algorithm ($\rho_n = 1, \forall n$): Jointly design Alice's transmit power and phase shift of each IRS reflection element, where IRS reflection amplitudes are fixed to 1.
- Low-complexity algorithm: Proposed Algorithm 2.
- Without IRS: No IRS in the considered system and only Alice's transmit power P_a is designed.

In Fig. 6.2, we plot the received SNR at Bob achieved by different algorithms versus the number of IRS elements for different values of the covertness level ϵ. In this figure, we first observe that Bob's SNR decreases as ϵ decreases for all schemes. This is due to the fact that the covertness constraint becomes more stringent as ϵ

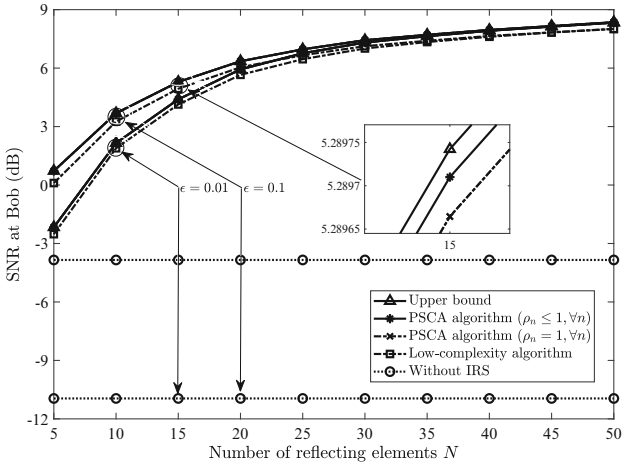


Fig. 6.2 Bob's SNR versus the number of reflecting elements at IRS for different values of the covertness level ϵ

decreases. As expected, the developed algorithms with IRS significantly outperform the algorithm without IRS in terms of achieving a higher SNR at Bob, which demonstrates the benefits of introducing IRS into covert communications. We also observe that Bob's SNR achieved by all the algorithms with IRS increases with the number of reflecting elements N. As a larger N not only enables Bob to receive a stronger reflection signal from the IRS, but also makes the covertness constraint easier to be satisfied, which will be confirmed in Fig. 6.3. In addition, Bob's SNR achieved by PSCA algorithm ($0 \leq \rho_n \leq 1, \forall n$) and PSCA algorithm ($\rho_n = 1, \forall n$) approaches that of the upper bound, which demonstrates that the proposed PSCA algorithms can achieve near-optimal performance. This also implies that the performance gain achieved by adjusting IRS's phase shifts is superior to that achieved by varying IRS's reflection amplitudes in the context of IRS-assisted covert communications with perfect CSI. This is because the IRS reflected channel suffers form the effect of double path loss [3]. As such, adjusting the IRS reflection amplitudes would significantly reduce the SNR at Bob. In addition, considering that the global CSI is available, IRS can adjust its phase shifts to ensure that the privacy information power leaked to Willie is relatively small, while guaranteeing a certain communication quality. Following these facts, IRS prefers to adjust its phase shifts rather than its amplitudes for the case with global CSI available. In this figure, it can be observed that Bob's SNR obtained by the low-complexity algorithm is slightly lower than that obtained by the PSCA algorithms, which shows that the proposed low-complexity algorithm can effectively strike a good balance between the covert communication performance and computational complexity.

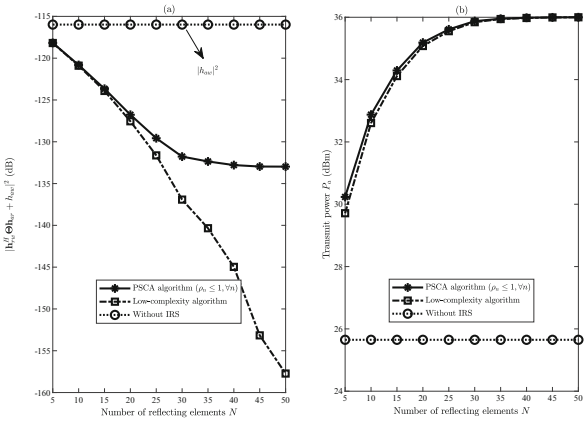


Fig. 6.3 The value of $|\mathbf{h}_{rw}^H \Theta \mathbf{h}_{ar} + h_{aw}|^2$ and transmit power at Willie versus the number of reflecting elements at IRS for covertness level $\epsilon = 0.1$

In Fig. 6.3, we plot the value of $|\mathbf{h}_{rw}^H \boldsymbol{\Theta} \mathbf{h}_{ar} + h_{aw}|^2$, which is the channel power gain received at Willie, to reveal the fundamental reason why IRS can improve the covert communication performance. Recall that we adopt $\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1) \leq 2\epsilon^2$ as the covertness constraint, where $\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1)$ is an increasing function of $P_a|\mathbf{h}_{rw}^H \boldsymbol{\Theta} \mathbf{h}_{ar} + h_{aw}|^2$ (i.e., the received energy at Willie), which implies that the covertness constraint is dominated by $P_a|\mathbf{h}_{rw}^H \boldsymbol{\Theta} \mathbf{h}_{ar} + h_{aw}|^2$. In Fig. 6.3a, we first observe that $|\mathbf{h}_{rw}^H \boldsymbol{\Theta} \mathbf{h}_{ar} + h_{aw}|^2$ achieved by the algorithms with IRS is always lower than that of the algorithm without IRS, which indicates that with the aid of an IRS, Alice can use a higher transmit power to improve the covert communication performance while meeting the same covertness constraint. This also shows that the IRS not only enhances the transmission from Alice to Bob, but also deteriorates Willie's detection performance. In Fig. 6.3a, we also observe that the value of $|\mathbf{h}_{rw}^H \boldsymbol{\Theta} \mathbf{h}_{ar} + h_{aw}|^2$ achieved by the PSCA algorithms is larger than that achieved by the low-complexity algorithm. This is the main reason why the PSCA algorithms can slightly outperform the low-complexity algorithm.

In Fig. 6.4, we plot Bob's SNR and Alice's transmit power P_a achieved by different schemes versus the IRS horizontal location for different values of the reflecting element number N. In Fig. 6.4a, we first observe that with a larger N, e.g., $N = 50$, the optimal horizontal location of the IRS will be closer to Bob, while the optimal horizontal location of the IRS moves closer to Willie as N decreases. The is because the covertness constraint becomes easier to be satisfied as N increases. In general, this figure shows that the optimal horizontal location of the IRS is between Alice and Bob to strike a tradeoff between the communication quality from Alice to Bob and the covertness constraint. Surprisingly, in Fig. 6.4b we observe that the transmit power P_a gradually increases as the IRS moves closer to Willie, which

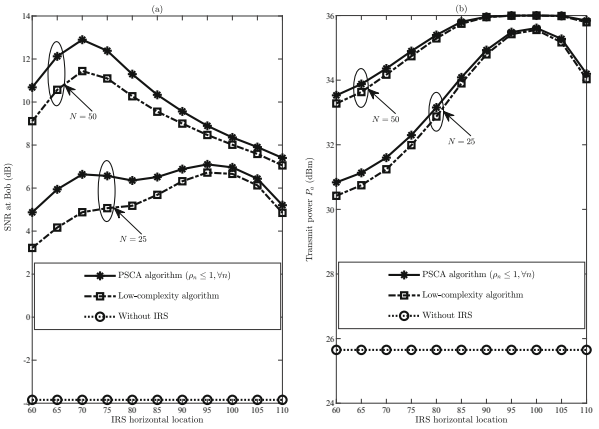


Fig. 6.4 Received SNR at Bob and transmit power at Alice versus IRS horizontal location for covertness level $\epsilon = 0.1$

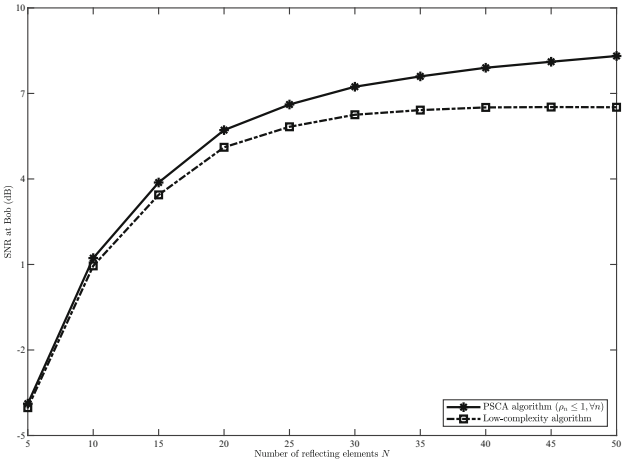


Fig. 6.5 Received SNR at Bob versus the number of reflecting elements at IRS for $\epsilon = 0$ (i.e., perfect covertness)

further verifies that IRS can reduce Willie's channel power gain $|\mathbf{h}_{rw}^H \boldsymbol{\Theta} \mathbf{h}_{ar} + h_{aw}|^2$ and thus degrade its detection performance, especially when the IRS is close to Willie.

In Fig. 6.5, as expected we observe that the SNR achieved by all the schemes increases with N. In addition to the reasons presented in Fig. 6.2, another reason is that the value of $\sum_{n=1}^{N} |a_n|$ (i.e., the total channel quality of the reflected path from Alice to Willie) increases with N. This leads to the fact that the condition of perfect covertness (i.e., $\sum_{n=1}^{N} |a_n| \geq |h_{aw}|$) becomes easier to be satisfied as

N increases. In general, this figure confirms that perfect covertness can indeed be obtained with the aid of IRS in the context of covert communications, which also verifies the correctness of Theorem 6.1.

6.5.2 *Without Willie's Instantaneous CSI*

In this subsection, corresponding the considered three different scenarios, "$\rho_n = 1, \forall n$" denotes the solution with the IRS's reflection amplitude being fixed to 1, "$\rho_n = \rho_0, \forall n$" denotes the solution with all elements of the IRS sharing the same reflection amplitude ρ_0, and "$\rho_n \leq 1, \forall n$" denotes solution with the optimal reflection amplitude of each IRS element. We note that the transmit power P_a is optimally designed in the above three solutions.

In Fig. 6.6, we plot Bob's SNR and Alice's transmit power P_a achieved by our solutions for different values of ϵ. As expected, we first observe from Fig. 6.6a that Bob's SNR achieved by all solutions decreases as the covertness level becomes harsher. We also observe that the solution with "$\rho_n \leq 1, \forall n$" achieves the highest SNR relative to the solutions of both "$\rho_n = \rho_0, \forall n$" and "$\rho_n = 1, \forall n$", while the solution with "$\rho_n = \rho_0, \forall n$" achieves a higher SNR than the solution with "$\rho_n = 1, \forall n$". This demonstrates that the IRS reflection amplitude control can effectively improve the covert communication performance when Willie's instantaneous CSI is not available. In Fig. 6.6b, we first observe that the required transmit power P_a achieved by our developed solutions decreases as the number of reflection elements N increases, which is different from that observed in the case with Willie's instantaneous CSI, where P_a increases with N. This is attributed to the fact that without Willie's instantaneous CSI, the covertness constraint is

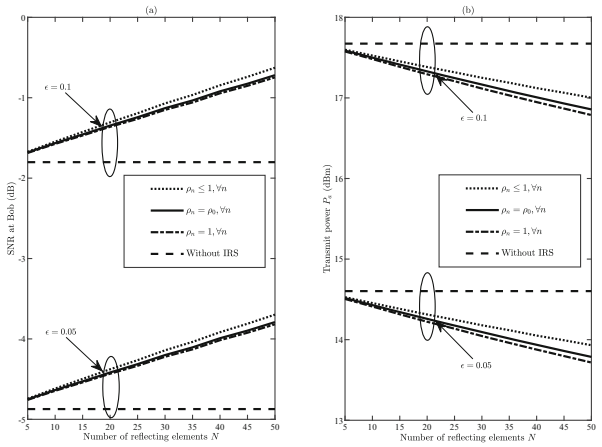


Fig. 6.6 Received SNR at Bob and transmit power at Alice versus the number of reflecting elements for different values of covertness level ϵ, where $\sigma_b^2 = -90$ dBm

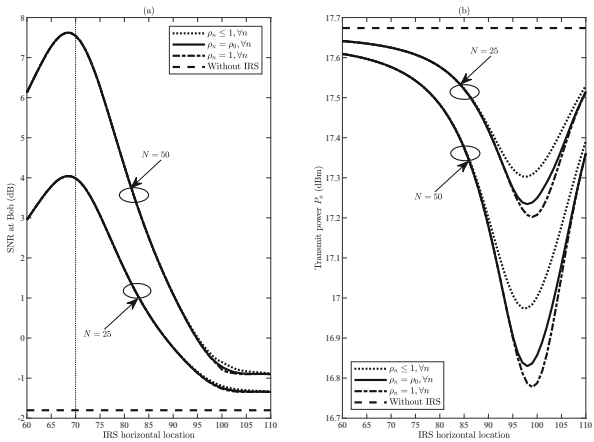


Fig. 6.7 Received SNR at Bob and transmit power at Alice versus IRS horizontal location for covertness level $\epsilon = 0.1$, where $\sigma_b^2 = -90\,\text{dBm}$

only related to the IRS reflection amplitudes and Alice's transmit power P_a, but is independent of IRS phase shifts. As such, the average covertness constraint $\frac{P_a}{\sigma_w^2}\left(\chi_{rw}\sum_{n=1}^{N}\rho_n^2|h_{ar_n}|^2 + \chi_{aw}\right) \le \bar{\epsilon}$ is harder to be satisfied as N increases. Interestingly, we also observe that P_a is higher in the system without IRS relative to that in the system with IRS, which is completely different from the case with Willie's instantaneous CSI.

In Fig. 6.7, we plot Bob's SNR and Alice's transmit power P_a achieved by different solutions versus the IRS horizontal location. We first observe from Fig. 6.7a that the optimal IRS horizontal location is close to the LHS of Bob (denoted by the verticle dashed line in this figure). This is due to the fact that satisfying the covertness constraint becomes challenging as IRS moves closer to Willie. We note that the optimal IRS horizontal location is to balance the transmission quality and communication covertness, since it not only guarantees a small reflection path loss from IRS to Bob, but also makes the covertness constraint easier to be satisfied. We also note that this observation is different from the case with Willie's instantaneous CSI, in which the covertness constraint becomes easier to be satisfied as the IRS moves closer to Willie. In addition, we observe from Fig. 6.7b that the transmit power P_a achieved by our developed solutions decreases as the IRS moves closer to Willie. This is attributed to the fact that the covertness constraint becomes harder to be satisfied as the reflect-path gain from IRS to Willie becomes larger.

6.6 Conclusion

In this chapter, we tackled covert communication system designs by considering the assistance of an IRS in the cases with global CSI and without Willie's instantaneous CSI. For the case with global CSI, we proved that the perfect covertness can be achieved if the channel quality of the reflected path is higher than that of the direct path. Then, we developed a PSCA algorithm and a low-complexity two-stage

algorithm to jointly design the IRS's reflection coefficients and Alice's transmit power. For the case without the Willie's instantaneous CSI, our analysis showed that the phase shift of each IRS element is independent of the covertness constraint, based on which the optimal phase shifts and reflection amplitudes together with the Alice's transmit power are determined. Our examinations showed that deploying an IRS is able to enhance the reflection signal at Bob and deteriorate the detection performance at Willie by properly designing the reflection coefficients, so as to improve covert communication performance. Interestingly, it was revealed that the optimal horizontal location of the IRS is between Bob and Willie for the case with global CSI, while it is close to the LHS of Bob for the case without Willie's instantaneous CSI. To further unleash the potential of IRS-aided covert communications, one challenge to be addressed in future works is how to obtain accurate CSI covertly without using the traditional pilot-based channel estimation methods. Addressing this challenge may call for new emerging techniques (e.g., machine learning) to conduct passive channel estimation (e.g., based on three-dimensional images).

Appendix

Proof of Theorem 6.1

We first note that the perfect covertness implies the required covertness level $\epsilon = 0$. In addition, we observe from (P1) that $\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1)$ in covertness constraint (6.8b) monotonically increases with the received energy at Willie (i.e., $P_a|\mathbf{v}^H\mathbf{a} + h_{aw}|^2$), and $P_a|\mathbf{v}^H\mathbf{a} + h_{aw}|^2 = 0$ means Willie cannot detect any transmission. Thus, under the perfect covertness constraint, problem (P1) can be reformulated into problem (P1′). We note that problem (P1′) is not always feasible when the transmit power P_a is non-zero. In addition, one can verify that $P_a = P_{\max}$ is the optimal solution to problem (P1′) when $E_w \triangleq |\mathbf{v}^H\mathbf{a} + h_{aw}|^2 = 0$. In the following, we focus on deriving the condition of $E_w = 0$. To this end, we first recall that $v_n = \rho_n e^{-j\theta_n}, \forall n$, it follows that

$$E_w = \left| \sum_{n=1}^{N} \rho_n |a_n| e^{j(\arg(a_n)+\theta_n)} + |h_{aw}| e^{j \arg(h_{aw})} \right|^2. \tag{6.49}$$

We note that $E_w = 0$ only when the signs of the real and imaginary part of $\sum_{n=1}^{N} \rho_n |a_n| e^{j(\arg(a_n)+\theta_n)}$ and $|h_{aw}| e^{j \arg(h_{aw})}$ are opposite. We also note that if each summation term $\rho_n |a_n| e^{j(\arg(a_n)+\theta_n)}$ has the same phase for coherent combining, the synthesized $\sum_{n=1}^{N} \rho_n |a_n| e^{j(\arg(a_n)+\theta_n)}$ achieves the largest modulus, which is given by $\sum_{n=1}^{N} \rho_n |a_n|$. As a result, if

$$\sum_{n=1}^{N} \rho_n |a_n| \geq |h_{aw}|, \tag{6.50}$$

we can always adjust reflection amplitude ρ_n and reflection phase shift θ_n such that $E_w = 0$. We note that the maximum value of $\sum_{n=1}^{N} \rho_n |a_n|$ is $\sum_{n=1}^{N} |a_n|$ due to $\rho_n \in [0, 1], \forall n$. Following above discussions, we can conclude that the perfect covertness can be achieved with non-zero transmit power if and only if $\sum_{n=1}^{N} |a_n| \geq |h_{aw}|$. This completes the proof of Theorem 6.1.

Proof of Lemma 6.1

We first note that the second term on the LHS of (6.16) is a linear function of the concerned optimization variable $\mathbf{W}$, while the right-hand side (RHS) of (6.16) is a constant. As such, we only need to prove that the first term on the LHS of (6.16) is convex with respect to $\mathbf{W}$, which is redefined as

$$f(\mathbf{W}) = \left(1 + \frac{\text{Tr}(\mathbf{AW})}{\sigma_w^2}\right) \ln\left(1 + \frac{\text{Tr}(\mathbf{AW})}{\sigma_w^2}\right). \tag{6.51}$$

To proceed, we first note that $x \ln(x)$ is a convex function of x for $x > 0$ [46]. Then, following the fact that $\mathbf{A} \succeq 0$ and $\mathbf{W} \succeq 0$, we have that $f(\mathbf{W})$ is convex with respect to $\mathbf{W}$ since the affine transformation of $x \ln(x)$ is convex with respect to x. This completes the proof of Lemma 6.1.

Proof of Theorem 6.2

As per (6.34), in order to determine $\mathbb{E}_X[\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1)]$, we have to derive the distribution of X. To this end, we first rewrite $\mathbf{h}_{rw}^H \mathbf{\Theta} \mathbf{h}_{ar} + h_{aw}$ as

$$\mathbf{h}_{rw}^H \mathbf{\Theta} \mathbf{h}_{ar} + h_{aw} = \sum_{n=1}^{N} h_{rw_n}^* \rho_n e^{j\theta_n} h_{ar_n} + h_{aw}, \tag{6.52}$$

where h_{rw_n} and h_{ar_n} are the n-th element of $\mathbf{h}_{rw}$ and $\mathbf{h}_{ar}$, respectively. As a result, $\mathbf{h}_{rw}^H \mathbf{\Theta} \mathbf{h}_{ar} + h_{aw}$ follows the distribution $\mathcal{CN}(0, \delta)$, where $\delta \triangleq \chi_{rw} \sum_{n=1}^{N} \rho_n^2 |h_{ar_n}|^2 + \chi_{aw}$. Then, the probability density function (pdf) of X denoted as $f_X(x)$ is an exponential distribution with parameter δ^{-1}. As such, $\mathbb{E}_X[\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1)]$ can be rewritten as

$$\mathbb{E}_X\left[\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1)\right] = \int_0^\infty L\left[\ln\left(1+\frac{P_a x}{\sigma_w^2}\right) - \frac{P_a x}{P_a x+\sigma_w^2}\right] f_X(x)dx,$$
$$= L\left(1+\frac{\sigma_w^2}{\delta P_a}\right) e^{\frac{\sigma_w^2}{\delta P_a}} E_1\left(\frac{\sigma_w^2}{\delta P_a}\right) - L. \tag{6.53}$$

Following (6.53), the covertness constraint $\mathbb{E}_X\left[\mathcal{D}(\mathbb{P}_0|\mathbb{P}_1)\right] \leq 2\epsilon^2$ can be equivalently rewritten as

$$g\left(\frac{\sigma_w^2}{\delta P_a}\right) \leq 1 + \frac{2\epsilon^2}{L}, \tag{6.54}$$

where $g\left(\frac{\sigma_w^2}{\delta P_a}\right) \triangleq \left(1+\frac{\sigma_w^2}{\delta P_a}\right) e^{\frac{\sigma_w^2}{\delta P_a}} E_1\left(\frac{\sigma_w^2}{\delta P_a}\right)$. We note that an exact analytical expression for $g\left(\frac{\sigma_w^2}{\delta P_a}\right)$ is mathematically intractable, since it involves an exponential integral function.

To overcome this difficulty, we next show that $g\left(\frac{\sigma_w^2}{\delta P_a}\right)$ is a monotonically decreasing function of $\frac{\sigma_w^2}{\delta P_a}$. To this end, we first define $g(x) = (1+x)e^x E_1(x)$, where $x \geq 0$. Then, the first derivative of $g(x)$ with respect to x is given by

$$\frac{dg(x)}{dx} = (x+2)e^x E_1(x) - \frac{x+1}{x}$$
$$= (x+2)e^x\left(\int_x^\infty \frac{e^{-t}}{t}dt - s(x)\right), \tag{6.55}$$

where $s(x) = \frac{x+1}{x(x+2)e^x}$. We note that the first derivative of $s(x)$ with respect to x is given by

$$\frac{ds(x)}{dx} = \frac{e^{-x}\left(-2-x(x+2)^2\right)}{x^2(x+2)^2}. \tag{6.56}$$

Considering that $\frac{ds(x)}{dx}$ is a continuous function of x for $x > 0$, we have

$$\int_x^\infty \frac{e^{-t}\left(-2-t(t+2)^2\right)}{t^2(t+2)^2}dt = s(\infty) - s(x)$$
$$= -s(x). \tag{6.57}$$

As per (6.57), we can rearrange (6.55) as

$$\frac{dg(x)}{dx} = (x+2)e^x\left(\int_x^\infty \frac{e^{-t}}{t} + \frac{e^{-t}\left(-2-t(t+2)^2\right)}{t^2(t+2)^2}dt\right)$$

$$= (x+2)e^{x}\int_{x}^{\infty}\frac{-2e^{-t}}{t^{2}(t+2)^{2}}dt. \tag{6.58}$$

Following the fact that the integrand $\frac{-2e^{-t}}{t^2(t+2)^2}$ is always less than or equal to 0, we have $\frac{dg(x)}{dx} \leq 0$ must hold for $x > 0$. As a result, $g(x)$ is a monotonically decreasing function of x for $x > 0$. Following the above fact, we have $g\left(\frac{\sigma_w^2}{\delta P_a}\right)$ given in (6.54) as a monotonically increasing function of $\frac{\delta P_a}{\sigma_w^2}$. Then, the covertness constraint (6.54) can be equivalently rewritten as that given in (6.35), which completes the proof of Theorem 6.2.

References

1. Wong, V.W.S., Schober, R., Ng, D.W.K., Wang, L.-C.: Key Technologies for 5G Wireless Systems. Cambridge University Press, Cambridge (2017)
2. Zhang, J., Björnson, E., Matthaiou, M., Ng, D.W.K., Yang, H., Love, D.J.: Prospective multiple antenna technologies for beyond 5G. IEEE J. Sel. Areas Commun. **38**(8), 1637–1660 (2020)
3. Wu, Q., Zhang, S., Zheng, B., You, C., Zhang, R.: Intelligent reflecting surface-aided wireless communications: a tutorial. IEEE Trans. Commun. **69**(5), 3313–3351 (2021)
4. Ning, B., Chen, Z., Chen, W., Fang, J.: Beamforming optimization for intelligent reflecting surface assisted MIMO: a sum-path-gain maximization approach. IEEE Wireless Commun. Lett. **9**(7), 1105–1109 (2020)
5. Han, Y., Tang, W., Jin, S., Wen, C., Ma, X.: Large intelligent surface-assisted wireless communication exploiting statistical CSI. IEEE Trans. Veh. Technol. **68**(8), 8238–8242 (2019)
6. Peng, Z., Li, T., Pan, C., Ren, H., Xu, W., Renzo, M.D.: Analysis and optimization for RIS-aided multi-pair communications relying on statistical CSI. IEEE Trans. Veh. Technol. **70**(4), 3897–3901 (2021)
7. Zhi, K., Pan, C., Ren, H., Wang, K.: Power scaling law analysis and phase shift optimization of RIS-aided massive MIMO systems with statistical CSI. Available via arXiv. https://arxiv.org/abs/2010.13525
8. Wu, Q., Zhang, R.: Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming. IEEE Trans. Wireless Commun. **18**(11), 5394–5409 (2019)
9. Huang, C., Zappone, A., Alexandropoulos, G.C., Debbah, M., Yuen, C.: Reconfigurable intelligent surfaces for energy efficiency in wireless communication. IEEE Trans. Wireless Commun. **18**(8), 4157–4170 (2019)
10. Pan, C., Ren, H., Wang, K., Xu, W., Elkashlan, M., Nallanathan, A., Hanzo, L.: Multicell MIMO communications relying on intelligent reflecting surfaces. IEEE Trans. Wirel. Commun. **19**(8), 5218–5233 (2020)
11. Huang, C., Mo, R., Yuen, C.: Reconfigurable intelligent surface assisted multiuser MISO systems exploiting deep reinforcement learning. IEEE J. Sel. Areas Commun. **38**(8), 1839–1850 (2020)
12. Pan, C., Ren, H., Wang, K., Elkashlan, M., Nallanathan, A., Wang, J., Hanzo, L.: Intelligent reflecting surface aided MIMO broadcasting for simultaneous wireless information and power transfer. IEEE J. Sel. Areas Commun. **38**(8), 1719–1734 (2020)
13. Wu, Q., Zhang, R.: Weighted sum power maximization for intelligent reflecting surface aided SWIPT. IEEE Wirel. Commun. Lett. **9**(5), 586–590 (2020)
14. Pan, C., et al.: Reconfigurable intelligent surfaces for 6G systems: principles, applications, and research directions. IEEE Commun. Mag. **59**(6), 14–20 (2021)

15. Huang, C., Hu, S., Alexandropoulos, G.C., Zappone, A., Yuen, C., Zhang, R., Renzo, M.D., and Debbah, M., Holographic MIMO surfaces for 6G wireless networks: Opportunities, challenges, and trends. IEEE Wireless Commun. **27**(5), 118–125 (2020)
16. Cui, M., Zhang, G., Zhang, R.: Secure wireless communication via intelligent reflecting surface. IEEE Wirel. Commun. Lett. **8**(5), 1410–1414 (2019)
17. Chu, Z., Hao, W., Xiao, P., Shi, J.: Intelligent reflecting surface aided multi-antenna secure transmission. IEEE Wirel. Commun. Lett. **9**(1), 108–112 (2020)
18. Guan, X., Wu, Q., Zhang, R.: Intelligent reflecting surface assisted secrecy communication: is artificial noise helpful or not? IEEE Wirel. Commun. Lett. **9**(6), 778–782 (2020)
19. Dong, L., Wang, H.: Enhancing secure MIMO transmission via intelligent reflecting surface. IEEE Trans. Wirel. Commun. **19**(11), 7543–7556 (2020)
20. Dong, L., Wang, H.: Secure MIMO transmission via intelligent reflecting surface. IEEE Wirel. Commun. Lett. **9**(6), 787–790 (2020)
21. Hong, S., Pan, C., Ren, H., Wang, K., Nallanathan, A.: Artificial-noise-aided secure MIMO wireless communications via intelligent reflecting surface. IEEE Trans. Commun. **68**(12), 7851–7866 (2020)
22. Yu, X., Xu, D., Sun, Y., Ng, D.W.K., Schober, R.: Robust and secure wireless communications via intelligent reflecting surfaces. IEEE J. Sel. Areas Commun. **38**(11), 2637–2652 (2020)
23. Hong, S., Pan, C., Ren, H., Wang, K., Chai, K.K., Nallanathan, A.: Robust transmission design for intelligent reflecting surface aided secure communication systems with imperfect cascaded CSI. IEEE Trans. Wirel. Commun. **20**(4), 2487–2501 (2021)
24. Yan, S., Zhou, X., Hu, J., Hanly, S.V.: Low probability of detection communication: Opportunities and challenges. IEEE Wirel. Commun. **26**(5), 19–25 (2019)
25. He, B., Yan, S., Zhou, X., Lau, V.K.N.: On covert communication with noise uncertainty. IEEE Commun. Lett. **21**(4), 941–944 (2017)
26. Wang, J., Tang, W., Zhu, Q., Li, X., Rao, H., Li, S.: Covert communication with the help of relay and channel uncertainty. IEEE Wirel. Commun. Lett. **8**(1), 317–320 (2019)
27. Bash, B.A., Goeckel, D., Towsley, D.: Limits of reliable communication with low probability of detection on AWGN channels. IEEE J. Sel. Areas Commun. **31**(9), 1921–1930 (2013)
28. Shahzad, K., Zhou, X., Yan, S., Hu, J., Shu, F., Li, J.: Achieving covert wireless communications using a full-duplex receiver. IEEE Trans. Wirel. Commun. **17**(12), 8517–8530 (2018)
29. Li, K., Kelly, P.A., Goeckel, D.: Optimal power adaptation in covert communication with an uninformed jammer. IEEE Trans. Wirel. Commun. **19**(5), 3463–3473 (2020)
30. Hu, J., Yan, S., Shu, F., Wang, J.: Covert transmission with a self-sustained relay. IEEE Trans. Wirel. Commun. **18**(8), 4089–4102 (2019)
31. Zhou, X., Yan, S., Hu, J., Sun, J., Li, J., Shu, F.: Joint optimization of a UAV's trajectory and transmit power for covert communications. IEEE Trans. Signal Process. **67**(16), 4276–4290 (2019)
32. Wang, H., Zhang, Y., Zhang, X., Li, Z.: Secrecy and covert communications against UAV surveillance via multi-hop networks. IEEE Trans. Commun. **68**(1), 389–401 (2020)
33. Yan, S., Cong, Y., Hanly, S.V., Zhou, X.: Gaussian signalling for covert communications. IEEE Trans. Wirel. Commun. **18**(7), 3542–3553 (2019)
34. He, B., Yan, S., Zhou, X., Jafarkhani, H.: Covert wireless communication with a poisson field of interferers. IEEE Trans. Wirel. Commun. **17**(9), 6005–6017 (2018)
35. Zheng, T., Wang, H., Ng, D.W.K., Yuan, J.: Multi-antenna covert communications in random wireless networks. IEEE Trans. Wirel. Commun. **18**(3), 1974–1987 (2019)
36. Yan, S., He, B., Zhou, X., Cong, Y., Swindlehurst, A.L.: Delay-intolerant covert communications with either fixed or random transmit power. IEEE Trans. Inf. Forensics Secur. **14**(1), 129–140 (2019)
37. Lu, X., Hossain, E., Shafique, T., Feng, S., Jiang, H., Niyato, D.: Intelligent reflecting surface enabled covert communications in wireless networks. IEEE Netw. **34**(5), 148–155 (2020)
38. Si, J., Li, Z., Cheng, J., Guan, L., Al-Dhahir, N.: Covert transmission assisted by intelligent reflecting surface. IEEE Trans. Commun. **69**(8), 5394–5408 (2021)

39. Sun, X., Yan, S., Yang, N., Ding, Z., Shen, C., Zhong, Z.: Short-packet downlink transmission with non-orthogonal multiple access. IEEE Trans. Wirel. Commun. **17**(7), 4550–4564 (2018)
40. Liu, H., Yuan, X., Zhang, Y.J.A.: Matrix-calibration-based cascaded channel estimation for reconfigurable intelligent surface assisted multiuser MIMO. IEEE J. Sel. Areas Commun. **38**(11), 2621–2636 (2020)
41. Wei, L., Huang, C., Alexandropoulos, G.C., Yuen, C., Zhang, Z., Debbah, M.: Channel estimation for RIS-empowered multi-user MISO wireless communications. IEEE Trans. Commun. **69**(6), 4144–4157 (2021)
42. Xie, H., Xu, J., Liu, Y.-F.: Max-min fairness in IRS-aided multi-cell MISO systems with joint transmit and reflective beamforming. IEEE Trans. Wirel. Commun. **20**(2), 1379–1393 (2021)
43. Mursia, P., Sciancalepore, V., Garcia-Saavedra, A., Cottatellucci, L., Pérez, X.C., Gesbert, D.: RISMA: reconfigurable intelligent surfaces enabling beamforming for IoT massive access. IEEE J. Sel. Areas Commun. **39**(4), 1072–1085 (2021)
44. Abeywickrama, S., Zhang, R., Wu, Q., Yuen, C.: Intelligent reflecting surface: Practical phase shift model and beamforming optimization. IEEE Trans. Commun. **68**(9), 5849–5863 (2020)
45. Chen, X., Ng, D.W.K., Gerstacker, W.H., Chen, H.: A survey on multiple-antenna techniques for physical layer security. IEEE Commun. Surveys Tuts. **19**(2), 1027–1053 (2017)
46. Boyd, S., Vandenberghe, L.: Convex Optimization. Cambridge University Press, Cambridge (2004)
47. Hiriart-Urruty, J., Lemarechal, C.: Convex Analysis and Minimization Algorithms I: Fundamentals. Springer, New York (1996)
48. Lipp, T., Boyd, S.: Variations and extension of the convex-concave procedure. Optim. Eng. **17**(2), 263–287 (2016)
49. Li, W., Chang, T., Lin, C., Chi, C.: Coordinated beamforming for multiuser MISO interference channel under rate outage constraints. IEEE Trans. Signal Process. **61**(5), 1087–1103 (2013)
50. Tervo, O., Tran, L., Juntti, M.: Optimal energy-efficient transmit beamforming for multi-user MISO downlink. IEEE Trans. Signal Process. **63**(20) (2015)
51. Guan, X., Wu, Q., Zhang, R.: Joint power control and passive beamforming in IRS-assisted spectrum sharing. IEEE Commun. Lett. **24**(7), 1553–1557 (2020)

Chapter 7
Intelligent Reflecting Surface Aided Secure Transmission with Colluding Eavesdroppers

This chapter studies a secure MISO communication system aided by an IRS, where multiple colluding Eves coexist. We aim to maximize the SSR via jointly optimizing the beamforming vectors, the AN and the phase shifts at the IRS subject to the maximum transmit power constraint and unit modulus constraints. To address the non-convex optimization problem, we first propose an AO algorithm based on SDR and obtain a high-quality sub-optimal solution. In order to reduce the high computational complexity, a low-complexity alternating optimization (LC-AO) algorithm is developed, in which the beamforming vectors, AN and the IRS phase shifts are optimized alternately by the generalized power iteration (GPI) and the Riemannian manifold conjugate gradient (RMCG) algorithm, respectively. Simulation results show the advantages of deploying the IRS in improving the system secrecy performance.

7.1 Introduction

In order to cope with the explosive growth of mobile data traffic and the connection of massive device in the 5G wireless networks, various key technologies such as UDN, massive MIMO, and mmWave communications have been advocated [1], [2]. However, the required high complexity and hardware cost, as well as increased energy consumption are still key issues that have not been addressed. In addition, although 5G physical layer technology can usually adapt to the wireless environment varying in space and time, radio propagation environment is essentially uncontrollable.

Due to these reasons, IRS has been considered as a promising new technology, which can reconfigure the wireless propagation environment by controlling reflection with software [3]. Specifically, an IRS composes a large number of low-cost passive reflecting elements, each of which can independently induce the

F. Shu, J. Wang, *Intelligent Reflecting Surface-Aided Physical-Layer Security*,
Wireless Networks, https://doi.org/10.1007/978-3-031-41812-9_7

phase shift of the incident signal. By properly adjusting the passive beamforming, the reflected signals from the IRS and the signals from other paths can be combined constructively to enhance the desired signal power at the receiver or destructively to eliminate undesired signals such as co-channel interference. Due to these advantages, IRS has been leveraged in several wireless communication systems, including MISO system in [4], multiuser MIMO downlink system in [5] and multigroup multicast system in [6], etc.

On the other hand, physical layer security has received wide attention in recent years. It is known that IRS can improve the secrecy data rate (DR) by increasing the DR of legitimate receivers while decreasing the DR of Eves. Hence, IRS can be used for secure communication under the wiretap channel. Many recent studies have utilized IRS to secure the physical layer of wireless communications [7–10]. In [8], the authors investigated the joint optimization of active transmit and passive reflect beamforming to maximize the SR in an IRS-aided MISO secure communication system. Shi et al. presented an investigation of an IRS-aided secure wireless information and power transfer system to maximize the harvested power[9]. The authors in [10] considered the SR maximization problem in an AN-aided secure MIMO communication system with an IRS. All the reported researches only considered the non-colluding Eves scenario. However, in real network environments, Eves usually cooperate with each other to jointly decode confidential information, resulting in degradation of the SR. Some prior works [11], [12] indicated that colluding Eves can cause a severe threat to wireless communication security. The colluding Eves case represents a worst case from the perspective of security, since it makes the secure system more valuable. Therefore, it is necessary to investigate the performance advantages when an IRS is considered in secure system with colluding Eves. To the best of the authors' knowledge, this is the first work that takes the colluding Eves case into consideration in the secure IRS-aided systems. The contributions of our work are summarized as follows:

1. We consider an IRS-aided secure multiuser MISO system in the presence of multiple colluding Eves, and formulate a non-convex SSR maximization problem by jointly optimizing the beamforming vectors, the AN, and the phase shifts at the IRS. To address the problem, we first transform the original problem into a more tractable form. Then, the design of the beamforming vectors, AN and IRS phase shifts are handled by AO based on SDR technique.
2. Due to the high computational complexity of SDR-based method, we propose a low-complexity alternating optimization (LC-AO) algorithm. Specifically, given the phase shifts of IRS, the generalized power iteration (GPI) is adopted for optimizing the beamforming vectors and AN. Then, given the beamforming vectors and AN, the optimization problem for IRS phase shifts is solved by utilizing the Riemannian manifold conjugate gradient (RMCG) algorithm. Simulation results show the proposed algorithms significantly improve the secrecy performance.

Notation $\mathbb{E}\{\cdot\}$ denotes the expectation operation. $|\cdot|$, $||\cdot||$ and $\mathrm{Re}\{\cdot\}$ represent the absolute value of a scalar, the 2-norm of a vector and the real part of a complex number, respectively. $(\cdot)^*$, $(\cdot)^T$, $(\cdot)^H$ and $\mathrm{Tr}(\cdot)$ denote conjugate, transpose, conjugate

transpose and trace operations, respectively. diag$(\cdot)$ represents the diagonalization operation. blkdiag$(\mathbf{A}_1, \cdots, \mathbf{A}_n)$ is a block diagonal matrix whose diagonal elements are $\mathbf{A}_1, \cdots, \mathbf{A}_n$. unt$(\mathbf{a})$ forms a vector whose elements are $\frac{a_1}{|a_1|}, \cdots, \frac{a_n}{|a_n|}$. The distribution of a circularly symmetric complex Gaussian random variable with zero mean and variance σ^2 is denoted by $\mathcal{CN}(0, \sigma^2)$. $\circ$ represents the Hadamard product between two matrices.

7.2 System Model and Problem Formulation

We consider an IRS-aided secure communication system, which comprises an M-antenna BS, an N-element IRS, K single-antenna legitimate users in the set of $\mathcal{K} = \{1, \cdots, K\}$, and L single-antenna Eves in the set of $\mathcal{L} = \{1, \cdots, L\}$, as shown in Fig. 7.1. The Eves collude with each other to jointly overhear confidential information transmitted to the users. We assume that all the CSIs are perfectly known at the BS.[1] The transmit signal at the BS can be expressed as $\mathbf{x} = \sum_{k=1}^{K} \mathbf{w}_k s_k + \mathbf{z}$, where $\mathbf{w}_k \in \mathbb{C}^{M\times 1}$ and s_k represent the beamforming vector for the k-th user and the corresponding information symbol, respectively. Without loss of generality, it is assumed that $\mathbb{E}\{|s_k|^2\} = 1, \forall k$. $\mathbf{z} \sim \mathcal{CN}(0, \mathbf{Z})$ denotes the AN vector with zero mean and covariance matrix $\mathbf{Z}$. We denote the channel from the BS to the IRS, BS to the k-th user, BS to the l-th Eve, IRS to the k-th user and IRS to the l-th Eve as $\mathbf{G} \in \mathbb{C}^{N\times M}$,$\mathbf{h}_{ab,k}^H \in \mathbb{C}^{1\times M}$, $\mathbf{h}_{ae,l}^H \in \mathbb{C}^{1\times M}$, $\mathbf{h}_{ib,k}^H \in \mathbb{C}^{1\times N}$, $\mathbf{h}_{ie,l}^H \in \mathbb{C}^{1\times N}$, respectively. In addition, the phase shift matrix $\mathbf{\Theta}$ at the IRS is given by $\mathbf{\Theta} = \text{diag}(e^{j\theta_1}, e^{j\theta_2}, \cdots, e^{j\theta_N})$, where θ_n is the phase shift of the n-th reflecting element at the IRS. Thus, the received signals at the k-th user and the l-th Eve can be respectively written as

$$y_{b,k} = (\mathbf{h}_{ib,k}^H \mathbf{\Theta} \mathbf{G} + \mathbf{h}_{ab,k}^H)(\sum_{k=1}^{K} \mathbf{w}_k s_k + \mathbf{z}) + n_{bk}, \tag{7.1}$$

$$y_{e,l} = (\mathbf{h}_{ie,l}^H \mathbf{\Theta} \mathbf{G} + \mathbf{h}_{ae,l}^H)(\sum_{k=1}^{K} \mathbf{w}_k s_k + \mathbf{z}) + n_{el}, \tag{7.2}$$

where $n_{bk} \sim \mathcal{CN}(0, \sigma_b^2)$ and $n_{el} \sim \mathcal{CN}(0, \sigma_e^2)$ are the additive white Gaussian noises. Let us define $\mathbf{v} = [e^{j\theta_1}, \cdots, e^{j\theta_N}]^H \in \mathbb{C}^{N\times 1}$, $\mathbf{u} = [\mathbf{v}; 1]$, $\mathbf{H}_{ib,k} = \text{diag}\{\mathbf{h}_{ib,k}^H\}\mathbf{G} \in \mathbb{C}^{N\times M}$, $\mathbf{H}_{ie,l} = \text{diag}\{\mathbf{h}_{ie,l}^H\}\mathbf{G} \in \mathbb{C}^{N\times M}$, $\mathbf{H}_{b,k} = [\mathbf{H}_{ib,k}; \mathbf{h}_{ab,k}^H]$, $\mathbf{H}_{e,l} = [\mathbf{H}_{ie,l}; \mathbf{h}_{ae,l}^H]$. Accordingly, the achievable DR at the k-th user is given by $R_k = \log_2(1 + \gamma_k)$, where

[1] In practice, the results in this chapter serve as theoretical performance upper bounds for the considered system, and can be seen as the benchmark for the imperfect CSI case.

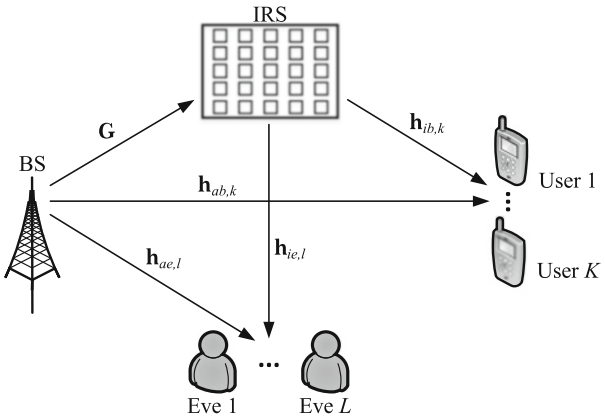


Fig. 7.1 An IRS-aided secure communication system with colluding Eves

$$\gamma_k = \frac{|\mathbf{u}^H \mathbf{H}_{b,k} \mathbf{w}_k|^2}{\sum_{i \neq k}^{K} |\mathbf{u}^H \mathbf{H}_{b,k} \mathbf{w}_i|^2 + |\mathbf{u}^H \mathbf{H}_{b,k} \mathbf{z}|^2 + \sigma_b^2}. \tag{7.3}$$

When the L Eves cooperate to wiretap the k-th user, they can be seen as an Eve with L antennas. Then, the achievable DR is given by $R_k^e = \log_2(1 + \sum_{l=1}^{L} \gamma_{e,k})$ [13], where

$$\gamma_{e,k} = \frac{|\mathbf{u}^H \mathbf{H}_{e,l} \mathbf{w}_k|^2}{\sum_{i \neq k}^{K} |\mathbf{u}^H \mathbf{H}_{e,l} \mathbf{w}_i|^2 + |\mathbf{u}^H \mathbf{H}_{e,l} \mathbf{z}|^2 + \sigma_e^2}. \tag{7.4}$$

In this chapter, we maximize the SSR by jointly optimizing $\mathbf{w}_k$, $\mathbf{z}$ and $\boldsymbol{\Theta}$, subject to the transmit power constraint and unit modulus constraints. The optimization problem can be formulated as

$$(\text{P1}): \max_{\{\mathbf{w}_k\}, \mathbf{z}, \boldsymbol{\Theta}} \sum_{k=1}^{K} (R_k - R_k^e) \tag{7.5a}$$

$$\text{s.t.} \quad \sum_{k=1}^{K} ||\mathbf{w}_k||^2 + ||\mathbf{z}||^2 \leq P, \tag{7.5b}$$

$$|\boldsymbol{\Theta}_{nn}| = 1, \quad \forall n = 1 \cdots N, \tag{7.5c}$$

where P is the maximum transmit power of the BS. Note that the expression of R_k^e in (7.4) is difficult to tackle and the optimization variables are coupled, which make problem (P1) difficult to solve optimally in general. Besides, the non-convex unit modulus constraints aggravate the difficulty. In the following, we propose two algorithms to solve problem (P1).

7.3 Proposed Solutions

7.3.1 SDR-Based Method

In this subsection, we decompose the original problem into two subproblems by employing AO algorithm. For each subproblem, we transform it into an SDP problem by applying SDR. We first define $\mathbf{W}_k = \mathbf{w}_k \mathbf{w}_k^H$ and $\mathbf{U} = \mathbf{u}\mathbf{u}^H$, then R_k and R_k^e can be rewritten as

$$R_k = \log_2 \left(1 + \frac{\mathrm{Tr}(\mathbf{H}_{b,k}^H \mathbf{U} \mathbf{H}_{b,k} \mathbf{W}_k)}{\mathrm{Tr}(\mathbf{H}_{b,k}^H \mathbf{U} \mathbf{H}_{b,k} (\sum_{i \neq k}^K \mathbf{W}_i + \mathbf{Z})) + \sigma_b^2} \right), \tag{7.6}$$

$$R_k^e = \log_2 \left(1 + \sum_{l=1}^{L} \frac{\mathrm{Tr}(\mathbf{H}_{e,l}^H \mathbf{U} \mathbf{H}_{e,l} \mathbf{W}_k)}{\mathrm{Tr}(\mathbf{H}_{e,l}^H \mathbf{U} \mathbf{H}_{e,l} (\sum_{i \neq k}^K \mathbf{W}_i + \mathbf{Z})) + \sigma_e^2} \right). \tag{7.7}$$

By applying Jensen's inequality, R_k^e is lower bounded as

$$\bar{R}_k^e = \frac{1}{L} \sum_{l=1}^{L} \log_2 \left(1 + \frac{L \mathrm{Tr}(\mathbf{H}_{e,l}^H \mathbf{U} \mathbf{H}_{e,l} \mathbf{W}_k)}{\mathrm{Tr}(\mathbf{H}_{e,l}^H \mathbf{U} \mathbf{H}_{e,l} (\sum_{i \neq k}^K \mathbf{W}_i + \mathbf{Z})) + \sigma_e^2} \right). \tag{7.8}$$

Then, we can replace the objective function with its tractable upper bound and further recast it in the form of difference of the convex functions, i.e., $\sum_{k=1}^K (R_k - \bar{R}_k^e) = -f_1 - f_2 + g_1 + g_2$, where

$$f_1 = -\sum_{k=1}^{K} \log_2 (\mathrm{Tr}(\mathbf{H}_{b,k}^H \mathbf{U} \mathbf{H}_{b,k} (\sum_{i=1}^{K} \mathbf{W}_i + \mathbf{Z})) + \sigma_b^2), \tag{7.9}$$

$$f_2 = -\sum_{k=1}^{K} \sum_{l=1}^{L} \frac{1}{L} \log_2 (\mathrm{Tr}(\mathbf{H}_{e,l}^H \mathbf{U} \mathbf{H}_{e,l} (\sum_{i \neq k}^{K} \mathbf{W}_i + \mathbf{Z})) + \sigma_e^2),$$

$$g_1 = -\sum_{k=1}^{K} \log_2 (\mathrm{Tr}(\mathbf{H}_{b,k}^H \mathbf{U} \mathbf{H}_{b,k} (\sum_{i \neq k}^{K} \mathbf{W}_i + \mathbf{Z})) + \sigma_b^2),$$

$$g_2 = -\sum_{k=1}^{K} \sum_{l=1}^{L} \frac{1}{L} \log_2 (\mathrm{Tr}(\mathbf{H}_{e,l}^H \mathbf{U} \mathbf{H}_{e,l} (\sum_{i \neq k}^{K} \mathbf{W}_i + \mathbf{Z})) + L \mathrm{Tr}(\mathbf{H}_{e,l}^H \mathbf{U} \mathbf{H}_{e,l} \mathbf{W}_k) + \sigma_e^2).$$

Consequently, the original problem (P1) can be rewritten as

$$(\mathrm{P2}): \min_{\{\mathbf{W}_k\}, \mathbf{Z}, \mathbf{U}} \quad f_1 + f_2 - g_1 - g_2 \tag{7.10}$$

$$\text{s.t.} \quad \text{C1}: \sum_{k=1}^{K} \text{Tr}(\mathbf{W}_k) + \text{Tr}(\mathbf{Z}) \leq P, \quad \text{C2}: \mathbf{W}_k \succeq 0, \forall k, \mathbf{Z} \succeq 0$$
$$\text{C3}: \mathbf{U}_{n,n} = 1, \quad \forall n = 1 \cdots N+1, \quad \text{C4}: \mathbf{U} \succeq 0.$$

where the rank-one constraints are dropped by adopting SDR. Next, we divide (P2) into two subproblems by applying AO and obtain the first-order Taylor approximation of g_i, $(i = 1, 2)$. Then each subproblem can be turned into a convex problem and efficiently solved via using CVX [14]. Since the solution obtained by SDR can not be guaranteed to be rank-one, Gaussian randomization is adopted to recover the rank-one solution to problem (P2). According to [15], the complexity of solving the problem (P2) is $O(M^{6.5} + N^{6.5})$, which is extremely high. To reduce the complexity, we propose an LC-AO algorithm in next subsection.

7.3.2 *Proposed LC-AO Algorithm*

In this subsection, we develop a new AO algorithm to solve problem (P1). Specifically, a GPI-based algorithm is proposed for designing the beamforming vectors and AN. Then, we apply the RMCG algorithm to design IRS phase shifts.

With fixed phase shifts at the IRS, we transform the optimization problem (7.5a) into a product form of Rayleigh quotients. To facilitate it, we define $\bar{\mathbf{w}}_k = \mathbf{w}_k/\sqrt{P}, \forall k$, $\bar{\mathbf{z}} = \mathbf{z}/\sqrt{P}$ and reformulate the beamforming and AN optimization problem as

$$\text{(P3-1)}: \max_{\{\bar{\mathbf{w}}_k\}, \bar{\mathbf{z}}} \sum_{k=1}^{K} (R_k - R_k^e) \quad \text{s.t.} \sum_{k=1}^{K} ||\bar{\mathbf{w}}_k||^2 + ||\bar{\mathbf{z}}||^2 \leq 1. \tag{7.11}$$

Next, we make a large vector as $\bar{\mathbf{w}} = [\bar{\mathbf{w}}_1^T, \cdots, \bar{\mathbf{w}}_K^T, \bar{\mathbf{z}}^T]^T \in \mathbb{C}^{M(K+1)\times 1}$. Assuming that the norm of $\bar{\mathbf{w}}$ equals to one, i.e., $||\bar{\mathbf{w}}|| = 1$, R_k can be rewritten as

$$R_k = \log_2 \left(\frac{\bar{\mathbf{w}}^H \mathbf{A}_k \bar{\mathbf{w}}}{\bar{\mathbf{w}}^H \mathbf{B}_k \bar{\mathbf{w}}} \right), \tag{7.12}$$

where

$$\mathbf{A}_k = \text{blkdiag}(\mathbf{P}_k, \cdots, \mathbf{P}_k) + \mathbf{I}_{M(K+1)} \frac{\sigma_b^2}{P}, \tag{7.13}$$

$$\mathbf{B}_k = \mathbf{A}_k - \text{blkdiag}(\mathbf{0}, \cdots, \mathbf{P}_k, \cdots, \mathbf{0}). \tag{7.14}$$

Here, $\mathbf{P}_k = \mathbf{H}_{b,k}^H \mathbf{U} \mathbf{H}_{b,k}$, $\mathbf{A}_k, \mathbf{B}_k \in \mathbb{C}^{M(K+1)\times M(K+1)}$ are block diagonal matrices. The nonzero block $\mathbf{P}_k$ is located at the k-th block in the block diagonal matrix in (7.14).

Similarly, R_k^e can be rewritten as

$$R_k^e = \log_2 \left(\sum_{l=1}^{L} \left(\frac{\bar{\mathbf{w}}^H \mathbf{C}_{l,k} \bar{\mathbf{w}}}{\bar{\mathbf{w}}^H \mathbf{D}_{l,k} \bar{\mathbf{w}}} \right) \right), \tag{7.15}$$

where

$$\mathbf{C}_{l,k} = \text{blkdiag}(\mathbf{Q}_l, \cdots, L\mathbf{Q}_l, \cdots, \mathbf{Q}_l) + \mathbf{I}_{M(K+1)} \frac{\sigma_e^2}{P}, \tag{7.16}$$

$$\mathbf{D}_{l,k} = L \times \text{blkdiag}(\mathbf{Q}_l, \cdots, \mathbf{0}, \cdots, \mathbf{Q}_l) + \mathbf{I}_{M(K+1)} \frac{L\sigma_e^2}{P}. \tag{7.17}$$

Here, $\mathbf{Q}_l = \mathbf{H}_{e,l}^H \mathbf{U} \mathbf{H}_{e,l}$, $\mathbf{C}_{l,k}, \mathbf{D}_{l,k} \in \mathbb{C}^{M(K+1)\times M(K+1)}$, $L\mathbf{Q}_l$ and $\mathbf{0}$ are located at the k-th block in the block diagonal matrices in (7.16) and (7.17), respectively. Based on above transformation, problem (P3-1) can be represented as

$$\text{(P3-2)}: \max_{\{\bar{\mathbf{w}}_k\}} \log_2 \prod_{k=1}^{K} \left(\frac{\bar{\mathbf{w}}^H \mathbf{A}_k \bar{\mathbf{w}}}{\bar{\mathbf{w}}^H \mathbf{B}_k \bar{\mathbf{w}}} \right) \left(\sum_{l=1}^{L} \frac{\bar{\mathbf{w}}^H \mathbf{C}_{l,k} \bar{\mathbf{w}}}{\bar{\mathbf{w}}^H \mathbf{D}_{l,k} \bar{\mathbf{w}}} \right)^{-1}. \tag{7.18}$$

Note that the power constraint in (7.11) is removed because it is already met by the assumption of $||\bar{\mathbf{w}}|| = 1$. Then, We are able to find a sub-optimal solution which satisfies the first-order optimality condition. The following lemma shows the first-order optimality condition of the problem (P3-2) in (7.18).

Lemma 7.1 *The first-order optimality condition of (7.18) is*

$$\mathbf{A}(\bar{\mathbf{w}})\bar{\mathbf{w}} = \lambda(\bar{\mathbf{w}})\mathbf{B}(\bar{\mathbf{w}})\bar{\mathbf{w}}, \tag{7.19}$$

where

$$\lambda(\bar{\mathbf{w}}) = \prod_{k=1}^{K} \left(\frac{\bar{\mathbf{w}}^H \mathbf{A}_k \bar{\mathbf{w}}}{\bar{\mathbf{w}}^H \mathbf{B}_k \bar{\mathbf{w}}} \right) \left(\sum_{l=1}^{L} \frac{\bar{\mathbf{w}}^H \mathbf{C}_{l,k} \bar{\mathbf{w}}}{\bar{\mathbf{w}}^H \mathbf{D}_{l,k} \bar{\mathbf{w}}} \right)^{-1}, \tag{7.20}$$

$\mathbf{A}(\bar{\mathbf{w}})$ *and* $\mathbf{B}(\bar{\mathbf{w}})$ *are given by*

$$\mathbf{A}(\bar{\mathbf{w}}) = \sum_{k=1}^{K}\left[\frac{\mathbf{A}_k}{\bar{\mathbf{w}}^H\mathbf{A}_k\bar{\mathbf{w}}} + \sum_{m=1}^{L}\left\{\frac{\frac{\bar{\mathbf{w}}^H\mathbf{C}_{m,k}\bar{\mathbf{w}}}{\bar{\mathbf{w}}^H\mathbf{D}_{m,k}\bar{\mathbf{w}}}}{\sum_{l=1}^{L}\frac{\bar{\mathbf{w}}^H\mathbf{C}_{l,k}\bar{\mathbf{w}}}{\bar{\mathbf{w}}^H\mathbf{D}_{l,k}\bar{\mathbf{w}}}}\left(\frac{\mathbf{D}_{m,k}}{\bar{\mathbf{w}}^H\mathbf{D}_{m,k}\bar{\mathbf{w}}}\right)\right\}\right]\prod_{k=1}^{K}\left(\frac{\bar{\mathbf{w}}^H\mathbf{A}_k\bar{\mathbf{w}}}{\bar{\mathbf{w}}^H\mathbf{B}_k\bar{\mathbf{w}}}\right), \tag{7.21}$$

$$\mathbf{B}(\bar{\mathbf{w}}) = \sum_{k=1}^{K}\left[\frac{\mathbf{B}_k}{\bar{\mathbf{w}}^H\mathbf{B}_k\bar{\mathbf{w}}} + \sum_{m=1}^{L}\left\{\frac{\frac{\bar{\mathbf{w}}^H\mathbf{C}_{m,k}\bar{\mathbf{w}}}{\bar{\mathbf{w}}^H\mathbf{D}_{m,k}\bar{\mathbf{w}}}}{\sum_{l=1}^{L}\frac{\bar{\mathbf{w}}^H\mathbf{C}_{l,k}\bar{\mathbf{w}}}{\bar{\mathbf{w}}^H\mathbf{D}_{l,k}\bar{\mathbf{w}}}}\left(\frac{\mathbf{C}_{m,k}}{\bar{\mathbf{w}}^H\mathbf{C}_{m,k}\bar{\mathbf{w}}}\right)\right\}\right] \times \prod_{k=1}^{K}\left(\sum_{l=1}^{L}\frac{\bar{\mathbf{w}}^H\mathbf{C}_{l,k}\bar{\mathbf{w}}}{\bar{\mathbf{w}}^H\mathbf{D}_{l,k}\bar{\mathbf{w}}}\right), \tag{7.22}$$

respectively.

Proof The first-order optimality condition is satisfied if $\partial\lambda(\bar{\mathbf{w}})/\partial\bar{\mathbf{w}}^H = 0$. Setting $\partial\lambda(\bar{\mathbf{w}})/\partial\bar{\mathbf{w}}^H = 0$ and simplifying it, we may obtain (7.19). □

We can treat (7.19) as a generalized eigenvalue problem regarding matrices $\mathbf{A}(\bar{\mathbf{w}})$ and $\mathbf{B}(\bar{\mathbf{w}})$, i.e., $\mathbf{B}^{-1}(\bar{\mathbf{w}})\mathbf{A}(\bar{\mathbf{w}})\bar{\mathbf{w}} = \lambda(\bar{\mathbf{w}})\bar{\mathbf{w}}$, where $\lambda(\bar{\mathbf{w}})$ is an eigenvalue of $\mathbf{B}^{-1}(\bar{\mathbf{w}})\mathbf{A}(\bar{\mathbf{w}})$ and $\bar{\mathbf{w}}$ is the corresponding eigenvector. Thus, we need to find the principal eigenvector so that (7.19) is satisfied and $\lambda(\bar{\mathbf{w}})$ becomes the maximum eigenvalue, which means the objective function reaches its maximum. The main idea is to apply the GPI to seek the principal eigenvector of $\mathbf{B}^{-1}(\bar{\mathbf{w}})\mathbf{A}(\bar{\mathbf{w}})$ [16]. The detailed steps are described in Algorithm 1.

Algorithm 1 GPI-based algorithm

1. **Initialization**: $\bar{\mathbf{w}}^{(0)}$, ϵ and $t = 0$.
2. **repeat**
3. Build matrix $\mathbf{A}(\bar{\mathbf{w}}^{(t)})$.
4. Build matrix $\mathbf{B}(\bar{\mathbf{w}}^{(t)})$.
5. Compute $\bar{\mathbf{w}}^{(t+1)} = \mathbf{B}^{-1}.(\bar{\mathbf{w}}^{(t)})\mathbf{A}(\bar{\mathbf{w}}^{(t)})\bar{\mathbf{w}}^{(t)}$.
6. Normalize $\bar{\mathbf{w}}^{(t+1)} = \bar{\mathbf{w}}^{(t+1)}/||\bar{\mathbf{w}}^{(t+1)}||$.
7. $t \leftarrow t + 1$.
8. **until** $||\bar{\mathbf{w}}^{(t+1)} - \bar{\mathbf{w}}^{(t)}|| \le \epsilon$

Then, we consider IRS phase shifts with fixed $\mathbf{w}_k$ and $\mathbf{z}$. Let us define $\boldsymbol{\phi}_{i,k} = \mathbf{H}_{ib,k}\mathbf{w}_i$, $\mu_{i,k} = \mathbf{h}_{ab,k}^H\mathbf{w}_i$, $\boldsymbol{\psi}_k = \mathbf{H}_{ib,k}\mathbf{z}$, $\kappa_k = \mathbf{h}_{ab,k}^H\mathbf{z}$, $\boldsymbol{\varphi}_{i,l} = \mathbf{H}_{ie,l}\mathbf{w}_i$, $\eta_{i,l} = \mathbf{h}_{ae,l}^H\mathbf{w}_i$, $\boldsymbol{\chi}_l = \mathbf{H}_{ie,l}\mathbf{z}$ and $\iota_l = \mathbf{h}_{ae,l}^H\mathbf{z}$. R_k and R_k^e can be respectively rewritten as $R_k = \log_2(1+\bar{\gamma}_k)$ and $R_k^e = \log_2(1+\sum_{l=1}^{L}\bar{\gamma}_{e,k})$, where

$$\bar{\gamma}_k = \frac{|\mathbf{v}^H\boldsymbol{\phi}_{k,k} + \mu_{k,k}|^2}{\sum_{i\neq k}^{K}|\mathbf{v}^H\boldsymbol{\phi}_{i,k} + \mu_{i,k}|^2 + |\mathbf{v}^H\boldsymbol{\psi}_k + \kappa_k|^2 + \sigma_b^2}, \tag{7.23}$$

$$\bar{\gamma}_{e,k} = \frac{|\mathbf{v}^H \boldsymbol{\varphi}_{k,l} + \eta_{k,l}|^2}{\sum_{i\neq k}^{K} |\mathbf{v}^H \boldsymbol{\varphi}_{i,l} + \eta_{i,l}|^2 + |\mathbf{v}^H \boldsymbol{\chi}_l + \iota_l|^2 + \sigma_e^2}. \tag{7.24}$$

The phase optimization subproblem is equivalent to

$$\text{(P4-1)}: \min_{\mathbf{v}} \quad f = -\sum_{k=1}^{K} (R_k - R_k^e) \tag{7.25a}$$

$$\text{s.t.} \quad |v_n| = 1, \quad \forall n = 1, \cdots N. \tag{7.25b}$$

The constraint of $\mathbf{v}$ in (7.25b) can be regarded as a complex circle manifold. Thus, we can efficiently solve the problem P(4-1) via the RMCG optimization [17], [18]. The RMCG algorithm includes the following main steps in each iteration.

Firstly, we need to find the Riemannian gradient of function f at point $\mathbf{v}_j$, which is calculated by protecting the Euclidean gradient onto the tangent space, i.e.,

$$\text{grad}_{\mathbf{v}_j} f = \nabla_{\mathbf{v}_j} f - \text{Re}\{\nabla_{\mathbf{v}_j} f \circ \mathbf{v}_j^*\} \circ \mathbf{v}_j, \tag{7.26}$$

where $\nabla_{\mathbf{v}_j} f$ is given by

$$\begin{aligned}
\nabla_{\mathbf{v}_j} f = \sum_{k=1}^{K} \frac{2}{\ln 2} \Bigg(& -\frac{\sum_{i=1}^{K} (\boldsymbol{\phi}_{i,k} \boldsymbol{\phi}_{i,k}^H \mathbf{v}_j + \boldsymbol{\phi}_{i,k} \mu_{i,k}^*) + \boldsymbol{\psi}_k \boldsymbol{\psi}_k^H \mathbf{v}_j + \boldsymbol{\psi}_k \kappa_k^*}{\sum_{i=1}^{K} |\mathbf{v}_j^H \boldsymbol{\phi}_{i,k} + \mu_{i,k}|^2 + |\mathbf{v}_j^H \boldsymbol{\psi}_k + \kappa_k|^2 + \sigma_b^2} \\
& + \frac{\sum_{i\neq k}^{K} (\boldsymbol{\phi}_{i,k} \boldsymbol{\phi}_{i,k}^H \mathbf{v}_j + \boldsymbol{\phi}_{i,k} \mu_{i,k}^*) + \boldsymbol{\psi}_k \boldsymbol{\psi}_k^H \mathbf{v}_j + \boldsymbol{\psi}_k \kappa_k^*}{\sum_{i\neq k}^{K} |\mathbf{v}_j^H \boldsymbol{\phi}_{i,k} + \mu_{i,k}|^2 + |\mathbf{v}_j^H \boldsymbol{\psi}_k + \kappa_k|^2 + \sigma_b^2} \\
& + \sum_{l=1}^{L} \frac{\boldsymbol{\varphi}_{k,l} \boldsymbol{\varphi}_{k,l}^H \mathbf{v}_j + \boldsymbol{\varphi}_{k,l} \eta_{k,l}^*}{\mathbf{J}_k} \\
& - \sum_{l=1}^{L} \frac{|\mathbf{v}_j^H \boldsymbol{\varphi}_{k,l} + \eta_{k,l}|^2 (\sum_{i\neq k}^{K} (\boldsymbol{\varphi}_{k,l} \boldsymbol{\varphi}_{i,l}^H \mathbf{v}_j + \boldsymbol{\varphi}_{i,l} \eta_{i,l}^*) + \boldsymbol{\chi}_l \boldsymbol{\chi}_l^H \mathbf{v}_j + \boldsymbol{\chi}_l \iota_l^*)}{(\sum_{i\neq k}^{K} |\mathbf{v}_j^H \boldsymbol{\varphi}_{i,l} + \eta_{i,l}|^2 + |\mathbf{v}_j^H \boldsymbol{\chi}_l + \iota_l|^2 + \sigma_e^2) \mathbf{J}_k} \Bigg)
\end{aligned} \tag{7.27}$$

with parameters $\mathbf{J}_k = (\sum_{i\neq k}^{K} |\mathbf{v}_j^H \boldsymbol{\varphi}_{i,l} + \eta_{i,l}|^2 + |\mathbf{v}_j^H \boldsymbol{\chi}_l + \iota_l|^2 + \sigma_e^2)(1 + \sum_{l=1}^{L} \bar{\gamma}_{e,k})$. Then, we update the search direction of the Riemannian gradient as

$$\boldsymbol{\xi}_{j+1} = -\text{grad}_{\mathbf{v}_{j+1}} f + \alpha_j \mathcal{T}(\boldsymbol{\xi}_j), \tag{7.28}$$

where α_j denotes Polak-Ribiere parameter, $\boldsymbol{\xi}_j$ is the search direction at the previous iteration, and $\mathcal{T}(\boldsymbol{\xi}_j) = \boldsymbol{\xi}_j - \text{Re}\{\boldsymbol{\xi}_j \circ \mathbf{v}_j^*\} \circ \mathbf{v}_j$ is the vector transport that maps a tangent vector from one tangent space to another tangent space. The next point can be updated as $\bar{\mathbf{v}}_{j+1} = \mathbf{v}_j + \beta_j \boldsymbol{\xi}_j$, where β_j is the Armijo step size. Finally, we have

to adopt retraction to map $\bar{\mathbf{v}}_{j+1}$ back to the manifold as follows $\mathbf{v}_{j+1} = \text{unt}(\bar{\mathbf{v}}_{j+1})$. The entire procedure of RMCG algorithm is summarized in Algorithm 2.

Algorithm 2 RMCG algorithm

1. **Initialization**: $\mathbf{v}_0$, ε and $j = 0$.
2. Calculate $\boldsymbol{\xi}_0 = -\text{grad}_{\mathbf{v}_0} f$ according to (7.26).
3. **repeat**
4. Choose the Armijo step size β_j based on [17].
5. Find $\mathbf{v}_{j+1}$ via retraction.
6. Update Riemannian gradient $\text{grad}_{\mathbf{v}_{j+1}} f$ based on (7.26).
7. Calculate the vector transport $\mathcal{T}(\boldsymbol{\xi}_j)$.
8. Choose Polak-Ribiere parameter α_j based on [17] and compute search direction $\boldsymbol{\xi}_{j+1}$ by using (7.28).
9. $j \leftarrow j + 1$.
10. **until** $|f(\mathbf{v}_{j+1}) - f(\mathbf{v}_j)| \leq \varepsilon$

The overall algorithm in this subsection is an iterative optimization algorithm, where the variables are alternatively optimized by using iterative updating methods in every outer-loop iteration. Specifically, for the GPI-based algorithm, the main complexity lies in the matrix inverse operations of $\mathbf{B}(\bar{\mathbf{w}})$, the complexity order of which is $O(\frac{1}{3}KM^3)$ [16]. For the RMCG algorithm, the complexity is dominated by calculating the Euclidean gradient, which is $O(K^2N^2)$. Therefore, the total complexity of the proposed LC-AO algorithm is given by $O(I_O(\frac{1}{3}I_G KM^3 + I_R K^2 N^2))$, where I_O,I_G and I_R represent the iteration times required by the overall algorithm, GPI-based algorithm and RMCG algorithm, respectively. It can be observed that the complexity of the proposed LC-AO algorithm is lower than that of the SDR method in the previous subsection (i.e., $O(M^{6.5} + N^{6.5})$).

7.4 Simulation Results

In this section, we provide simulation results to assess the effectiveness of the proposed algorithms. The BS and the IRS are located at (0 m, 5 m) and (70 m, 5 m), respectively. All users and Eves are randomly distributed in a circle centered at (70 m, 0 m) and (50 m, 0 m) with radius 5 m, respectively. We assume the direct link channels follow Rayleigh fading, while the IRS-related channels follow Rician fading with Rician factor $\rho = 3$, and the path loss is given by $PL = PL_0 - 10\alpha \log_{10}(\frac{d}{d_0})$, where $PL_0 = -30$ dB is the path loss at the reference distance $d_0 = 1$ m, α is the path loss exponent. In particular, the path loss exponent for the BS-IRS link, the BS-user/Eve link and the IRS-user/Eve link are set as 2.2, 2.5 and 3.5, respectively. The other simulation parameters are set as $M = 8$, $K = 3$, $\sigma_b^2 = \sigma_e^2 = -90$ dBm. For comparison, we provide the following four benchmark schemes: (1) No-IRS: IRS is not employed in the system, only the beamforming vectors and AN are designed. (2) Random phase shifts: The phase shifts of IRS are

generated randomly from $[0, 2\pi]$. (3) Successive convex approximation method in [19]. (4) No-AN: There is no use of AN, the beamforming vectors and phase shifts are optimized.

Figure 7.2 shows the convergence behaviours of the proposed algorithms for $N = 30$ and 50. It can be seen that both the proposed algorithms converge within limited iterations. The performance of the SDR-based method is slightly better than that of the LC-AO, but LC-AO converges faster because it has lower computational complexity than the SDR-based method. In addition, for the case with more phase shifts, i.e., $N = 50$, the convergence speed of both algorithms becomes lower since the number of variables and constraints increase.

Figure 7.3 illustrates the SSR versus maximum transmit power at the BS when $N = 50$ and $L = 2$. We notice that the SSR for all the schemes monotonically increase with the maximum transmit power. Besides, we can see that the proposed two algorithms achieve similar performance since both of them lead to locally opti-

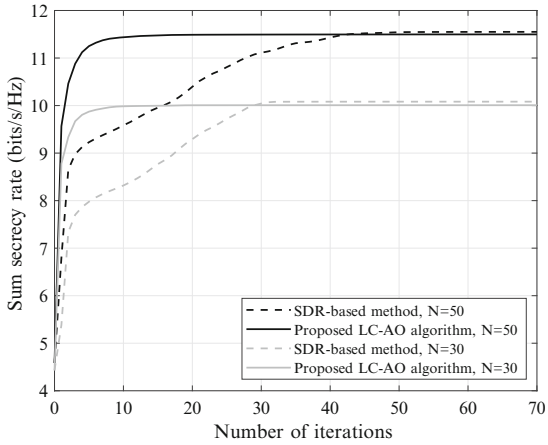


Fig. 7.2 Convergence behaviour of the proposed algorithms

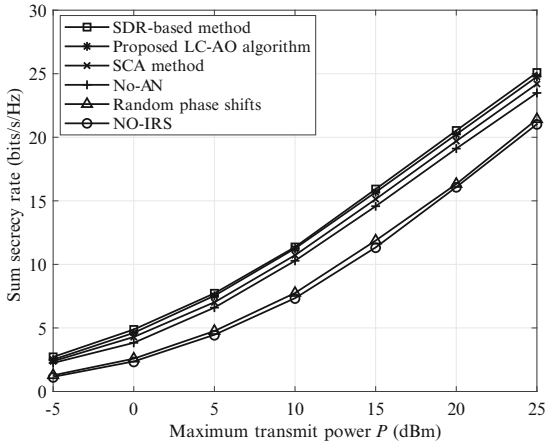


Fig. 7.3 SSR versus maximum transmit power P

mal solutions. The two proposed algorithms outperform the benchmark schemes, especially when transmit power at the BS becomes larger. AN can also improve the security, but it is less evidently than using IRS. This reveals the benefit of deploying an IRS and the effectiveness of optimizing the phase shifts.

Figures 7.4 and 7.5 depict the SSR versus the number of IRS reflecting elements and the number of Eves when $P = 10$ dBm, respectively, while $L = 2$ in Fig. 7.4 and $N = 50$ in Fig. 7.5. From Fig. 7.4, it is observed that the SSR of all the IRS-aided schemes increase as N increases. From Fig. 7.5, it is seen that the SSR of all the schemes monotonically decrease with the number of Eves L. This is because more colluding Eves combine their observations to decode confidential information, which causes a dramatic performance degradation. From both figures, we can see that the both proposed algorithms still obviously outperform the benchmark schemes due to the performance gain attained by deploying an IRS.

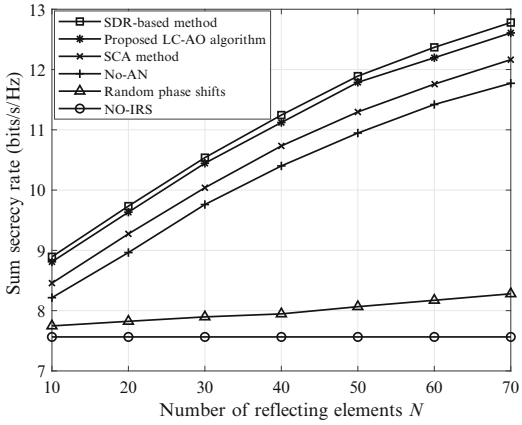


Fig. 7.4 SSR versus the number of reflecting elements N

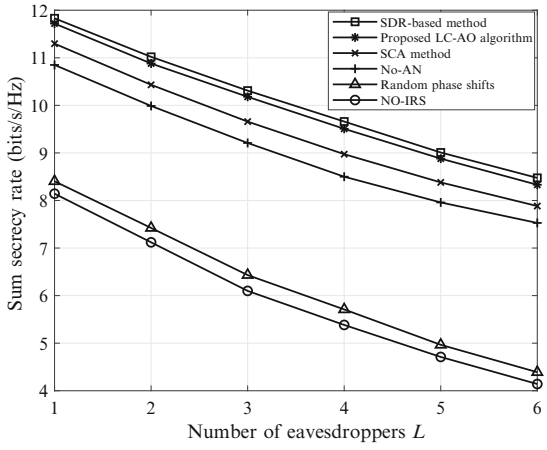


Fig. 7.5 SSR versus the number of Eves L

7.5 Conclusion

In this chapter, we studied an IRS-aided multiuser MISO secure communication system with mutiple colluding Eves. To maximize system SSR, we investigated the joint design of the beamforming vectors, AN and IRS phase shifts. For the formulated non-convex problem, we first proposed an SDR-based algorithm to solve it in an alternating manner. Then, a novel LC-AO algorithm was provided, in which the GPI-based algorithm and the RMCG algorithm were applied to optimize the beamforming vectors, AN and the phase shifts at the IRS, respectively. Simulation results demonstrated that the proposed algorithms can achieve similar performance. Furthermore, with the assistant of IRS, the SSR of the proposed algorithms is significantly improved compared to that of the benchmark schemes.

References

1. Andrews, J.G., Buzzi, S., Choi, W., Hanly, S.V., Lozano, A., Soong, A.C.K., Zhang, J.C.: What will 5G be? IEEE J. Sel. Areas Commun. **32**(6), 1065–1082 (2014)
2. Pan, C., Elkashlan, M., Wang, J., Yuan, J., Hanzo, L.: User-centric C-RAN architecture for ultra-dense 5G networks: challenges and methodologies. IEEE Commun. Mag. **56**(6), 14–20 (2018)
3. Wu, Q., Zhang, R.: Towards smart and reconfigurable environment: intelligent reflecting surface aided wireless network. IEEE Commun. Mag. **58**(1), 106–112 (2020)
4. Wu, Q., Zhang, R.: Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming. IEEE Trans. Wirel. Commun. **18**(11), 5394–5409 (2019)
5. Pan, C., Ren, H., Wang, K., Elkashlan, M., Nallanathan, A., Wang, J., Hanzo, L.: Intelligent reflecting surface aided MIMO broadcasting for simultaneous wireless information and power transfer. IEEE J. Sel. Areas Commun. **38**(8), 1719–1734 (2020)
6. Zhou, G., Pan, C., Ren, H., Wang, K., Nallanathan, A.: Intelligent reflecting surface aided multigroup multicast MISO communication systems. IEEE Trans. Signal Process. **68**, 3236–3251 (2020)
7. Shu, F., Teng, Y., Li, J., Huang, M., Shi, W., Li, J., Wu, Y., Wang, J.: Enhanced secrecy rate maximization for directional modulation networks via IRS. IEEE Trans. Commun. **69**(12), 8388–8401 (2021)
8. Cui, M., Zhang, G., Zhang, R.: Secure wireless communication via intelligent reflecting surface. IEEE Wirel. Commun. Lett. **8**(5), 1410–1414 (2019)
9. Shi, W., Zhou, X., Jia, L., Wu, Y., Shu, F., Wang, J.: Enhanced secure wireless information and power transfer via intelligent reflecting surface. IEEE Commun. Lett. **25**(4), 1084–1088 (2021)
10. Hong, S., Pan, C., Ren, H., Wang, K., Nallanathan, A.: Artificial-noise-aided secure MIMO wireless communications via intelligent reflecting surface. IEEE Trans. Commun. **68**(12), 7851–7866 (2020)
11. Zhang, Y., Shen, Y., Wang, H., Yong, J., Jiang, X.: On secure wireless communications for IoT under eavesdropper collusion. IEEE Trans. Autom. Sci. Eng. **13**(3), 1281–1293 (2016)
12. Choi, J., Park, J.: Sum secrecy spectral efficiency maximization in downlink MU-MIMO: colluding eavesdroppers. IEEE Trans. Veh. Technol. **70**(1), 1051–1056 (2021)
13. Geraci, G., Singh, S., Andrews, J.G., Yuan, J., Collings, I.B., Huang, M., Wu, Y., Wang, J., You, X.: Secrecy rates in broadcast channels with confidential messages and external eavesdroppers. IEEE Trans. Wirel. Commun. **13**(5), 2931–2943 (2014)

14. Grant, M., Boyd, S.: CVX: Matlab software for disciplined convex programming (2020). Available. http://cvxr.com/cvx
15. Wang, K.-Y., So, A.M.-C., Chang, T.-H., Ma, Chi, C.-Y.: Outage constrained robust transmit optimization for multiuser MISO downlinks: tractable approximations by conic optimization. IEEE Trans. Signal Process. **62**(21), 5690–5705 (2014)
16. Choi, J., Lee, N., Hong, S.-N., Caire, G.: Joint user selection, power allocation, and precoding design with imperfect CSIT for multi-cell MU-MIMO downlink systems. IEEE Trans. Wirel. Commun. **19**(1), 162–176 (2020)
17. Absil, P.-A., Mahony, R., Sepulchre, R.: Optimization Algorithms on Matrix Manifolds. Princeton University Press, Princeton (2009)
18. Zargari, S., Khalili, A., Zhang, R.: Energy efficiency maximization via joint active and passive beamforming design for multiuser MISO IRS-aided SWIPT. IEEE Wirel. Commun. Lett. **10**(3), 557–561 (2021)
19. Guan, X., Wu, Q., Zhang, R.: Joint power control and passive beamforming in IRS-assisted spectrum sharing. IEEE Commun. Lett. **24**(7), 1553–1557 (2020)

Chapter 8
Secure Multigroup Multicast Communication Systems via Intelligent Reflecting Surface

This chapter considers a secure multigroup multicast MISO communication system aided by an IRS. Specifically, we aim to minimize the transmit power at Alice via jointly optimizing the transmit beamformer, AN vector and phase shifts at the IRS subject to the secrecy rate constraints as well as the unit modulus constraints of IRS phase shifts. To tackle the optimization problem, we first transform it into a SDR problem, and then alternately update the transmit beamformer and AN matrix as well as the phase shifts at the IRS. In order to reduce the high computational complexity, we further propose a low-complexity algorithm based on SOCP. We decouple the optimization problem into two sub-problems and optimize the transmit beamformer, AN vector and the phase shifts alternately by solving two corresponding SOCP sub-problem. Simulation results show that the proposed SDR and SOCP schemes require half or less transmit power than the scheme without IRS, which demonstrates the advantages of introducing IRS and the effectiveness of the proposed methods.

8.1 Introduction

For beyond 5G and 6G communication systems, due to the fact that a massive number of mobile users are required to be supported, various techniques were proposed to improve the spectrum efficiency and energy efficiency, such as massive MIMO, mmWave communication and so on [1–3]. However, the hardware cost and energy consumption of these technologies increase as the number of deployed base stations (BSs) increase. Moreover, excessive number of active components can also lead to serious interference issue in wireless networks. A new and revolutionary technology, IRS achieves high spectrum efficiency and energy efficiency with low hardware cost [4–6]. Specifically, an IRS consists of a large number of low-cost, passive and reflecting units, which reflect the signal by dynamically adjusting the

F. Shu, J. Wang, *Intelligent Reflecting Surface-Aided Physical-Layer Security*,
Wireless Networks, https://doi.org/10.1007/978-3-031-41812-9_8

phase shifts of the elements. The reflected signals gather at the desired receiver to improve the received signal strength, while destructively at the non-intended receiver for reducing the interference [7, 8].

Due to those above-mentioned benefits, several IRS-aided wireless communication systems were investigated to enhance the communication performance, such as the received SNR, energy efficiency and SR. Explicity, the authors in [9] proposed a joint active and passive beamforming design for an IRS-assisted single-user and multiple-user MISO communication system, where SDR and alternating optimization algorithm are performed to optimize the transmit beamformer and the phase shifts at the IRS for minimizing the total transmit power. In order to reduce the computational complexity incurred by SDR technique, Yu et al. proposed a pair of efficient algorithms (i.e., fixed point iteration and manifold techniques) to optimize the phase shifts at the IRS. It is worth mentioning that the two proposed methods are capable of obtaining locally optimal solutions [10]. To maximize the energy efficiency in MISO systems, the authors of [11] performed gradient descent/sequential fractional programming method to optimize the phase shifts at the IRS, and using Dinkelbach method for optimizing the power allocation factor.

On the other hand, the broadcast nature of wireless channels leads to that the information sent to a legitimate receiver can be also gathered by the unintended receivers (eavesdroppers) [12–15]. Traditionally, the security problem was ensured by the encryption technique, which requires complex key management. By contrast, physical layer security provides a new approach by fully exploring the random nature of communication channels to arrive a secure transmission [16–18]. As such, the complex key management is circumvented. It is known that the IRS could enhance the received signal power to the legitimate receiver, while the power received at Eves will be also enhanced. Therefore, how to improve the secrecy performance for the IRS-aided communication systems becomes a non-trivial problem [19–21]. Shen et al. considered the SR maximization problem in a secure single-user MISO communication with an IRS, in which MM algorithm was applied and a closed-form solution was obtained [19]. Resource allocation problem for secure IRS-aided multiuser MISO system and SR maximization problem for secure MIMO system were investigated by jointly optimizing the transmit beamformer, AN covariance matrix and the phase shifts at the IRS, respectively [20, 21]. However, the authors in [20] did not consider the links between BS and users. In addition, secure SWIPT system assisted by the IRS was optimized to maximize the harvested power in [22]. All the mentioned systems are demonstrated that the significant performance gains (e.g., security or the received signal power) of the communication system can be achieved by introducing an IRS. In practical communications, obtaining an accurate CSI of communication nodes is challenging, especially for the case that an IRS is further considered in the communication system. To solve this issue, several channel estimation methods and robust transmission designs were proposed [23–25]. The authors designed the transmission protocol and verified the efficiency of the channel estimation based on the ON/OFF model [23, 24]. In Addition, Huang et al. proposed a deep learning method to promptly optimize the transmit beamformer and the phase shifts at the IRS [25].

Clearly, the above-mentioned contributions focus on exploiting IRS for enhancing the performance profits in unicast or broadcast transmissions. For broadcast transmissions, BS sends the same stream to all sheathed users, which can not provide personalized service timely according to the requirement of each customer. For unicast transmissions, BS sends an independent data stream to each user, which causes severe interference and high system complexity in the fact of a large number of users. To address these issues, the multicast transmission has attracted widely attention and it has great potential in many applications such as popular TV programme and live video streaming [26]. In addition, the data rate of each group is limited by the user with the worse-channel gains in multicast system. Physical layer multicasting via beamforming is shown to be useful for alleviating the pressure of huge wireless data traffic and for boosting the spectrum and energy efficiency [27–29]. An IRS-assisted multigroup multicast MISO communication system is studied to maximize the sum rate of all the multicasting groups by the joint optimization of the precoding matrix at the BS and the reflection coefficients at the IRS [30]. Since the transmitter serves multiple legitimate users by using a single beamforming vector, the multicast system becomes more vulnerable to eavesdropping from the perspective of security. Therefore, it is necessary to investigate the performance advantages when an IRS is considered in secure multigroup multicast systems.

Motivated by the above discussions, we investigate the physical layer security for an IRS-aided multigroup multicast system. To elaborate, the multiple-antenna Alice transmits independently confidential information data stream to each legitimate multiple group in the presence of Eves. To improve the security of the system, Alice also transmits AN to disturb Eves' decoding. All the legitimate receivers and Eves are assumed to be equipped with a single antenna. The legitimate users in the same group receive the same information, but they are interfered by the signals sent to other groups. The main contributions of this chapter are summarized as follows:

1. For the first time we formulate a transmit power minimization problem by jointly optimizing the transmit beamforming vector and the AN vector of Alice as well as the phase shifts at the IRS for the IRS-aided multigroup multicast system in the presence of Eves subject to a non-convex uni-modular constraint and the SR constraint.
2. To solve the problem, an iterative and alternating optimization algorithm based on SDR technique is proposed. Specifically, we first transform the optimization problem into an SDR problem by dropping the rank-one constraints. Then the alternating optimization method is applied to separately optimize the transmit beamforming matrix and the AN matrix as well as the phase shifts at the IRS. In each subproblem, MM algorithm is used to obtain the upper bound of the concave logarithm function. Thus each subproblem can be transformed into a convex problem and then be solved directly. Furthermore, the Gaussian randomization method is adopted to obtain a high quality sub-optimal solution.
3. To reduce the computational complexity of the SDR algorithm, we further propose an efficient algorithm in an iterative manner based on SOCP technique. Specifically, we decouple the problem into two subproblems for optimizing the

transmit beamforming vector, AN vector and the phase shift at the IRS, respectively. We handle the non-convex SR constraints by introducing the first-order Taylor expansion and then transform them into a SOCP for each subproblem, which is finally solved by SCA method. Simulation results demonstrate that our proposed two IRS-aided schemes are capable of saving transmit power significantly, when compared with no IRS-aided scheme.

This rest of this chapter is organized as follows. Section 8.2 describes an IRS-aided system model for a secure multigroup multicast MISO communication system. Then, an associated power minimization problem is formulated. The SDR-based method is developed to solve the non-convex optimization problem in Sect. 8.3. Section 8.4 provides an SOCP-based alternative method to reduce the computational complexity of the SDR approach. Section 8.5 shows our numerical simulation results to validate the performance improvement of the proposed algorithms. Finally, Sect. 8.6 draws our conclusions.

Notations Scalars are presented by lowercase letters. Vectors and matrices are denoted by boldface uppercase and lowercase letters, respectively. $|\cdot|$ denotes the modulus of a scalar and $\|\cdot\|$ denotes the Euclidean norm of a vector. $(\cdot)^H$, $\mathrm{Tr}(\cdot)$ and $\angle(\cdot)$ denote the conjugate transpose, the trace of a matrix and the angle of a complex number, respectively.

8.2 System Model

Figure 8.1 sketches an IRS-aided downlink multigroup multicast MISO system, where Alice is equipped with M transmit antennas serving multiple users (Bobs) in K multicast groups with assistance of an IRS in the presence of L Eves. All receivers are equipped with a single antenna while the IRS has N reflecting elements. Denoting $\mathcal{G}_k(\forall k \in \mathcal{K} = \{1, \ldots, K\})$ as the k-th group of the desired users, and the total number of user is denoted as $T = \sum_{k=1}^{K} |\mathcal{G}_k|$. Assume that each user belongs to one unique multicast group, i.e., $\mathcal{G}_i \bigcap \mathcal{G}_j = \emptyset, i \neq j, \forall i, j \in \mathcal{K}$. Moreover, the set of Eves is denoted as $\mathcal{L} = \{1, \ldots, L\}$. The transmitted signal at Alice can be expressed as

$$\mathbf{x} = \sum_{k=1}^{K} \mathbf{w}_k s_k + \mathbf{q}_{AN}, \tag{8.1}$$

where $\mathbf{w}_k \in \mathbb{C}^{M\times 1}$ is the beamforming vector forcing the CM to the desired k-th Bob group, and $\mathbf{q}_{AN} \in \mathbb{C}^{M\times 1}$ is the generalized AN vector assumed to obey a circularly symmet- ric complex Gaussian (CSCG) distribution $\mathcal{CN}(0, \mathbf{Q})$, where $\mathbf{Q}$ is a covariance matrix of the AN. In addition, s_k denotes the CM for Bobs in the k-th group. Without loss of generality, we assume s_k is i.i.d. CSCG random variable with

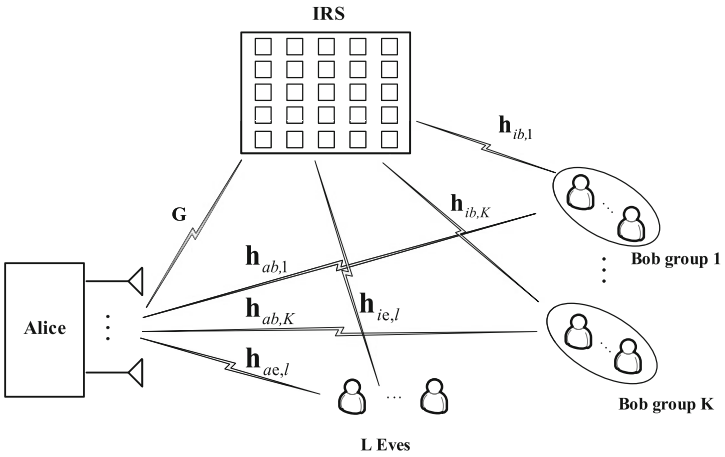


Fig. 8.1 An IRS-aided secure multigroup multicast communication system

zero mean and unit variance, i.e., $s_k \sim \mathcal{CN}(0, 1)$. Thus, the total transmit power at Alice is $\mathbb{E}\left\{\mathbf{x}^H\mathbf{x}\right\} = \sum_{i=k}^{K} \|\mathbf{w}_k\|^2 + \|\mathbf{q}_{AN}\|^2$.

In this chapter, a quasi-static fading environment is assumed. The baseband equivalent channel responses from Alice to the IRS, from Alice to the j-th user in the k-th Bob group, from Alice to the l-th Eve, from the IRS to the j-th user in the k-th Bob group and from the IRS to the l-th Eve are denoted by $\mathbf{G} \in \mathbb{C}^{N\times M}$, $\mathbf{h}_{ab,kj}^H \in \mathbb{C}^{1\times M}$, $\mathbf{h}_{ae,l}^H \in \mathbb{C}^{1\times M}$, $\mathbf{h}_{ib,kj}^H \in \mathbb{C}^{1\times N}$ and $\mathbf{h}_{ie,l}^H \in \mathbb{C}^{1\times N}$, respectively. The reflecting coefficient channel of the IRS is denoted as $\mathbf{\Theta} = \text{diag}(\boldsymbol{\beta}\mathbf{e}^{j\boldsymbol{\theta}_1}, \cdots, \boldsymbol{\beta}\mathbf{e}^{j\boldsymbol{\theta}_N})$, where $\beta \in [0, 1]$ denotes the amplitude reflection coefficient and $\boldsymbol{\theta} = [\theta_1, \cdots, \theta_N]$ is the phase shift vector at the IRS where $\theta_n \in (0, 2\pi]$, $1 \le n \le N$, respectively [31]. In practice, each element of the IRS is favorable to be designed to maximize the signal reflection due to the fact that it is expensive and complex to implement independent control of the reflection amplitude and phase shift [9]. Hence, we assume that $\boldsymbol{\beta} = 1$ for simplicity. As such, the received signal at the j-th user in the k-th Bob group can be written as

$$y_{b,kj} = (\mathbf{h}_{ib,kj}^H \mathbf{\Theta}\mathbf{G} + \mathbf{h}_{ab,kj}^H)\mathbf{x} + n_{bk}, \tag{8.2}$$

where $n_{bk} \sim \mathcal{CN}(0, \sigma_b^2)$ is the complex AWGN. Similarly, the received signal at the l-th Eve is

$$y_{e,l} = (\mathbf{h}_{ie,l}^H \mathbf{\Theta}\mathbf{G} + \mathbf{h}_{ae,l}^H)\mathbf{x} + n_{el}, \tag{8.3}$$

where n_{el} is the complex AWGN variable following the distribution $n_{el} \sim \mathcal{CN}(0, \sigma_e^2)$.

By applying the channel estimation methods discussed in [23–25], we assume that the CSIs of all channels are perfectly available at Alice, and Alice is responsible

for optimizing the optimal phase shifts and sending them back to the IRS controller. In addition, when Eves are active users in this system but are untrusted by Bobs, its CSI can be estimated at Eves and sent back to Alice [32, 33]. It is worth noting that the assumption of having perfect CSI knowledge at Alice is idealistic and the acquisition of CSI for IRS-links/Eves is quite challenging. Hence, the results in this chapter can be considered as an upper bound of theoretical performance for the considered system. In the future work, we will focus on the robust transmit design in the considered systems and provide more detailed results for it. Moreover, we assume that $\sigma_b^2 = \sigma_e^2 = \sigma^2$. Let us define $\mathbf{v} = [e^{j\theta_1}, \cdots, e^{j\theta_N}]^H \in \mathbb{C}^{N\times 1}$, $\mathbf{u} = [\mathbf{v}; 1]$, $\mathbf{H}_{b,kj} = \text{diag}\{\mathbf{h}_{ib,kj}^H\}\mathbf{G} \in \mathbb{C}^{N\times M}$, $\mathbf{H}_{e,l} = \text{diag}\{\mathbf{h}_{ie,l}^H\}\mathbf{G} \in \mathbb{C}^{N\times M}$, $\mathbf{H}_{kj} = [\mathbf{H}_{b,kj}; \mathbf{h}_{ab,kj}^H]$ and $\mathbf{H}_l = [\mathbf{H}_{e,l}; \mathbf{h}_{ae,l}^H]$. According to (8.2) and (8.3), the achievable transmission rate at the j-th user in the k-th Bob group and the l-th Eve intending to wiretap the j-th legitimate user in the k-th Bob group can be expressed as [28]

$$R_{b,kj} = \log_2(1 + \text{SINR}_{b(k,j)}), \quad \forall k, j, \tag{8.4}$$

and

$$R_{e,l} = \log_2(1 + \text{SINR}_{e(k,l)}), \quad \forall k, l, \tag{8.5}$$

respectively, where

$$\text{SINR}_{b(k,j)} = \frac{|\mathbf{u}^H\mathbf{H}_{kj}\mathbf{w}_k|^2}{\sum_{g\neq k}^K |\mathbf{u}^H\mathbf{H}_{kj}\mathbf{w}_g|^2 + |\mathbf{u}^H\mathbf{H}_{kj}\mathbf{q}_{AN}|^2 + \sigma^2}, \tag{8.6}$$

$$\text{SINR}_{e(k,l)} = \frac{|\mathbf{u}^H\mathbf{H}_l\mathbf{w}_k|^2}{\sum_{g\neq k}^K |\mathbf{u}^H\mathbf{H}_l\mathbf{w}_g|^2 + |\mathbf{u}^H\mathbf{H}_l\mathbf{q}_{AN}|^2 + \sigma^2}. \tag{8.7}$$

The corresponding achievable SR of user j, $j \in \mathcal{G}_k$ in Bob group k, $k \in \mathcal{K}$ is defined by

$$R_{s,kj} = \left[0, \min_{j\in\mathcal{G}_k} R_{b,kj} - \max_{\forall l} R_{e,l}\right]^+. \tag{8.8}$$

In this chapter, we aim to minimize the total transmit power required at Alice subject to the minimum SR constraints at Bobs and phase shift constraints at the IRS by jointly optimizing the transmit beamformings, AN at Alice and the reflect phase shifts at the IRS. Thus, the resultant optimization problem can be mathematically formulated as

$$\text{(P1)}: \min_{\{\mathbf{w}_k\},\mathbf{q}_{AN},\mathbf{u}} \quad \sum_{k=1}^K \|\mathbf{w}_k\|^2 + \|\mathbf{q}_{AN}\|^2 \tag{8.9a}$$

$$\text{s.t.} \quad R_{s,kj} \geq \gamma_s, \quad \forall k \in \mathcal{K}, l \in \mathcal{L}, j \in \mathcal{G}_k, \tag{8.9b}$$

$$|u_n|^2 = 1, \quad \forall n = 1 \cdots N, u_{N+1} = 1, \tag{8.9c}$$

where $\gamma_s \geq 0$ is the minimum target SR for Bobs. However, it is observed that problem (P1) is a non-convex optimization problem and thus difficult to solve optimally. This is due to the fact that constraints (8.9b) are non-convex with respect to $\{\mathbf{w}_k, \mathbf{q}_{AN}, \mathbf{v}\}$ and (8.9c) are non-linear equality constraints. In general, there is no standard method for solving such non-convex optimization problems optimally. Hence, we will propose two efficient algorithms to solve problem (P1) sub-optimally.

8.3 SDR-Based Alternating Optimization Method

In this section, we propose an SDR-based AO method to solve problem (P1). Moreover, this method could not only obtain a high-quality solution but also provide a good reference level. To facilitate processing, problem (P1) is first relaxed as an SDR problem and then the SDR problem is decoupled into two subproblems. When phase shift $\mathbf{v}$ is fixed, the subproblem can be solved by applying one-dimensional exhaustive search [34]. Considering the computational complexity of the algorithm and the sub-optimal result after AO, we apply MM algorithm to tackle the non-convexity of $R_{s,kj}$ for each subproblem. Specifically, we first define $\mathbf{W}_k = \mathbf{w}_k \mathbf{w}_k^H$, $\mathbf{Q} = \mathbf{q}_{AN} \mathbf{q}_{AN}^H$ and $\mathbf{U} = \mathbf{u}\mathbf{u}^H$, then SR constraints (8.9b) can be rewritten as

$$f_1(\mathbf{W}_k, \mathbf{Q}, \mathbf{U}) + f_2(\mathbf{W}_k, \mathbf{Q}, \mathbf{U}) - g_1(\mathbf{W}_k, \mathbf{Q}, \mathbf{U}) - g_2(\mathbf{W}_k, \mathbf{Q}, \mathbf{U}) \geq \gamma_s, \quad \forall k, j, l, \tag{8.10}$$

where

$$f_1(\mathbf{W}_k, \mathbf{Q}, \mathbf{U}) = \log(\mathrm{Tr}(\mathbf{H}_{kj}^H \mathbf{U} \mathbf{H}_{kj} (\sum_{k=1}^{K} \mathbf{W}_k + \mathbf{Q})) + \sigma^2), \tag{8.11}$$

$$f_2(\mathbf{W}_k, \mathbf{Q}, \mathbf{U}) = \log(\mathrm{Tr}(\mathbf{H}_l^H \mathbf{U} \mathbf{H}_l (\sum_{g \neq k}^{K} \mathbf{W}_g + \mathbf{Q})) + \sigma^2), \tag{8.12}$$

$$g_1(\mathbf{W}_k, \mathbf{Q}, \mathbf{U}) = \log(\mathrm{Tr}(\mathbf{H}_{kj}^H \mathbf{U} \mathbf{H}_{kj} (\sum_{g \neq k}^{K} \mathbf{W}_g + \mathbf{Q})) + \sigma^2), \tag{8.13}$$

$$g_2(\mathbf{W}_k, \mathbf{Q}, \mathbf{U}) = \log(\mathrm{Tr}(\mathbf{H}_l^H \mathbf{U} \mathbf{H}_l (\sum_{k=1}^{K} \mathbf{W}_k + \mathbf{Q})) + \sigma^2). \tag{8.14}$$

Afterwards, by replacing (8.9b) with (8.10) and dropping the rank-one constraints, the SDR of (P1) can be expressed as

$$\text{(P2)}: \min_{\{\mathbf{W}_k\},\mathbf{Q},\mathbf{U}} \quad \sum_{k=1}^{K} \text{Tr}(\mathbf{W}_k) + \text{Tr}(\mathbf{Q}) \tag{8.15a}$$

$$\text{s.t.} \quad f_1 + f_2 - g_1 - g_2 \geq \gamma_s, \quad \forall k, j, l, \tag{8.15b}$$

$$\mathbf{U}_{n,n} = 1, \quad \forall n = 1 \cdots N + 1, \tag{8.15c}$$

$$\mathbf{U} \succeq 0, \mathbf{W}_k \succeq 0, \mathbf{Q} \succeq 0. \tag{8.15d}$$

However, problem (P2) is still non-convex because constraints (8.15b) are non-convex as well as variables $\mathbf{W}_k$ and $\mathbf{Q}$ are coupled with $\mathbf{U}$. As a result, in the following, problem (P2) is first decomposed into two non-convex subproblems. Then both the non-convex subproblems are converted into convex ones by applying the MM algorithm.

8.3.1 Optimization with Respect to $\{\mathbf{W}_k, \mathbf{Q}\}$

By fixing the phase shift matrix $\mathbf{U}$ as $\mathbf{U}^t$, $g_i(\mathbf{W}_k, \mathbf{Q}, \mathbf{U}^t)$, $(i = 1, 2)$ are concave functions with respect to $\mathbf{W}_k$ and $\mathbf{Q}$. As a result, $g_i, (i = 1, 2)$ can be upper bounded as

$$\begin{aligned} g_i(\mathbf{W}_k, \mathbf{Q}, \mathbf{U}^t) \leq\ & g_i(\tilde{\mathbf{W}}_k, \tilde{\mathbf{Q}}, \mathbf{U}^t) + \text{Tr}(\nabla_{\mathbf{W}_k} g_i(\tilde{\mathbf{W}}_k, \tilde{\mathbf{Q}}, \mathbf{U}^t)^H (\mathbf{W}_k - \tilde{\mathbf{W}}_k)) \\ & + \text{Tr}(\nabla_{\mathbf{Q}} g_i(\tilde{\mathbf{W}}_k, \tilde{\mathbf{Q}}, \mathbf{U}^t)^H (\mathbf{Q} - \tilde{\mathbf{Q}})) \\ \triangleq\ & \tilde{g}_i(\mathbf{W}_k, \mathbf{Q}, \mathbf{U}^t). \end{aligned} \tag{8.16}$$

where $\nabla_{\mathbf{W}_k} g_i$ and $\nabla_{\mathbf{Q}} g_i$, $(i = 1, 2)$ are the gradients of the function $g_i(\mathbf{W}_k, \mathbf{Q}, \mathbf{U}^t)$ with respect to the optimization variable $\mathbf{W}_k$ and $\mathbf{Q}$, respectively.

Based on the above transformation, the transmit precoder matrices $\mathbf{W}_k$ and AN matrix $\mathbf{Q}$ can be optimized by solving the following problem (P2-1). It can be verified that problem (P2-1) is a convex problem and can be solved by the existing solvers such as CVX [35].

$$\text{(P2-1)}: \min_{\{\mathbf{W}_k\},\mathbf{Q}} \quad \sum_{k=1}^{K} \text{Tr}(\mathbf{W}_k) + \text{Tr}(\mathbf{Q}) \tag{8.17a}$$

$$\text{s.t.} \quad f_1 + f_2 - \tilde{g}_1 - \tilde{g}_2 \geq \gamma_s, \quad \forall k, j, l, \tag{8.17b}$$

$$\mathbf{W}_k \succeq 0, \mathbf{Q} \succeq 0. \tag{8.17c}$$

8.3.2 Optimization with Respect to $\mathbf{U}$

Similarly, by fixing $\{\mathbf{W}_k, \mathbf{Q}\}$ as $\{\mathbf{W}_k^t, \mathbf{Q}^t\}$, $g_i(\mathbf{W}_k^t, \mathbf{Q}_{AN}^t, \mathbf{U})$, $(i = 1, 2)$ are concave functions with respect to $\mathbf{U}$. Consequently, the upper-bounds of g_i, $(i = 1, 2)$ with respect to $\mathbf{U}$ can be respectively expressed as

$$\begin{aligned} g_i(\mathbf{W}_k^t, \mathbf{Q}^t, \mathbf{U}) &\leq g_i(\tilde{\mathbf{W}}_k^t, \tilde{\mathbf{Q}}^t, \tilde{\mathbf{U}}) + \mathrm{Tr}(\nabla_{\mathbf{U}} g_i(\mathbf{W}_k^t, \mathbf{Q}^t, \tilde{\mathbf{U}})^H (\mathbf{U} - \tilde{\mathbf{U}})) \\ &\triangleq \bar{g}_i(\mathbf{W}_k^t, \mathbf{Q}^t, \mathbf{U}), \end{aligned} \tag{8.18}$$

where $\nabla_{\mathbf{U}} g_i$, $(i = 1, 2)$ are the gradient of the function $g_i(\mathbf{W}_k^t, \mathbf{Q}^t, \mathbf{U})$ in terms of the optimization variable $\mathbf{U}$.

According to (8.18), the optimization problem of the phase shift matrix $\mathbf{U}$ is given by

$$\text{(P2-2):} \quad \text{find} \quad \mathbf{U} \tag{8.19a}$$

$$\text{s.t.} \quad f_1 + f_2 - \bar{g}_1 - \bar{g}_2 \geq \gamma_s, \quad \forall\, k, j, l, \tag{8.19b}$$

$$(8.15c), \ \mathbf{U} \succeq 0. \tag{8.19c}$$

Problem (P2-2) is a standard convex optimization problem, which can be optimally solved existing convex optimization solvers (e.g., CVX) [35].

8.3.3 Overall Algorithm and Complexity Analysis

By optimizing the problem (P2-1) and problem (P2-2) alternately, we obtain a sub-optimal solution to problem (P2). However, the solution obtained by solving problem (P2) can not be guaranteed to be a feasible solution of the original problem (P1) since the rank-one constraints are relaxed in problem (P2). To address this problem, the Gaussian randomization method is used to recover the rank-one solutions. Different from [9] that the Gaussian randomization method is used in each iteration, we apply the Gaussian randomization method only once when obtaining the final solution of problem (P2). This is due to the fact that using the Gaussian randomization method in each iteration may lead to non-convergence and high complexity.

Because the objective value of problem (P2) of the proposed SDR-based method decrease in each iteration. Besides, the optimal value of (P2) has a lower bound due to the SR constraints. Therefore, the convergence of the proposed SDR-based AO algorithm can be guaranteed.

In the following, we analyze the computational complexity of the SDR method. Observing that problem (P2-1) has TL LMI constraints of size 1, K LMI constraints of size M and 1 LMI constraints of size M. The number of decision variables n_1 is on the order of $(K + 1)M^2$. Problem (P2-2) has TL LMI constraints of size 1,

1 LMI constraints of size 1, 1 LMI constraints of size N. The number of decision variables n_2 is on the order of N^2 [36]. Hence, the overall complexity is

$$O\Big(n_1 D_1 \sqrt{TL + KM + M}\big((TL + KM^3 + M^3) + n_1(TL + KM^2 + M^2) + n_1^2\big) + n_2 D_2 \sqrt{TL + 1 + N}\big((TL + N^3 + 1) + n_2(TL + N^2 + 1) + n_2^2\big)\Big), \tag{8.20}$$

where D_1 and D_2 denote the numbers of iterations in problem (P2-1) and in problem (P2-2), respectively. It is observed that the computational complexity is on the order of $M^{6.5}$ or $N^{6.5}$, which is extremely high and unpractical. Considering the difficulty of the hardware implementation in practice, the computational complexity is an important indicator. Therefore, it is necessary to study a tradeoff between computational complexity and performance.

8.4 Low-Complexity SOCP-Based Algorithm

In this section, we aim to propose a low-complexity SOCP-based algorithm to solve problem (P1).

Define $\gamma_{b(k,j)}$ and $\gamma_{e(k,l)}$ as the minimum signal to interference plus noise ratio (SINR) at the j-th user in the k-th Bob group and the maximum SINR at the l-th Eve, respectively. Then, the optimization problem (P1) can be mathematically recast as

$$\text{(P3):} \quad \min_{\{\mathbf{w}_k\},\mathbf{q}_{AN},\mathbf{v},\boldsymbol{\gamma}_b,\boldsymbol{\gamma}_e} \quad \sum_{k=1}^{K} \|\mathbf{w}_k\|^2 + \|\mathbf{q}_{AN}\|^2 \tag{8.21a}$$

$$\text{s.t.} \quad \text{SINR}_{b(k,j)} \geq \gamma_{b(k,j)}, \quad \forall k, j, \tag{8.21b}$$

$$\text{SINR}_{e(k,l)} \leq \gamma_{e(k,l)}, \quad \forall k, l, \tag{8.21c}$$

$$1 + \gamma_{b(k,j)} \geq 2^{\gamma_s}(1 + \gamma_{e(k,l)}) \quad \forall k, j, l, \tag{8.21d}$$

$$|v_n|^2 = 1, \quad \forall n = 1 \cdots N. \tag{8.21e}$$

Note that the optimization variables $\{\mathbf{w}_k, \mathbf{q}_{AN}\}$ and $\mathbf{v}$ are mutually coupled in constraints (8.21b)) and (8.21c). Moreover, the constraints (8.21e) are uni-modular. Hence, it is non-trivial to solve this problem. In the following, we optimize problem (P3) by applying alterative manner.

8.4.1 Optimization with Respect to Beamforming Vector and AN

For given phase shifts at the IRS, the problem (P3) is reduced to

$$\text{(P3-1)}: \min_{\{\mathbf{w}_k\},\mathbf{q}_{AN},\boldsymbol{\gamma}_b,\boldsymbol{\gamma}_e} \quad \sum_{k=1}^{K}\|\mathbf{w}_k\|^2+\|\mathbf{q}_{AN}\|^2 \tag{8.22a}$$

$$\text{s.t.} \quad \text{SINR}_{b(k,j)}(\mathbf{w}_k,\mathbf{q}_{AN}) \geq \gamma_{b(k,j)}, \quad \forall k,j, \tag{8.22b}$$

$$\text{SINR}_{e(k,l)}(\mathbf{w}_k,\mathbf{q}_{AN}) \leq \gamma_{e(k,l)}, \quad \forall k,l, \tag{8.22c}$$

$$(8.21\text{d}). \tag{8.22d}$$

Problem (P3-1) is non-convex due to the non-convex constraints (8.22b) and (8.22c). To address them, we focus on converting them into convex ones.

Note that (8.22b) and (8.22c) can be respectively rearranged as

$$\sum_{g\neq k}^{K}|\mathbf{u}^H\mathbf{H}_{kj}\mathbf{w}_g|^2+|\mathbf{u}^H\mathbf{H}_{kj}\mathbf{q}_{AN}|^2+\sigma^2 \leq \frac{|\mathbf{u}^H\mathbf{H}_{kj}\mathbf{w}_k|^2}{\gamma_{b(k,j)}}, \quad \forall k,j, \tag{8.23}$$

$$\frac{|\mathbf{u}^H\mathbf{H}_l\mathbf{w}_k|^2}{\gamma_{e(k,l)}} \leq \sum_{g\neq k}^{K}|\mathbf{u}^H\mathbf{H}_l\mathbf{w}_g|^2+|\mathbf{u}^H\mathbf{H}_l\mathbf{q}_{AN}|^2+\sigma^2, \quad \forall k,l. \tag{8.24}$$

Obviously, constraints (8.23) and (8.24) are in the form of the superlevel of convex functions, which allows us to apply the first-order approximation technique to transform them into convex constraints. Specifically, for a complex value x, it is well known that

$$\frac{|x|^2}{r} \geq \frac{2\Re(\tilde{x}^*x)}{\tilde{r}}-\frac{\tilde{x}^*\tilde{x}}{\tilde{r}^2}r \triangleq F(x,r,\tilde{x},\tilde{r}). \tag{8.25}$$

Based on (8.25), (8.23) and (8.24) can be respectively approximated as

$$\begin{aligned}\sum_{g\neq k}^{K}|\mathbf{u}^H\mathbf{H}_{kj}\mathbf{w}_g|^2+|\mathbf{u}^H\mathbf{H}_{kj}\mathbf{q}_{AN}|^2+\sigma^2 \\ \leq F(\mathbf{u}^H\mathbf{H}_{kj}\mathbf{w}_k,\gamma_{b(k,j)},\mathbf{u}^H\mathbf{H}_{kj}\tilde{\mathbf{w}}_k,\tilde{\gamma}_{b(k,j)}), \quad \forall k,j,\end{aligned} \tag{8.26}$$

$$\begin{aligned}\frac{|\mathbf{u}^H\mathbf{H}_l\mathbf{w}_k|^2}{\gamma_{e(k,l)}} \leq \sum_{g\neq k}^{K}F(\mathbf{u}^H\mathbf{H}_l\mathbf{w}_g,1,\mathbf{u}^H\mathbf{H}_l\tilde{\mathbf{w}}_g,1) \\ +F(\mathbf{u}^H\mathbf{H}_l\mathbf{q}_{AN},1,\mathbf{u}^H\mathbf{H}_l\tilde{\mathbf{q}}_{AN},1)+\sigma^2, \quad \forall k,l.\end{aligned} \tag{8.27}$$

According to the above transformation, problem (P3-1) can be converted into the following problem

$$\text{(P3-1')}: \min_{\{\mathbf{w}_k\},\mathbf{q}_{AN},\boldsymbol{\gamma}_b,\boldsymbol{\gamma}_e} \sum_{k=1}^{K} \|\mathbf{w}_k\|^2 + \|\mathbf{q}_{AN}\|^2 \tag{8.28a}$$

$$\text{s.t.} \quad (8.26),\ (8.27),\ (8.21d). \tag{8.28b}$$

Problem (P3-1') is an SOCP problem and its optimal solution can be found by using CVX.

8.4.2 Optimization with Respect to Phase Shifts

By fixing $\mathbf{w}_k$ and $\mathbf{q}_{AN}$, problem (P3) is reduced to

$$\text{(P3-2)}: \min_{\mathbf{u},\boldsymbol{\gamma}_b,\boldsymbol{\gamma}_e} \quad 1 \tag{8.29a}$$

$$\text{s.t.} \quad \text{SINR}_{b(k,j)}(\mathbf{u}) \geq \gamma_{b(k,j)}, \quad \forall k, j, \tag{8.29b}$$

$$\text{SINR}_{e(k,l)}(\mathbf{u}) \leq \gamma_{e(k,l)}, \quad \forall k, l, \tag{8.29c}$$

$$(8.21d), \tag{8.29d}$$

$$|u_n| = 1, \quad \forall n = 1 \cdots N, u_{N+1} = 1. \tag{8.29e}$$

It is observed that problem (P3-2) is still non-convex due to the non-convex constraints (8.29b) and (8.29c) as well as the unit modulus constraint (8.29e), which leads to problem (P3-2) difficult to solve. Therefore, we concentrate on dealing with these constraints in the next.

For the non-convex constraints (8.29b) and (8.29c), similar to (8.23) and (8.24), they can be transformed into

$$\sum_{g\neq k}^{K} |\mathbf{u}^H \mathbf{H}_{kj} \mathbf{w}_g|^2 + |\mathbf{u}^H \mathbf{H}_{kj} \mathbf{q}_{AN}|^2 + \sigma^2 \tag{8.30}$$

$$\leq F(\mathbf{u}^H \mathbf{H}_{kj} \mathbf{w}_k, \gamma_{b(k,j)}, \tilde{\mathbf{u}}^H \mathbf{H}_{kj} \mathbf{w}_k, \tilde{\gamma}_{b(k,j)}), \quad \forall k, j,$$

$$\frac{|\mathbf{u}^H \mathbf{H}_l \mathbf{w}_k|^2}{\gamma_{e(k,l)}} \leq \sum_{g\neq k}^{K} F(\mathbf{u}^H \mathbf{H}_l \mathbf{w}_g, 1, \tilde{\mathbf{u}}^H \mathbf{H}_l \mathbf{w}_g, 1) \tag{8.31}$$

$$+ F(\tilde{\mathbf{u}}^H \mathbf{H}_l \mathbf{q}_{AN}, 1, \mathbf{u}^H \mathbf{H}_l \mathbf{q}_{AN}, 1) + \sigma^2, \quad \forall k, l,$$

respectively. So far, the non-convex constraints (8.29b) and (8.29c) have been converted into the convex constraints (8.30) and (8.31), respectively. For the unit modulus constraint (8.29e), it can be relaxed as

$$|u_n|^2 \leq 1, \quad \forall n = 1 \cdots N, u_{N+1} = 1, \tag{8.32}$$

which is convex now.

Following the above transformation, problem (P3-2) can be recast as the following SOCP problem

$$\text{(P3-2')}: \min_{\mathbf{u}, \boldsymbol{\gamma}_b, \boldsymbol{\gamma}_e} \quad 1 \quad \text{s.t.} \quad (8.30),\ (8.31),\ (8.32), \tag{8.33}$$

which can be efficiently solved by CVX. Then the solution to problem (P3-2) can be obtained by applying the projection method [37]. Denote the solutions of (P3-2) and (P3-2') as $\{\mathbf{u}^*, \boldsymbol{\gamma}_b^*, \boldsymbol{\gamma}_e^*\}$ and $\{\mathbf{u}^\dagger, \boldsymbol{\gamma}_b^*, \boldsymbol{\gamma}_e^*\}$, respectively, the optimal solution to (P3-2) is given by

$$\mathbf{u}^* = e^{j\angle(\mathbf{u}^\dagger / \mathbf{u}_{N+1}^\dagger)}, \tag{8.34}$$

where the $\angle(\cdot)$ is the radian value of the phase angle of a complex number.

8.4.3 Overall Algorithm and Complexity Analysis

Due to the fact that the objective value of problem (P3) is non-increasing in each iteration. Meanwhile, the objective value of problem (P3) is lower bounded by a finite value, thus the convergence of the SOCP-based algorithm can be guaranteed.

In terms of the complexity, problem (P3-1') consists of T SOC constraints of dimension $K+3$, KL SOC of dimension 3 and TL LMI of size 1. The number of decision variables n_1 is on the order of $M+M+T+KL$. Problem (P3-2') includes T SOC constraints of dimension $K+3$, KL SOC constraints of dimension 3 and $TL+N+1$ LMI of size 1. The number of decision variables n_2 is on the order of $N+T+KL$. Therefore, the computation complexity is

$$\begin{aligned} O\Big(& n_1 D_1 \sqrt{TL + 2(T+KL)} \big(T(K+3)^2 + 3^2 KL + n_1(TL+1) + n_1^2 \big) \\ & + n_2 D_2 \sqrt{TL + N + 1 + 2(T+KL)} \big(T(K+3)^2 + 3^2 KL \\ & + n_2(TL+N+1) + n_2^2 \big) \Big), \end{aligned} \tag{8.35}$$

where D_1 and D_2 denote the numbers of iterations in problem (P3-1') and problem (P3-2'), respectively. Obviously, computational complexity is on the order of M^3 or N^3, which is much lower that of the SDR method (i.e., $M^{6.5}$ or $N^{6.5}$).

8.5 Simulation and Analysis

In this section, numerical results are provided to evaluate the performance of our proposed two algorithms. In this chapter, we consider a three-dimensional (3D) coordinate setup as shown in Fig. 8.2, where Alice and IRS are located at (d_{xa} m, 0 m, 2 m) and (0 m, 100 m, 2 m), respectively, and all Eves are randomly distributed in a circle centered at (d_{xe} m, d_{ye} m, 0 m) with radius $r_E = 5$ m. To study the effect of the IRS on scattered and centralized user groups, two different setups are considered: (1) The centralized user groups (Setup (a)), all the legitimate users are randomly distributed in a circle centered at (d_{xb} m, d_{yb} m, 0) with radius $r_B = 10$ m, in which the users are divided into K groups, and each group receives a separate privacy message; (2) The scattered user groups (Setup (b)), the circle centers of K Bob groups lie uniformly along the line from (d_{xb} m, $d_{yb} - 20$ m, 0 m) to (d_{xb} m, $d_{yb} + 20$ m, 0 m) , and the radius of each user group is $r_B = 2.5$ m. All the channels are assumed to follow the Rayleigh fading model and the path loss at the distance d is modeled as $PL(d) = PL_0 - 10\alpha \log_{10}(\frac{d}{d_0})$, where $PL_0 = -30$ dB denotes the path loss at the reference distance $d_0 = 1$ m, α denotes the path loss exponent. Specifically, the path loss exponents of Alice-IRS, IRS-Eves/Bobs and Alice-Eves/Bobs channels are set to be 2.2, 2.5 and 3.5, respectively. Unless specified otherwise later, the other simulation parameters are set as: $M = 8$, $N = 50$, $\sigma_b^2 = \sigma_e^2 = -90$ dBm, $K = 3$, $|\mathcal{G}_1| = |\mathcal{G}_2| = 2$, $L = 2$, $d_{xa} = 10$ m, $d_{xb} = 10$ m, $d_{xe} = 8$ m, $d_{yb} = 100$ m and $d_{ye} = 90$ m. For comparison, the benchmark schemes are given as follows: (1) Without IRS: There is no use of the IRS and only the transmit beamformer $\mathbf{w}_k$ and AN are designed [38]. (2) Random phase shifts: The phase shifts of IRS are set randomly in $[0, 2\pi]$, the transmit beamformer $\mathbf{w}_k$ and AN are optimized.

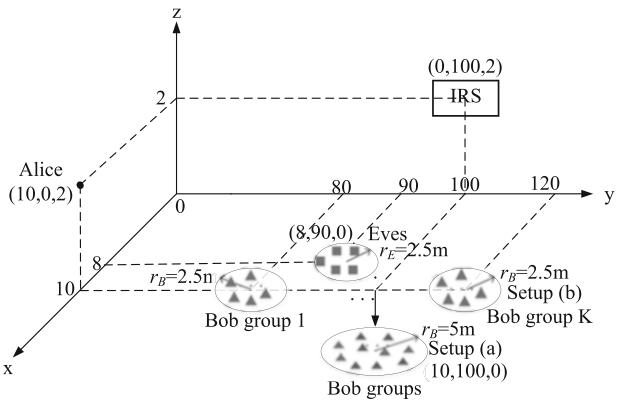


Fig. 8.2 Simulation setup

Figure 8.3 demonstrates the convergence performance of the proposed SDR and SCOP algorithms with $\gamma_s = 1$ bps/Hz. It is observed that the both algorithms converge within a small number of iterations under different setups. Besides, it is worth noticing that the proposed SOCP-based algorithm not only has less computation complexity than the proposed SDR-based algorithm, but also converges faster.

Figure 8.4 shows the transmit power at Alice under different values of SR threshold r_s. From Fig. 8.4, we can first notice that, the minimum transmit power

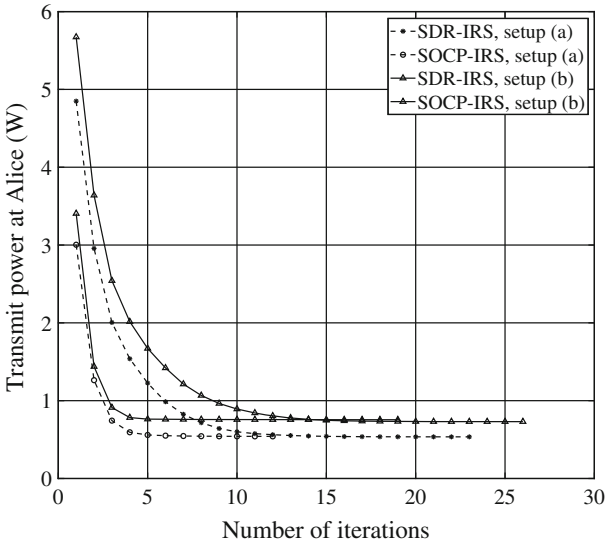
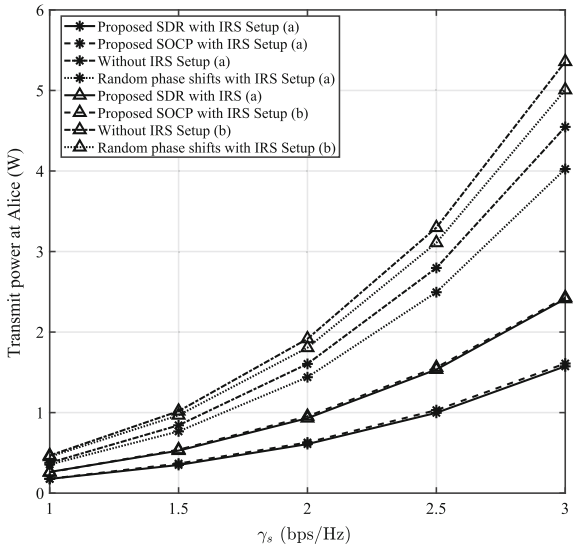


Fig. 8.3 Convergence performance of different algorithms

Fig. 8.4 Transmit power at Alice versus secrecy rate threshold γ_s



at Alice required by all the schemes increases as γ_s increases in both Setup (a) and (b). Compare to Setup (a), since the user groups are scattered in Setup (b), it requires more transmit power to satisfy the SR constraints. Then, it is observed that the both proposed algorithms have the similar performance. This is due to the fact that the both algorithms could guarantee to converge to a local or even global optimum. Finally, we can note that the proposed schemes outperform the NO-IRS scheme as well as the random phase shifts scheme, and the performance gap increases with γ_s. The former validates the advantages of the IRS in the multigroup multicast system, and the later presents the effectiveness of optimizing the phase shifts at the IRS.

The transmit power at Alice versus the number of reflecting elements at the IRS N is shown in Fig. 8.5 with $\gamma_s = 1$ bps/Hz. It is noted that the transmit power at Alice obtained by the both proposed schemes decreases significantly as N increases for the two setups. What's more, the transmit power in Setup (a) decays faster than that in Setup (b), which is because the IRS locates near all the Bob groups in Setup (a) but far from some Bob groups in Setup (b). Hence, the received signal at Bobs from the reflection of the IRS in Setup (a) is larger than that in Setup (b). Besides, it is worth noting that the performance gaps between the IRS-aided schemes and the NO-IRS scheme increase as N increases in both setups. This is expected since when the IRS's aperture becomes larger, more degrees of freedom become available for the passive beamforming of the IRS. And thus the proportion of the signal reflected by the IRS to the received signal at Bob groups increases as N increases.

In Fig. 8.6, we gradually increase the number of groups K for both Setup (a) and (b) to study the effect on the transmit power at Alice with $\gamma_s = 0.5$ bps/Hz. Obviously, the transmit power at Alice of all the schemes increases as K increases. Compare to the case without IRS, the transmit power required by applying the two

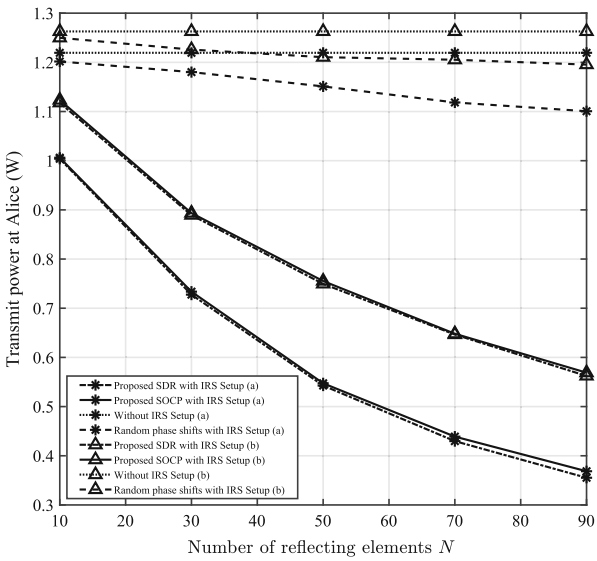


Fig. 8.5 Transmit power at Alice versus N

proposed algorithms with IRS is significantly reduced. Additionally, for the two setups, the performance gaps between the NO-IRS scheme and the two IRS-aided schemes increase rapidly with the increase of K, which further demonstrates the efficiency of the IRS in enhancing the performance of the multicast systems.

In Fig. 8.7, we plot the transmit power at Alice versus the distance between Alice and the center of user groups d_{yb} with $d_{xa} = 3\,\text{m}$, $d_{xb} = 3\,\text{m}$, $d_{xe} = 2\,\text{m}$, $K = 2$,

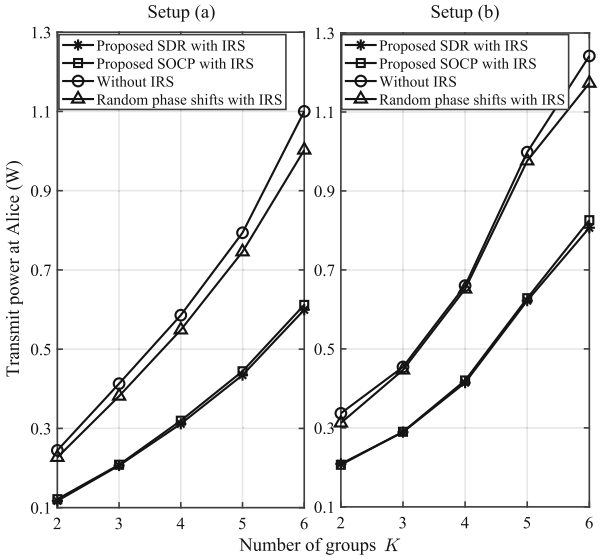


Fig. 8.6 Transmit power at Alice versus K

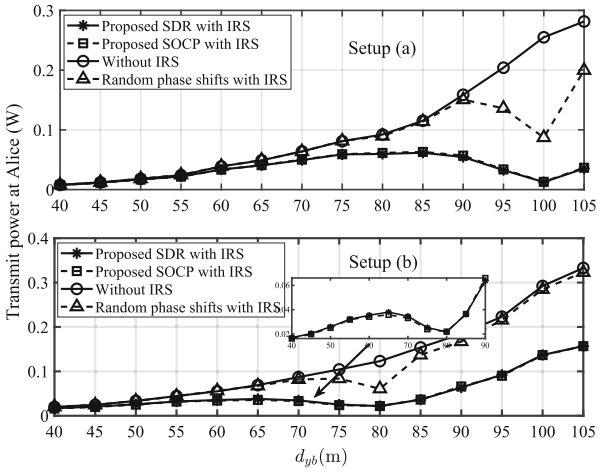


Fig. 8.7 Transmit power at Alice versus the distance d_{yb}

$N = 100$ and $\gamma_s = 0.5$ bps/Hz. First, it is observed that the proposed two schemes require less transmit power than the other benchmark schemes in Setups (a) and (b). Second, when the user groups move far away from Alice, the required transmit power increases for all the schemes due to the larger signal attenuation. However, the transmit power of the three IRS-aided schemes decreases greatly when user groups approaches the IRS. It implies that a large Alice-users distance does not necessarily lead to a higher transmit power in IRS-aided wireless networks. This is because the user groups farther away from Alice may be closer to the IRS and thus it is able to receive stronger reflected signal from the IRS. As a result, the user groups near either Alice or IRS requires lower transmit power than user groups far away from both of them. Specifically, in Setup (a), when the user groups close to either the IRS (e.g., $d_{yb} = 100$ m) or Alice (e.g., $d_{yb} = 40$ m), the required transmit power at Alice is lower than the users far away from both Alice and IRS. Different from Setup (a) in which all the user groups are concentrated in a circle, the transmit power at Alice becomes smaller with $d_{yb} = 80$ m instead of 100 m in Setup (b). This is because the user groups are scattered, i.e., one user group at 60 m (close to Alice) and one at 100 m (close to IRS), and the transmit power at Alice required by all user groups is minimal at this moment.

8.6 Conclusion

In this chapter, we investigated a novel IRS-aided secure multigroup multicast MISO communication system. By jointly optimizing the transmit beamformer, AN vector and phase shifts at the IRS, we minimized the transmit power at Alice subject to the secrecy rate constraints. For this non-convex optimization problem, we first proposed an SDR method based on the alterative optimization and obtained a high-quality solution. Due to the high computation complexity of the proposed SDR method, the SOCP method with low complexity is then presented. The simulation results demonstrate that the proposed SOCP algorithm can obtain the similar performance as the SDR algorithm. Besides, it is shown that the transmit power required at Alice of the two proposed schemes have a significant drop compare to that of the scheme without IRS.

References

1. Huang, C., Hu, S., Alexandropoulos, C., Zappone, A., Yuen, C., Zhang, R., Di Renzo, M., Di Renzo, M., Debbah, M.: Holographic MIMO surfaces for 6g wireless networks: opportunities, challenges, and trends. IEEE Wirel. Commun. **27**(5), 118-125 (2020)
2. Wu, Y., Wen, C., Chen, W., Jin, S., Schober, R., Caire, G.: Data-aided secure massive MIMO transmission under the pilot contamination attack. IEEE Trans. Commun. **67**(7), 4765–4781 (2019)

3. Shu, F., Qin, Y., Liu, T., Gui, L., Zhang, Y., Li, J., Han, Z.: Low-complexity and high-resolution DOA estimation for hybrid analog and digital massive MIMO receive array. IEEE Trans. Commun. **66**(6), 2487–2501 (2018)
4. Zhang, J., Zhang, Y., Zhong, C., Zhang, Z.: Robust Design for Intelligent Reflecting Surfaces Assisted MISO Systems. IEEE Commun. Lett. **24**(10), 2353–2357 (2020)
5. Abeywickrama, S., Zhang, R., Wu, Q., Yuen, C.: Intelligent reflecting surface: practical phase shift model and beamforming optimization. IEEE Trans. Commun. **68**(9), 5849–5863 (2020)
6. Mei, W., Zhang, R.: Cooperative Beam Routing for Multi-IRS Aided Communication. IEEE Wirel. Commun. Lett. (Early access, 2020)
7. Ozdogan, O., Bjornson, E., Larsson, E.G.: Intelligent Reflecting Surfaces: Physics, Propagation, and Pathloss Modeling. IEEE Wirel. Commun. Lett. **9**(5), 581–585 (2020)
8. Hu, X., Zhong, C., Zhang, Y., Chen, X., Zhang, Z.: Location information aided multiple intelligent reflecting surface systems. IEEE Trans. Commun. **68**(12), 7948–7962 (2020)
9. Wu, Q., Zhang, R.: Intelligent reflecting surface enhanced wireless network via joint active and passive. IEEE Trans. Wirel. Commun. **18**(11), 5394–5409 (2019)
10. Yu, X., Xu, D., Schober, R.: MISO wireless communication systems via intelligent reflecting surface. In: IEEE/CIC International Conference on Communication in China (ICCC), pp. 735–740 (2019)
11. Huang, C., Zappone, A., Alexandropoulos, G.C., Debbah, M., Yuen, C.: Reconfigurable intelligent surfaces for energy efficiency in wireless communication. IEEE Trans. Wirel. Commun. **18**(8), 4157–4170 (2019)
12. Chen, X., Ng, D.W.K., Gerstacker, W.H., Chen, H.: A survey on multiple-antenna techniques for physical layer security. IEEE Commun. Surveys Tuts. **19**(2), 1027–1053 (2017)
13. Wang, H., Yin, Q., Xia, X.: Distributed beamforming for physical-layer security of two-way relay networks. IEEE Trans. Signal Process. **60**(7), 3532–3545 (2012)
14. Hu, J., Shu, F., Li, J.: Robust synthesis method for secure directional modulation with imperfect direction angle. IEEE Commun. Lett. **20**(6), 1084–1087 (2016)
15. Xia, G., Shu, F., Zhang, Y., Wang, J., ten Brink, S., Speidel, J.: Antenna selection method of maximizing secrecy rate for green secure spatial modulation. IEEE Trans. Green Commun. Netw. **3**(2), 288–301 (2019)
16. Zhao, N., Yu, F.R., Li, M., Leung, V.C.M.: Anti-eavesdropping schemes for interference alignment (IA)-based wireless networks. IEEE Trans. Wirel. Commun. **15**(8), 5719–5732 (2016)
17. Zhou, X., Wu, Q., Yan, S., Shu, F., Li, J.: UAV-enabled secure communications: joint trajectory and transmit power optimization. IEEE Trans. Veh. Technol. **68**(4), 4069–4073 (2019)
18. Xia, G., Lin, Y., Liu, T., Shu, F., Hanzo, L.: Transmit antenna selection and beamformer design for secure spatial modulation with rough CSI of Eve. IEEE Trans. Wirel. Commun. **19**(7), 4643–4656 (2020)
19. Shen, H., Xu, W., Gong, S., He, Z., Zhao, C.: Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications. IEEE Commun. Lett. **23**(9), 1488–1492 (2019)
20. Xu, D., Yu, X., Sun, Y., Ng, D.W.K., Schober, R.: Resource allocation for secure IRS-assisted multiuser MISO systems. In: 2019 IEEE Globecom Workshops (GC Wkshps), pp. 1–6 (2019)
21. Hong, S., Pan, C., Ren, H., Wang, K., Nallanathan, A.: Artificial-noise-aided secure MIMO wireless communications via intelligent reflecting surface. IEEE Trans. Commun. **68**(12), 7851–7866 (2020)
22. Shi, W., Zhou, X., Jia, L., Wu, Y., Shu, F., Wang, J.: Enhanced secure wireless information and power transfer via intelligent reflecting surface. IEEE Commun. Lett. (Early access, 2020)
23. He, Z., Yuan, X.: Cascaded channel estimation for large intelligent metasurface assisted massive MIMO. IEEE Wirel. Commun. Lett. **9**(2), 210–214 (2020)
24. Zheng, B., Zhang, R.: Intelligent reflecting surface-enhanced OFDM: channel estimation and reflection optimization. IEEE Wirel. Commun. Lett. **9**(4), 518–522 (2020)
25. Huang, C., Mo, R., Yuen, C.: Reconfigurable intelligent surface assisted multiuser MISO systems exploiting deep reinforcement learning. IEEE J. Sel. Areas Commun. **38**(8), 1839–1850 (2020)

26. Doan, T.X., Ngo, H.Q., Duong, T.Q., Tourki, K.: On the performance of multigroup multicast cell-free massive MIMO. IEEE Commun. Lett. **21**(12), 2642–2645 (2017)
27. Chen, E., Tao, M.: ADMM-based fast algorithm for multi-group multicast beamforming in large-scale wireless systems. IEEE Trans. Commun. **65**(6), 2685–2698 (2017)
28. Shu, F., Xu, L., Wang, J., Zhu, W., Xiaobo, Z.: Artificial-noise-aided secure multicast precoding for directional modulation systems. IEEE Trans. Veh. Technol. **67**(7), 6658–6662 (2018)
29. Qi, C., Chen, H., Deng, Y., Nallanathan, A.: Energy efficient multicast precoding for multiuser multibeam satellite communications. IEEE Wirel. Commun. Lett. **9**(4), 567–570 (2020)
30. Zhou, G., Pan, C., Ren, H., Wang, K., Nallanathan, A.: Intelligent reflecting surface aided multigroup multicast MISO communication systems. IEEE Trans. Signal Process. **68**, 3236–3251 (2020)
31. Shu, F., Li, J., Huang, M., Shi, W., Teng, Y., Li, J., Wu, Y., Wang, J.: Enhanced secrecy rate maximization for directional modulation networks via IRS. IEEE Trans. Commun. **69**(12), 8388–8401 (2021)
32. Cui, M., Zhang, G., Zhang, R.: Secure wireless communication via intelligent reflecting surface. IEEE Wirel. Commun. Lett. **8**(5), 1410–1414 (2019)
33. Guan, X., Wu, Q., Zhang, R.: Intelligent reflecting surface assisted secrecy communication: is artificial noise helpful or not? IEEE Wirel. Commun. Lett. **9**(6), 778–782 (2020)
34. Li, Q., Ma, W.: Spatially selective artificial-noise aided transmit optimization for MISO multi-eves secrecy rate maximization. IEEE Trans. Signal Process. **61**(10), 2704–2717 (2013)
35. Grant, M., Boyd, S.: CVX: MATLAB software for disciplined convex programming (2014). Available: http://cvxr.com/cvxAvailable
36. Wang, K., So, A.M., Chang, T., Ma, W., Chi, C.: Outage constrained robust transmit optimization for multiuser MISO downlinks: tractable approximations by conic optimization. IEEE Trans. Signal Process. **62**(21), 5690–5705 (2014)
37. Chen, J., Liang, Y., Pei, Y., Guo, H.: Intelligent reflecting surface: a programmable wireless environment for physical layer security. IEEE Access. **7**, 82599–82612 (2019)
38. Kim, W., Ha, S., Koh, J., Kang, J.: Artificial noise-aided secure beamforming for multigroup multicast. In: 15th IEEE Annual Consumer Communications and Networking Conference (CCNC), pp. 1–4 (2019)

Chapter 9
Beamforming Design for IRS-Aided Decode-and-Forward Relay Wireless Network

As a low-cost and low-power-consumption passive reflector, IRS can make a significant rate improvement by building a programmable wireless environment. To improve the rate performance and coverage range of wireless networks, an IRS-aided DF relay network is proposed with multiple antennas at relay station (RS). To achieve a high rate, an alternately iterative structure (AIS) of maximizing receive power (Max-RP) at RS is proposed to jointly optimize the beamforming vectors at RS and phase shifts at IRS. Considering its high-complexity, two low-complexity Max-RP schemes of NSP plus MRC and intelligent reflecting surface element selection (IRSES) plus MRC are presented to reduce this complexity, respectively. For the former, NSP is used to separate the reflected signal from IRS and the direct transmitted signal from source and MRC is adopted to combine the two signals at RS. For the latter, the basic concept of IRSES is as follows: IRS is partitioned into M subsets of elements and adjusting the phases of all elements per subset make all reflected signals and the direct signal from source phase alignment at the corresponding antenna of relay. Simulation results show that the proposed three methods perform much better than the existing network with single-antenna relay in terms of rate performance. In particular, a 85% rate gain over existing scheme is achieved in the high SNR region. Moreover, it is verified that the positions of RS and IRS have a substantial impact on rate performance, and there exists an optimal positions of RS and IRS.

9.1 Introduction

With the explosive growth of communication device nodes in wireless sensor network (WSN), there are more stringent requirements in terms of energy efficiency and extended coverage [1]. Relay has a strong ability to process signal for extended communication coverage and improved rate performance [2, 3]. However, the

F. Shu, J. Wang, *Intelligent Reflecting Surface-Aided Physical-Layer Security*,
Wireless Networks, https://doi.org/10.1007/978-3-031-41812-9_9

conventional relay is an active device, which is costly and requires additional high energy consumption to process the signal [4], it is crucial to develop a energy-efficient and green communication network.

Compared with the conventional relay, since IRS does not require any radio frequency chain and baseband circuit and is made up of low-cost and passive reflecting units, its lower-energy-consumption and passive property is very attractive [5, 6]. Thus, IRS can be regarded as a green reflect-to-forward relay. It is anticipated that IRS will be potentially applied to the diverse future wireless networks such as WiFi 7, mobile communications like 6G, space communication, marine communication, and emergency communication [7]. For example, for mobile communications, IRS will be used to significantly enhance the coverage of blind areas, especially cell edges. Due to the ability of intelligently adjusting the amplitude and phase shift of the incident signal by a smart controller [8], IRS may form helpful controlled multi-paths, ingeniously improve the propagation environment and provide new degrees of freedom, which can be used to enhance the wireless network performance. Recently, IRS has attracted much attention from both academia and industry [9]. IRS may be adopted to aid many wireless communication directions as follows: directional modulation [10], [11], spatial modulation [12, 13], multicast transmission [14, 15], covert wireless communication [16, 17], UAV communication [18, 19], and SWIPT [20, 21].

A combination of a relay and an IRS was shown to improve energy efficiency [22], spectral efficiency [23] and rate performance [24–26]. In [22], the authors proposed a multi-user mobile communication network model with the help of a relay and an IRS, where two sub-optimal methods based on AO, called SVD plus uplink-downlink duality, and SVD plus ZF methods were presented to implement an enhanced performance from BS to multi-users in terms of energy efficiency. To increase spectral efficiency, in [23] a novel network was proposed, where some IRS elements act as active relays to amplify incident signals, and the remaining elements reflect signals. A spectral efficiency maximization problem was formulated and solved by the alternating optimization method. Aiming at improving rate performance, the authors proposed two kinds of IRS plus DF relay [24]: distributed and centralized. Subsequently, a sequential optimization algorithm was presented to address the power allocation and optimization of IRS phases, and it was demonstrated that IRS and DF relay can work in a synergistic manner to enhance the achievable rate. In [25], a network consisting of two side-by-side intelligent surfaces connected via a full-duplex relay was proposed to achieve the promising rate gains with much smaller number of reflecting elements. Moreover, a hybrid network consisting of an IRS and a single-antenna DF relay was proposed to save a massive IRS elements compared with only IRS in [26]. In [27], a communication system with multiple antennas at both transmitter and receiver is considered.

From the above literature, it can be concluded that IRS has the advantages of low cost and low energy consumption, and relay has a strong signal processing ability such as AF and DF. It is interesting to combine relay and IRS while keeping the advantages of relay and IRS. The hybrid network combines both advantages of IRS

and relay to strike a good balance among circuit cost, energy efficiency and rate performance.

The application scenarios in the above literature are common, a hybrid network combining IRS and multi-antenna relay is proposed to employ to WSN scenario, which consists of a data collecting center and many other non-center nodes. The data collecting center collects all data from other nodes, then send them to internet with the help of relay and IRS. Furthermore, when data collecting center-relay or relay-destination direct link has shadow fading, or in extreme cases is completely blocked. The proposed hybrid network is still appropriate for the practical scenario, where an IRS is placed on a high big building and can see source, relay and destination. In other words, the signal from source can still be transmitted to relay and destination with the help of the IRS. This means that adding IRS can create new reflective paths among source, relay and destination.

In this book chapter, in order to improve the data rate of the proposed hybrid network or dramatically extend its coverage range, three efficient beamforming methods are proposed to achieve this goal, which are as follow:

To make a dramatic rate improvement, an IRS-aided multi-antenna relay network model is proposed. We focus on the design of beamforming in the first time slot due to the fact that the system model can be converted into a typical IRS-aided three-point model. A Max-RP using AIS is proposed to maximize RP by alternately optimizing the beamforming vector at RS and phase shifts at IRS. Due to the rule of Max-RP, the closed-form expressions of the beamforming vector at RS and phase shifts at IRS are derived. From the simulation results, the proposed Max-RP method using AIS can harvest up to 86% rate gain over existing network of an IRS plus a single-antenna relay in [26] in the high SNR region. The total computational complexity is $O\{L_2(N^4 + 8MN^3 + 5N^3 + 24MN^2 - 2N^2)\}$, and the highest order is N^4 float-point operations (FLOPs), which is high.

To reduce the high computational complexity of the above method, a low-complexity NSP-based Max-RP plus MRC is proposed in the first time slot. The two independent receive beamforming vectors are used at RS. They utilize NSP to separate the signal from source and the reflected signal from IRS and maximize the receive power of the corresponding signal. Finally, MRC is adopted to combine the two signals to improve the SNR of receive signal at RS. Our simulation results show that the rate of the proposed NSP-based Max-RP plus MRC method is 84% higher than that of the existing system with an IRS and a single-antenna relay in [26] in the high SNR region. Its computational complexity is $O\{N^3 + M^3 + M^2N + MN^2\}$, which is much lower than the Max-RP method using AIS.

To further reduce the computational complexity, the IRSES-based Max-RP plus MRC method is proposed. Here, in the first time slot, according to the number M of RS antennas, IRS elements are divided into M subsets with each subset having the same number of elements. Each subset is mapped into one antenna at RS. In other words, there is one-to-one mapping relationship between subsets at IRS and antennas at RS. Adjusting the phases of all elements per subset aligns the phases of all reflected signals and the direct signal from source at the corresponding antenna of relay. Finally, MRC is adopted to combine all received signals at RS.

From the simulation results, the proposed Max-RP based on IRSES plus MRC method achieves a substantial rate improvement over existing system in [26]. The complexity is $O\{15MK+8M+10K+L_5(18MN+2M+3N)\}$, which is extremely lower than the above proposed two methods.

The remainder of this book chapter is organized as follows. In Sect. 9.2, we describe an IRS-aided DF relay network. In Sect. 9.3, we demonstrate three methods for a better rate performance of the proposed network. We present our simulation results in Sect. 9.4, and draw conclusions in Sect. 9.5.

Notation Scalars, vectors and matrices are respectively represented by letters of lower case, bold lower case, and bold upper case. $(\cdot)^*$, $(\cdot)^H$, $(\cdot)^\dagger$ stand for matrix conjugate, conjugate transpose, and Moore-Penrose pseudo inverse, respectively. $\mathbb{E}\{\cdot\}$, $\|\cdot\|$, $\mathrm{tr}(\cdot)$, and $\arg(\cdot)$ denote expectation operation, 2-norm, the trace of a matrix, and the phase of a complex number, respectively. The sign $\mathbf{I}_N$ is the $N \times N$ identity matrix.

9.2 System Model

As shown in Fig. 9.1, the IRS-aided DF relay network consists of a half-duplex DF RS with M transmit antennas, an IRS with N reflecting elements, a data collector (S) and a base station (D) equipped with a single antenna each. As a data collecting center node, S collects all data from other sensor nodes, and transmits them towards D with the help of IRS and RS. Here, the network is operated in a time division half-duplex scenario. The distance from S to D are assumed so far that there is no direct link between them [26]. Due to path loss, the power of signals reflected by the IRS twice or more are such weak that they can be ignored. Moreover, all CSI is assumed to be perfectly known to S, RS, IRS and D. In the first time slot, the received signal at RS is written by

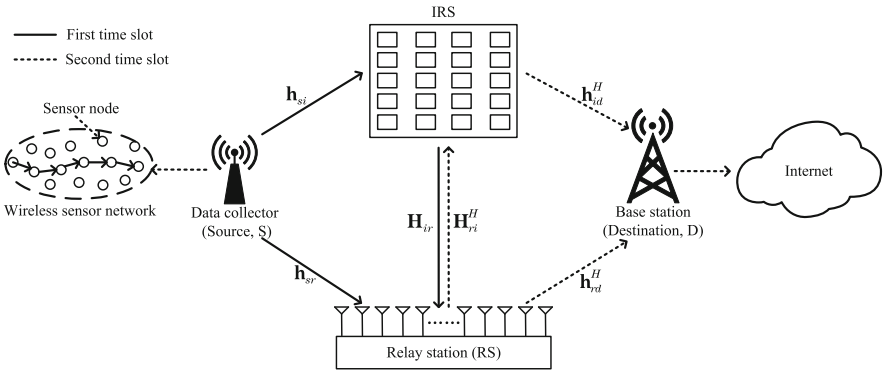


Fig. 9.1 System model for an IRS-aided DF relay network

$$\mathbf{y}_r = \sqrt{P_s}(\mathbf{h}_{sr} + \mathbf{H}_{ir}\boldsymbol{\Theta}_1\mathbf{h}_{si})s + \mathbf{n}_r, \tag{9.1}$$

where s and P_s are the transmit signal and power from S, respectively. $\mathbb{E}\{s^H s\} = 1$. Without loss of generality, we assume a Rayleigh fading environment. Let $\mathbf{h}_{sr} \in \mathbb{C}^{M\times 1}$, $\mathbf{H}_{ir} \in \mathbb{C}^{M\times N}$ and $\mathbf{h}_{si} \in \mathbb{C}^{N\times 1}$ represent the channels from S to RS, from IRS to RS, and from S to IRS. $\boldsymbol{\Theta}_1$ is the diagonal reflection-coefficient matrix of IRS, which is denoted as $\boldsymbol{\Theta}_1 = \text{diag}(e^{j\theta_{11}}, \cdots, e^{j\theta_{1N}})$, $\boldsymbol{\theta}_1 = [e^{j\theta_{11}}, \cdots, e^{j\theta_{1N}}]^T$, $\theta_{1i} \in (0, 2\pi]$ is the phase shift of the ith element. $\mathbf{n}_r \in \mathbb{C}^{M\times 1}$ is the AWGN with distribution $\mathbf{n}_r \sim \mathcal{CN}(0, \sigma_r^2\mathbf{I}_{N_r})$. Then the received signal at RS after receive beamforming can be expressed as

$$y_r = \sqrt{P_s}\mathbf{u}_r^H(\mathbf{h}_{sr} + \mathbf{H}_{ir}\boldsymbol{\Theta}_1\mathbf{h}_{si})s + \mathbf{u}_r^H\mathbf{n}_r, \tag{9.2}$$

where $\mathbf{u}_r^H \in \mathbb{C}^{1\times M}$ is the receive beamforming vector, $\|\mathbf{u}_r^H\|^2 = 1$. The achievable rate at RS is given by

$$R_r = \log_2\left(1 + \frac{P_R}{\sigma_r^2}\right), \tag{9.3}$$

where

$$P_R = P_s\text{tr}\left\{\mathbf{u}_r^H(\mathbf{h}_{sr} + \mathbf{H}_{ir}\boldsymbol{\Theta}_1\mathbf{h}_{si})(\mathbf{h}_{sr} + \mathbf{H}_{ir}\boldsymbol{\Theta}_1\mathbf{h}_{si})^H\mathbf{u}_r\right\}. \tag{9.4}$$

In the second time slot, it is assumed that the original signal s can be correctly decoded by RS. The transmit signal from RS is $\mathbf{x}_r = \mathbf{u}_t s$, where $\mathbf{u}_t \in \mathbb{C}^{M\times 1}$ is the transmit beamforming vector, $\|\mathbf{u}_t\|^2 = 1$. The received signal at D is as follows

$$y_d = \sqrt{P_r}(\mathbf{h}_{rd}^H + \mathbf{h}_{id}^H\boldsymbol{\Theta}_2\mathbf{H}_{ri}^H)\mathbf{u}_t s + n_d, \tag{9.5}$$

where P_r is the transmit power from RS, $\mathbf{h}_{rd}^H \in \mathbb{C}^{1\times M}$, $\mathbf{h}_{id}^H \in \mathbb{C}^{1\times N}$ and $\mathbf{H}_{ri}^H \in \mathbb{C}^{N\times M}$ are the channels from RS to D, from IRS to D, and from RS to IRS, respectively. The diagonal reflection-coefficient matrix of IRS is represented as $\boldsymbol{\Theta}_2 = \text{diag}\left(e^{j\theta_{21}}, \cdots, e^{j\theta_{2N}}\right)$, $\boldsymbol{\theta}_2 = [e^{j\theta_{21}}, \cdots, e^{j\theta_{2N}}]^T$, $\theta_{2i} \in (0\ ,\ 2\pi]$ is the phase shift of the ith element. n_d is the AWGN with distribution $n_d \sim \mathcal{CN}\left(0, \sigma_d^2\right)$. The achievable rate at D can be expressed as

$$R_d = \log_2\left(1 + \frac{P_D}{\sigma_d^2}\right), \tag{9.6}$$

where

$$P_D = P_r\text{tr}\left\{\mathbf{u}_t^H(\mathbf{h}_{rd}^H + \mathbf{h}_{id}^H\boldsymbol{\Theta}_2\mathbf{H}_{ri}^H)^H(\mathbf{h}_{rd}^H + \mathbf{h}_{id}^H\boldsymbol{\Theta}_2\mathbf{H}_{ri}^H)\mathbf{u}_t\right\}. \tag{9.7}$$

The achievable rate of the proposed system is defined as follows

$$R_s = \frac{1}{2}\min\{R_r, R_d\}. \tag{9.8}$$

9.3 Proposed Three High-Performance Beamforming Schemes

In this section, according to (9.3), maximizing rate is equivalent to Max-RP due to the fact that the log function is a monotone increasing function of RP. In the first time slot, three Max-RP methods: AIS-based Max-RP, NSP-based Max-RP plus MRC, and IRSES-based Max-RP plus MRC, are proposed to optimize the phase shift vector $\boldsymbol{\theta}_1$ of IRS and the receive beamforming vector $\mathbf{u}_r$ of RS. In the second time slot, RS, IRS and destination form a typical three-point IRS-aided network, where an alternating iteration in [28] are adopted to design the transmit beamforming vector at RS and adjust the phases of IRS.

9.3.1 Proposed AIS-Based Max-RP Method

For the first time slot, the corresponding optimization problem can be casted as

$$\begin{aligned} \max_{\boldsymbol{\Theta}_1, \mathbf{u}_r^H} \quad & P_s \mathrm{tr}\left\{\mathbf{u}_r^H(\mathbf{h}_{sr} + \mathbf{H}_{ir}\boldsymbol{\Theta}_1\mathbf{h}_{si})(\mathbf{h}_{sr} + \mathbf{H}_{ir}\boldsymbol{\Theta}_1\mathbf{h}_{si})^H\mathbf{u}_r\right\} \\ \text{s.t.} \quad & \|\mathbf{u}_r^H\|^2 = 1,\ |\boldsymbol{\theta}_1(i)| = 1,\ \forall i = 1, \cdots, N. \end{aligned} \tag{9.9}$$

Let us define $\mathbf{H}_{si} = \mathrm{diag}\{\mathbf{h}_{si}\}$, we have $\boldsymbol{\Theta}_1\mathbf{h}_{si} = \mathbf{H}_{si}\boldsymbol{\theta}_1$. Firstly, by fixing $\mathbf{u}_r^H$, (9.9) is reduced to

$$\begin{aligned} \max_{\boldsymbol{\theta}_1} \quad & P_s \mathrm{tr}(\boldsymbol{\theta}_1^H\mathbf{H}_{si}^H\mathbf{H}_{ir}^H\mathbf{u}_r\mathbf{u}_r^H\mathbf{H}_{ir}\mathbf{H}_{si}\boldsymbol{\theta}_1) + P_s\mathrm{tr}(\boldsymbol{\theta}_1^H\mathbf{H}_{si}^H\mathbf{H}_{ir}^H\mathbf{u}_r\mathbf{u}_r^H\mathbf{h}_{sr}) \\ & + P_s\mathrm{tr}(\boldsymbol{\theta}_1\mathbf{h}_{sr}^H\mathbf{u}_r\mathbf{u}_r^H\mathbf{H}_{ir}\mathbf{H}_{si}) \\ \text{s.t.} \quad & \boldsymbol{\theta}_1^H\boldsymbol{\theta}_1 = N. \end{aligned} \tag{9.10}$$

The Lagrangian function associated with the above optimization (9.10) is defined as

$$\begin{aligned} L(\boldsymbol{\theta}_1, \lambda) = & P_s \mathrm{tr}(\boldsymbol{\theta}_1^H\mathbf{H}_{si}^H\mathbf{H}_{ir}^H\mathbf{u}_r\mathbf{u}_r^H\mathbf{H}_{ir}\mathbf{H}_{si}\boldsymbol{\theta}_1) + P_s\mathrm{tr}(\boldsymbol{\theta}_1^H\mathbf{H}_{si}^H\mathbf{H}_{ir}^H\mathbf{u}_r\mathbf{u}_r^H\mathbf{h}_{sr}) \\ & + P_s\mathrm{tr}(\boldsymbol{\theta}_1\mathbf{h}_{sr}^H\mathbf{u}_r\mathbf{u}_r^H\mathbf{H}_{ir}\mathbf{H}_{si}) + \lambda(\boldsymbol{\theta}_1^H\boldsymbol{\theta}_1 - N), \end{aligned} \tag{9.11}$$

where λ is the Lagrange multiplier, if $(\boldsymbol{\theta}_1, \lambda)$ is the optimal solution to the above equation, the partial derivative of the Lagrangian function with respect to $\boldsymbol{\theta}_1$ should be set to be zero as follows

$$\begin{aligned}\frac{\partial L(\boldsymbol{\theta}_1, \lambda)}{\partial \boldsymbol{\theta}_1} &= P_s \mathbf{H}_{si}^H \mathbf{H}_{ir}^H \mathbf{u}_r \mathbf{u}_r^H \mathbf{H}_{ir} \mathbf{H}_{si} \boldsymbol{\theta}_1 + P_s \mathbf{H}_{si}^H \mathbf{H}_{ir}^H \mathbf{u}_r \mathbf{u}_r^H \mathbf{h}_{sr} + \lambda \boldsymbol{\theta}_1 \\ &= 0, \end{aligned} \tag{9.12}$$

which gives the solution

$$\theta_{1i} = -\arg\{(\lambda {P_s}^{-1} \mathbf{I}_N + \mathbf{H}_{si}^H \mathbf{H}_{ir}^H \mathbf{u}_r \mathbf{u}_r^H \mathbf{H}_{ir} \mathbf{H}_{si})^{\dagger} (\mathbf{H}_{si}^H \mathbf{H}_{ir}^H \mathbf{u}_r \mathbf{u}_r^H \mathbf{h}_{sr})\}_i. \tag{9.13}$$

Inserting (9.13) back into the restriction of (9.10), we have an equation associated with Lagrange multiplier as follows

$$\det\left(\lambda {P_s}^{-1} \mathbf{I}_N + \mathbf{H}_{si}^H \mathbf{H}_{ir}^H \mathbf{u}_r \mathbf{u}_r^H \mathbf{H}_{ir} \mathbf{H}_{si}\right) = b, \tag{9.14}$$

where

$$b = \left(\det(N^{-1} \mathbf{H}_{si}^H \mathbf{H}_{ir}^H \mathbf{u}_r \mathbf{u}_r^H \mathbf{h}_{sr} \mathbf{h}_{sr}^H \mathbf{u}_r \mathbf{u}_r^H \mathbf{H}_{ir} \mathbf{H}_{si})\right)^{\frac{1}{2}}. \tag{9.15}$$

Further, in accordance with the rank inequality: rank $\mathbf{A} \leq \min\{m, n\}$, where $\mathbf{A} \in \mathbb{C}^{m \times n}$, we can get

$$\operatorname{rank}(\mathbf{H}_{si}^H \mathbf{H}_{ir}^H \mathbf{u}_r \mathbf{u}_r^H \mathbf{h}_{sr} \mathbf{h}_{sr}^H \mathbf{u}_r \mathbf{u}_r^H \mathbf{H}_{ir} \mathbf{H}_{si}) \leq \operatorname{rank}(\mathbf{u}_r^H) = 1. \tag{9.16}$$

Therefore, $b = 0$. Then we have the eigen decomposition as follows

$$\mathbf{H}_{si}^H \mathbf{H}_{ir}^H \mathbf{u}_r \mathbf{u}_r^H \mathbf{H}_{ir} \mathbf{H}_{si} = \mathbf{U} \boldsymbol{\Sigma} \mathbf{U}^H, \tag{9.17}$$

where $\mathbf{U}$ is a unitary matrix composed of eigenvectors and $\mathbf{U}\mathbf{U}^H = \mathbf{U}^H\mathbf{U} = \mathbf{I}_N$. $\boldsymbol{\Sigma}$ is a diagonal matrix composed of eigenvalues. Substituting the above equation in (9.14) yields the following simplified equation

$$\begin{aligned}\det\left\{\mathbf{U}\left(\lambda {P_s}^{-1} \mathbf{I}_N + \boldsymbol{\Sigma}\right)\mathbf{U}^H\right\} &= \det\left\{\mathbf{U}\mathbf{U}^H\left(\lambda {P_s}^{-1} \mathbf{I}_N + \boldsymbol{\Sigma}\right)\right\} \\ &= \det\left(\lambda {P_s}^{-1} \mathbf{I}_N + \boldsymbol{\Sigma}\right) \\ &= 0. \end{aligned} \tag{9.18}$$

It can be observed that $\operatorname{rank}(\mathbf{H}_{si}^H \mathbf{H}_{ir}^H \mathbf{u}_r \mathbf{u}_r^H \mathbf{H}_{ir} \mathbf{H}_{si}) = 1$, so there is a nonzero eigenvalue and $N - 1$ zero eigenvalues in $\mathbf{H}_{si}^H \mathbf{H}_{ir}^H \mathbf{u}_r \mathbf{u}_r^H \mathbf{H}_{ir} \mathbf{H}_{si}$. Then we construct the following equation

$$\mathbf{H}_{si}^H \mathbf{H}_{ir}^H \mathbf{u}_r \mathbf{u}_r^H \mathbf{H}_{ir} \mathbf{H}_{si} (\mathbf{H}_{si}^H \mathbf{H}_{ir}^H \mathbf{u}_r) = \|\mathbf{u}_r^H \mathbf{H}_{ir} \mathbf{H}_{si}\|^2 \mathbf{H}_{si}^H \mathbf{H}_{ir}^H \mathbf{u}_r, \tag{9.19}$$

where $\|\mathbf{u}_r^H \mathbf{H}_{ir} \mathbf{H}_{si}\|^2$ is the only nonzero eigenvalue (ie. the largest eigenvalue), so we have

$$\mathbf{\Sigma} = \begin{bmatrix} \|\mathbf{u}_r^H \mathbf{H}_{ir} \mathbf{H}_{si}\|^2 & 0 \cdots 0 \\ 0 & 0 \cdots 0 \\ \vdots & \vdots \ddots \vdots \\ 0 & 0 \cdots 0 \end{bmatrix}_{N \times N}. \tag{9.20}$$

Substituting (9.20) into (9.18) yields

$$\begin{vmatrix} \lambda + \|\mathbf{u}_r^H \mathbf{H}_{ir} \mathbf{H}_{si}\|^2 P_s & 0 \cdots 0 \\ 0 & \lambda \cdots 0 \\ \vdots & \vdots \ddots \vdots \\ 0 & 0 \cdots \lambda \end{vmatrix}_{N \times N} = 0, \tag{9.21}$$

which is expanded as follows

$$\lambda^N + \|\mathbf{u}_r^H \mathbf{H}_{ir} \mathbf{H}_{si}\|^2 P_s \lambda^{N-1} = 0, \tag{9.22}$$

which forms the set of candidate solutions

$$\lambda \in \{0, -\|\mathbf{u}_r^H \mathbf{H}_{ir} \mathbf{H}_{si}\|^2 P_s\}. \tag{9.23}$$

Plugging (9.23) into (9.13), we find that $\lambda = -\|\mathbf{u}_r^H \mathbf{H}_{ir} \mathbf{H}_{si}\|^2 P_s$ is not suitable for (9.13). Inserting $\lambda = 0$ back into (9.13) yields the following solution

$$\theta_{1i} = -\arg\{(\mathbf{H}_{si}^H \mathbf{H}_{ir}^H \mathbf{u}_r \mathbf{u}_r^H \mathbf{H}_{ir} \mathbf{H}_{si})^\dagger (\mathbf{H}_{si}^H \mathbf{H}_{ir}^H \mathbf{u}_r \mathbf{u}_r^H \mathbf{h}_{sr})\}_i. \tag{9.24}$$

And then by fixing $\mathbf{\Theta}_1$, the optimization problem in (9.9) can be converted into

$$\begin{aligned} \max_{\mathbf{u}_r^H} \quad & P_s \mathrm{tr}(\mathbf{u}_r^H \mathbf{B} \mathbf{u}_r) \\ \text{s.t.} \quad & \|\mathbf{u}_r^H\|^2 = 1, \end{aligned} \tag{9.25}$$

where

$$\mathbf{B} = (\mathbf{h}_{sr} + \mathbf{H}_{ir} \mathbf{\Theta}_1 \mathbf{h}_{si})(\mathbf{h}_{sr} + \mathbf{H}_{ir} \mathbf{\Theta}_1 \mathbf{h}_{si})^H, \tag{9.26}$$

is a Hermitian symmetric matrix. Similar to (9.11), we have

$$L(\mathbf{u}_r, \mu) = P_s \mathrm{tr}(\mathbf{u}_r^H \mathbf{B} \mathbf{u}_r) + \mu(\|\mathbf{u}_r^H\|^2 - 1), \tag{9.27}$$

where μ denotes the Lagrange multiplier. Setting the partial derivative of the Lagrange function $L(\mathbf{u}_r, \mu)$ with respect to $\mathbf{u}_r$ equals 0, we have

$$P_s \mathbf{B}\mathbf{u}_r + \mu \mathbf{u}_r = 0. \tag{9.28}$$

Similar to (9.16), rank($\mathbf{B}$)= 1, so there is a nonzero eigenvalue in $\mathbf{B}$. It indicates that $\mathbf{u}_r$ is the eigenvector corresponding to the nonzero eigenvalue of the matrix $\mathbf{B}$. Similar to (9.19), we obtain the solution

$$\mathbf{u}_r = \frac{\mathbf{h}_{sr} + \mathbf{H}_{ir}\boldsymbol{\Theta}_1\mathbf{h}_{si}}{\|\mathbf{h}_{sr} + \mathbf{H}_{ir}\boldsymbol{\Theta}_1\mathbf{h}_{si}\|}. \tag{9.29}$$

It can be observed that when one of the optimization variables $\boldsymbol{\Theta}_1$ and $\mathbf{u}_r^H$ is fixed, the objective function in (9.9) is convex with respect to the other variable, in each iteration the objective function value monotonically increases with a finite upper-bound. Therefore, it can be guaranteed that the alternately iterative (AI) algorithm is convergent. AI between θ_{1i} and $\mathbf{u}_r$ are performed until the condition of convergence is reached. When θ_{1i} and $\mathbf{u}_r$ are optimal, the R_r in (9.3) is maximized. The proposed alternate iteration algorithm for obtaining an optimal solution R_r is summarized in Algorithm 1. According to (9.8), we make a comparison between

Algorithm 1 Proposed alternate iteration algorithm

1. Initialize the receive beamforming $\mathbf{u}_r^1$, set the convergence error ε and the iteration number t = 1.
2. **repeat**
3. Solve (9.10) for a given $\mathbf{u}_r^t$, denote the optimal solution as $\boldsymbol{\theta}_1^t$ and θ_{1i}^t.
4. Solve (9.25) for a given $\boldsymbol{\theta}_1^t$, denote the optimal solution as $\mathbf{u}_r^{t+1}$.
5. Update $t = t+1$.
6. **until**

$\left|R_r^{t+1} - R_r^t\right| \leq \varepsilon$.

R_r and R_d, and multiply the minimum value by 1/2 to obtain the system rate R_s. The total complexity of proposed AIS-based Max-RP method is obtained as follows

$$\begin{aligned} &O\{L_2(N^4 + 8MN^3 + 5N^3 + 24MN^2 - 2N^2) + (3L_1 + 18L_2)MN \\ &\quad + (5L_1 + 2L_2)M + (4L_1 + 3L_2)N\}, \end{aligned} \tag{9.30}$$

where L_1 and L_2 are the AI numbers in the first time slot and the second time slot, respectively. Obviously, the highest order of computational complexity is N^4 float-point operations (FLOPs), which is high. So a low-complexity NSP-based Max-RP plus MRC method is proposed to reduce the computational complexity in the next subsection.

9.3.2 Proposed NSP-Based Max-RP Plus MRC Method

Considering the two signals from IRS and source node overlap together and interfere with each other, in order to explore the two-way diversity gain, two individual receiving beamforming vectors at RS are used to separate them respectively and MRC is used to combine them to exploit the multiple diversities. After beamforming, the received signals at RS are rewritten by

$$y_{rs} = \sqrt{P_s}\mathbf{u}_{rs}^H\mathbf{h}_{sr}s + \sqrt{P_s}\mathbf{u}_{rs}^H\mathbf{H}_{ir}\boldsymbol{\Theta}_1\mathbf{h}_{si}s + \mathbf{u}_{rs}^H\mathbf{n}_r, \tag{9.31}$$

$$y_{ri} = \sqrt{P_s}\mathbf{u}_{ri}^H\mathbf{h}_{sr}s + \sqrt{P_s}\mathbf{u}_{ri}^H\mathbf{H}_{ir}\boldsymbol{\Theta}_1\mathbf{h}_{si}s + \mathbf{u}_{ri}^H\mathbf{n}_r, \tag{9.32}$$

where $\mathbf{u}_{rs}^H \in \mathbb{C}^{1\times M}$ and $\mathbf{u}_{ri}^H \in \mathbb{C}^{1\times M}$ are defined as the beamforming vectors for S and IRS, respectively, which extract the independent signals from S and IRS, respectively. $\|\mathbf{u}_{rs}^H\|^2 = 1$ and $\|\mathbf{u}_{ri}^H\|^2 = 1$. We assume that $\mathbf{u}_{rs}^H$ and $\mathbf{u}_{ri}^H$ are in the null-space of channel $\mathbf{H}_{ir}$ and $\mathbf{h}_{sr}$, respectively. It is obvious that

$$\mathbf{u}_{rs}^H\mathbf{H}_{ir} = \mathbf{0}^T,\ \mathbf{u}_{ri}^H\mathbf{h}_{sr} = 0, \tag{9.33}$$

which mean that the signals from S and IRS do not interfere with each other at RS. Correspondingly, (9.31) and (9.32) are reduced to

$$y_{rs} = \sqrt{P_s}\mathbf{u}_{rs}^H\mathbf{h}_{sr}s + \mathbf{u}_{rs}^H\mathbf{n}_r, \tag{9.34}$$

$$y_{ri} = \sqrt{P_s}\mathbf{u}_{ri}^H\mathbf{H}_{ir}\boldsymbol{\Theta}_1\mathbf{h}_{si}s + \mathbf{u}_{ri}^H\mathbf{n}_r. \tag{9.35}$$

Maximizing R_r is equal to maximizing the power of y_{rs} and y_{ri}, respectively. The corresponding optimization problem of the power of y_{rs} is given by

$$\begin{aligned} \max_{\mathbf{u}_{rs}^H} \quad & P_s\mathrm{tr}(\mathbf{u}_{rs}^H\mathbf{h}_{sr}\mathbf{h}_{sr}^H\mathbf{u}_{rs}) \\ \text{s.t.} \quad & \|\mathbf{u}_{rs}^H\|^2 = 1,\ \mathbf{u}_{rs}^H\mathbf{H}_{ir} = \mathbf{0}^T. \end{aligned} \tag{9.36}$$

According to the second constraint of the above optimization problem, let us define $\mathbf{u}_{rs}$ as follows

$$\mathbf{u}_{rs} = (\mathbf{I}_M - \mathbf{H}_{ir}(\mathbf{H}_{ir}^H\mathbf{H}_{ir})^\dagger\mathbf{H}_{ir}^H)\mathbf{v}_{rs} = \mathbf{P}\mathbf{v}_{rs}, \tag{9.37}$$

where $\mathbf{P} = \mathbf{I}_M - \mathbf{H}_{ir}(\mathbf{H}_{ir}^H\mathbf{H}_{ir})^\dagger\mathbf{H}_{ir}^H$, $\mathbf{v}_{rs}$ is a new variable and $\|\mathbf{v}_{rs}\| = 1$. Inserting the above equation back into (9.36), we obtain the simplified optimization problem as follows

$$\max_{\mathbf{v}_{rs}^H} \quad P_s\mathbf{v}_{rs}^H\mathbf{P}^H\mathbf{h}_{sr}\mathbf{h}_{sr}^H\mathbf{P}\mathbf{v}_{rs}$$

$$\text{s.t.} \qquad \|\mathbf{v}_{rs}\|^2 = 1. \tag{9.38}$$

Similar to (9.25), the solution $\mathbf{v}_{rs}$ is given by

$$\mathbf{v}_{rs} = \frac{\mathbf{P}^H \mathbf{h}_{sr}}{\|\mathbf{P}^H \mathbf{h}_{sr}\|}, \tag{9.39}$$

which yields

$$\mathbf{u}_{rs} = \frac{\mathbf{P}\mathbf{v}_{rs}}{\|\mathbf{P}\mathbf{v}_{rs}\|} = \frac{(\mathbf{I}_M - \mathbf{H}_{ir}(\mathbf{H}_{ir}^H \mathbf{H}_{ir})^{\dagger}\mathbf{H}_{ir}^H)^2 \mathbf{h}_{sr}}{\|(\mathbf{I}_M - \mathbf{H}_{ir}(\mathbf{H}_{ir}^H \mathbf{H}_{ir})^{\dagger}\mathbf{H}_{ir}^H)^2 \mathbf{h}_{sr}\|}. \tag{9.40}$$

In the same manner, the optimization problem of the power of y_{ri} is also written by

$$\begin{aligned} &\max_{\mathbf{u}_{ri}^H, \boldsymbol{\theta}_1} \quad P_s \text{tr}(\mathbf{u}_{ri}^H \mathbf{H}_{ir} \mathbf{H}_{si} \boldsymbol{\theta}_1 \boldsymbol{\theta}_1^H \mathbf{H}_{si}^H \mathbf{H}_{ir}^H \mathbf{u}_{ri}) \\ &\text{s.t.} \qquad \|\mathbf{u}_{ri}^H\|^2 = 1,\ \mathbf{u}_{ri}^H \mathbf{h}_{sr} = 0,\ \boldsymbol{\theta}_1^H \boldsymbol{\theta}_1 = N. \end{aligned} \tag{9.41}$$

For a given $\mathbf{u}_{ri}$, the solution θ_{1i} can be expressed as

$$\theta_{1i} = -\arg\{\mathbf{H}_{si}^H \mathbf{H}_{ir}^H \mathbf{u}_{ri}\}_i. \tag{9.42}$$

For a given $\boldsymbol{\theta}_1$, the solution $\mathbf{u}_{ri}$ can be represented as

$$\mathbf{u}_{ri} = \frac{(\mathbf{I}_M - \mathbf{h}_{sr}(\mathbf{h}_{sr}^H \mathbf{h}_{sr})^{\dagger}\mathbf{h}_{sr}^H)^2 \mathbf{H}_{ir}\mathbf{H}_{si}\boldsymbol{\theta}_1}{\|(\mathbf{I}_M - \mathbf{h}_{sr}(\mathbf{h}_{sr}^H \mathbf{h}_{sr})^{\dagger}\mathbf{h}_{sr}^H)^2 \mathbf{H}_{ir}\mathbf{H}_{si}\boldsymbol{\theta}_1\|}. \tag{9.43}$$

Similar to Algorithm 1, $\mathbf{u}_{ri}$ and $\boldsymbol{\theta}_1$ are performed via AI procedure to obtain the maximum power of y_{ri}. Then the joint received signal at RS by applying MRC can be expressed as

$$\begin{aligned} y_r &= \frac{(\mathbf{u}_{rs}^H \mathbf{h}_{sr})^H y_{rs} + (\mathbf{u}_{ri}^H \mathbf{H}_{ir}\mathbf{H}_{si}\boldsymbol{\theta}_1)^H y_{ri}}{\|\mathbf{u}_{rs}^H \mathbf{h}_{sr} + \mathbf{u}_{ri}^H \mathbf{H}_{ir}\mathbf{H}_{si}\boldsymbol{\theta}_1\|} \\ &= \sqrt{P_s}\left(\frac{\mathbf{h}_{sr}^H \mathbf{u}_{rs}\mathbf{u}_{rs}^H \mathbf{h}_{sr} + \boldsymbol{\theta}_1^H \mathbf{H}_{si}^H \mathbf{H}_{ir}^H \mathbf{u}_{ri}\mathbf{u}_{ri}^H \mathbf{H}_{ir}\mathbf{H}_{si}\boldsymbol{\theta}_1}{\|\mathbf{u}_{rs}^H \mathbf{h}_{sr} + \mathbf{u}_{ri}^H \mathbf{H}_{ir}\mathbf{H}_{si}\boldsymbol{\theta}_1\|}\right) s \\ &\quad + \left(\frac{\mathbf{h}_{sr}^H \mathbf{u}_{rs}\mathbf{u}_{rs}^H + \boldsymbol{\theta}_1^H \mathbf{H}_{si}^H \mathbf{H}_{ir}^H \mathbf{u}_{ri}\mathbf{u}_{ri}^H}{\|\mathbf{u}_{rs}^H \mathbf{h}_{sr} + \mathbf{u}_{ri}^H \mathbf{H}_{ir}\mathbf{H}_{si}\boldsymbol{\theta}_1\|}\right) \mathbf{n}_r. \end{aligned} \tag{9.44}$$

The signals from S and IRS received by RS are independent, thus the achievable rate at RS can be calculated as

$$R_r = \log_2\left(1 + \frac{(\|\mathbf{u}_{rs}^H \mathbf{h}_{sr}\|^4 + \|\mathbf{u}_{ri}^H \mathbf{H}_{ir}\mathbf{H}_{si}\boldsymbol{\theta}_1\|^4)P_s}{\|\mathbf{u}_{rs}^H \mathbf{h}_{sr} + \mathbf{u}_{ri}^H \mathbf{H}_{ir}\mathbf{H}_{si}\boldsymbol{\theta}_1\|^2\sigma_r^2}\right). \tag{9.45}$$

Compare R_r and R_d to obtain the system rate R_s. The complexity of the proposed NSP-based Max-RP plus MRC method is written by

$$\begin{aligned} &O\{N^3 + 2(1+L_3)M^3 + 2(1+L_3)M^2N + (4+3L_3)MN^2 \\ &+ (4+3L_3)M^2 - L_3N^2 - (1-5L_3-18L_4)MN - (1-4L_3-2L_4)M \\ &+ (1+2L_3+3L_4)N\}, \end{aligned} \tag{9.46}$$

where L_3 and L_4 respectively denote the AI numbers in the first time slot and the second time slot. The highest order of complexity is N^3 FLOPs, which is lower than AIS-based Max-RP Method and still very high. To further reduce the computational complexity, an IRSES-based Max-RP plus MRC method is proposed in the following subsection.

9.3.3 *Proposed IRSES-Based Max-RP Plus MRC Method*

As shown in Fig. 9.2, according to the number M of RS antennas, the N elements in IRS are randomly divided into M suarrays evenly, each of which is mapped into one antenna at RS with $\frac{N}{M} = K$ elements. Figure 9.3 is the block diagram for IRSES-based Max-RP plus MRC method at RS, the details are described as below.

A subarray denoted as $\mathcal{E}_{I,m}$ is randomly chosen to reflect the signal from S to antenna m of RS, $\mathcal{E}_{I,m} = \{1_m, 2_m, \cdots, K_m\}$. Let $\mathcal{E}_I = \mathcal{E}_{I,1} \cup \mathcal{E}_{I,2} \cdots \cup \mathcal{E}_{I,M}$ be the subarray set. $\mathcal{E}_{I,1}, \mathcal{E}_{I,2}, \cdots, \mathcal{E}_{I,M}$ is a partition of set $\mathcal{E}_I$, and $\mathcal{E}_{I,m} \cap \mathcal{E}_{I,n} = \Phi$, where $m, n \in \{1, 2, \cdots, M\}$. The remaining subsets are denoted as $\mathcal{E}_{I,-m}$, and $\mathcal{E}_I =$

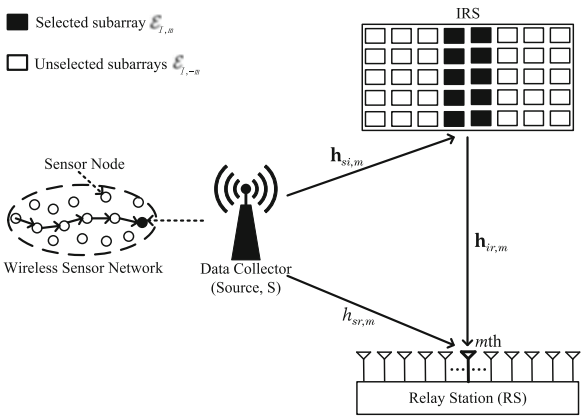


Fig. 9.2 System model for IRSES-based Max-RP plus MRC method in the first time slot

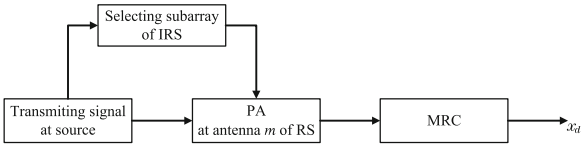


Fig. 9.3 Block diagram for IRSES-based Max-RP plus MRC method

$\mathcal{E}_{I,m} \cup \mathcal{E}_{I,-m}$. The received signal of antenna m at RS can be written by

$$y_{r,m} = \sqrt{P_s}(h_{sr,m} + \mathbf{h}_{ir,m}\boldsymbol{\Theta}_{1,m}\mathbf{h}_{si,m})s + \sqrt{P_s}\mathbf{h}_{ir,-m}\boldsymbol{\Theta}_{1,-m}\mathbf{h}_{si,-m}s + n_{r,m}, \tag{9.47}$$

where $h_{sr,m} \in \mathbb{C}^{1\times 1}$ is the mth element of $\mathbf{h}_{sr}$, $\mathbf{h}_{ir,m} \in \mathbb{C}^{1\times K}$ denotes the channel from the selected subset $\mathcal{E}_{I,m}$ to antenna m at RS, and includes K elements which are determined by $\mathcal{E}_{I,m}$ in the mth row of $\mathbf{H}_{ir}$. $\mathbf{h}_{si,m} \in \mathbb{C}^{K\times 1}$ represents the channel from S to $\mathcal{E}_{I,m}$ and also consists of K elements decided by $\mathcal{E}_{I,m}$ in K rows of $\mathbf{h}_{si}$. The diagonal reflection-coefficient matrix of elements in $\mathcal{E}_{I,m}$ is denoted as $\boldsymbol{\Theta}_{1,m} = \text{diag}(e^{j\theta_{1,m}(1)}, \cdots, e^{j\theta_{1,m}(K)})$. $\mathbf{h}_{ir,-m} \in \mathbb{C}^{1\times(N-K)}$ is the channel from the unselected subset $\mathcal{E}_{I,-m}$ to antenna m at RS, $\mathbf{h}_{si,-m} \in \mathbb{C}^{(N-K)\times 1}$ is the channel from S to $\mathcal{E}_{I,-m}$. $\boldsymbol{\Theta}_{1,-m}$ is the diagonal reflection-coefficient matrix of elements in $\mathcal{E}_{I,-m}$, which can be expressed as $\boldsymbol{\Theta}_{1,-m} = \text{diag}(e^{j\theta_{1,-m}(1)}, \cdots, e^{j\theta_{1,-m}(N-K)})$. $n_{r,m}$ is the AWGN with the distribution of $n_{r,m} \sim \mathcal{CN}\left(0, \sigma_{r,m}^2\right)$. While according to law of large numbers, the signals reflected by the unselected subset $\mathcal{E}_{I,-m}$ overlap to zero at antenna m. Equation (9.47) is simplified and expanded as follows

$$\begin{aligned} y_{r,m} &= \sqrt{P_s}(h_{sr,m} + \mathbf{h}_{ir,m}\boldsymbol{\Theta}_{1,m}\mathbf{h}_{si,m})s + n_{r,m} \\ &= \sqrt{P_s}\left(h_{sr,m} + \sum_{i=1}^{K}\mathbf{h}_{ir,m}(i)\boldsymbol{\Theta}_{1,m}(i,i)\mathbf{h}_{si,m}(i)\right)s + n_{r,m}, \end{aligned} \tag{9.48}$$

where $\mathbf{h}_{ir,m}(i)$ and $\mathbf{h}_{si,m}(i)$ are the ith element of $\mathbf{h}_{ir,m}$ and $\mathbf{h}_{si,m}$, respectively. $\boldsymbol{\Theta}_{1,m}(i,i)$ is the ith element in diagonal of $\boldsymbol{\Theta}_{1,m}$. The phases of K elements in $\mathcal{E}_{I,m}$ are adjusted to make the phases of all reflected signals and the direct signal from S aligned at antenna m of RS. So as to maximize the power of the signal received by antenna m for obtaining better rate performance. Thus, the corresponding phase shift of the ith element is calculated as

$$\theta_{1,m}(i) = \arg(h_{sr,m}) - \arg(\mathbf{h}_{ir,m}(i)) - \arg(\mathbf{h}_{si,m}(i)). \tag{9.49}$$

Finally, MRC is adopted to combine all received signals at RS, the received signal can be expressed as follows

$$y_r = [u_{r,1}, u_{r,2}, \cdots, u_{r,M}][y_{r,1}, y_{r,2}, \cdots, y_{r,M}]^T, \tag{9.50}$$

where

$$u_{r,m} = \frac{(h_{sr,m} + \mathbf{h}_{ir,m}\boldsymbol{\Theta}_{1,m}\mathbf{h}_{si,m})^H}{\|h_{sr,m} + \mathbf{h}_{ir,m}\boldsymbol{\Theta}_{1,m}\mathbf{h}_{si,m}\|}. \tag{9.51}$$

The achievable rate at RS can be represented as

$$R_r = \log_2\left(1 + \frac{\sum_{m=1}^{M} \|h_{sr,m} + \mathbf{h}_{ir,m}\boldsymbol{\Theta}_{1,m}\mathbf{h}_{si,m}\|^4 P_s}{\sum_{m=1}^{M} \|h_{sr,m} + \mathbf{h}_{ir,m}\boldsymbol{\Theta}_{1,m}\mathbf{h}_{si,m}\|^2 \sigma_{r,m}^2}\right). \tag{9.52}$$

Further, taking the minimum of R_r and R_d to obtain achievable rate R_s. The complexity of the proposed IRSES-based Max-RP plus MRC method is given by

$$O\{15MK + 8M + 10K + L_5(18MN + 2M + 3N)\}, \tag{9.53}$$

where L_5 is the AI number in the second time slot. It can be seen that the highest order of complexity is MN FLOPs, which is much lower than the above two methods. Especially in massive IRS scenario, the gap among the complexity of the proposed three methods is more obvious.

9.4 Numerical Results

In this section, numerical simulations are performed to evaluate and compare the rate performance between an IRS-aided multi-antenna DF relay network and that with single-antenna RS in [26]. Additionally, it is assumed that IRS and RS are deployed with the same abscissas, the positions of S, RS, IRS, and D are given as (0,0), (50 m,0), (50 m,10 m) and (100 m,0), respectively. The amplitude attenuation of the received signal is $(d)^{-(\frac{\alpha}{2})}$ caused by path loss, where d is the distance between transmitter and receiver, and α is the path-loss exponent. The antenna gains at S, RS and D are 5 dBi, 5 dBi, and 2 dBi, respectively. System parameters are set as follows: $P_s = P_r = 10$ dBW, $\alpha = 2.4$, and $\sigma_d^2 = \sigma_r^2 = \sigma_w^2$. SNR is defined as $(P_s + P_r)/\sigma_w^2$.

Figure 9.4 shows the achievable rate versus the number of iterations with $M = 50$ and $N = 50$ in the first time slot. It is obvious that the proposed AIS-based Max-RP and NSP-based Max-RP plus MRC methods require about only three iterations to achieve the rate ceil.

Figure 9.5 plots the curves of computational complexity versus N with $M = 50$. It demonstrates that the computational complexities of the proposed three methods, AIS-based Max-RP, NSP-based Max-RP plus MRC, and IRSES-based Max-RP plus MRC, increase as N increases. Clearly, the first and third methods have the highest and lowest computational complexities, respectively. The second one is in between them.

Figure 9.6 shows the curves of achievable rate versus SNR with $M = 16$ and $N = 160$. It is clear that the rate performance of the proposed three methods with fixed IRS phases (i.e., $\boldsymbol{\Theta} = \mathbf{I}$) to eliminate the impact of IRS elements on the performance

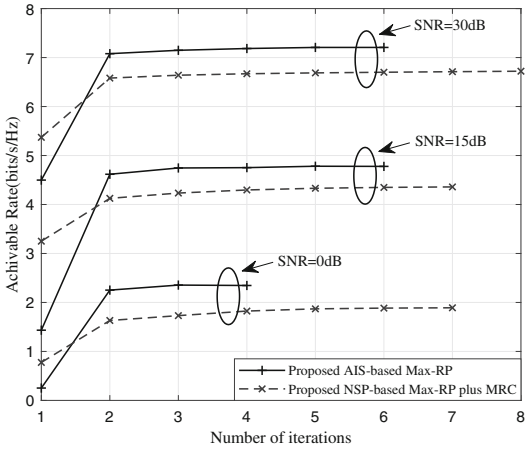


Fig. 9.4 Convergence of proposed methods with M = 50 and N = 50

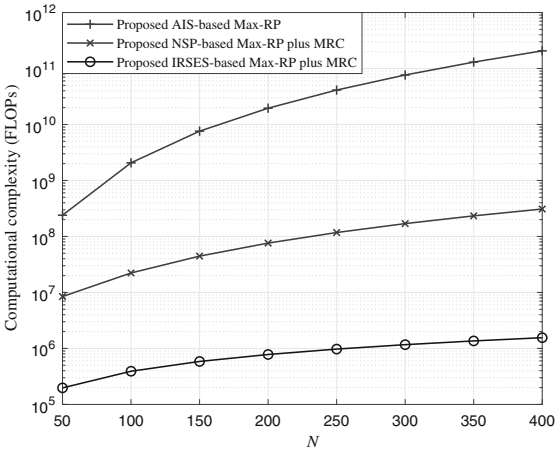


Fig. 9.5 Computational complexity versus N with M = 50

is more than 5.24 bits/s/Hz, which is 25.6% higher than that of the existing system with an IRS and a single-antenna relay in [26]. Compared to the above methods with $\boldsymbol{\Theta} = \mathbf{I}$, the performance of the proposed three methods with joint RS active beamforming and IRS passive beamforming can approximately harvest up to 25.1% rate gain. Therefore, it is verified that the rate gain results from the increased number of antennas at RS and from the joint RS active beamforming and IRS passive beamforming.

Figure 9.7 illustrates the curves of achievable rate versus SNR with M = 50 and N = 200. It can be seen that the proposed methods make a significant performance improvement over that with single-antenna RS in [26]. For example, when SNR equals 30 dB, the proposed worst method, IRSES-based Max-RP plus MRC, can harvest up to 78.6% rate gain over that method in [26]. The best method AIS-based Max-RP approximately has a 80.8% rate gain over that in [26]. This shows that as

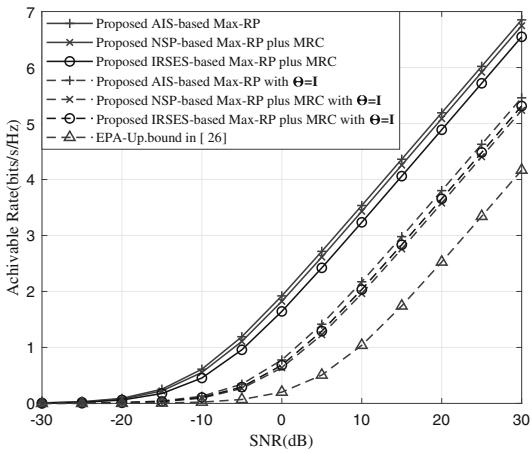


Fig. 9.6 Achievable rate versus SNR with $M = 16$ and $N = 160$

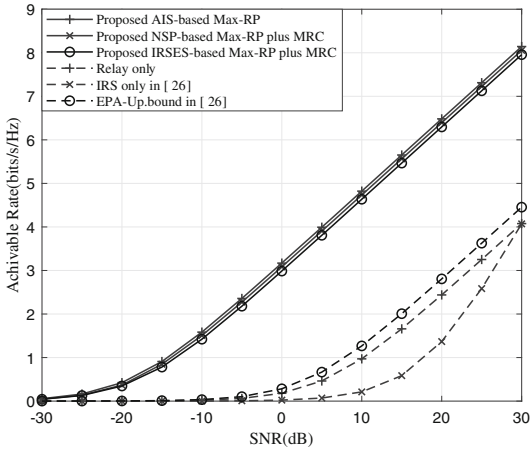


Fig. 9.7 Achievable rate versus SNR with $M = 50$ and $N = 200$

SNR increases, significant rate gains are achieved for the proposed network with IRS plus multi-antenna RS.

Figure 9.8 demonstrates the achievable rate versus the number N of reflecting elements at IRS. It is observed that the proposed three methods still outperform the method with single-antenna RS in [26]. For small-scale and medium-scale IRS, the proposed three methods have the following increasing order on rate as follows: NSP-based Max-RP plus MRC, AIS-based Max-RP and IRSES-based Max-RP plus MRC. As the number of elements at IRS goes to a large-scale, their order are becomes as follows: IRSES-based Max-RP plus MRC, NSP-based Max-RP plus MRC and AIS-based Max-RP.

Figure 9.9 shows the curves of achievable rate versus M with $N = 200$ and SNR = 30 dB. It can be seen that as the number M of antennas at RS increases, the rate performance increases. The proposed three methods: AIS-based Max-RP, NSP-based Max-RP plus MRC and IRSES-based Max-RP plus MRC have harvested

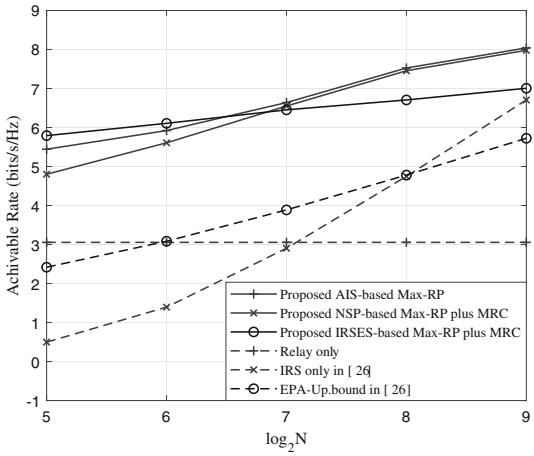


Fig. 9.8 Achievable rate versus N with $M = 16$ and SNR = 30 dB

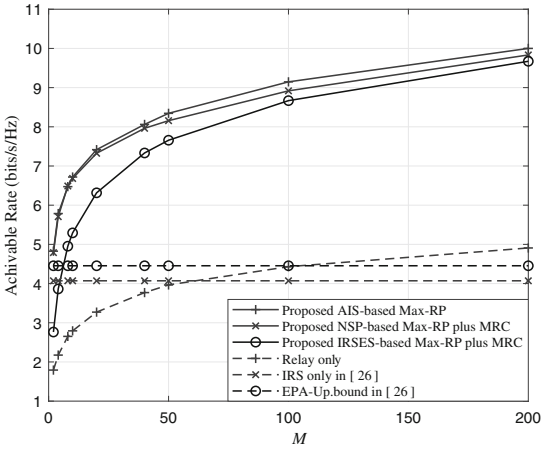


Fig. 9.9 Achievable rate versus M with $N = 200$ and SNR = 30 dB

significant rate performance gains over that in [26], IRS-only-aided network and relay-only-aided network.

In order to observe the effect of positions of IRS and RS on rate performance, Fig. 9.10 shows how to move both IRS and RS, where IRS and RS move toward D together along the direction parallel to the line segment SD with d denoting the horizontal distance from S to IRS and RS. Figure 9.11 plots the corresponding curves of achievable rate versus d with $M = 50$, $N = 200$ and SNR = 30 dB. When $d = 30$ m, the proposed three methods can achieve their largest rate peak. While $d > 30$ m, the rate performance degrades gradually. Regardless of d, the proposed three methods: AIS-based Max-RP, NSP-based Max-RP plus MRC and IRSES-based Max-RP plus MRC still perform much better than that in [26], IRS-only-aided network and relay-only-aided network in terms of rate performance.

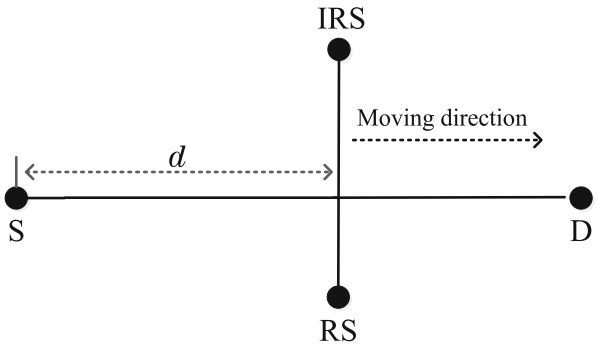
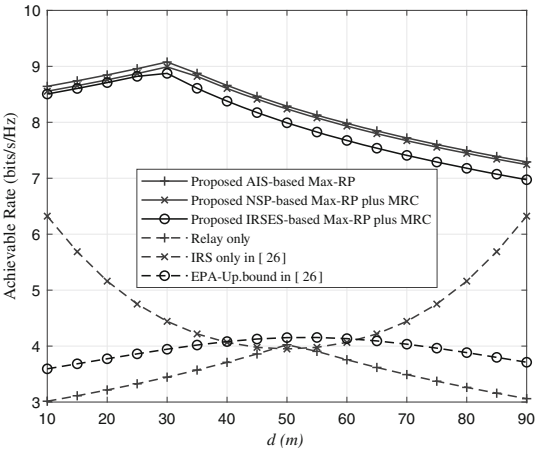


Fig. 9.10 How to move IRS and RS

Fig. 9.11 Achievable rate versus distance with $M = 50$, $N = 200$ and SNR = 30 dB



9.5 Conclusion

In this book chapter, we have made an investigation on an IRS-aided DF relay network with multi-antenna at RS. In order to improve the rate performance, three high-performance schemes, namely AIS-based Max-RP, NSP-based Max-RP plus MRC and IRSES-based Max-RP plus MRC, were proposed. The third method is very attractive due to its low-complexity and excellent rate performance for small and medium-scale IRSs. Simulation results show that the proposed three methods can approximately harvest up to 85% rate gain over existing network with single-antenna RS in almost all SNR regions. Thus, an IRS-aided multi-antenna relay network will provide an enhanced network performance and extended network coverage for the future mobile communications, WSN, and internet of things.

References

1. Huang, P., Hao, Y., Lv, T., Xing, J., Yang, J., Mathiopoulos, P.T.: Secure beamforming design in relay-assisted Internet of Things. IEEE Internet Things J. **6**(4), 6453–6464 (2019)
2. Yilmaz, E., Zakhour, R., Gesbert, D., Knopp, R.: Multi-pair two-way relay channel with multiple antenna relay station. In: Proceedings of the IEEE International Conference on Communications (ICC), pp. 1–5 (2010)
3. Farhadi, G., Beaulieu, N.C.: On the ergodic capacity of multi-hop wireless relaying systems. IEEE Trans. Commun. **8**(5), 2286–2291 (2009)
4. Gu, Q., Wu, D., Su, X., Jin, J., Yuan, Y., Wang, J.: Performance comparison between reconfigurable intelligent surface and relays: theoretical methods and a perspective from operator (2021). Available via arXiv. https://arxiv.org/abs/2101.12091
5. Wu, Q., Zhang, R.: Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network. IEEE Commun. **58**(1), 106–112 (2020)
6. Hua, M., Wu, Q.: Joint dynamic passive beamforming and resource allocation for IRS-aided full-duplex WPCN (2021). Available via arXiv. https://arxiv.org/abs/2108.06660
7. Liang, Y., Chen, J., Long, R., He, Z., Lin, X., Huang, C., Liu, S., Shen, X., Renzo, M.D.: Reconfigurable intelligent surfaces for smart wireless environments: channel estimation, system design and applications in 6G networks. Sci. China Inf. Sci. **64**(10), 1–21 (2021)
8. Wang, H., Bai, J., Dong, L.: Intelligent reflecting surfaces assisted secure transmission without eavesdropper's CSI. IEEE Signal Process. Lett. **27**, 1300–1304 (2020)
9. Basar, E., Di Renzo, M., De Rosny, J., Debbah, M., Alouini, M.S., Zhang, R.: Wireless communications through reconfigurable intelligent surfaces. IEEE Access. **7**, 116753–116773 (2019)
10. Shu, F., Teng, Y., Li, J., Huang, M., Shi, W., Li, J., Wu, Y., Wang, J.: Enhanced secrecy rate maximization for directional modulation networks via IRS. IEEE Trans. Commun. **69**(12), 8388–8401 (2021)
11. Lai, L., Hu, J., Chen, Y., Zheng, H., Yang, N.: Directional modulation-enabled secure transmission with intelligent reflecting surface. In: Proceedings of the IEEE 3rd International Conference on Information Communication and Signal Processing (ICICSP), pp. 450–453 (2020)
12. Shu, F., Yang, L., Jiang, X., Cai, W., Shi, W., Huang, M., Wu, Y., Wang, J., You, X.: Beamforming and transmit power design for intelligent reconfigurable surface-aided secure spatial modulation. IEEE J. Sel. Topics Signal Process. **16**(5), 933–949 (2022)
13. Luo, S., Yang, P., Che, Y., Yang, K., Wu, K., Teh, K.C., Li, S.: Spatial modulation for RIS-assisted uplink communication: joint power allocation and passive beamforming design. IEEE Trans. Commun. **69**(10), 7017–7031 (2021)
14. Shi, W., Li, J., Xia, G., Wang, Y., Zhou, X., Zhang, Y., Shu, F.: Secure multigroup multicast communication systems via intelligent reflecting surface. China Commun. **18**(3), 39–51 (2021)
15. Hua, M., Wu, Q., Ng, D.W.K., Zhao, J., Yang, L.: Intelligent reflecting surface-aided joint processing coordinated multipoint transmission. IEEE Trans. Commun. **69**(3), 1650–1665 (2021)
16. Zhou, X., Yan, S., Wu, Q., Shu, F., Ng, D.W.K.: Intelligent reflecting surface (IRS)-aided covert wireless communications with delay constraint. IEEE Trans. Wirel. Commun. **21**(1), 532–547 (2022)
17. Lu, X., Hossain, E., Shafique, T., Feng, S., Jiang, H., Niyato, D.: Intelligent reflecting surface enabled covert communications in wireless networks. IEEE Netw. **34**(5), 148–155 (2020)
18. Pan, Y., Wang, K., Pan, C., Zhu, H., Wang, J.: UAV-assisted and intelligent reflecting surfaces-supported terahertz communications. IEEE Wirel. Commun. Lett. **10**(6), 1256–1260 (2021)
19. Wei, Z., Cai, Y., Sun, Z., Ng, D.W.K., Yuan, J., Zhou, M., Sun, L.: Sum-rate maximization for IRS-assisted UAV OFDMA communication systems. IEEE Trans. Wirel. Commun. **20**(4), 2530–2550 (2021)

20. Wu, Q., Zhang, R.: Weighted sum power maximization for intelligent reflecting surface aided SWIPT. IEEE Wirel. Commun. Lett. **9**(5), 586–590 (2020)
21. Shi, W., Zhou, X., Jia, L., Wu, Y., Shu, F., Wang, J.: Enhanced secure wireless information and power transfer via intelligent reflecting surface. IEEE Commun. Lett. **25**(4), 1084–1088 (2021)
22. Obeed, M., Chaaban, A.: Relay–reconfigurable intelligent surface cooperation for energy-efficient multiuser systems. In: Proceedings of the IEEE International Conference on Communications Workshops (ICC Workshops), pp. 1–6 (2021)
23. N. Nguyen, T., Vu, Q.D., Lee, K., Juntti, M.: Spectral efficiency optimization for hybrid relay-reflecting intelligent surface. In: Proceedings of the IEEE International Conference on Communications Workshops (ICC Workshops), pp. 1–6 (2021)
24. Yildirim, I., Kilinc, F., Basar, E., Alexandropoulos, G.C.: Hybrid RIS-empowered reflection and decode-and-forward relaying for coverage extension. IEEE Commun. Lett. **25**(5), 1692–1696 (2021)
25. Ying, X., Demirhan, U., Alkhateeb, A.: Relay aided intelligent reconfigurable surfaces: Achieving the potential without so many antennas (2020). Available via arXiv. https://arxiv.org/abs/2006.06644
26. Abdullah, Z., Chen, G., Lambotharan, S., Chambers, J.A.: A hybrid relay and intelligent reflecting surface network and its ergodic performance analysis. IEEE Wirel. Commun. Lett. **9**(10), 1653–1657 (2020)
27. Xia, G., Lin, Y., Zhou, X., Zhang, W., Shu, F., Wang, J.: Hybrid precoding design for secure generalized spatial modulation with finite-alphabet inputs. IEEE Trans. Commun. **69**(4), 2570–2584 (2021)
28. Wu, Q., Zhang, R.: Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming. IEEE Trans. Wirel. Commun. **18**(11), 5394–5409 (2019)

Chapter 10
Performance Analysis of Wireless Network Aided by Discrete-Phase-Shifter IRS

Discrete phase shifter of IRS generates phase quantization error (QE) and degrades the receive performance at the receiver. To make an analysis of the PL caused by IRS with phase QE, based on the law of large numbers, the closed-form expressions of SNR PL, achievable rate (AR), and bit error rate (BER) are successively derived under LoS channels and Rayleigh channels. Moreover, based on the Taylor series expansion, the approximate simple closed form of PL of IRS with approximate QE is also given. The simulation results show that the performance losses of SNR and AR decrease as the number of quantization bits increases, while they gradually increase with the number of IRS phase shifter elements increases. Regardless of LoS channels or Rayleigh channels, when the number of quantization bits is larger than or equal to 3, the performance losses of SNR and AR are less than 0.23dB and 0.08bits/s/Hz, respectively, and the BER performance degradation is trivial. In particular, the PL difference between IRS with QE and IRS with approximate QE is negligible when the number of quantization bits is not less than 2.

10.1 Introduction

With the rapid development of wireless networks, the demands for high rate, high quality, and ubiquitous wireless services will result in high energy consumption like 5G systems [1]. To achieve an innovative, energy-efficient and low-cost wireless network, IRS has emerged as a new and promising solution. IRS, consisting of a large number of low-cost passive reflective elements integrated on a plane, can significantly enhance the performance of wireless communication networks by intelligently reconfiguring the wireless propagation environment [2–4]. There are heavy research activities on the investigation of various IRS-aided wireless networks [5–15].

F. Shu, J. Wang, *Intelligent Reflecting Surface-Aided Physical-Layer Security*,
Wireless Networks, https://doi.org/10.1007/978-3-031-41812-9_10

Assuming that the LoS channels are employed, the authors in [16] maximized the SR by jointly optimizing IRS phases, and the trajectory and power control of UAV, based on the successive convex approximation, and the SR was significantly improved with the assistance of IRS. In [17], the authors discussed the characteristics of the UAV and IRS, and two cases were investigated by combining UAV and IRS to enhance the network throughput and security. In [18], a secure IRS-aided directional modulation network was investigated, and two alternating iterative algorithms, general alternating iterative and null-space projection, were proposed to maximize the SR. An IRS-assisted downlink multi-user multi-antenna system in the absence of direct links between the BS and user was proposed in [19], a hybrid beamforming scheme with continuous digital beamforming for the BS and discrete analog beamforming for the IRS was proposed to maximize sum-rate. In [20], the phase shifters of multiple IRSs were optimized to maximize rate, based on the least-squares method, the substantial rate gains were achieved compared to the baseline schemes. The problem of joint active and passive beamforming optimization for an IRS-aided downlink multi-user MIMO system was investigated in [21], where a vector approximate message passing algorithm was proposed to optimize the IRS phase shifts. In [22], the transmit covariance matrix and passive beamforming matrices of the two cooperative IRSs were jointly optimized to maximize rate, and a novel low-complexity alternating optimization algorithm was presented.

Actually, there are many works focusing on the beamforming methods and converge analysis in the Rayleigh channels. An IRS-assisted MISO system without eavesdropper's CSI was proposed in [23], in order to enhance the security, the oblique manifold method and minorization-maximization algorithms were proposed to jointly optimize the precoder and IRS phase shift. In [24], the continuous transmit beamforming at the access point (AP) and discrete reflect beamforming at the IRS were jointly optimized to minimize the transmit power at AP. An efficient alternating optimization algorithm was proposed and near-optimal performance was achieved. An IRS-aided secure multigroup multicast MISO communication system was proposed in [25], and the semidefinite relaxation scheme and a low-complexity algorithm based on second-order cone programming were designed to minimize the transmit power. In [26], based on the Arimoto-Blahut algorithm, the source precoders and IRS phase shift matrix in the full-duplex MIMO two-way communication system were optimized to maximize the sum rate. A fast converging alternating algorithm to maximize the sum rate was proposed in [27]. Compared to the algorithm in [26], the proposed algorithm achieved a faster convergence rate and lower computational complexity. In [28], the convergence analysis for an IRS-aided communication network was presented, and the results revealed that the larger coverage could be provided by using IRS. In [29], the authors proposed to invoke an IRS at the cell boundary of multiple cells to assist the downlink transmission to cell-edge users, and the precoding matrices at the BSs and IRS phase shifts were jointly optimized to maximize the weighted sum rate of all users.

For a continuous phase shift IRS-aided network, it is difficult to implement in practice due to a higher circuit cost than that with finite-phase shifters, especially when the number of elements for IRS tends to large scale. Similar to that discrete-

quantized radio frequency phase shifter in directional modulation networks would cause PL in [30–32], using discrete-phase shifters in IRS will also result in substantial PL in IRS-aided wireless network [19, 24, 33]. Choosing a proper number of quantization bits for discrete-phase shifters with a given PL will provide a valuable reference for the future system design. Thus, in what follows, we will present an analysis on impact of discrete-phase shifters on the performance of IRS-aided wireless network system in this book chapter.

In this book chapter, to make an analysis of PL caused by discrete-phase shifters, an IRS-aided wireless network is considered. We assume that all channels are LoS channels. Based on the law of large numbers, the closed-form expressions of SNR PL, AR, and BER are successively derived. Simulation results show that the performance losses of SNR and AR gradually decrease as the number of quantization bits increases, while they gradually increase as the number of IRS phase shifter increases. When the number of quantization bits is equal to 3, the performance losses of SNR and AR are respectively less than 0.23 dB and 0.08 bits/s/Hz, and the BER performance degradation is negligible. In the Rayleigh fading channels, with the weak law of large numbers and the Rayleigh distribution, the closed-form expression of SNR PL is derived while AR and BER with PL are given. In addition, based on the Taylor series expansion, the simple approximate performance loss (APL) expression of SNR is derived whereas AR and BER with APL are given. Simulation results show that the SNR, AR and BER PL tendencies in the Rayleigh channels are similar to those in LoS channels. That is, 3-bit phase shifters are sufficient to achieve an omitted PL. In particular, the approximate simple expression of PL makes a good approximation to the true PL when the number of quantization bits is larger than or equal to 2.

The remainder of this chapter is organized as follows. Section 10.2 describes the system model of a typical IRS-aided three-node wireless network. The performance loss derivations in the LoS and Rayleigh channels are presented in Sects. 10.3 and 10.4, respectively. Numerical simulation results are presented in Sect. 10.5. Finally, we draw conclusions in Sect. 10.6.

Notations Throughout this chapter, boldface lower case and upper case letters represent vectors and matrices, respectively. Signs $(\cdot)^T$, $(\cdot)^H$, $(\cdot)^{-1}$, $\|\cdot\|_2$, and $|\cdot|$ denote the transpose operation, conjugate transpose operation, inverse operation, 2-norm operation, and absolute value operation, respectively. The symbol $\mathbb{C}^{N\times N}$ denotes the space of $N \times N$ complex-valued matrix. The notation $\mathbf{I}_N$ represents the $N \times N$ identity matrix.

10.2 System Model

As shown in Fig. 10.1, an IRS-aided wireless network system is considered. Herein, the base station (Alice) and user (Bob) are equipped with single antenna. The IRS is equipped with M low-cost passive reflecting elements and reflects signal only one

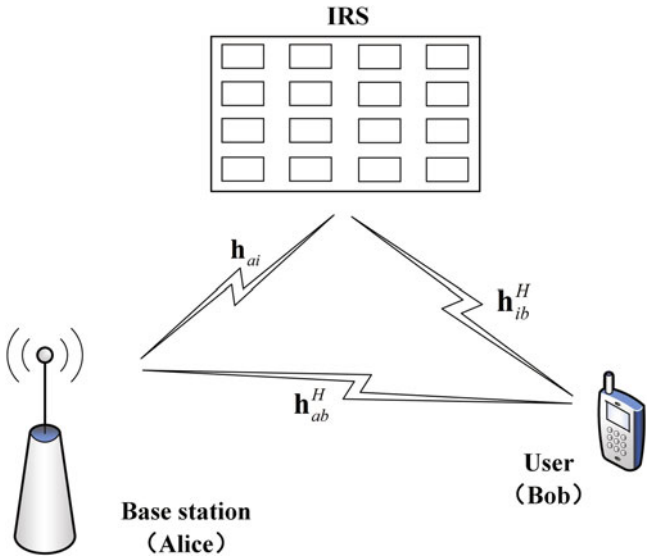


Fig. 10.1 System model of IRS-aided wireless network

time slot. The Alice→IRS, Alice→Bob, and IRS→Bob channels are the LoS or Rayleigh channels.

The transmit signal at Alice is given by

$$s = \sqrt{P_a}x, \tag{10.1}$$

where P_a denotes the total transmit power, x is the confidential message and satisfies $\mathbb{E}[\|x\|^2] = 1$.

Taking the path loss into consideration, the received signal at Bob is

$$\begin{aligned} y_b &= \left(\sqrt{g_{aib}}\mathbf{h}_{ib}^H\mathbf{\Theta}\mathbf{h}_{ai} + \sqrt{g_{ab}}\mathbf{h}_{ab}^H\right)s + n_b \\ &= \left(\sqrt{g_{aib}P_a}\mathbf{h}_{ib}^H\mathbf{\Theta}\mathbf{h}_{ai} + \sqrt{g_{ab}P_a}h_{ab}^H\right)x + n_b, \end{aligned} \tag{10.2}$$

where $g_{aib} = g_{ai}g_{ib}$ represents the equivalent path loss coefficient of Alice→IRS channel and IRS→Bob channel, and g_{ab} is the path loss coefficient of Alice→Bob channel. n_b denotes the additive white Gaussian noise (AWGN) at Bob with the distribution $\mathcal{CN} \sim (0, \sigma^2)$. $\mathbf{\Theta} = \text{diag}\left(e^{j\phi_1}, \cdots, e^{j\phi_m}, \cdots, e^{j\phi_M}\right)$ represents the diagonal reflection coefficient matrix of IRS, where $\phi_m \in [0, 2\pi)$ denotes the phase shift of reflection element m. $\mathbf{h}_{ai} \in \mathbb{C}^{M\times 1}$, $\mathbf{h}_{ab}^H = h_{ab}^H \in \mathbb{C}^{1\times 1}$, and $\mathbf{h}_{ib}^H \in \mathbb{C}^{1\times M}$ are the Alice→IRS, Alice→Bob, and IRS→Bob channels, respectively.

10.3 Performance Loss Derivation and Analysis in the LoS Channels

In this section, it is assumed that all channels are the LoS channels. The use of IRS with discrete phase shifters may lead to phase quantization errors. In what follows, we will make a comprehensive investigation of the impact of IRS with discrete phase shifters on SNR, AR, and BER.

Defining $\mathbf{h}_{ai} = \mathbf{h}(\theta_{ai})$, $\mathbf{h}_{ib} = \mathbf{h}(\theta_{ib})$, the steering vector arrival or departure from IRS is

$$\mathbf{h}(\theta) = \left[e^{j2\pi\Psi_\theta(1)}, \ldots, e^{j2\pi\Psi_\theta(m)}, \ldots, e^{j2\pi\Psi_\theta(M)}\right]^T, \tag{10.3}$$

and the phase function $\Psi_\theta(m)$ is given by

$$\Psi_\theta(m) \triangleq -\frac{(m-(M+1)/2)d\cos\theta}{\lambda}, m = 1, \ldots, M, \tag{10.4}$$

where m denotes the m-th antenna, d is the spacing of adjacent transmitting antennas, θ represents the direction angle of arrival or departure, and λ represents the wavelength.

The receive signal (10.2) can be casted as

$$\begin{aligned} y_b^{LoS} &= \left(\sqrt{g_{aib}P_a}\mathbf{h}^H(\theta_{ib})\boldsymbol{\Theta}\mathbf{h}(\theta_{ai}) + \sqrt{g_{ab}P_a}h_{ab}^H\right)x + n_b \\ &= \sqrt{g_{aib}P_a}\left(\sum_{m=1}^{M} e^{j\left(-2\pi\Psi_{\theta_{ib}}(m)+\phi_m+2\pi\Psi_{\theta_{ai}}(m)\right)}\right)x \\ &\quad + \sqrt{g_{ab}P_a}|h_{ab}|e^{-j\varphi_{ab}}x + n_b \\ &= \sqrt{g_{aib}P_a}e^{-j\varphi_{ab}}\left[\left(\sum_{m=1}^{M} e^{j\left(-2\pi\Psi_{\theta_{ib}}(m)+\phi_m+2\pi\Psi_{\theta_{ai}}(m)+\varphi_{ab}\right)}\right)\right. \\ &\quad \left. + \sqrt{g_{ab}P_a}|h_{ab}|\right]x + n_b, \end{aligned} \tag{10.5}$$

where φ_{ab} is the phase of h_{ab}.

As shown above, considering we only adjust the phases of IRS elements, if all IRS phases are adjusted to have the same phase as that of LoS path, then all $(M+1)$-path signals form a constructive combining at Bob. If the phase shifter at IRS is continuous, and the transmit signal at Alice is forwarded perfectly to Bob by the IRS, the m-th phase shift at IRS can be designed as follows

$$\phi_m = 2\pi\Psi_{\theta_{ib}}(m) - 2\pi\Psi_{\theta_{ai}}(m) - \varphi_{ab}. \tag{10.6}$$

In what follows, for convenience of deriving, φ_{ab} is chosen to be zero. Then (10.5) can be converted to

$$y_b^{LoS} = \sqrt{g_{aib} P_a} M x + \sqrt{g_{ab} P_a} |h_{ab}| x + n_b. \tag{10.7}$$

10.3.1 Derivation of Performance Loss in LoS Channels

Assuming the discrete phase shifters is employed by IRS, and the discrete phases per phase shifters at IRS employs a k-bit phase quantizer, each reflection element's phase feasible set is

$$\Omega = \left\{ \frac{\pi}{2^k}, \frac{3\pi}{2^k}, \cdots, \frac{(2^{k+1}-1)\pi}{2^k} \right\}. \tag{10.8}$$

Assuming that ϕ_m is the desired continuous phase of the m-th element at IRS, and the final discrete phase is chosen from phase feasible set Ω, which is given by

$$\overline{\phi_m} = \arg\min_{\overline{\phi_m} \in \Omega} \| \overline{\phi_m} - \phi_m \|_2. \tag{10.9}$$

In general, $\overline{\phi_m} \neq \phi_m$, which means that phase mismatching may lead to performance loss at Bob. Let us define the m-th phase quantization error at IRS as follows

$$\Delta\phi_m = \overline{\phi_m} - \phi_m. \tag{10.10}$$

It is assumed that the above phase quantization error follows uniform distribution with probability density function (PDF) as follows

$$f(x) = \begin{cases} \frac{1}{2\Delta x}, & x \in [-\Delta x, \Delta x], \\ 0, & \text{otherwise}, \end{cases} \tag{10.11}$$

where

$$\Delta x = \frac{\pi}{2^k}. \tag{10.12}$$

In the presence of phase quantization error, the receive signal (10.2) becomes

$$\begin{aligned} \widehat{y_b}^{LoS} &= \left(\sqrt{g_{aib} P_a} \mathbf{h}^H(\theta_{ib}) \mathbf{\Theta} \mathbf{h}(\theta_{ai}) + \sqrt{g_{ab} P_a} h_{ab}^H \right) x + n_b \\ &= \sqrt{g_{aib} P_a} \left(\sum_{m=1}^{M} e^{j\left(-2\pi \Psi_{\theta_{ib}}(m) + \overline{\phi_m} + 2\pi \Psi_{\theta_{ai}}(m)\right)} \right) x + \sqrt{g_{ab} P_a} |h_{ab}| x + n_b \end{aligned}$$

$$= \sqrt{g_{aib} P_a} \left(\sum_{m=1}^{M} e^{j\Delta\phi_m} \right) x + \sqrt{g_{ab} P_a} |h_{ab}| x + n_b. \tag{10.13}$$

Observing the above equation, it is apparently that if and only if $\Delta\phi_m = 0$, the phase alignment at user is achieved to realize the optimal coherent combining gain M^2. Due to the use of finite phase shifting, in general, $\Delta\phi_m$ is random and is unequal to zero, this means that the combining gain is lower than or far less than M^2. In other words, the receive performance decays.

In accordance with the law of large numbers in [34] and (10.11), we can obtain

$$\begin{aligned} \frac{1}{M} \sum_{m=1}^{M} e^{j\Delta\phi_m} &\approx \mathbb{E}\left(e^{j\Delta\phi_m} \right) \\ &= \int_{-\Delta x}^{\Delta x} e^{j\Delta\phi_m} f\left(\Delta\phi_m\right) d\left(\Delta\phi_m\right) \\ &= \int_{-\Delta x}^{\Delta x} \frac{e^{j\Delta\phi_m}}{2\Delta x} d\left(\Delta\phi_m\right) \\ &= \frac{1}{2\Delta x} \int_{-\Delta x}^{\Delta x} \cos\left(\Delta\phi_m\right) d\left(\Delta\phi_m\right). \end{aligned} \tag{10.14}$$

A further simplification of (10.14) yields

$$\begin{aligned} \frac{1}{M} \sum_{m=1}^{M} e^{j\Delta\phi_m} &\approx \frac{1}{2\Delta x} \int_{-\Delta x}^{\Delta x} \cos\left(\Delta\phi_m\right) d\left(\Delta\phi_m\right) \\ &= \frac{1}{2\Delta x} \cdot 2\sin(\Delta x) \\ &= \frac{\sin(\Delta x)}{\Delta x} \\ &= \operatorname{sinc}\left(\frac{\pi}{2^k}\right). \end{aligned} \tag{10.15}$$

Plugging (10.15) in (10.13) yields

$$\widehat{y_b}^{LoS} \approx \sqrt{g_{aib} P_a} M \operatorname{sinc}\left(\frac{\pi}{2^k}\right) x + \sqrt{g_{ab} P_a} |h_{ab}| x + n_b. \tag{10.16}$$

In what follows, to simplify (10.16), we consider that the number of quantization bits is large, that is, $\Delta\phi_m$ goes to zero. Using the Taylor series expansion [35], we have the following approximation

$$\cos\left(\Delta\phi_m\right) \approx 1 - \frac{\Delta\phi_m^2}{2}, \tag{10.17}$$

then (10.14) can be rewritten as

$$\begin{aligned}\frac{1}{M}\sum_{m=1}^{M} e^{j\,\Delta\phi_m} &\approx \frac{1}{2\Delta x}\int_{-\Delta x}^{\Delta x} \cos\left(\Delta\phi_m\right) d\left(\Delta\phi_m\right) \\ &\approx \frac{1}{2\Delta x}\int_{-\Delta x}^{\Delta x} \left(1 - \frac{\Delta\phi_m^2}{2}\right) d\left(\Delta\phi_m\right) \\ &= \frac{1}{2\Delta x}\left(2\Delta x - \frac{1}{3}(\Delta x)^3\right) \\ &= 1 - \frac{1}{6}\left(\frac{\pi}{2^k}\right)^2. \end{aligned} \tag{10.18}$$

At this point, the receive signal at Bob under the approximate phase quantization error is

$$\widetilde{y_b}^{LoS} \approx \sqrt{g_{aib}P_a}\left(1 - \frac{1}{6}\left(\frac{\pi}{2^k}\right)^2\right)Mx + \sqrt{g_{ab}P_a}|h_{ab}|x + n_b. \tag{10.19}$$

10.3.2 Performance Loss of SNR at Bob

In accordance with (10.7), the SNR expression with no PL, i.e., $k \to \infty$, is given by

$$\mathrm{SNR}^{LoS} = \frac{\left(\sqrt{g_{aib}P_a}M + \sqrt{g_{ab}P_a}|h_{ab}|\right)^2}{\sigma^2}. \tag{10.20}$$

From (10.16) and (10.19), the expressions of the SNR with PL and approximate PL are

$$\widehat{\mathrm{SNR}}^{LoS} = \frac{\left(\sqrt{g_{aib}P_a}M\,\mathrm{sinc}\left(\frac{\pi}{2^k}\right) + \sqrt{g_{ab}P_a}|h_{ab}|\right)^2}{\sigma^2}, \tag{10.21}$$

and

$$\widetilde{\mathrm{SNR}}^{LoS} = \frac{\left(\sqrt{g_{aib}P_a}\left(1 - \frac{1}{6}\left(\frac{\pi}{2^k}\right)^2\right)M + \sqrt{g_{ab}P_a}|h_{ab}|\right)^2}{\sigma^2}, \tag{10.22}$$

respectively, where k is a finite positive integer.

Then the SNR PL and APL are given by

$$\widehat{L}^{LoS} = \frac{\mathrm{SNR}^{LoS}}{\widehat{\mathrm{SNR}}^{LoS}} = \frac{\left(\sqrt{g_{aib}}M + \sqrt{g_{ab}}|h_{ab}|\right)^2}{\left(\sqrt{g_{aib}}M\mathrm{sinc}\left(\frac{\pi}{2^k}\right) + \sqrt{g_{ab}}|h_{ab}|\right)^2}$$
$$= \left(1 + \frac{\sqrt{g_{aib}}\left(1 - \mathrm{sinc}\left(\frac{\pi}{2^k}\right)\right)}{\sqrt{g_{aib}}\mathrm{sinc}\left(\frac{\pi}{2^k}\right) + \frac{1}{M}\sqrt{g_{ab}}|h_{ab}|}\right)^2, \tag{10.23}$$

and

$$\widetilde{L}^{LoS} = \frac{\mathrm{SNR}^{LoS}}{\widetilde{\mathrm{SNR}}^{LoS}} = \frac{\left(\sqrt{g_{aib}}M + \sqrt{g_{ab}}|h_{ab}|\right)^2}{\left(\sqrt{g_{aib}}\left(1 - \frac{1}{6}\left(\frac{\pi}{2^k}\right)^2\right)M + \sqrt{g_{ab}}|h_{ab}|\right)^2}$$
$$= \left(1 + \frac{\sqrt{g_{aib}} \cdot \frac{1}{6}\left(\frac{\pi}{2^k}\right)^2}{\sqrt{g_{aib}}\left(1 - \frac{1}{6}\left(\frac{\pi}{2^k}\right)^2\right) + \frac{1}{M}\sqrt{g_{ab}}|h_{ab}|}\right)^2, \tag{10.24}$$

respectively. From (10.23) and (10.24), and k being a finite positive integer, it can be found that $\widehat{L}^{LoS}$ and $\widetilde{L}^{LoS}$ gradually decrease as k increases, while they gradually increase as M increases.

10.3.3 Performance Loss of Achievable Rate at Bob

According to (10.7), (10.16), and (10.19), the achievable rate at Bob with no PL, PL, and APL are given by

$$R^{LoS} = \log_2\left(1 + \frac{\left(\sqrt{g_{aib}P_a}M + \sqrt{g_{ab}P_a}|h_{ab}|\right)^2}{\sigma^2}\right), \tag{10.25}$$

$$\widehat{R}^{LoS} = \log_2\left(1 + \frac{\left(\sqrt{g_{aib}P_a}M\mathrm{sinc}\left(\frac{\pi}{2^k}\right) + \sqrt{g_{ab}P_a}|h_{ab}|\right)^2}{\sigma^2}\right), \tag{10.26}$$

and

$$\widetilde{R}^{LoS} = \log_2 \left(1 + \frac{\left(\sqrt{g_{aib} P_a} \left(1 - \frac{1}{6} \left(\frac{\pi}{2^k} \right)^2 \right) M + \sqrt{g_{ab} P_a} |h_{ab}| \right)^2}{\sigma^2} \right), \tag{10.27}$$

respectively.

10.3.4 Performance Loss of BER at Bob

In accordance with [34], the expression of BER is

$$\mathrm{BER}(z) \approx \beta Q \left(\sqrt{\mu z} \right), \tag{10.28}$$

where β and μ depend on the type of approximation and the modulation type, β represents the number of nearest neighbors to a constellation at the minimum distance, and μ is a constant that is related to minimum distance to average symbol energy, z denotes the SNR per symbol, $Q(z)$ represents the probability that a Gaussian random variable x with mean zero and variance one exceeds the value z, i.e.,

$$Q(z) = \int_z^{+\infty} \frac{1}{\sqrt{2\pi}} e^{\frac{-x^2}{2}} dx. \tag{10.29}$$

Assuming the quadrature phase shift keying (QPSK) is employed as the modulation scheme, according to (10.7), (10.16), and (10.19), the BERs at Bob with no PL, PL, and APL are given by

$$\mathrm{BER}^{LoS} \approx Q \left(\sqrt{\frac{\left(\sqrt{g_{aib} P_a} M + \sqrt{g_{ab} P_a} |h_{ab}| \right)^2}{\sigma^2}} \right), \tag{10.30}$$

$$\widehat{\mathrm{BER}}^{LoS} \approx Q \left(\sqrt{\frac{\left(\sqrt{g_{aib} P_a} M \mathrm{sinc} \left(\frac{\pi}{2^k} \right) + \sqrt{g_{ab} P_a} |h_{ab}| \right)^2}{\sigma^2}} \right), \tag{10.31}$$

and

$$\widetilde{\mathrm{BER}}^{LoS} \approx Q\left(\sqrt{\frac{\left(\sqrt{g_{aib}P_a}\left(1-\frac{1}{6}\left(\frac{\pi}{2^k}\right)^2\right)M+\sqrt{g_{ab}P_a}|h_{ab}|\right)^2}{\sigma^2}}\right), \tag{10.32}$$

respectively. This completes the derivations of the corresponding SNR performance loss, ARs and BERs with PL and APL in LoS channels.

10.4 Performance Loss Derivation and Analysis in the Rayleigh Channels

In this section, we make an analysis of the impact of discrete phase shift of IRS on SNR, AR, and BER. The corresponding closed-form expressions of SNR performance loss, AR, and BER are derived in the Rayleigh fading channels.

10.4.1 Derivation of Performance Loss in the Rayleigh Channels

Assuming all channels are Rayleigh channels obeying the Rayleigh distribution, the corresponding PDF is as follows

$$f_\alpha(x) = \begin{cases} \frac{x}{\alpha^2}e^{-\frac{x^2}{2\alpha^2}}, & x \in [0,+\infty), \\ 0, & \text{otherwise}, \end{cases} \tag{10.33}$$

where $\alpha > 0$ represents the Rayleigh distribution parameter.

Assuming discrete phase shifters is employed by IRS, there is a phase quantization error due to the effect of phase mismatching, i.e., $\Delta\phi_m \neq 0$, then the performance loss is incurred. Due to the phase mismatching of discrete phase shifters in IRS, the receive signal (10.2) can be rewritten as

$$\begin{aligned} \widehat{y}_b^{RL} &= \left(\sqrt{g_{aib}P_a}\mathbf{h}_{ib}^H\boldsymbol{\Theta}\mathbf{h}_{ai}+\sqrt{g_{ab}P_a}h_{ab}^H\right)x+n_b \\ &= \left(\sqrt{g_{aib}P_a}\sum_{m=1}^{M}(|h_{ib}(m)||h_{ai}(m)|e^{j\Delta\phi_m})+\sqrt{g_{ab}P_a}|h_{ab}|\right)x+n_b \end{aligned} \tag{10.34}$$

$$= \Big(\sqrt{g_{aib}P_a}\Big(M \cdot \underbrace{\frac{1}{M}\sum_{m=1}^{M}(|h_{ib}(m)||h_{ai}(m)|\cos(\Delta\phi_m))}_{W} +$$

$$jM \cdot \underbrace{\frac{1}{M}\sum_{m=1}^{M}(|h_{ib}(m)||h_{ai}(m)|\sin(\Delta\phi_m))}_{G}\Big) + \sqrt{g_{ab}P_a}\mathbb{E}(|h_{ab}|)\Big)x + n_b.$$

Using the weak law of large numbers, and the fact that $|h_{ai}(m)|$ and $|h_{ib}(m)|$ are i.i.d. Rayleigh distributions with parameters α_{ai} and α_{ib}, respectively, and their elements are independent of each other, we have

$$\begin{aligned} G &\approx \mathbb{E}(|h_{ib}(m)||h_{ai}(m)|\sin(\Delta\phi_m)) \qquad (10.35)\\ &= \iiint |h_{ib}(m)||h_{ai}(m)|\sin(\Delta\phi_m) f_{\alpha_{ib}}(|h_{ib}(m)|) f_{\alpha_{ai}}(|h_{ai}(m)|) \bullet \\ &\quad f(\sin(\Delta\phi_m))\, d(\Delta\phi_m)\, d(|h_{ai}(m)|)\, d(|h_{ib}(m)|). \end{aligned}$$

Since $|h_{ib}(m)|$, $|h_{ai}(m)|$, and $\sin(\Delta\phi_m)$ are independent of each other, (10.35) can be further converted to

$$\begin{aligned} G &\approx \int_0^{+\infty} |h_{ib}(m)| f_{\alpha_{ib}}(|h_{ib}(m)|) \int_0^{+\infty} |h_{ai}(m)| f_{\alpha_{ai}}(|h_{ai}(m)|) \bullet \\ &\quad \int_{-\Delta x}^{\Delta x} \sin(\Delta\phi_m) f(\Delta\phi_m)) d(\Delta\phi_m) d(|h_{ai}(m)|) d(|h_{ib}(m)|) \\ &= 0. \qquad (10.36) \end{aligned}$$

Due to the fact that $|h_{ib}(m)|$, $|h_{ai}(m)|$, and $\cos(\Delta\phi_m)$ are also independent of each other, similar to the derivation of (10.35) and (10.36), we have

$$\begin{aligned} W &= \frac{1}{M}\sum_{m=1}^{M}(|h_{ib}(m)||h_{ai}(m)|\cos(\Delta\phi_m)) \\ &\approx \mathbb{E}(|h_{ib}(m)||h_{ai}(m)|\cos(\Delta\phi_m)) \\ &= \int_0^{+\infty} |h_{ib}(m)| f_{\alpha_{ib}}(|h_{ib}(m)|) \int_0^{+\infty} |h_{ai}(m)| f_{\alpha_{ai}}(|h_{ai}(m)|) \bullet \\ &\quad \int_{-\Delta x}^{\Delta x} \cos(\Delta\phi_m) f(\Delta\phi_m) d(\Delta\phi_m) d(|h_{ai}(m)|) d(|h_{ib}(m)|) \\ &= \mathrm{sinc}\left(\frac{\pi}{2^k}\right) \int_0^{+\infty} |h_{ib}(m)| f_{\alpha_{ib}}(|h_{ib}(m)|) \int_0^{+\infty} |h_{ai}(m)| \bullet \end{aligned}$$

$$f_{\alpha_{ai}}\left(|h_{ai}(m)|\right) d\left(|h_{ai}(m)|\right) d\left(|h_{ib}(m)|\right)$$
$$= \operatorname{sinc}\left(\frac{\pi}{2^k}\right)\frac{\pi}{2}\alpha_{ai}\alpha_{ib}. \tag{10.37}$$

Plugging (10.36) and (10.37) into (10.34) yields

$$\widehat{y}_b^{RL} \approx \left(\sqrt{g_{aib}P_a}M\operatorname{sinc}\left(\frac{\pi}{2^k}\right)\frac{\pi}{2}\alpha_{ai}\alpha_{ib} + \sqrt{\frac{g_{ab}P_a\pi}{2}}\alpha_{ab}\right)x + n_b, \tag{10.38}$$

where α_{ab} is the Rayleigh distribution parameter of channel from Alice to Bob.

To simplify (10.38), in terms of (10.17) and the fact that $|h_{ib}|$, $|h_{ai}|$, and $\Delta\phi_m^2$ are independent of each other, we can obtain

$$\begin{aligned}
W &\approx \frac{1}{M}\sum_{m=1}^{M}|h_{ib}(m)|\,|h_{ai}(m)|\left(1-\frac{\Delta\phi_m^2}{2}\right)\\
&= \frac{1}{M}\sum_{m=1}^{M}|h_{ib}(m)|\,|h_{ai}(m)| - \frac{1}{M}\sum_{m=1}^{M}|h_{ib}(m)|\,|h_{ai}(m)|\,\frac{\Delta\phi_m^2}{2}\\
&= \mathbb{E}\left(|h_{ib}(m)|\,|h_{ai}(m)|\right) - \mathbb{E}\left(|h_{ib}(m)|\,|h_{ai}(m)|\,\frac{\Delta\phi_m^2}{2}\right)\\
&= \int_0^{+\infty}|h_{ib}(m)|f_{\alpha_{ib}}\left(|h_{ib}(m)|\right)\int_0^{+\infty}|h_{ai}(m)|f_{\alpha_{ai}}\left(|h_{ai}(m)|\right)\bullet\\
&\quad d\left(|h_{ai}(m)|\right) d\left(|h_{ib}(m)|\right) - \int_0^{+\infty}|h_{ib}(m)|f_{\alpha_{ib}}\left(|h_{ib}(m)|\right)\bullet\\
&\quad \int_0^{+\infty}|h_{ai}(m)|f_{\alpha_{ai}}\left(|h_{ai}(m)|\right)\int_{-\Delta x}^{\Delta x}\frac{\Delta\phi_m^2}{2}f\left(\Delta\phi_m\right)\right) d\left(\Delta\phi_m\right)\bullet\\
&\quad d\left(|h_{ai}(m)|\right) d\left(|h_{ib}(m)|\right)\\
&= \frac{\pi}{2}\alpha_{ai}\alpha_{ib} - \frac{1}{6}\left(\frac{\pi}{2^k}\right)^2\frac{\pi}{2}\alpha_{ai}\alpha_{ib}\\
&= \left(1-\frac{1}{6}\left(\frac{\pi}{2^k}\right)^2\right)\frac{\pi}{2}\alpha_{ai}\alpha_{ib}.
\end{aligned} \tag{10.39}$$

Plugging (10.39) into (10.34) yields

$$\widetilde{y}_b^{RL} \approx \left(\sqrt{g_{aib}P_a}M\left(1-\frac{1}{6}\left(\frac{\pi}{2^k}\right)^2\right)\frac{\pi}{2}\alpha_{ai}\alpha_{ib} + \sqrt{\frac{g_{ab}P_a\pi}{2}}\alpha_{ab}\right)x + n_b. \tag{10.40}$$

Assuming there is no quantization error, i.e., $\Delta\phi_m = 0$, the receive signal (10.38) degrades to

$$y_b^{RL} = \left(\sqrt{g_{aib}P_a}M\frac{\pi}{2}\alpha_{ai}\alpha_{ib} + \sqrt{\frac{g_{ab}P_a\pi}{2}}\alpha_{ab}\right)x + n_b. \tag{10.41}$$

10.4.2 Performance Loss of SNR at Bob

Based on (10.41), (10.38), and (10.40), the SNR expressions of no PL, PL, and APL are given by

$$\mathrm{SNR}^{RL} = \frac{\left(\sqrt{g_{aib}P_a}M\frac{\pi}{2}\alpha_{ai}\alpha_{ib} + \sqrt{\frac{g_{ab}P_a\pi}{2}}\alpha_{ab}\right)^2}{\sigma^2}, \tag{10.42}$$

$$\widehat{\mathrm{SNR}}^{RL} = \frac{\left(\sqrt{g_{aib}P_a}M\mathrm{sinc}\left(\frac{\pi}{2^k}\right)\frac{\pi}{2}\alpha_{ai}\alpha_{ib} + \sqrt{\frac{g_{ab}P_a\pi}{2}}\alpha_{ab}\right)^2}{\sigma^2}, \tag{10.43}$$

and

$$\widetilde{\mathrm{SNR}}^{RL} = \frac{\left(\sqrt{g_{aib}P_a}M\left(1-\frac{1}{6}\left(\frac{\pi}{2^k}\right)^2\right)\frac{\pi}{2}\alpha_{ai}\alpha_{ib} + \sqrt{\frac{g_{ab}P_a\pi}{2}}\alpha_{ab}\right)^2}{\sigma^2}, \tag{10.44}$$

respectively.

Then the SNR PL and APL are given as

$$\begin{aligned}\widehat{L}^{RL} = \frac{\mathrm{SNR}^{RL}}{\widehat{\mathrm{SNR}}^{RL}} &= \frac{\left(\sqrt{g_{aib}}M\frac{\pi}{2}\alpha_{ai}\alpha_{ib} + \sqrt{\frac{g_{ab}\pi}{2}}\alpha_{ab}\right)^2}{\left(\sqrt{g_{aib}}M\mathrm{sinc}\left(\frac{\pi}{2^k}\right)\frac{\pi}{2}\alpha_{ai}\alpha_{ib} + \sqrt{\frac{g_{ab}\pi}{2}}\alpha_{ab}\right)^2} \\ &= \left(1 + \frac{\sqrt{g_{aib}}\frac{\pi}{2}\alpha_{ai}\alpha_{ib}\left(1-\mathrm{sinc}\left(\frac{\pi}{2^k}\right)\right)}{\sqrt{g_{aib}}\mathrm{sinc}\left(\frac{\pi}{2^k}\right)\frac{\pi}{2}\alpha_{ai}\alpha_{ib} + \frac{1}{M}\sqrt{\frac{g_{ab}\pi}{2}}\alpha_{ab}}\right)^2,\end{aligned} \tag{10.45}$$

and

$$\widetilde{L}^{RL} = \frac{\mathrm{SNR}^{RL}}{\widetilde{\mathrm{SNR}}^{RL}} = \frac{\left(\sqrt{g_{aib}}M\frac{\pi}{2}\alpha_{ai}\alpha_{ib} + \sqrt{\frac{g_{ab}\pi}{2}}\alpha_{ab}\right)^2}{\left(\sqrt{g_{aib}}M\left(1-\frac{1}{6}\left(\frac{\pi}{2^k}\right)^2\right)\frac{\pi}{2}\alpha_{ai}\alpha_{ib} + \sqrt{\frac{g_{ab}\pi}{2}}\alpha_{ab}\right)^2}$$

$$= \left(1 + \frac{\sqrt{g_{aib}}\frac{1}{6}\left(\frac{\pi}{2^k}\right)^2 \frac{\pi}{2}\alpha_{ai}\alpha_{ib}}{\sqrt{g_{aib}}\left(1 - \frac{1}{6}\left(\frac{\pi}{2^k}\right)^2\right)\frac{\pi}{2}\alpha_{ai}\alpha_{ib} + \frac{1}{M}\sqrt{\frac{g_{ab}\pi}{2}}\alpha_{ab}}\right)^2, \tag{10.46}$$

respectively. Observing (10.45) and (10.46), we can find two tendencies: both of $\widehat{L}^{RL}$ and $\widetilde{L}^{RL}$ gradually decrease as k increases, while they gradually increase with increases in the value of M.

10.4.3 Performance Loss of Achievable Rate at Bob

In accordance with (10.41), (10.38), and (10.40), the achievable rates at Bob in the absence of PL, in the presence of PL and APL are given by

$$R^{RL} = \log_2\left(1 + \frac{\left(\sqrt{g_{aib}P_a}M\frac{\pi}{2}\alpha_{ai}\alpha_{ib} + \sqrt{\frac{g_{ab}P_a\pi}{2}}\alpha_{ab}\right)^2}{\sigma^2}\right), \tag{10.47}$$

$$\widehat{R}^{RL} = \log_2\left(1 + \frac{\left(\sqrt{g_{aib}P_a}M\,\mathrm{sinc}\left(\frac{\pi}{2^k}\right)\frac{\pi}{2}\alpha_{ai}\alpha_{ib} + \sqrt{\frac{g_{ab}P_a\pi}{2}}\alpha_{ab}\right)^2}{\sigma^2}\right), \tag{10.48}$$

and

$$\widetilde{R}^{RL} = \log_2\left(1 + \frac{\left(\sqrt{g_{aib}P_a}M\left(1 - \frac{1}{6}\left(\frac{\pi}{2^k}\right)^2\right)\frac{\pi}{2}\alpha_{ai}\alpha_{ib} + \sqrt{\frac{g_{ab}P_a\pi}{2}}\alpha_{ab}\right)^2}{\sigma^2}\right), \tag{10.49}$$

respectively.

10.4.4 Performance Loss of BER at Bob

From (10.41), (10.38), and (10.40), when the QPSK modulation is assumed to be employed, the BERs at Bob with no PL, PL, and APL are given by

$$\mathrm{BER}^{RL} \approx Q\left(\sqrt{\frac{\left(\sqrt{g_{aib}P_a}M\frac{\pi}{2}\alpha_{ai}\alpha_{ib} + \sqrt{\frac{g_{ab}P_a\pi}{2}}\alpha_{ab}\right)^2}{\sigma^2}}\right), \tag{10.50}$$

$$\widehat{\mathrm{BER}}^{RL} \approx Q\left(\sqrt{\frac{\left(\sqrt{g_{aib}P_a}M\mathrm{sinc}\left(\frac{\pi}{2^k}\right)\frac{\pi}{2}\alpha_{ai}\alpha_{ib}+\sqrt{\frac{g_{ab}P_a\pi}{2}}\alpha_{ab}\right)^2}{\sigma^2}}\right), \tag{10.51}$$

and

$$\widetilde{\mathrm{BER}}^{RL} \approx Q\left(\sqrt{\frac{P_a\left(\sqrt{g_{aib}}M\left(1-\frac{1}{6}\left(\frac{\pi}{2^k}\right)^2\right)\frac{\pi}{2}\alpha_{ai}\alpha_{ib}+\sqrt{\frac{g_{ab}\pi}{2}}\alpha_{ab}\right)^2}{\sigma^2}}\right), \tag{10.52}$$

respectively. It is noted that the above derived results may be extended to the scenarios of high-order digital modulations like M-ary phase shift keying (MPSK), M-ary quadrature amplitude modulation (MQAM).

10.5 Simulation Results and Discussions

In this section, the simulation results are presented to evaluate the effect of phase mismatching caused by IRS with discrete phase shifters from three different aspects: SNR, AR, and BER. The path loss at the distance $\bar{d}$ is modeled as $g(\bar{d}) = \mathrm{PL}_0 - 10\gamma\log_{10}\frac{\bar{d}}{d_0}$, where $\mathrm{PL}_0 = -30$ dB represents the path loss reference distance $d_0 = 1$ m, and γ is the path loss exponent. The path loss exponents of Alice→IRS, IRS→Bob, and Alice→Bob channels are respectively chosen as 2, 2, and 2 in the LoS channels, and the one are respectively set to be 2.5, 2.5, and 3.5 in the Rayleigh channels. The default system parameters are chosen as follows: $M = 128$, $d = \lambda/2$, $\theta_{ab} = \pi/2$, $\theta_{ai} = \pi/4$, $d_{ab} = 100$ m, $d_{ai} = 30$ m, $P_a = 30$ dBm. $\alpha_{ai} = \alpha_{ib} = \alpha_{ab} = 0.5$.

Figures 10.2 and 10.3 plot the curves of SNR PL versus the number k of quantization bits ranging from 1 to 6 in LoS and Rayleigh channels, respectively, where three different IRS element numbers M are chosen: 8, 64 and 1024. It can be seen from the two subfigures that regardless of the case of PL or APL, the SNR PL in the LoS channels and Rayleigh channels decreases as the number of quantization bits k increases, while it increases with M increases. They coincide with the conclusions of the theoretical analysis in Sects. 10.3 and 10.4. In addition, when k is larger than or equal to 3, the SNR PL is less than 0.23 dB even when the number of IRS phase shift elements M tends to large scale (e.g., $M = 1024$). This means that 3 bits is sufficient to achieve a trivial PL.

Figures 10.4 and 10.5 show the curves of AR versus the number k of quantization bits ranging from 1 to 6 in LoS and Rayleigh channels, respectively, where the SNR

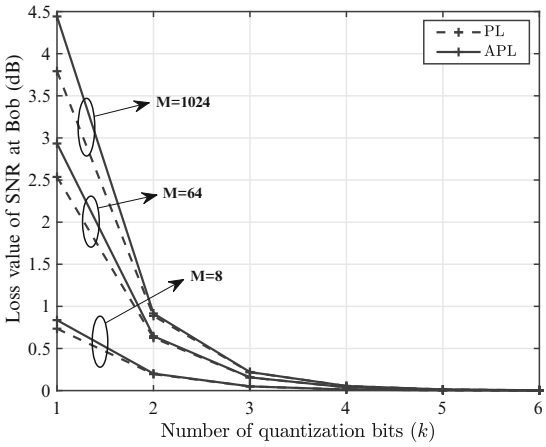


Fig. 10.2 Curves of loss of SNR versus the number k of quantization bits. (LoS channels)

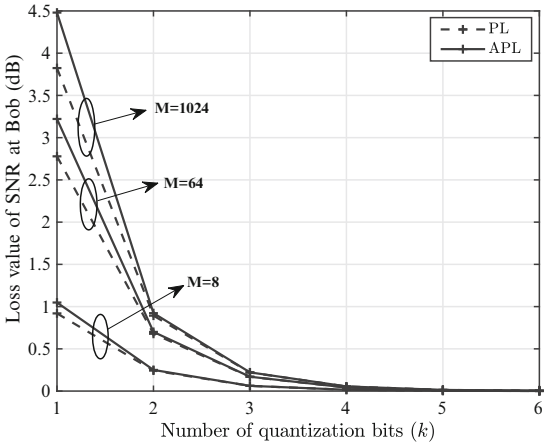


Fig. 10.3 Curves of loss of SNR versus the number k of quantization bits. (Rayleigh channels)

is equal to 15dB. From Figs. 10.4 and 10.5, it is seen that the AR PL at Bob decreases as k increases, and increases as M increases. Additionally, the AR increases as the number of IRS phase shift elements M increases. Compared with the case of no PL, 3 quantization bits achieves a AR PL less than 0.08 bits/s/Hz in the cases of PL and APL regardless of the number of IRS phase shift elements. When the number of quantization bits is larger than or equal to 2, the simple APL expression coincides with the true PL.

Figure 10.6 illustrates the curves of BER versus the number k of quantization bits from 1 to 6, where SNR is equal to -5 dB. From Fig. 10.6, it can be seen that with increasing the number k of quantization bits, the BER performances of PL and APL rapidly approach that no PL. When k reaches up to 3, the BER performances of PL and APL are almost identical to that of no PL, which means that it is feasible in practice to use discrete phase shifters with $k = 3$ to achieve a trivial performance

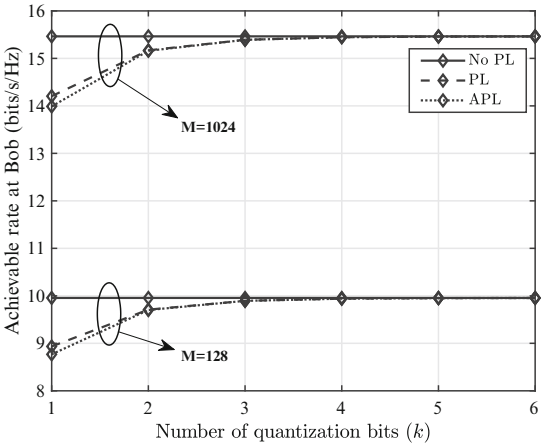


Fig. 10.4 Curves of AR versus the number k of quantization bits. (LoS channels)

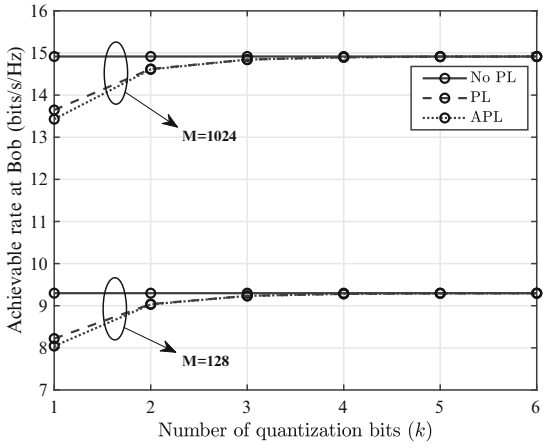


Fig. 10.5 Curves of AR versus the number k of quantization bits. (Rayleigh channels)

loss. This dramatically reduces the circuit cost and the required CSI amount fed back from BS or user.

10.6 Conclusion

In this book chapter, the performance of IRS with discrete phase shifters of wireless network has been investigated. To make an analysis of the PL caused by IRS with phase quantization error, we considered two scenarios: LoS and Rayleigh channels. The closed-form expressions of SNR PL, AR, and BER with PL were derived using the law of large numbers and some mathematic approximation techniques. With the help of the Taylor series expansion, the simple approximate PL expressions of IRS with approximate quantization error were also provided. Simulation results

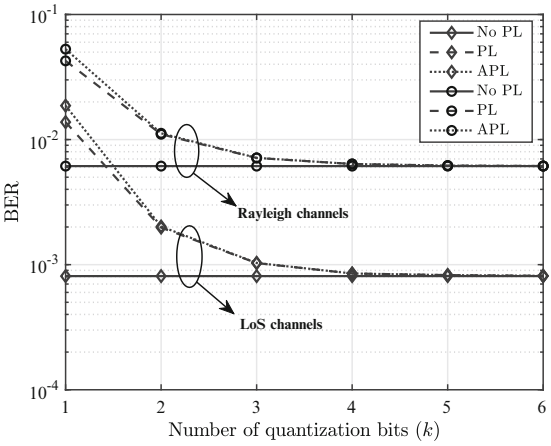


Fig. 10.6 Curves of BER versus the number k of quantization bits

showed that when the number of quantization bits is larger than or equal to 3, the performance losses of SNR and AR are less than 0.23 dB and 0.08 bits/s/Hz, respectively, and the corresponding degradation on BER is negligible. The simple approximate expression approaches the true PL when the number of quantization bits is larger than or equal to 2.

References

1. Nguyen, V., Truong, T.P., Nguyen, T.M.T., Noh, W., Cho, S.: Achievable rate analysis of two-hop interference channel with coordinated IRS relay. IEEE Trans. Wireless Commun. **21**(9), 7055–7071 (2022)
2. Wu, Q., Zhang, R.: Towards smart and reconfigurable environment: intelligent reflecting surface aided wireless network. IEEE Commun. Mag. **58**(1), 106–112 (2020)
3. Tang, W., Dai, J., Chen, M., Wong, K., Li, X., Zhao, X., Jin, S., Cheng, Q., Cui, T.: MIMO transmission through reconfigurable intelligent surface: system design, analysis, and implementation. IEEE J. Sel. Areas Commun. **38**(11), 2683–2699 (2020)
4. Gao, Y., Yong, C., Xiong, Z., Zhao, J., Xiao, Y., Niyato, D.: Reflection resource management for intelligent reflecting surface aided wireless networks. IEEE Trans. Commun. **69**(10), 6971–6986 (2021)
5. Huang, C., Zappone, A., Alexandropoulos, G.C., Debbah, M., Yuen, C.: Reconfigurable intelligent surfaces for energy efficiency in wireless communication. IEEE Trans. Wireless Commun. **18**(8), 4157–4170 (2019)
6. Guan, X., Wu, Q., Zhang, R.: Intelligent reflecting surfaces assisted secrecy commuincation: is artificial noise helpful or not? IEEE Wireless Commun. Lett. **9**(6), 778–782 (2020)
7. Dong, R., Shu, F., Chen, R., Wu, Y., Pan, C., Wang, J.: Beamforming and power allocation for double-RIS-aided two-way directional modulation network. https://arxiv.org/abs/2201.09063
8. Hong, S., Pan, C., Ren, H., Wang, K., Nallanathan, A.: Artificial-noise-aided secure MIMO wireless communications via intelligent reflecting surface. IEEE Trans. Commun. **68**(12), 7851–7866 (2020)
9. Wang, X., Shu, F., Shi, W., Liang, X., Dong, R., Li, J., Wang, J.: Beamforming design for IRS-aided decode-and-forward relay wireless network. IEEE Trans. Green Commun. Netw. **6**(1), 198–207 (2022)

10. Yang, L., Guo, W., Ansari, I.S.: Mixed dual-hop FSO-RF communication systems through reconfigurable intelligent surface. IEEE Commun. Lett. **24**(7), 1558–1562 (2020)
11. Zhu, Q., Gao, Y., Xiao, Y., Mumtaz, S.: Intelligent reflecting surface aided wireless networks: dynamic user access and system sum-rate maximization. IEEE Trans. Commun. **70**(4), 2870–2881 (2022)
12. Ahmed, A.H., Samir, M., Elhattab, M., Assi, C., Sharafeddine, S.: Reconfigurable intelligent surface enabled vehicular communication: joint user scheduling and passive beamforming. IEEE Trans. Veh. Technol. **71**(3), 2333–2345 (2022)
13. Mei, W., Zhang, R.: Performance analysis and user association optimization for wireless network aided by multiple intelligent reflecting surface. IEEE Trans. Commun. **69**(6), 6296–6312 (2021)
14. Yang, L., Yang, J., Xie, W., Hasna, M.O., Tsiftsis, T., Renzo, M.D.: Secrecy performance analysis of RIS-aided wireless communication systems. IEEE Trans. Veh. Technol. **69**(10), 12296–12300 (2020)
15. Pang, X., Zhao, N., Tang, J., Wu, C., Niyato, D., Wong, K.K.: IRS-assisted secure UAV transmission via joint trajectory and beamforming design. IEEE Trans. Commun. **70**(2), 1140–1152 (2022)
16. Fang, S., Chen, G., Li, Y.: Joint optimization for secure intelligent reflecting surface assisted UAV networks. IEEE Commun. Lett. **10**(2), 276–280 (2021)
17. Pang, X., Sheng, M., Zhao, N., Tang, J., Niyato, D., Wong, K.K.: When UAV meets IRS: expanding air-ground networks via passive reflection. IEEE Wireless Commun. **28**(5), 164–170 (2021)
18. Shu, F., Teng, Y., Li, J., Huang, M., Shi, W., Li, J., Wu, Y., Wang, J.: Enhanced secrecy rate maximization for directional modulation networks via IRS. IEEE Trans. Commun. **69**(12), 8388–8401 (2021)
19. Di, B., Zhang, H., Song, L., Li, Y., Han, Z., Poor, H.V.: Hybrid beamforming for reconfigurable intelligent surface based multi-user communications: achievable rates with limited discrete phase shifts. IEEE J. Sel. Areas Commun. **38**(8), 1809–1822 (2020)
20. Choi, J., Kwon, G., Park, H.: Multiple intelligent reflecting surfaces for capacity maximization in LOS MIMO systems. IEEE Wireless Commun. Lett. **10**(8), 1727–1731 (2021)
21. Rehman, H.U., Bellili, F., Mezghani, A., Hossain, E.: Joint active and passive beamforming design for IRS-assisted multi-user MIMO systems: a VAMP-based approach. IEEE Trans. Commun. **69**(10), 6734–6749 (2021)
22. Han, Y., Zhang, S., Duan, L., Zhang, R.: Double-IRS aided MIMO communication under LoS channel: Capacity maximization and scaling. IEEE Trans. Wireless Commun. **70**(4), 2820–2837 (2022)
23. Wang, H.M., Bai, J., Limeng, D.: Intelligent reflecting surfaces assisted secure transmission without eavesdropper's CSI. IEEE Signal Process Lett. **27**, 1300–1304 (2020)
24. Wu, Q., Zhang, R.: Beamforming optimization for intelligent reflecting surface with discrete phase shifts. In: IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 7830–7833, (2019)
25. Shi, W., Li, J., Xia, G., Wang, Y., Zhou,, Zhang, Y., Shu, F.: Secure multigroup multicast communication systems via intelligent reflecting surface. China Commun. **18**(3), 39–51 (2021)
26. Zhang, Y., Zhong, C., Zhang, Z., Lu, W.: Sum rate optimization for two way communications with intelligent reflecting surface. IEEE Commun. Lett. **24**(5), 1090–1094 (2020)
27. Shen, H., Ding, T., Xu, W., Zhao, C.: Beamforming design with fast convergence for IRS-aided full-duplex communication. IEEE Commun. Lett. **24**(12), 2849–2853 (2020)
28. Yang, L., Yang, Y., Hasna, M.O., Alouini, M.S.: Coverage, probability of SNR gain, and DOR analysis of RIS-aided communication systems. IEEE Wireless Commun. Lett. **9**(8), 1268–1272 (2020)
29. Pan, C., Ren, H., Wang, K., Xu, W., Elkashlan, M., Nallanathan, A., Hanzo, L.: Multicell MIMO communications relying on intelligent reflecting surfaces. IEEE Trans. Wireless. Commun. **19**(8), 5218–5233 (2020)

30. Li, J., Xu, L., Lu, P., Liu, T., Zhang, Z., Hu, J., Shu, F., Wang, J.: Performance analysis of directional modulation with finite-quantized RF phase shifters in analog beamforming structure. IEEE Access. **7**, 97457–97465 (2019)
31. Wei, Z., Masouros, C., Liu, F.: Secure directional modulation with few-bit phase shifters: optimal and iterative-closed-form designs. IEEE Trans. Commun. **69**(1), 486–500 (2021)
32. Dong, R., Shi, B., Zhan, X., Shu, F., Wang, J.: Performance analysis of massive hybrid directional modulation with mixed phase shifters. IEEE Trans. Veh. Technol. **71**(4), 5604–5608 (2022)
33. You, C., Zheng, B., Zhang, C.R.: Channel estimation and passive beamforming for intelligent reflecting surface: Discrete phase shift and progressive refinement. IEEE J. Sel. Areas Commun. **38**(11), 2604–2620 (2020)
34. Wasserman, L.: All of Statistics: A Concise Course in Statistical Inference. Springer, Berlin (2004)
35. Moon, T.K., Stirling, W.C.: Mathematical Methods and Algorithms for Signal Processing. Marsha Horron (1999)

Chapter 11
Conclusions and Future Research Directions

We have made an interesting investigation of IRS-aided PLS wireless networks in this book, where multiple different application network scenarios, such as DM, SM, covert wireless communications, secure multigroup multicast communication systems, have been discussed. It is one's goal to ensure that private data information can be transmitted securely in wireless networks. It has been shown that introducing IRS into PLS wireless networks can more effectively prevent confidential information from being intercepted or eavesdropped by illegal users, so that ensuring the communication between transmitter and legal users is secure. This book can be a valuable reference for wireless communication engineers and researchers in related fields.

With the popularization of secure communication, IRS-aided PLS can be considered as a new research direction and an important technology for large and complex communication networks in the future, such as 6G. In particular, since the IRS-aided PLS technique not only can ensure secure communication, but also can improve rate performance, the IRS-assisted PLS technology can be regarded as a promising technology, which can be potentially applied to some new application scenarios, such as vehicular network, satellite communication, radar communication, smart medical systems, smart city, massive direction finding, etc.

However, there are still some challenges and open problems, which are needed to be further studied.

1. CSI acquisition: In practice, due to the lack of cooperation between transmitter/IRS and eavesdropper, the CSI may be imperfect. The acquisition of perfect CSI in IRS-aided PLS network is a challenging task. It is mainly manifested in the following aspects. First, it is especially difficult to obtain the CSI associated with the eavesdropper due to the hidden nature of eavesdroppers. However, the CSI of eavesdroppers is known in the scenario where eavesdroppers are also active users in the system but untrusted by legal users. In this case, the CSI can be achieved by modern adaptive system design, where channels are estimated at legal user and eavesdropper and sent back to transmitter. Second, in IRS-assisted

F. Shu, J. Wang, *Intelligent Reflecting Surface-Aided Physical-Layer Security*,
Wireless Networks, https://doi.org/10.1007/978-3-031-41812-9_11

PLS systems, because of the limited signal processing capability at the IRS, the perfect CSI of IRS-links is challenging to obtain. Depending on whether the IRS is equipped with an RF link, there are two ways to obtain the CSI. When each element of the IRS is equipped with a low-power receive RF chain for channel estimation, the channels related to AP-IRS/IRS-user links can be estimated at the IRS based on their training signals. To reduce the computational overhead, the elements of the IRS could be divided into subarrays based on the rows or columns. Each sub-array is equipped with one receive RF chain for channel estimation. If there are no receive RF chains at the elements of the IRS, channel estimation becomes very challenging because the elements have no dedicated signal processing capability. One practical method for IRS channel estimation is to employ an ON/OFF-based IRS reflection pattern (element-by-element of IRS is set ON or all elements of IRS are switched ON).

2. Deployment and design of IRS: The physical design of IRSs including the number, distribution, and geometry of IRSs and the impact of IRS deployment on PLS may be an interesting direction of research but is not well explored in the literature. In addition, the impact of different number of IRS elements and their distribution on PLS needs to be further explored. The positioning accuracy of the IRS assisted system depends to a large extent on the location of the IRS. Therefore, it is important to find the optimal physical design and the placement to enhance IRS-assisted PLS. In scenarios where no eavesdropper is present, it has been demonstrated that the user's achievable rate can be maximised when the IRS is close to the transmitter or receiver. However, there is no clear conclusion on the location of the IRS when there is an eavesdropper in the system or when there is a monitor present.
3. The existing research on SM was based on the Rayleigh fading model. How to extend SM system to other types of fading channels is very important for the practical application and deployment of SM. In addition, how to construct the security optimization problem in the relevant channel environment is worth pondering.
4. In wireless communication, the scattering of electromagnetic waves caused by the atmosphere and the reflection or diffraction of the electromagnetic waves created by the surrounding buildings and other surface objects will cause multipath propagation of radio signals. In practice, due to the lack of cooperation between transmitter and eavesdropper, the CSI may be imperfect. For DM, if the directional angle from transmitter to eavesdropper is available, AN can be forced to its direction by beamforming. Once eavesdropper communicates with its data center, transmitter or legal user may estimate its directional angle. The basic idea of multiple parallel transmissions can be extended to the scenario of imperfect CSI. In our view, the joint optimization problem will become harder to address due to the imperfect CSI constraint.