# Design and Optimization of IRS-Backscatter Enabled Physical Layer Security


**Bingxue Wu**

Department of Electronic and Electrical Engineering

University of Sheffield

Supervisors: Prof. Xiaoli Chu, Prof. Jie Zhang

This thesis is submitted for the approval of the

*Doctor of Philosophy*

May 2026

Dedication

To my family and all who supported me along this path.

To caffeine, curiosity, and the occasional existential crisis.

Though the journey was full of twists and challenges,

your love and encouragement carried me through,

and the outcome makes it all worthwhile.

# Acknowledgements

Throughout the course of my PhD journey, I have been fortunate to receive invaluable support and guidance from many people.

First and foremost, I would like to express my heartfelt thanks to Professor Xu and my other mentors for their generous guidance, encouragement, and expertise. Your support has been instrumental in shaping both this research and my academic growth.

I am also deeply grateful to my family and friends for their unwavering support and companionship. Your patience, understanding, and encouragement sustained me through the most challenging times.

Lastly, a special thank you to my cat - Nietzsche. Your quiet presence, random zoomies, and occasional cuddles brought comfort and calm when I needed it most.

# Abstract

With the continuous proliferation of wireless communication technologies and the ubiquity of smart devices, the demand for seamless connectivity is escalating. This necessitates secure, energy-efficient, and high-performance communication systems. Conventional security techniques, typically based on cryptography or active jamming, often impose excessive computational or energy burdens, making them unsuitable for next-generation networks. To address these challenges, this thesis investigates the design and optimization of low-complexity and energy-efficient intelligent reflecting surface (IRS)-assisted backscatter communication systems, aiming to achieve secure and reliable communications with significantly reduced computational and hardware overhead.

This research represents a shift from reactive security paradigms toward a proactive, design-oriented approach, leveraging the capabilities of IRS technology. The thesis contributes three distinct yet complementary system architectures. The first focuses on IRS-backscatter designs for hybrid confidential information and artificial noise transmission, ensuring robustness against eavesdropping. The second extends this paradigm to simultaneously transmitting and reflecting reconfigurable intelligent surface (STAR-RIS) architectures, enabling secure indoor multi-user communications through simultaneous reflection and transmission control. The third explores IRS-backscatter enabled downlink systems under radar communication coexistence (RCC), bridging secure communication and integrated sensing, and advancing the vision of intelligent dual-functional wireless networks.

Extensive simulations are conducted to evaluate these systems, demonstrating significant improvements across secrecy rate, energy efficiency, computational complexity, and scalability. The backscatter-based designs prove highly energy-efficient and resistant to passive

eavesdropping, while the STAR-RIS and RCC frameworks show strong potential for secure multi-user connectivity and spectrum-efficient coexistence with radar sensing.

In paving the way for future wireless networks, this thesis contributes critical building blocks toward realizing an intelligent wireless ecosystem capable of proactively countering security threats while optimizing performance. The findings hold important implications for sixth-generation (6G) and beyond, where embedding intelligence into the propagation environment will be essential to meet the rigorous demands of emerging applications.

# Table of contents

# Abbreviations

**AN** Artificial Noise

**AO** Alternating Optimization

**BS** Base Station

**CSI** Channel State Information

**CSIT** Channel State Information at the Transmitter

**CVX** Convex Optimization Software

**DQN** Deep Q-Networks

**FCL** Fully Connected Layer

**GAT** Graph Attention Network

**GCN** Graph Convolutional Network

**GNN** Graph Neural Network

**IoT** Internet of Things

**IPM** Interior-Point Method

**IRS** Intelligent Reflecting Surface

**ISAC** Integrated Sensing and Communication

**LEO** Low Earth Orbit

**LFM** Linear Frequency Modulated

**MDP** Markov Decision Process

**MEMS** Microelectromechanical Systems

**MIMO** Multiple-Input Multiple-Output

**ML** Machine Learning

**MLP** Multilayer Perceptron

**NOMA** Non-Orthogonal Multiple Access

**PIN** Positive-Intrinsic-Negative

**PLS** Physical Layer Security

**QoS** Quality of Service

**RCC** Radar Communication Coexistence

**RCS** Radar Cross Section

**RF** Radio Frequency

**RIS** Reconfigurable Intelligent Surface

**RL** Reinforcement Learning

**ROC** Receiver Operating Characteristic

**RSMA** Rate-splitting Multiple Access

**SCA** Successive Convex Approximation

**SDP** Semidefinite Program

**SDR** Semidefinite Relaxation

**SGD** Stochastic Gradient Descent

**SIC** Successive Interference Cancellation

**SINR** Signal-to-Interference-Plus-Noise Ratio

**SNR** Signal-to-Noise Ratio

**STAR-RIS** Simultaneous Transmitting and Reflecting Reconfigurable Intelligent Surface

**THz** Terahertz

**UAV** Unmanned Aerial Vehicle

**ULP** Ultra-Low Power

**WSR** Weighted Sum Rate

**ZF** Zero Forcing

# Chapter 1

# Introduction

The development of wireless communication systems has been motivated by an ever-increasing need for higher data rates, better coverage, increased reliability, and stronger security. This is where existing solutions are reaching the ultimate limit in the 6G and inter-6G wireless system era. The objective of this thesis is to design and optimize secure/efficient algorithms and schemes for achieving communication efficiency and physical layer security (PLS) in intelligent reflecting surface (IRS)-assisted and backscatter communication paradigms, with design principles that can be extended to broader wireless systems.

## 1.1 IRS and Backscatter Communications: Background and Research Progress

Control and manipulation of electromagnetic wave propagation has become a transformative strategy to address the intrinsic limitations of traditional wireless communications. In great contrast to conventional wireless, where the propagation environment is treated as an unpredictable random medium, remarkable progress on the metamaterial technology and IRS have allowed for unprecedented control on the wireless channels.

### 1.1.1 IRS: From Concept to Reality

IRS, also called reconfigurable intelligent surfaces (RISs), are an innovative communication concept. These surfaces are composed of numerous inexpensive passive devices, which are capable of independently modulating the amplitude and phase distribution of incident electromagnetic waves. The basic concept of the IRS technology is that constructive and destructive interference patterns are generated for strengthening the signal paths and attenuating the interfering signal paths, respectively [1–3].

The origin of the IRS concept dates back to the general research on metamaterials which are man-made materials designed to have an effective electromagnetic property not present in naturally occurring materials [4]. Earlier, work was mainly on the development of theory and on the proof-of-concept demonstrations. But, the recent years have seen significant strides in real-world IR implementation, where researchers are able to prove that large-scale IRS deployments for different wireless communication systems are in fact not costly when they were previously thought to be.

The operational paradigm of IRS fundamentally differs from that of conventional active relaying systems, representing a transformative approach to wireless communication [5]. Traditional relay systems, whether employing amplify-and-forward (AF) or decode-and-forward (DF) protocols, necessitate comprehensive signal processing operations including signal reception, decoding, amplification, and retransmission, which inherently require dedicated radio-frequency (RF) chains and power amplifiers [6, 7]. In stark contrast, IRS technology leverages a planar metamaterial surface comprising a large number of passive reflecting elements that can independently manipulate the amplitude and phase of incident electromagnetic waves without the need for complex signal processing or power amplification [8, 9]. This passive-based operational model yields substantial advantages in terms of energy efficiency, with recent comparative analyses demonstrating that IRS configurations can achieve up to 48 bits/joule energy efficiency compared to 30 bits/joule for relay-only systems under equivalent conditions [10]. Furthermore, IRS eliminates the noise amplification issues inherent in AF relays and the processing delays associated with DF relays, while offering superior spectral efficiency due to its full-duplex operation without self-interference cancellation requirements

[11]. The reconfigurable nature of IRS elements enables sophisticated adaptive control mechanisms where reflection coefficients can be dynamically optimized based on real-time channel state information (CSI), system objectives, and performance criteria [12, 13]. Each reflecting element's complex reflection coefficient can be independently controlled to achieve optimal passive beamforming gains [14]. Advanced optimization frameworks employing evolutionary game theory, deep reinforcement learning, and alternating optimization (AO) techniques have been developed to address the non-convex nature of reflection coefficient optimization problems [15, 16]. The adaptive control system continuously monitors channel conditions and dynamically adjusts the IRS configuration to maximize desired performance metrics such as signal-to-interference-plus-noise ratio (SINR), sum rate, or energy efficiency, while simultaneously mitigating interference and enhancing coverage [17, 18]. This intelligent adaptation capability, combined with the cost-effectiveness and scalability of passive implementation, positions IRS as a key enabling technology for next-generation wireless networks [19, 20].

There has been extensive research in the area of IRS-aided wireless communication systems, and a number of different system set-ups and optimization schemes have been considered. The joint optimization of transmit beamforming at the base station (BS) and reflection beamforming at the IRS has been recently recognized as a non-trivial design challenge[21]. Since the design variables are coupled with each other, the optimization problems are generally non-convex and therefore, sophisticated optimization methods (e.g., AO, semidefinite relaxation (SDR), and Riemannian optimization) are called for.

The deployment issues of IRS have also been well-considered in relevant literature, when IRS is employed in both indoor and outdoor. For indoor scenario, IRS can be implanted into walls, ceilings or windows, which help to improve the coverage and alleviate the death area. Outdoors, IRS can be mounted on building walls, billboards, or custom support structures to enhance signal quality and increase coverage area. The best positions of IRS elements are affected by multiple factors including the positions of transmitters and receivers, CSI condition and interference condition.

### 1.1.2 Simultaneously Transmitting and Reflecting RIS (STAR-RIS)

A revolutionary advancement in RISs technology is the development of STAR-RIS, which represents a paradigm shift from conventional half-space coverage to comprehensive full-space electromagnetic wave manipulation [22, 23].Unlike traditional RIS architectures that are constrained to either pure reflection or transmission modes, STAR-RIS integrates dual-functional capabilities that enable each surface element to simultaneously support reflection and transmission of incident signals, thereby achieving 360-degree spatial coverage and overcoming the topological limitations inherent in conventional reflecting-only or transmitting-only systems[24, 25]. This innovative bi-directional operational paradigm fundamentally transforms the geometric constraints of wireless communication systems by eliminating the requirement for transmitters and receivers to be co-located on the same side of the intelligent surface, thus enabling more flexible network deployment strategies and enhanced system connectivity [26, 27].

The operational versatility of STAR-RIS is realized through three distinct transmission protocols, each offering unique advantages for different application scenarios and system requirements [28]. The Energy Splitting (ES) protocol enables each surface element to allocate the incident signal power dynamically between transmission and reflection operations, providing continuous control over signal distribution with four independent degrees of freedom: transmission amplitude, transmission phase reflection amplitude, and reflection phase, subject to the energy conservation constraint [29, 30]. The Mode Switching (MS) protocol operates each element in either pure transmission or pure reflection mode at any given time, offering binary operation with simplified hardware implementation but reduced flexibility [31, 32]. The Time Switching (TS) protocol alternates between global transmission and reflection phases across all surface elements, enabling time-division coordination while maintaining full-element utilization during each operational phase [33, 34]. Recent comparative studies demonstrate that ES protocol achieves superior spectral efficiency due to its enhanced degrees of freedom, while MS and TS protocols offer implementation advantages in terms of hardware complexity and power consumption [35, 36]. In this work, the ES

protocol is adopted due to its flexibility in jointly optimizing reflection and transmission coefficients.

The advanced capabilities of STAR-RIS have catalyzed significant research interest in diverse application domains, ranging from secure communications and energy harvesting to massive multiple access and mobile edge computing [37, 38]. Experimental prototypes and theoretical analyses have demonstrated substantial performance gains, with STAR-RIS systems achieving up to 15 dB additional system gain compared to conventional RIS implementations, while simultaneously expanding coverage areas and improving signal quality across both spatial regions [39]. Furthermore, the integration of STAR-RIS with emerging technologies such as non-orthogonal multiple access (NOMA), rate-splitting multiple access (RSMA), and cooperative relaying has shown promising results in enhancing spectral efficiency, energy efficiency, and user fairness [40, 41]. These multifaceted advantages position STAR-RIS as a transformative technology for next-generation wireless networks, offering unprecedented flexibility in signal propagation control and opening new possibilities for intelligent wireless environment design.

### 1.1.3 Backscatter Communications: Enabling Ultra-Low Power Connectivity

Backscatter communication represents another revolutionary approach to wireless connectivity, particularly relevant for Internet of Things (IoT) and ambient intelligence applications. This technology enables battery-free devices to communicate by modulating and reflecting ambient radio frequency (RF) signals rather than generating their own signals [42, 43].

The basic concept of backscatter communication is based on load modulation, in which a backscatter device (tag) changes its impedance to modulate the reflection coefficient of the incident RF signal. By altering between various impedance states, the tag can modulate information on the reflected signal, and communication is achieved without conventional RF signal generator circuitry. In conventional backscatter systems, this modulation is typically realized through simple binary switching (e.g., on–off keying), resulting in limited

modulation flexibility. Such design allows it to provide Ultra-low power (ULP) consumption, which is a perfect solution for applications needing for battery replacement or recharging problems [44–46]. The receiver does not require more bandwidth to perform energy harvesting, communication and sensing operations. In this way the use of separate RF sources can be dispensed with which significantly reduces system complexity as well as systems costs. However, ambient backscatter communication (AmBC) systems have their inherent challenges such as signal detection and channel estimation as well as interference condition faced by the diode-rectenna system from the interference sources in the environment.

It is worth noting that RIS-based systems can be viewed as a generalized form of backscatter communication. Unlike conventional backscatter devices that rely on discrete impedance switching, RIS elements enable continuous or multi-level control of reflection coefficients, including both amplitude and phase. This provides significantly enhanced degrees of freedom for signal modulation, beamforming, and interference management.

Research in backscatter communications has addressed various technical challenges, including signal detection algorithms, multiple access schemes, and performance optimization. Novel detector designs have been proposed to overcome the effects of direct-link interference and improve SINR [47]. Multiple antenna techniques have been explored to enhance the reliability and throughput of backscatter systems [45]. Furthermore, advanced modulation schemes and coding techniques have been developed to maximize the information transfer rate while maintaining low power consumption.

The coexistence of backscatter communication with other wireless systems has suggested new research opportunities. The cognitive approach in backscatter communication ensures spectrum sharing with primary wireless systems, and cooperative backscatter networks help multiple tags to collaborate for better performance [48]. Machine learning (ML) methods have also been utilized to optimize backscatter system, and adapt to time-varying channel environments.

### 1.1.4 Convergence of IRS and Backscatter Technologies

The integration of IRS with backscatter communication technologies represents a transformative evolution that synergistically combines the advantages of both paradigms to address the fundamental limitations of ULP wireless networks [49, 50]. In such systems, an ambient RF source (e.g., a base station or dedicated transmitter) illuminates the IRS, and the incident signal is directly processed by the surface. Unlike conventional architectures where a separate backscatter device performs modulation, the IRS itself acts as a backscatter transmitter by dynamically adjusting its reflection coefficients. Specifically, information is encoded onto the reflected signal through controlled variations of the IRS elements' impedance states, while their phase and amplitude responses are simultaneously optimized to shape the propagation direction. As a result, the IRS jointly performs signal modulation and beamforming, enabling the generation of an information-bearing reflected signal that is enhanced toward the intended receiver while suppressing undesired propagation directions, as illustrated in Fig. 1.1. Traditional AmBC systems, while offering significant energy efficiency advantages, suffer from inherent limitations including weak backscattered signal strength, susceptibility to direct-link interference, and restricted communication range due to the passive nature of signal reflection [51, 52]. The strategic deployment of IRS in backscatter communication environments enables intelligent manipulation of the electromagnetic propagation medium, facilitating enhanced signal quality through constructive beamforming and interference mitigation techniques that significantly improve detection performance and extend operational range [53, 54].

Contemporary research has explored diverse architectural configurations for IRS-enhanced backscatter systems, each targeting specific performance optimization objectives and deployment scenarios [55, 56]. In passive relay configurations, IRS functions as an intelligent signal conditioning element positioned between backscatter devices and readers, dynamically adjusting phase shifts to create favorable propagation conditions and enhance end-to-end communication reliability [57, 58]. Alternative implementations leverage IRS elements as distributed backscatter sensors, enabling simultaneous sensing and communication functionalities where each IRS element can modulate incident signals to convey sensor data

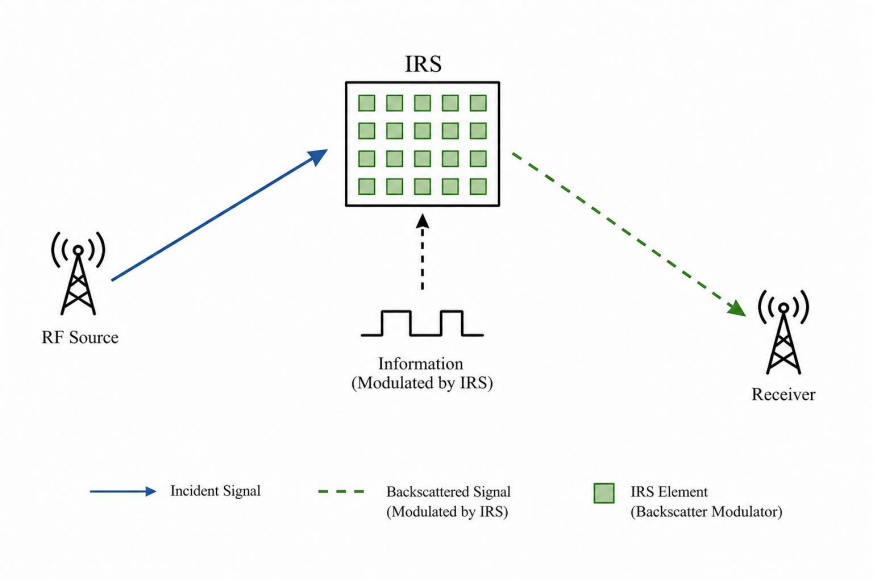


Fig. 1.1 Illustration of IRS-based backscatter communication. The IRS directly modulates the incident signal by adjusting its reflection coefficients, while simultaneously performing beamforming to enhance the signal toward the receiver.

while maintaining the surface's primary reflection capabilities [59, 60]. Advanced hybrid architectures integrate both functionalities, allowing dynamic mode switching between passive relay operation and active backscatter transmission based on network conditions and quality-of-service requirements [61, 62].

The convergence of these technologies necessitates comprehensive system-level optimization that carefully balances multiple conflicting performance metrics including power consumption, computational complexity, communication range, and data throughput [63, 64]. Power-complexity-performance tradeoff analysis reveals that while IRS integration significantly enhances backscatter communication capabilities, the associated computational overhead for optimal phase shift design and real-time adaptation can impose substantial processing requirements on resource-constrained devices [65, 66]. Recent studies demonstrate that intelligent resource allocation strategies, employing techniques such as block coordinate descent optimization and successive convex approximation (SCA), can achieve near-optimal performance while maintaining acceptable computational complexity for practical implementation scenarios [67, 68].

Energy harvesting represents a particularly promising application domain where IRS and backscatter technologies exhibit strong complementarity for sustainable IoT deployments [69, 70]. IRS can be strategically configured to focus ambient RF energy toward energy-harvesting backscatter devices through intelligent beamforming, effectively extending their operational range and supporting more sophisticated processing tasks while maintaining battery-free operation [71, 72]. This capability is especially valuable for perpetual IoT applications including wireless sensor networks, environmental monitoring systems, and biomedical implants, where device longevity and maintenance-free operation are critical requirements [73, 74]. Experimental implementations have demonstrated substantial improvements in harvested power levels, with optimized IRS configurations achieving up to 3-fold increases in energy collection efficiency compared to conventional ambient backscatter systems, thereby enabling more complex sensing and computation tasks while preserving the fundamental advantages of passive wireless communication [75, 76].

## 1.2 PLS Challenges in Wireless Communications

### 1.2.1 Fundamental Principles of PLS

PLS originates from the concept of the wiretap channel, first introduced by Wyner in [77], which laid the foundation for the theory of secure communication over noisy broadcast channels. The key insight is that the inherent spatial randomness and variability of wireless channels can be exploited to ensure security. Specifically, when the legitimate receiver's channel is stronger than that of a potential eavesdropper, secure communication can theoretically be achieved without the use of cryptographic keys [78].

PLS performance is traditionally measured by the secrecy capacity, which quantifies the maximum achievable rate of confidential information transmission that guarantees the eavesdroppers cannot decode the message. Positive secrecy capacity is obtained if the legitimate channel is stronger than the eavesdropping channel with respect SNR or similar important figures. The need for secure communications has driven a tremendous amount of research on strategies that improve the lawful link and degrade the eavesdropper's connection.

The realization of PLS has to cope with number of challenges. CSI is necessary to implement PLS techniques, but reliable CSI for eavesdroppers is difficult or even impossible to obtain. The problem is more complex when there are multiple eavesdroppers with unknown positions and power capabilities. In practice, secrecy performance can also be evaluated using metrics such as secrecy rate and secrecy outage probability, particularly under imperfect or unknown eavesdropper CSI.

### 1.2.2 Artificial Noise and Beamforming Approaches

Artificial noise (AN) injection has been widely recognized as one of the fundamental ways of realizing PLS in multi-antenna systems. At the heart of the approach is to transmit structured interference signals that can reduce the receive signal strength at eavesdroppers but with negligible effect on the actual signal quality of intended users. If the AN beamforming vectors are created properly, spatial nulls toward the legitimate receivers can be formed and the interference can be steered toward potential eavesdropping regions [79–81].

The optimal designs of information beamforming vectors and AN beamforming vectors need to be jointly optimized in the aforementioned AN-aided secure transmission systems [82, 83]. However, this joint optimization problem is generally non-convex and challenging to solve because of the interrelationship among various design variables and the existence of the secrecy rate constraints. And many optimization algorithms are designed to address this issue, such as SDR, SCA, AO and so on.

Beamforming is of fundamental importance to achieve PLS as it provides a means to control the spatial distribution of the transmitted signal. Multi-antenna transmitters are capable to direct narrow beams towards legitimate users and simultaneously place nulls in the direction the channel of known eavesdroppers [84–86]. However, traditional beamforming schemes have their limitations since it is difficult to know the location of eavesdroppers or the number of eavesdroppers is greater than the number of transmit antennas [87, 88]. To address this issue, practical PLS designs typically do not rely on precise eavesdropper CSI. Instead, AN injection, robust beamforming, and statistical CSI-based methods are

employed to degrade the signal quality in potential eavesdropping regions while preserving the performance of legitimate users.

### 1.2.3 Security Challenges in Emerging Wireless Technologies

The emergence of next-generation wireless technologies introduces unprecedented security vulnerabilities that cannot be adequately addressed by conventional security approaches, necessitating comprehensive rethinking of protection mechanisms across multiple technological domains [89, 90]. Massive multiple-input multiple-output (MIMO) systems, while offering substantial capacity improvements through spatial multiplexing, present fundamental security challenges related to CSI acquisition and pilot contamination attacks [91, 92]. The extensive antenna arrays and associated signal processing complexity create novel attack vectors for intelligent adversaries, particularly through pilot spoofing attacks where malicious entities transmit contaminated pilot sequences to compromise channel estimation processes, thereby enabling eavesdropping on subsequent data transmissions [93, 94]. Recent studies demonstrate that pilot contamination attacks can reduce system sum secrecy rates by up to 40% in massive MIMO environments, highlighting the critical need for robust detection mechanisms that employ ML techniques such as generative adversarial networks and deep neural networks to identify and mitigate these sophisticated threats [95, 96].

Millimeter-wave and terahertz (THz) communications, operating at frequencies ranging from 30 GHz to 10 THz, present a complex security paradigm characterized by both inherent advantages and unique vulnerabilities [97, 98]. The naturally high path loss and narrow beam characteristics of these frequency bands provide inherent security benefits through reduced spatial coverage and improved spatial isolation, making eavesdropping more challenging for unauthorized parties [99, 100]. However, these systems are simultaneously vulnerable to sophisticated attacks including beam alignment disruption, beam tracking interference, and targeted jamming that can exploit the high directivity requirements [101, 102]. The narrow beam vulnerability becomes particularly pronounced in mobile scenarios where precise beam alignment is crucial, as demonstrated by recent experimental studies showing that THz links can be effectively jammed with relatively low power when attackers position themselves

strategically within the beam path [103, 104]. Advanced threats such as "metasurface-in-the-middle" attacks have emerged, where adversaries deploy RISs to intercept and manipulate wireless backhaul communications in real-time [105].

IoT networks face distinctive security challenges stemming from the severe resource constraints of IoT devices and the massive scale of deployments across diverse application domains [106, 107]. Conventional cryptographic approaches often prove computationally intensive or energy-prohibitive for resource-constrained devices, with studies showing that traditional advanced encryption standard encryption can consume up to 70% of available processing power on low-end IoT microcontrollers [108, 109]. PLS emerges as a promising alternative that exploits the inherent randomness of wireless channels to establish secure communications without requiring complex key exchange protocols or computationally intensive encryption algorithms [110, 111]. Recent developments in lightweight cryptography, particularly the NIST-standardized ASCON family, demonstrate significant improvements in balancing security and efficiency, achieving comparable protection levels while reducing energy consumption by up to 60% compared to conventional approaches [112, 113]. However, the integration of PLS with IoT systems requires careful consideration of channel estimation accuracy, key generation rates, and synchronization requirements across heterogeneous device populations [114, 115].

NOMA systems introduce novel security challenges through their fundamental reliance on successive interference cancellation (SIC) and superposition coding principles [116, 117]. The shared transmission nature of NOMA creates opportunities for both external eavesdropping attacks, where unauthorized parties attempt to intercept signals intended for legitimate users, and internal eavesdropping scenarios where legitimate users may attempt to decode information intended for other users during the SIC process [118, 119]. Recent security analyses reveal that imperfect SIC implementation can lead to information leakage rates exceeding 20% in worst-case scenarios, particularly when strong users attempt to eavesdrop on weak users' communications [120, 121]. Power allocation strategies, user clustering algorithms, and interference management mechanisms become critical security components, with optimal solutions requiring joint optimization of secrecy rates and quality-of-service constraints

[122, 123]. Advanced security enhancement techniques include intelligent jamming strategies, adaptive beamforming, and dynamic user pairing algorithms that can achieve significant improvements in secrecy performance, with some approaches demonstrating up to 3-fold increases in achievable secrecy rates compared to conventional NOMA implementations [124, 125].

### 1.2.4 Machine Learning for PLS

The marriage of ML with PLS has been employed to achieve the security performance. Deep learning techniques may be applied for solving complex thereby being hard problems for security-related optimization which are difficult to obtain by traditional methodologies. Graph neural network (GNN) more specifically, have shown a promising potential for wireless communication problems as they are able to model intricate dependencies between network elements [126–130].

Reinforcement learning (RL)-based methods support adaptive security service that is able to learn to behave optimally according to the interaction with the RF environment [131, 132]. These methods can be particularly useful in situations that have unknown or dynamic eavesdropper behavior and one wishes to cause the legitimate system to be able to adjust its security strategy based on performance characterization. Since RL algorithms can deal with partial information and uncertainty, they are suitable for security scenarios.

Federated learning techniques that avoid transmitting raw data serve to mitigate privacy issues in distributed wireless networks while allowing joint learning [133–135]. This is especially true in the case of security applications since the exchange of sensitive information can violate the security of system resistance. Federated learning allows devices to participate in model training without revealing their data to the model, thus it makes it possible to construct defense mechanisms against security threats without sacrificing privacy [136].

The introduction of ML for PLS also gives rise to novel security threats, including model poisoning, adversarial attacks and privacy disclosure. Securing the ML algorithms themselves becomes an important consideration in the development of intelligent security

systems. Studies in this topic aim at designing the well-behaved AI systems resistant to a wide range of attacks.

## 1.3 Research Motivation and Contributions

The convergence of IRS, backscatter communications, and PLS represents a transformative opportunity to address the fundamental challenges facing next-generation wireless networks. While each of these technologies has demonstrated significant potential individually, their integration offers synergistic benefits that can substantially enhance both communication performance and security guarantees. Such a combination is particularly suitable for practical applications including IoT networks, smart environments, and industrial automation systems, where low-power devices require secure and reliable connectivity. In addition, it is relevant for scenarios such as wireless sensor networks, healthcare monitoring, and secure indoor communications, where IRS-assisted backscatter can provide energy-efficient communication while PLS mechanisms ensure protection against eavesdropping.

### 1.3.1 Research Motivation

The existing practices for wireless communication security and the recent advancement of new paradigms for novel system architectures determine the main theme of this research. However, computer security which is traditionally based on the complexity of computing problems and the fact that factoring large numbers is not feasible may be vulnerable when quantum computers become practical. In addition, there is a trend to have small devices for emerging application, e.g., in the area of IoT, and ambient intelligence, which imposes that security mechanisms do not add significant load on the computational capacity, or in energy consumption.

This work is particularly motivated by the high computational burden and energy consumption of conventional cryptography-based and artificial-noise-aided security schemes, which are unsuitable for large-scale 6G and IoT deployments.

PLS provides a fundamental solution to these issues by leveraging the nature of wireless channels themselves. However, traditional PLS methods are restricted because of the inability to control the wireless propagation environment. The recently proposed IRSs offer new means to design and mold wireless channels, allowing us to develop new kinds of PLS that were until now not feasible.

### 1.3.2 Core Contributions

This thesis makes several key contributions to the fields of IRS, backscatter communications, and PLS. The contributions are organized around three main themes: system design, optimization algorithms, and performance evaluation.

The first key contribution is the design of IRS-backscatter system architectures that exploit the capability of intelligent surfaces to enhance communication performance and improve security. In particular, a hybrid IRS-assisted framework is developed in which the IRS supports multiple functionalities, including enhancing the received signal quality at legitimate users through passive beamforming and generating AN to degrade potential eavesdropping channels.

The second significant contribution is the development of optimization frameworks based on ML techniques, particularly GNNs, for the joint design of active beamforming and IRS/STAR-RIS configurations. Compared with conventional optimization methods, the proposed approach can efficiently handle the high-dimensional and non-convex nature of the problem and adapt to varying channel conditions, providing improved performance and scalability.

The third contribution is the evaluation of security performance in IRS-assisted systems using secrecy rate-based metrics. The trade-offs between communication performance and security are investigated under different system parameters, including the number of IRS elements, user distributions, and channel conditions. Simulation results are provided to demonstrate the effectiveness of the proposed schemes in enhancing secrecy performance.

The fourth contribution focuses on the extension of IRS-assisted secure communication frameworks to more advanced system scenarios, including STAR-RIS-enabled multi-user

systems and radar-communication coexistence (RCC). In these scenarios, joint optimization of beamforming and surface configurations is performed to balance communication efficiency and security requirements. The results show that the proposed designs can effectively improve system performance under practical conditions.

Overall, this thesis provides a systematic investigation of IRS-assisted secure communication systems, combining system design, optimization, and simulation-based performance evaluation.

### 1.3.3 List of Papers

#### Published

B. Wu, S. Xu, Y. Shao, J. Zhang, and J. Zhang, "IRS backscatter based hybrid confidential information and AN for secrecy transmission," in *IEEE Commun. Lett.*, vol. 27, no. 2, pp. 462–466, Feb. 2023.

Y. Yao, B. Wu, Y. Shao, J. Zhang, and J. Zhang, "CPW-fed transparent antenna array using metal mesh," in *Proc. 17th Eur. Conf. Antennas Propag. (EuCAP)*, Mar. 2023, pp. 1–5.

Y. Du, S. Xu, G. Zhang, B. Wu, and J. Zhang, "Intelligent Reflecting Surface Backscatter Downlink Multi-User Communications With Radar Sensing," in *IEEE Trans. Veh. Technol.*, vol. 74, no. 5, pp. 8351–8356, May 2025.

#### Submitted

B. Wu, S. Xu, and J. Zhang, "Dual-Functional Design of STAR-RIS to Secure Indoor Multi-User Communications," *IEEE Trans. Veh. Technol.*.

#### Statement of Author Contribution

The contributions of the author to the published and submitted works listed below are summarized as follows.

1) IRS backscatter based hybrid confidential information and AN for secrecy transmission (IEEE Communications Letters, 2023)

For this work, B. Wu is the first author and made the primary contributions, including problem formulation, system model design, algorithm development, simulation implementation, and manuscript preparation.

2) CPW-fed transparent antenna array using metal mesh (EuCAP 2023)

For this work, B. Wu is not the first author. The contributions include assisting with simulation studies, contributing to manuscript preparation, and supporting the design and preparation of the presentation poster.

3) Intelligent Reflecting Surface Backscatter Downlink Multi-User Communications With Radar Sensing (IEEE Transactions on Vehicular Technology, 2025)

For this work, B. Wu contributed primarily to the implementation of simulation code and participated in the manuscript writing.

4) Dual-Functional Design of STAR-RIS to Secure Indoor Multi-User Communications (submitted to IEEE Transactions on Vehicular Technology)

For this work, B. Wu is the first author and made the main contributions, including system design, algorithm development, simulation implementation, and manuscript preparation.

## 1.4 Thesis organization

This thesis is organized into six chapters that progressively build from fundamental concepts to advanced system designs and performance analysis. Following this introductory chapter, the thesis proceeds as follows:

A full review of literature is presented in Chapter 2 to serve as the theoretical foundation for all chapters following. This chapter provides an overview of basic principles of IRS developed for channel modelling, and optimization and performance analysis. Signal detection, channel estimation, and multiple access methods are described, and we conclude with the basics of backscatter communications. Finally, the chapter also discusses the fundamentals of PLS such as information-theoretic security metrics and implementation aspects. The

chapter is closed with an overview of ML methods that are employed for wireless communications, specifically focusing on GNNs and how they are used for communication system optimization.

In Chapter 3, we propose the first major contribution of this thesis: a hybrid confidential information and AN system for secure communications (known as an IRS backscatter system). For this scenario, we present a new system paradigm, in which Alice (the sender) confidentially communicates with Bob (the intended receiver), while a third party, Eve (the eavesdropper), eavesdrop on the information flow. The novelty of the work is to use IRS for improving the legitimate and deceiving the eavesdropping communication channel at the same time. The chapter presents system modeling, the optimization problem formulation to minimize the transmit power under secrecy constraints, and the AO algorithm for joint active and passive beamforming design. Simulation results validate the effectiveness of the proposed algorithm over RIS-based schemes and classical beamforming.

The second and third main contribution is introduced in Chapter 4 that proposes the GNN-based STAR-RIS for secure indoor multi-user communications. In this chapter, we consider the more difficult scenario of indoor multi-user systems, where all legitimate users share the same vector consisting of confidential information and whenever a user receives confidential information, outdoor eavesdroppers work as hard as possible to overhear that user's information. The chapter presents a dual-functional STAR-RIS architecture that works at two time-scales: channel-level variation for reflection optimization and symbol-level variation for artificial noise adaptation. We propose a new GNN structure to optimize the beamforming vectors and STAR-RIS coefficients simultaneously. The GNN method allows scalable and flexible optimization over different number of users and IRS elements. Extensive simulation results show the remarkable performance gains over existing methods.

In Chapter 5, we present the fourth major contribution of this thesis, which investigates IRS-backscatter enabled downlink multi-user communications under RCC. The chapter begins with the motivation and system architecture, followed by a mathematical model that characterizes the dual-function radar waveform and the received signals at both users and

radar. A joint optimization problem is then formulated to design radar transmit signals, IRS coefficients, and user allocation, and an AO algorithm is proposed to solve it efficiently.

The computational complexity of the framework is analyzed, and extensive simulations are conducted to evaluate convergence, the impact of system parameters, and comparisons with baseline schemes. The results highlight clear trade-offs between secure communication rates and radar sensing requirements.

Chapter 6 concludes the thesis by summarizing the main contributions and discussing their practical implications for IRS- and STAR-RIS-assisted secure communication systems. Instead of providing broad and generic future visions, the chapter focuses on identifying the key limitations of the current work and proposing targeted research directions to address them. In particular, the discussion highlights several practical aspects that require further investigation, including robust channel estimation under imperfect CSI, geometry-aware IRS/STAR-RIS deployment, generalization of GNN-based optimization across different environments, and the impact of hardware constraints and non-ideal implementations. In addition, more realistic eavesdropping models and the integration of sensing, communication, and security are discussed as important extensions.

The thesis includes extensive appendices that provide detailed mathematical derivations, algorithm implementations, and additional simulation results. These appendices serve as valuable resources for researchers and practitioners interested in implementing the proposed techniques or extending the research in new directions.

We illustrate the practical significance of our theoretical findings with extensive simulation results with practical channel models and system parameters throughout the thesis. The simulation cases are designed to investigate the impact of key system parameters, including the number of users, transmit power, and the number of IRS/STAR-RIS elements, as well as the effects of imperfect CSI. Performance is assessed primarily in terms of weighted sum rate (WSR), which reflects both communication efficiency and security performance, along with robustness under channel estimation errors and varying eavesdropper distributions.

# Chapter 2

# Literature Review

## Overview

Recent advances in wireless communication systems, the development of intelligent, energy efficient and secure networks require the investigation of new paradigms that go far beyond standard solutions. This chapter gives a detailed theoretical base for the underlying technologies which are considered in the thesis, including what are referred to as IRS, backscatter communications, STAR-RIS, RCC systems and ML based methods for wireless communications optimization.

## 2.1 IRS Working Principles and Key Technologies

IRS is a novel paradigm that turns the programmable but challenging-to-control wireless propagation channel in traditional deployment of wireless networks to a favorable environment that is fully reconfigurable and controllable at transceivers' side [4, 137]. The basis of such IRS technology is precisely steering the electromagnetic wave propagation by regulating the phase and amplitude of incident signals. To understanding, Fig. 2.1 illustrates the working principles and key components of an IRS-assisted wireless communication system.

### 2.1.1 Electromagnetic Foundations and Wave Manipulation

The working mechanism of IRS is fundamentally based on electromagnetic wave theory and scattering. When an electromagnetic wave is incident on an IRS element, the reflected wave can be described using the generalized Snell's law of reflection that considers the phase discontinuity induced by the metasurface. For an incident wave of wave vector $\mathbf{k}_i$ and a reflected wave of wave vector $\mathbf{k}_r$, the relationship is given by:

$$k_{r,x} - k_{i,x} = \frac{1}{2\pi}\frac{\partial \Phi(x,y)}{\partial x} \tag{2.1}$$

where $\Phi(x,y)$ is SN phase profile and $k_{r,x}$ and $k_{i,x}$ are, respectively, the $x$-component of the reflected and incident wave numbers [137].

The scattering property of an IRS element can be represented by its (complex) reflection coefficient that specifies the amplitude and phase alteration imposed on the incoming wave. Then, the reflection coefficient of $l$-th element of IRS with totally $L$ elements can be formulated as:

$$\Gamma_l = |\Gamma_l| e^{j\phi_l} \tag{2.2}$$

where $|\Gamma_l| \in [0,1]$ is the amplitude reflection coefficient and $\phi_l \in [0, 2\pi)$ is a the phase shift induced by the $l$-th element. The limitation $|\Gamma_l| \leq 1$ represents the passive property of IRS elements that are unable to introduce signal gain.

The general response of an IRS consisting of $L$ elements can be described by the diagonal reflection matrix:

$$\Phi = \text{diag}(\Gamma_1, \Gamma_2, \ldots, \Gamma_L) = \text{diag}(|\Gamma_1| e^{j\phi_1}, |\Gamma_2| e^{j\phi_2}, \ldots, |\Gamma_L| e^{j\phi_L}) \tag{2.3}$$

This matrix representation enables systematic analysis and optimization of IRS-assisted communication systems within the framework of linear algebra and matrix theory.

### 2.1.2 Channel Modeling for IRS-Assisted Systems

Channel modeling for IRS-aided wireless systems entails the modeling of the combined channel with direct and IRS-reflected path s. We consider a communication system where a BS with $N_t$ antennas communicates with a user with $N_r$ antennas aided by an IRS with $L$ elements.

The received signal at the user can be expressed as:

$$\mathbf{y} = (\mathbf{H}_d + \mathbf{H}_r \Phi \mathbf{H}_t)\mathbf{x} + \mathbf{n} \tag{2.4}$$

where $\mathbf{H}_d \in \mathbb{C}^{N_r \times N_t}$ represents the direct channel from the BS to the user, $\mathbf{H}_t \in \mathbb{C}^{L \times N_t}$ denotes the channel from the BS to the IRS, $\mathbf{H}_r \in \mathbb{C}^{N_r \times L}$ characterizes the channel from the IRS to the user, $\mathbf{x} \in \mathbb{C}^{N_t \times 1}$ is the transmitted signal vector, and $\mathbf{n} \in \mathbb{C}^{N_r \times 1}$ represents the additive white Gaussian noise vector.

The effective channel incorporating the IRS contribution is given by:

$$\mathbf{H}_{\text{eff}} = \mathbf{H}_d + \mathbf{H}_r \Phi \mathbf{H}_t \tag{2.5}$$

This formulation captures the fundamental trade-off between the number of IRS elements, their individual reflection coefficients, and the resulting channel enhancement. The optimization of $\Phi$ to maximize communication performance represents a central challenge in IRS-assisted system design.

### 2.1.3 Metasurface Design and Implementation Considerations

Suffiently realizing IRS needs to realize subwavelength scattering structures in practice. Elements generally are made by patterning metal on a dielectric substrate, and the geometry is used to determine the electrical response. The most popular applications are as follows:

Patch Element: Rectangular or circular metal patches with certain dimensions and separation determining the resonant frequency and scattering properties. The phase reflection can be controlled by altering the patch size or slits and gaps.

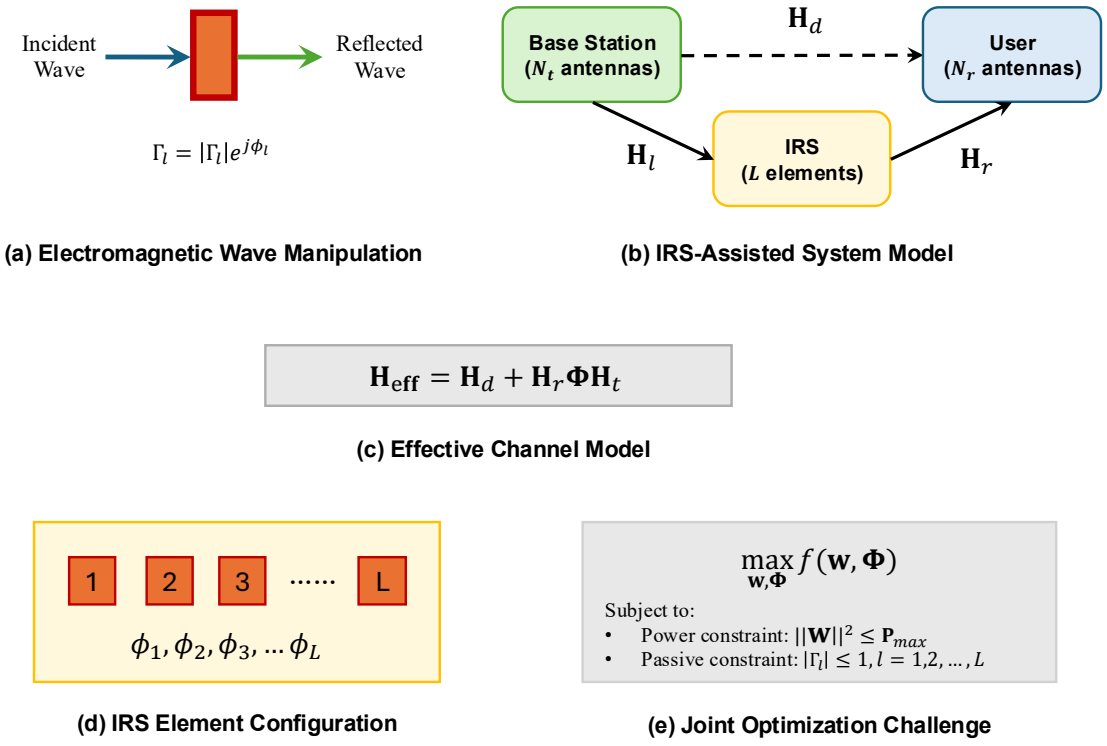


Fig. 2.1 IRS working principles and channel modeling fundamentals. (a) Electromagnetic wave manipulation showing incident wave reflection with controllable phase shift through reflection coefficient $\Gamma_l = |\Gamma_l| e^{j\phi_l}$. (b) IRS-assisted system model illustrating the BS, IRS panel with $L$ elements, and user with respective channel matrices $\mathbf{H}_t$, $\mathbf{H}_r$, and direct channel $\mathbf{H}_d$. (c) Effective channel formulation combining direct and IRS-reflected paths as $\mathbf{H}_{\text{eff}} = \mathbf{H}_d + \mathbf{H}_r \mathbf{\Phi} \mathbf{H}_t$. (d) IRS element configuration showing individual phase control capabilities for beamforming optimization. (e) Joint optimization challenge highlighting the non-convex nature of simultaneous active and passive beamforming design under power and passive element constraints.

Elements that are based on dipoles: They are linear conductors with dipsolar scattering. The phase response is determined by the length and orientation of the dipoles, which is often achieved using varactor diodes for dynamic control.

Ring Resonator Elements: Circular or rectangular ring devices that allow for excess degrees of freedom in phase manipulation by simply scaling all outer and inner radii.

Surface impedance characterizes the physical size of a metasurface element and its associated electromagnetic property's relationship. The reflection coefficient for a lossless metasurface element with a surface impedance $Z_s$ is:

$$\Gamma = \frac{Z_s - \eta_0}{Z_s + \eta_0} \tag{2.6}$$

where $\eta_0 = 377\ \Omega$ is the impedance of free space. By controlling the surface impedance through geometric and material parameters, the desired phase and amplitude response can be achieved.

The physical realization of reconfigurable IRS also involves the inclusion of active components, electro-magnetic switches such as the PIN or varactor diodes, or the micro-electromechanical systems (MEMS) switches. Such features facilitate that the reflection coefficients change dynamically based on control signals received from a central controller. The compromises among switch speed, power consumption and phase resolution are important factors to be considered in practical IRS design [138, 139].

### 2.1.4 Performance Analysis and Optimization

The performance analysis of IRS-assisted systems involves characterization of key metrics such as signal-to-noise ratio (SNR), channel capacity, and energy efficiency. For a single-user system with optimal beamforming and IRS configuration, the achievable rate is given by:

$$R = \log_2\left(1 + \frac{P\|\mathbf{H}_{\text{eff}}\mathbf{w}_{\text{opt}}\|^2}{\sigma^2}\right) \tag{2.7}$$

where $P$ is the transmit power, $\mathbf{w}_{\text{opt}}$ is the optimal transmit beamforming vector, and $\sigma^2$ is the noise power.

The joint optimization of transmit beamforming and IRS reflection coefficients represents a challenging non-convex optimization problem due to the multiplicative coupling between optimization variables. The general formulation can be expressed as:

$$\begin{aligned} \max_{\mathbf{w},\Phi} \quad & f(\mathbf{w},\Phi) \\ \text{s.t.} \quad & \|\mathbf{w}\|^2 \leq P_{\max} \\ & |\Gamma_l| \leq 1, \quad l = 1,2,\ldots,L \end{aligned} \tag{2.8}$$

where $f(\mathbf{w},\Phi)$ represents the objective function (e.g., sum rate, energy efficiency) and $P_{\max}$ is the maximum transmit power constraint.

## 2.2 Backscatter Communication Principles and Development

Backscatter communication is a disruptive method for wireless networking, which allows batteryless communication devices to modulate and reflect existing or dedicated RF signal to transfer information [140, 141]. This technology gets attracted a lot of attention because it can be a key for ULP IoT applications and ambient intelligence systems.

### 2.2.1 Fundamental Principles of Backscatter Communication

Backscatter communication is based on load modulation, in which the antenna load impedance of a backscatter device is varied to modulate the radar cross section (RCS) and hence the properties of the reflected signals. Conceptually, when an RF wave impinges on a backscatter device, the reflected signal can be expressed as [140]:

$$s_r(t) = \rho(t) \cdot s_i(t), \tag{2.9}$$

where $s_i(t)$ is the incident signal, $s_r(t)$ is the reflected signal, and $\rho(t)$ is the time-varying reflection coefficient that carries the information.

The reflection coefficient $\rho(t)$ is determined by the antenna load impedance $Z_L(t)$ as

$$\rho(t) = \frac{Z_L(t) - Z_a^*}{Z_L(t) + Z_a}, \tag{2.10}$$

where $Z_a$ is the antenna impedance and $Z_a^*$ denotes its complex conjugate. By switching the load impedance among multiple states, different reflection coefficients can be generated, enabling the encoding of digital information.

For example, in binary modulation, the load impedance alternates between two states:

$$Z_L(t) = \begin{cases} Z_1, & \text{for bit 0} \\ Z_2, & \text{for bit 1} \end{cases} \tag{2.11}$$

leading to two corresponding reflection coefficients

$$\rho_0 = \frac{Z_1 - Z_a^*}{Z_1 + Z_a}, \quad \rho_1 = \frac{Z_2 - Z_a^*}{Z_2 + Z_a}. \tag{2.12}$$

More generally, by selecting multiple impedance states, a set of complex reflection coefficients $\{\rho_m\}$ can be constructed to realize higher-order modulation schemes, where both amplitude and phase variations can be exploited.

### 2.2.2 Backscatter Communication Systems

Backscatter communication systems enable ULP wireless transmission by allowing devices to convey information through the reflection of incident RF signals rather than generating their own carrier signals. In a typical setup, an ambient RF source illuminates the environment, and a passive device modulates its information by adjusting its load impedance, thereby changing the reflection characteristics of the incident signal. This mechanism eliminates the need for active RF chains, making backscatter communication particularly suitable for energy-constrained applications such as IoT networks and large-scale sensor deployments [44, 142, 143].

From a system modeling perspective [43, 45], the received signal can be generally expressed as

$$y = \mathbf{g}^H \Theta \mathbf{h} x + n, \tag{2.13}$$

where $\mathbf{h}$ denotes the channel from the RF source to the reflecting device, $\mathbf{g}$ represents the channel from the device to the receiver, $\Theta$ is the reflection coefficient matrix, $x$ is the incident signal, and $n$ denotes additive noise. The matrix $\Theta = \text{diag}\{\beta_1 e^{j\theta_1}, \ldots, \beta_L e^{j\theta_L}\}$ captures how each reflecting element modulates the signal through amplitude $\beta_l$ and phase $\theta_l$ adjustments.

Traditional backscatter systems typically rely on simple modulation schemes, such as binary on-off keying, which limits their flexibility and achievable data rates. Recent advancements have extended this paradigm by integrating backscatter communication with IRS, where a large number of programmable elements enable fine-grained control of the reflection coefficients. In such IRS-backscatter systems [49, 50], the reflecting surface itself can be interpreted as a distributed modulator, where information is embedded into the reflected signal through coordinated adjustment of $\Theta$.

This integration introduces additional degrees of freedom that go beyond conventional backscatter communication. Specifically, the reflection coefficients can be jointly optimized to achieve both information modulation and spatial signal shaping. In a general form, the reflected signal can be viewed as a combination of multiple components,

$$\Theta = \Theta_{\text{s}} + \Theta_{\text{i}}, \tag{2.14}$$

where $\Theta_{\text{s}}$ corresponds to the information-bearing component and $\Theta_{\text{i}}$ represents additional components that can be used for interference shaping or other design objectives.

As a result, IRS-assisted backscatter systems provide a unified framework for signal modulation and propagation control. By properly designing $\Theta$, the system can enhance the desired signal at intended receivers while suppressing undesired signal leakage in other spatial directions. This capability not only improves communication reliability and coverage but also lays the foundation for advanced functionalities such as physical layer security and integrated sensing. Consequently, backscatter communication, when combined with IRS

technologies, evolves from a simple reflection-based mechanism into a powerful tool for intelligent wireless environment design.

## 2.3 STAR-RIS Introduction and Advantages

STAR-RIS are a great leap over traditional IRS in terms of full-space coverage and functionality improvement [144, 145]. Compared with the conventional IRS that can only reflect the incident power signal, the STAR-RIS can work in both transmission and reflection modes at the same time, thus achieving the 360-degree coverage and offering higher freedom degrees for the system optimization.

### 2.3.1 Theoretical Model and Principles

A STAR-RIS is an advanced metasurface architecture that enables simultaneous manipulation of electromagnetic waves in both reflection and transmission domains. Unlike conventional IRS, which operate only in reflection mode and provide coverage over a half-space, STAR-RIS extends the functionality to full-space coverage by jointly controlling both reflected and transmitted signals.

Specifically, each STAR-RIS element splits the incident signal into two components: a reflected component and a transmitted component. By adjusting the amplitude and phase of each component, the STAR-RIS can flexibly shape the propagation environment. This dual-functional capability introduces additional spatial degrees of freedom, which can be exploited to enhance communication performance and improve PLS.

From a signal processing perspective, the STAR-RIS is characterized by two coefficient matrices, corresponding to reflection and transmission operations as illustrated in Fig. 2.2. These coefficients determine how the incident signal is partitioned and phase-shifted. Due to physical constraints, the total energy of the reflected and transmitted components is limited by the incident signal power, leading to the following constraint at each element:

$$\alpha_l^{\mathrm{r}} + \alpha_l^{\mathrm{t}} \leq 1, \quad \forall l, \tag{2.15}$$

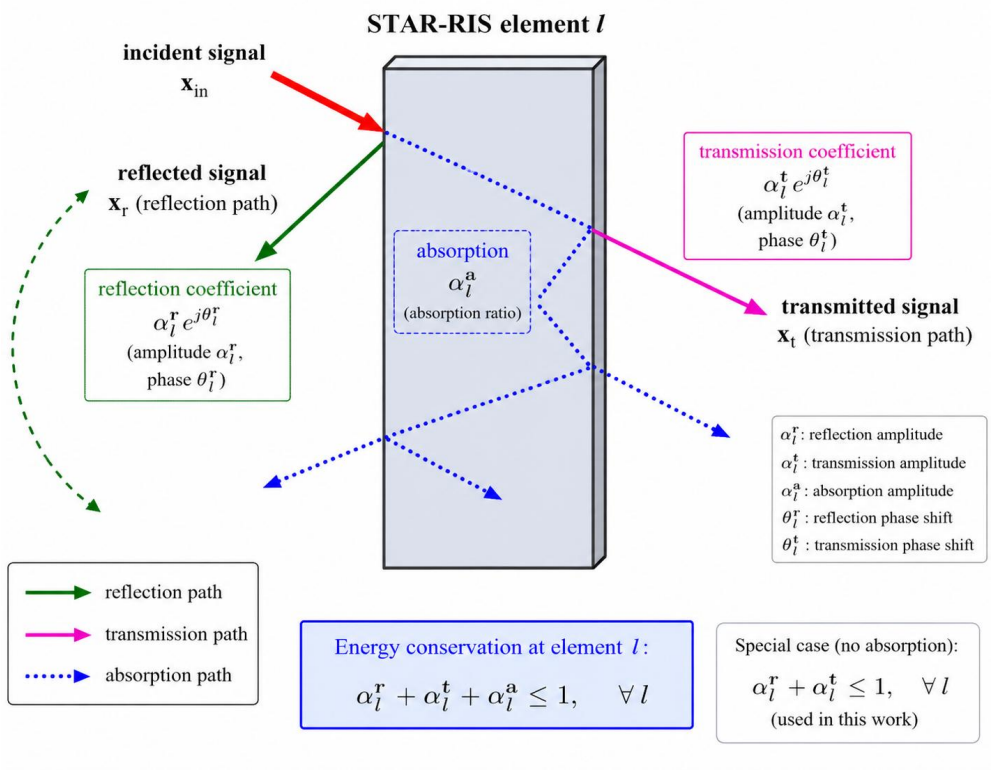


Fig. 2.2 Simplified illustration of STAR-RIS operation, where the incident signal is split into reflected and transmitted components. The amplitudes $\alpha_l^{\text{r}}$ and $\alpha_l^{\text{t}}$ control the signal partitioning subject to the energy conservation constraint $\alpha_l^{\text{r}} + \alpha_l^{\text{t}} \leq 1$.

which reflects the energy conservation property of the STAR-RIS hardware.

Compared with conventional IRS, the STAR-RIS provides significantly enhanced flexibility. In particular, it enables the system to serve users located on different sides of the surface simultaneously. For secure communication scenarios, this property is especially useful, as it allows the system to enhance legitimate users in one region while distributing AN toward potential eavesdroppers in another region.

It is important to clarify the distinction between the IRS-backscatter model considered in Chapter 3 and the STAR-RIS model adopted in this chapter. Although both models employ reconfigurable coefficient matrices with similar mathematical structures, their physical architectures and functionalities are fundamentally different.

In the IRS-backscatter system (Chapter 3), the controllable coefficients are used to implement backscatter-enabled passive modulation, where the reflected signal carries information

or AN through load-dependent scattering. In contrast, the STAR-RIS considered in this chapter is a dual-functional metasurface that simultaneously supports signal reflection and transmission.

Furthermore, unlike conventional IRS architectures that are limited to half-space (180-degree) coverage due to their reflecting-only operation, the STAR-RIS enables full-space (360-degree) coverage by simultaneously controlling the reflected and transmitted signals. This property allows the system to enhance legitimate users on one side while injecting AN toward potential eavesdroppers on the opposite side. As summarized in Table 2.1, the IRS-backscatter model in Chapter 3 and the STAR-RIS model in this chapter differ in terms of system architecture, functional roles of the coefficients, signal operation, and spatial coverage.

Table 2.1 Comparison between IRS-Backscatter and STAR-RIS

| **Aspect** | **IRS-Backscatter (Chapter 3)** | **STAR-RIS (Chapter 4)** |
|---|---|---|
| Architecture | IRS-assisted backscatter system | Simultaneous transmitting-and-reflecting RIS system |
| Function | Passive backscatter modulation | Dual reflection and transmission control |
| Coefficient role | Used for modulation and security | Used for beamforming and AN |
| Signal operation | Passive reradiation via backscatter | Simultaneous reflection and transmission |
| AN | Generated via backscatter modulation | Generated via transmission coefficients |
| Coverage | Half-space (180-degree) | Full-space (360-degree) |
| Security design | Hybrid signal + AN via backscatter | Spatial separation of users and eavesdroppers |

### 2.3.2 Multi-User System Modeling

A STAR-RIS enables simultaneous manipulation of incident signals in both transmission and reflection domains. Each element is characterized by complex transmission and reflection coefficients, defined as

$$\tau_l = |\tau_l| e^{j\phi_l^t}, \quad \rho_l = |\rho_l| e^{j\phi_l^r}, \tag{2.16}$$

where $\tau_l$ and $\rho_l$ denote the transmission and reflection coefficients of the $l$-th element, respectively. Although they share the same mathematical form, they correspond to two

different physical propagation modes. Specifically, $\rho_l$ controls the signal reflected toward the same side of the surface as the transmitter (reflection region), while $\tau_l$ controls the signal transmitted through the surface toward the opposite side (transmission region).

The overall STAR-RIS can be represented by two diagonal matrices:

$$\Phi^t = \text{diag}(\tau_1, \tau_2, \ldots, \tau_L), \tag{2.17}$$

$$\Phi^r = \text{diag}(\rho_1, \rho_2, \ldots, \rho_L), \tag{2.18}$$

which enable independent control of transmission and reflection responses.

Consider a STAR-RIS assisted communication system where a BS serves multiple users located on both sides of the surface. Users on the reflection side are served via the reflection mode, while users on the transmission side are served via the transmission mode.

For a user $k$ on the reflection side, the received signal is given by

$$y_k^r = \left(\mathbf{h}_{d,k}^r + \mathbf{h}_{r,k}^r \Phi^r \mathbf{h}_t\right) \mathbf{x} + n_k^r, \tag{2.19}$$

where $\mathbf{h}_{d,k}^r$ denotes the direct channel from the transmitter to user $k$, $\mathbf{h}_t$ is the channel from the transmitter to the STAR-RIS, and $\mathbf{h}_{r,k}^r$ represents the channel from the STAR-RIS to the user on the reflection side. The matrix $\Phi^r$ contains the reflection coefficients of the STAR-RIS elements.

For a user $j$ on the transmission side,

$$y_j^t = \left(\mathbf{h}_{d,j}^t + \mathbf{h}_{t,j}^t \Phi^t \mathbf{h}_t\right) \mathbf{x} + n_j^t, \tag{2.20}$$

where $\mathbf{h}_{t,j}^t$ represents the channel from the STAR-RIS to the user on the transmission side, and $\Phi^t$ contains the transmission coefficients. Unlike the reflection-side signal, this component corresponds to the signal transmitted through the STAR-RIS rather than reflected.

The overall system sum rate is expressed as

$$R_{\text{sum}} = \sum_{k=1}^{K_r} R_k^r + \sum_{j=1}^{K_t} R_j^t, \tag{2.21}$$

where $K_r$ and $K_t$ denote the numbers of users in the reflection and transmission regions, respectively.

### 2.3.3 Optimization Challenges and Solutions

The optimization of STAR-RIS systems involves joint design of the transmission coefficients $\Phi^t$, reflection coefficients $\Phi^r$, and active beamforming at the BS. The general optimization problem can be formulated as:

$$\begin{aligned} \max_{\mathbf{W},\Phi^t,\Phi^r} \quad & f(\mathbf{W},\Phi^t,\Phi^r) \\ \text{s.t.} \quad & \text{Tr}(\mathbf{W}) \le P_{\max} \\ & |\tau_l|^2 + |\rho_l|^2 \le 1, \quad l = 1,\ldots,L \\ & \gamma_k^r \ge \gamma_{\min}, \quad k = 1,\ldots,K_r \\ & \gamma_j^t \ge \gamma_{\min}, \quad j = 1,\ldots,K_t \end{aligned} \tag{2.22}$$

such that $\mathbf{W}$ is the precoding matrix, and $\gamma_k^r$ and $\gamma_j^t$ are the SINRs of reflection-side and transmission-side users, respectively, and $\gamma_{\min}$ is the SINR requirement.

This optimization is much more difficult than the ordinary IRS optimization as a result of:

- Enhanced dimensionality: Transmission and reflection coefficients must be simultaneously maximized
- Coupling constraints: Conductance conservation: Coupling coefficient between $\tau$ and $\rho$ is power conservation.
- Inter-user Interference: Users on the opposite side of the surface can interfere with each other

Advanced optimization methods, including SCA, fractional programming and AO, have been introduced to tackle these issues.

### 2.3.4 Practical Implementation Considerations

While the above discussion focuses on the theoretical modeling of STAR-RIS, it is important to relate the adopted coefficient-based formulation to practical hardware implementations [146].

Fig. 2.3 illustrates a circuit-level comparison between the IRS-backscatter and STAR-RIS architectures. For IRS-backscatter systems, each element is typically implemented using a load modulation circuit. Specifically, switchable impedance loads (e.g., $Z_0$ and $Z_1$) are connected to the antenna element via PIN diodes. By toggling between different load states, the reflected signal is modulated, enabling passive transmission of information or AN.

In contrast, the STAR-RIS requires a more advanced hardware structure to support simultaneous reflection and transmission. As shown in Fig. 2.3, each STAR-RIS element consists of two controllable branches corresponding to reflection and transmission. Tunable components such as varactor diodes are used to adjust the phase response, while PIN diodes or MEMS switches control the signal paths and amplitude responses.

From a signal processing perspective, the reflection and transmission coefficients introduced in the theoretical model correspond directly to these hardware-controlled responses. In particular, the amplitudes $\alpha_l^{\mathrm{r}}$ and $\alpha_l^{\mathrm{t}}$ represent the power allocation between reflection and transmission, while the phase shifts determine the beamforming direction. The constraint $\alpha_l^{\mathrm{r}} + \alpha_l^{\mathrm{t}} \leq 1$ reflects the physical energy conservation limitation, where part of the incident energy may be dissipated due to hardware losses.

This correspondence between circuit implementation and mathematical modeling ensures that the proposed STAR-RIS framework is not only theoretically sound but also practically realizable.

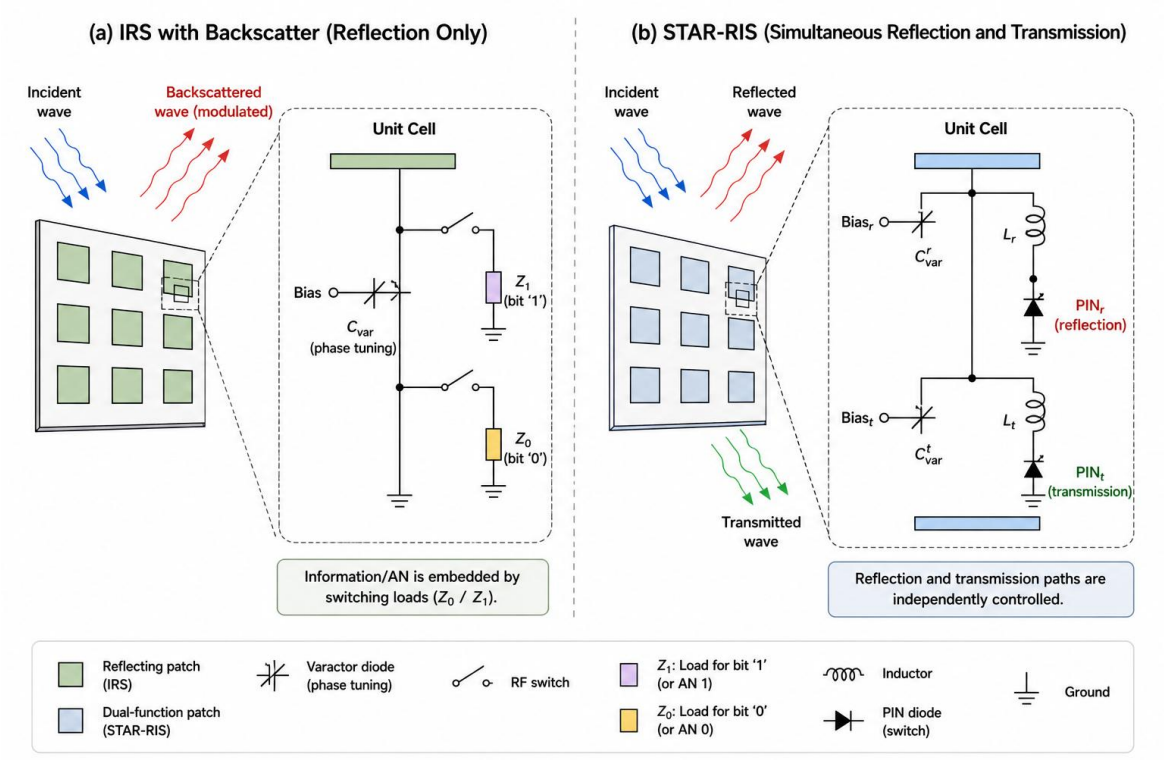


Fig. 2.3 Circuit-level comparison between IRS-backscatter and STAR-RIS elements. The IRS-backscatter element performs load modulation through switching impedance states, while the STAR-RIS element employs dual controllable branches to independently regulate reflection and transmission.

## 2.4 Radar and Communication Coexistence System Framework

The fusion of wireless communication and radar sensing capabilities is an important breakthrough in future wireless networks, especially under the background of autonomous systems, smart cities, and IoT applications [147]. This Preparation formulates the theoretical basis for RCC and integrated sensing and communication (ISAC) systems [148–150].

The integration between radar and communications results from their common use of electromagnetic wave propagation and of signal processing concepts. The two systems employ the same hardware elements, frequency bands and signal processing algorithms, and therefore, their combination becomes technically feasible and financially advantageous.

The base-band signal model of an integrated radar-communication system is given by:

$$s(t) = s_c(t) + s_r(t) \tag{2.23}$$

where $s_c(t)$ represents the communication signal component and $s_r(t)$ denotes the radar signal component. The design challenge lies in optimizing both components to achieve satisfactory performance for both functionalities. It should be noted that, although $s_c(t)$ and $s_r(t)$ are transmitted over the same physical medium, they may experience different effective channels due to their distinct propagation paths, target reflections, and beamforming designs. In particular, the radar component typically involves round-trip propagation via target scattering, while the communication component follows a direct or IRS-assisted link to the receiver.

For a general multi-carrier waveform applicable to joint radar and communication systems, the transmitted signal can be written as:

$$s(t) = \sum_{n=0}^{N-1} \sum_{k=0}^{K-1} d_{n,k} g(t - nT - kT_c) e^{j2\pi f_k t} \tag{2.24}$$

where $d_{n,k}$ represents the data symbols, $g(t)$ is the pulse shaping function, $T$ is the symbol duration, $T_c$ is the chip duration, $f_k$ is the subcarrier frequency, and $N$ and $K$ are the numbers of symbols and subcarriers, respectively.

## 2.5 Machine Learning Fundamentals and Algorithm Principles

The incorporation of ML methodologies in wireless communication systems has become a revolutionary paradigm in dealing with various complexities and headaches related to conventional networks. This chapter offers the groundwork of the ML algorithms used in this thesis, in focus are GNNs and their applications towards IRS-assisted systems.

### 2.5.1 Deep Learning Foundations for Wireless Communications

Deep learning has revolutionized wireless communications by providing powerful tools for pattern recognition, optimization, and decision making in complex, high-dimensional environments [151–153]. The fundamental building block of deep neural networks is the artificial neuron, which computes a weighted sum of inputs followed by a nonlinear activation function:

$$y = f\left(\sum_{i=1}^{n} w_i x_i + b\right) \tag{2.25}$$

where $x_i$ are input features, $w_i$ are weights, $b$ the bias term $f(\cdot)$ an activation function, and $n$ denotes the number of input features to the neuron.

For wireless communication tasks, the universal approximation theorem offers a theoretical guarantee to employ neural networks to approximate complicated channel models and optimization objectives. Any continuous function can be approximated to arbitrary precision by a multilayer perceptron (MLP) with enough hidden units:

$$\hat{f}(\mathbf{x}) = \sum_{j=1}^{M} \alpha_j \sigma\left(\sum_{i=1}^{d} w_{ji} x_i + b_j\right) \tag{2.26}$$

where $\sigma(\cdot)$ is the activation function, $\alpha_j$ are the output layer weights, $w_{ji}$ are the hidden layer weights, and $M$ is the number of hidden units, while $d$ represents the dimensionality of the input vector $\mathbf{x}$.

### 2.5.2 GNNs for Wireless Network Optimization

GNNs are particularly suitable for wireless systems due to their ability to model structured interactions among multiple entities. In STAR-RIS-assisted networks, the BS, STAR-RIS elements, and users are inherently coupled through wireless channels, which can be naturally represented as a graph.

As illustrated in Fig. 2.4, the overall framework consists of three main components: graph representation, GNN-based message passing, and output generation.

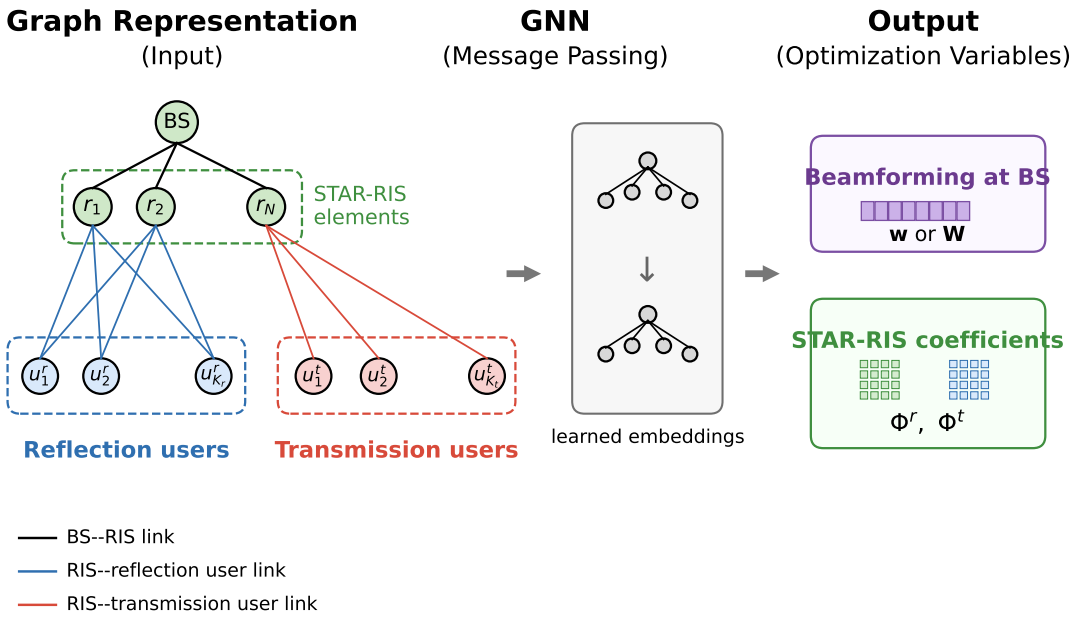


Fig. 2.4 GNN framework for STAR-RIS-assisted wireless optimization. The system is represented as a graph, where nodes correspond to the BS, STAR-RIS elements, and users, while edges denote wireless links. The GNN performs message passing over the graph and outputs the beamforming variables and STAR-RIS reflection and transmission coefficients.

**Graph representation:** The left part of Fig. 2.4 shows how the wireless system is mapped into a graph. The BS, STAR-RIS elements, and users are modeled as nodes. The edges correspond to physical wireless links, including the BS–RIS link, RIS–reflection-user links, and RIS–transmission-user links.

In particular, the STAR-RIS elements are grouped as intermediate nodes that connect the BS and users, capturing the cascaded channel structure. The reflection-side users and transmission-side users are explicitly separated, which corresponds to the two different propagation modes introduced in Chapter 2. This graph structure preserves both the spatial topology and the channel dependency of the system.

Each node is associated with features derived from system parameters, such as CSI, user type (reflection or transmission), and potentially location or QoS requirements. These features serve as the input to the GNN.

**Message passing mechanism:** The middle part of Fig. 2.4 illustrates the GNN module. The GNN updates node representations through iterative message passing, where each node aggregates information from its neighbors. The general update rule is given by

$$\mathbf{h}_v^{(l+1)} = \text{UPDATE}^{(l)}\left(\mathbf{h}_v^{(l)}, \text{AGGREGATE}^{(l)}\left(\{\mathbf{h}_u^{(l)} : u \in \mathcal{N}(v)\}\right)\right). \tag{2.27}$$

From a physical perspective, this operation corresponds to information exchange over the wireless network. For example, STAR-RIS element nodes receive information from both the BS and users, allowing them to learn how to jointly adjust reflection and transmission behaviors. Similarly, user nodes aggregate information from connected RIS elements, capturing interference and coupling effects.

Through multiple layers, the GNN effectively captures high-order interactions, which correspond to multi-hop signal propagation paths in the wireless system.

**Output mapping:** The right part of Fig. 2.4 shows the output of the GNN. After message passing, the learned node embeddings are mapped to the optimization variables of the system. Specifically, the outputs include beamforming vector or matrix at the BS, STAR-RIS reflection coefficient matrix $\Phi^r$, and STAR-RIS transmission coefficient matrix $\Phi^t$.

These variables correspond exactly to those in the system model and optimization problem formulated in Chapter 4.

**Connection to Chapter 4.4:** The proposed GNN framework establishes a direct mapping from the system state (i.e., graph-structured CSI and topology) to the optimization variables. In Section 4.4, this mapping is learned from data, enabling the GNN to approximate the solution of the joint beamforming and STAR-RIS optimization problem.

Compared with conventional iterative algorithms, which solve the optimization problem repeatedly for each channel realization, the GNN provides a feedforward solution once trained. This significantly reduces computational complexity while maintaining the ability to adapt to different channel conditions and user configurations.

Therefore, Fig. 2.4 not only illustrates the structure of the GNN, but also explicitly bridges the gap between the physical wireless system, the mathematical optimization problem, and the learning-based solution proposed in this thesis.

### 2.5.3 Optimization Algorithms for Non-Convex Problems

The optimization problems arising in IRS-assisted systems are typically non-convex due to the multiplicative coupling between optimization variables [154]. Several advanced optimization techniques have been developed to address these challenges:

**Alternating Optimization:** Decomposes the joint optimization problem into subproblems that are solved alternately:

$$\begin{aligned} \mathbf{x}^{(k+1)} &= \arg\min_{\mathbf{x}} f(\mathbf{x}, \mathbf{y}^{(k)}) \\ \mathbf{y}^{(k+1)} &= \arg\min_{\mathbf{y}} f(\mathbf{x}^{(k+1)}, \mathbf{y}) \end{aligned} \tag{2.28}$$

where $\mathbf{x}$ and $\mathbf{y}$ denote two blocks of optimization variables, and $k$ is the iteration index. At each step, one variable is optimized while the other is fixed, which reduces the original problem into simpler subproblems.

**SCA:** Approximates the non-convex problem with a sequence of convex problems:

$$f(\mathbf{x}) \approx f(\mathbf{x}^{(k)}) + \nabla f(\mathbf{x}^{(k)})^T(\mathbf{x}-\mathbf{x}^{(k)}) + \frac{1}{2}(\mathbf{x}-\mathbf{x}^{(k)})^T\mathbf{H}^{(k)}(\mathbf{x}-\mathbf{x}^{(k)}) \tag{2.29}$$

where $\nabla f(\mathbf{x}^{(k)})$ is the gradient of the objective function at iteration $k$, and $\mathbf{H}^{(k)}$ is a positive definite matrix used to construct a convex surrogate function. This approximation allows the original non-convex problem to be solved iteratively via convex optimization.

**SDR:** Relaxes rank constraints in matrix optimization problems:

$$\begin{aligned} \min \quad & \langle \mathbf{C}, \mathbf{X} \rangle \\ \text{s.t.} \quad & \langle \mathbf{A}_i, \mathbf{X} \rangle = b_i, \quad i = 1, \ldots, m \\ & \mathbf{X} \succeq 0 \\ & \operatorname{rank}(\mathbf{X}) = 1 \end{aligned} \tag{2.30}$$

where $\mathbf{X}$ is the optimization matrix variable, $\langle \cdot, \cdot \rangle$ denotes the matrix inner product, and $\mathbf{X} \succeq 0$ indicates that $\mathbf{X}$ is positive semidefinite. The rank-one constraint enforces a structured solution but makes the problem non-convex. By relaxing this constraint, the problem becomes a semidefinite program (SDP), which can be efficiently solved, followed by rank-one recovery techniques.

The rank constraint is relaxed to obtain a SDP, and various techniques are employed to recover rank-one solutions.

# Chapter 3

# IRS Backscatter Based Hybrid Confidential Information and AN for Secrecy Transmission

## Overview

Considering that the wireless medium, which is prone to eavesdropping attacks, the robust security schemes that can be performed effectively under complicated propagation environment should be investigated. In this chapter, we propose a new security transmission tactic by employing IRS empowered with backscatter communication principle to build a hybrid system that can strengthen beneficial communication links and weaken eavesdropper's links at the same time. The proposed scheme differs radically from conventional security techniques, and manipulates the incident signal onto the IRS, not as a mimicking signal but a predetermined ensemble of confidential information and virtual noise, by using some advanced remodulation techniques.

## 3.1 System Model and Design Principles

The traditional method for securing wireless links involves the use of mechanisms and the active noise generation at the transmitter, which significantly increases the complexity and

power consumption. The new system design suggested in this chapter is revolutionary and involves a paradigm shift since the security strengthening function is transferred to IRS acting as a smart backscatter reflector.This architectural concept allows the implementation of a dual-role security scheme where the IRS acts as a passive relay for licensed signal while emitting jamming signals for possible eavesdropping. This improves security by enhancing the signal strength at the legitimate receiver through constructive beamforming, while simultaneously degrading the signal quality at potential eavesdroppers via interference generation. As a result, the SINR gap between the legitimate user and the eavesdropper is enlarged, leading to improved secrecy performance.

The intuition behind this strategy is that conventional IRSs, although achieving channel improvement only, do not take advantage of the possibility of information computation and interference synthesis at the same time. As a result of combining the backscatter communication with IRS, the proposed system not only has the unique ability to modulate the single incoming signal into multiple separate signal components but also to optimize each of these components to satisfy different space channel rates. This conversion takes place inside the passive elements of the IRS, without needing additional active agents in the transmitter, while offering an unprecedented electromagnetic environment control.

The IRS-assisted security laid out in this system framework overcomes a fundamental limitation in the conventional security schemes, that is, the difficulty of generating the effective interference at the actively-modulated eavesdropper by intuitively suppressing its channels and not the legitimate channels. By designing the backscatter modulation pattern and the reflection coefficient, we design spatially selective interference patterns, which can be adaptively adjusted depending on the locations and channels between normal users and the eavesdropper.

## 3.2 Mathematical System Model

The proposed security system is mathematically based on an overall model developed to describe the involved fundamental interactions between the transmitted legitimate communi-

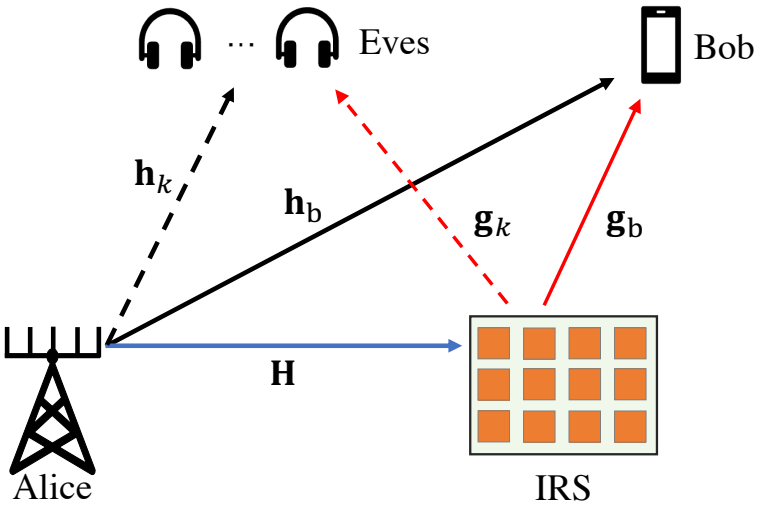


Fig. 3.1 Secrecy communication system via IRS-based backscatter modulation showing Alice transmitting to Bob while Eve attempts to eavesdrop, with the IRS providing dual functionality of signal enhancement and interference generation.

cation signals, the backscattered AN, and their collecting propagation paths in the system. Let us consider a secure communication system involving one $N$-antenna BS, who is also equipped with $N$ passive scattering-based reflecting elements, named as Alice, a single-antenna intended user, referred to as Bob, $K$ single-antenna passive eavesdroppers, named as Eve, and an IRS with $L$ reconfigurable elements deployed at a predefined location, as shown in Fig. 3.1.

In the model, all eavesdroppers are considered as legitimate users in the system but do not have the authority to access the secure information, rather, they are out of the circle of trust, in this context, "out of the circle of trust" is used to describe non-VIP users who can't join in the VIP services. The wireless channels are quasi-static Rician flat fading, and perfect CSI is assumed to be known for system optimization. Although practical systems would have channel estimation inaccuracies, the assumption of perfect CSI helps to determine basic performance limits of the coverage scheme and to gain understanding on the potential gains of the proposed approach.

According to this point, the received signals at Bob and $k$-th eavesdropper can be characterized by a unified mathematical model for direct links and the context-aware signal

processing of IRS. The signal at Bob contains a sum of the signal it received from the direct link to Alice and the returned signal via the IRS:

$$y_{\mathrm{b}} = \sqrt{P}\mathbf{h}_{\mathrm{b}}^{H}\mathbf{w}s + \sqrt{P}\mathbf{g}_{\mathrm{b}}^{H}\Psi\mathbf{H}\mathbf{w}s + n_{\mathrm{b}} \tag{3.1}$$

where $P$ represents the maximum transmit power available at Alice, $\mathbf{h}_{\mathrm{b}} \in \mathbb{C}^{N\times 1}$ denotes the direct channel vector from Alice to Bob, $\mathbf{g}_{\mathrm{b}} \in \mathbb{C}^{L\times 1}$ characterizes the channel from the IRS to Bob, $\mathbf{w} \in \mathbb{C}^{N\times 1}$ is the normalized beamforming vector for transmitting the confidential signal $s$ intended for Bob with $\mathbb{E}\{|s|^2\} = 1$, $\mathbf{H} \in \mathbb{C}^{L\times N}$ represents the channel matrix from Alice to the IRS, and $n_{\mathrm{b}} \sim \mathscr{CN}(0, \sigma_b^2)$ is the additive white Gaussian noise at Bob.

Similarly, the signal received at the $k$-th eavesdropper follows a parallel structure:

$$y_k = \sqrt{P}\mathbf{h}_k^{H}\mathbf{w}s + \sqrt{P}\mathbf{g}_k^{H}\Psi\mathbf{H}\mathbf{w}s + n_k \tag{3.2}$$

where $\mathbf{h}_k \in \mathbb{C}^{N\times 1}$ and $\mathbf{g}_k \in \mathbb{C}^{L\times 1}$ represent the channel gains from Alice to the $k$-th eavesdropper and from the IRS to the $k$-th eavesdropper, respectively, and $n_{\mathrm{k}} \sim \mathscr{CN}(0, \sigma_k^2)$ denotes the Gaussian white noise at the $k$-th eavesdropper.

The critical innovation in this system lies in the sophisticated design of the modulation-backscatter matrix $\Psi$, which enables the IRS to perform dual-functional signal processing. It should be noted that $\Psi$ can be interpreted as a generalized reflection matrix that incorporates both conventional phase/amplitude control and information modulation. Unlike the standard IRS reflection matrix, which only accounts for deterministic beamforming, $\Psi$ captures the additional modulation introduced by the backscatter operation. According to the backscatter communication principles established in the literature, this matrix can be expressed as:

$$\Psi = \mathrm{diag}(\psi_1, \psi_2, ..., \psi_L) \tag{3.3}$$

where each diagonal element $\psi_l$ represents the complex modulation coefficient of the $l$-th IRS element, defined as:

$$\psi_l = v_l + z_l s^{-1} s' \tag{3.4}$$

In this formulation, $\mathbf{v} = [v_1, v_2, ..., v_L]^H$ represents the passive beamforming vector optimized for enhancing the confidential signal transmission to Bob, while $\mathbf{z} = [z_1, z_2, ..., z_L]^H$ constitutes the AN beamforming vector designed to degrade the signal quality at eavesdroppers.

The constraint imposed by the passive nature of IRS elements requires that the total reflected power cannot exceed the incident power for any element:

$$[\mathbf{v}\mathbf{v}^H + \mathbf{z}\mathbf{z}^H]_{l,l} \leq 1, \quad \forall l \in \mathscr{L} \tag{3.5}$$

where $\mathscr{L} = \{1, 2, ..., L\}$ denotes the set of IRS element indices.

## 3.3 Signal Processing and Interference Generation

The IRS-backscatter system enhances secrecy by jointly designing two IRS-related vectors: the confidential-signal coefficient vector $\mathbf{v}$ and the artificial-noise coefficient vector $\mathbf{z}$. The vector $\mathbf{v}$ controls the IRS-assisted useful signal component, while $\mathbf{z}$ controls the IRS-generated AN. These two vectors are optimized to improve Bob's received signal quality and degrade the reception quality of potential eavesdroppers.

The IRS-reflected signal received at Bob can be written as

$$\mathbf{g}_b^H \Psi \mathbf{H}\mathbf{w}s = (\mathbf{v}^H s + \mathbf{z}^H s')\text{diag}\{\mathbf{g}_b^H\}\mathbf{H}\mathbf{w}. \tag{3.6}$$

This expression contains two components. The term

$$\mathbf{v}^H s\, \text{diag}\{\mathbf{g}_b^H\}\mathbf{H}\mathbf{w} \tag{3.7}$$

is the IRS-assisted confidential information component, which is designed to combine constructively with the direct signal at Bob. In contrast, the term

$$\mathbf{z}^H s'\, \text{diag}\{\mathbf{g}_b^H\}\mathbf{H}\mathbf{w} \tag{3.8}$$

is the AN component observed at Bob. The design objective is to restrict this AN leakage to Bob, for example by reducing its projected power over Bob's effective channel.

For the $k$-th eavesdropper, the IRS-reflected component is

$$\mathbf{g}_k^H \Psi \mathbf{H} \mathbf{w} s = (\mathbf{v}^H s + \mathbf{z}^H s') \mathrm{diag}\{\mathbf{g}_k^H\} \mathbf{H} \mathbf{w}. \tag{3.9}$$

In this case, the AN term

$$\mathbf{z}^H s' \, \mathrm{diag}\{\mathbf{g}_k^H\} \mathbf{H} \mathbf{w} \tag{3.10}$$

is intended to degrade the eavesdropper's received signal quality. Therefore, the optimization of $\mathbf{z}$ aims to make the AN strong over the eavesdropping channel while keeping its effect small at Bob.

Substituting the above components into the received signals gives

$$y_b = \sqrt{P} \mathbf{h}_b^H \mathbf{w} s + \sqrt{P} (\mathbf{v}^H s + \mathbf{z}^H s') \mathrm{diag}\{\mathbf{g}_b^H\} \mathbf{H} \mathbf{w} + n_b, \tag{3.11}$$

$$y_k = \sqrt{P} \mathbf{h}_k^H \mathbf{w} s + \sqrt{P} (\mathbf{v}^H s + \mathbf{z}^H s') \mathrm{diag}\{\mathbf{g}_k^H\} \mathbf{H} \mathbf{w} + n_k. \tag{3.12}$$

In (3.11), Bob's useful received signal is enhanced through both the direct link $\sqrt{P} \mathbf{h}_b^H \mathbf{w} s$ and the IRS-assisted confidential signal component controlled by $\mathbf{v}$. The vector $\mathbf{v}$ is designed such that the reflected confidential signal is aligned with Bob's effective channel. At the same time, $\mathbf{z}$ is designed to reduce the AN leakage at Bob.

In (3.12), the eavesdropper receives both the confidential signal and the AN through its own effective channel. The purpose of $\mathbf{z}$ is to increase the interference power at the eavesdropper, thereby reducing its SINR and achievable rate. Therefore, secrecy improvement is achieved by jointly enhancing Bob's effective channel through $\mathbf{v}$ and degrading the eavesdropping channel through $\mathbf{z}$.

It should be noted that this design requires knowledge of the eavesdropping channel if the AN is to be precisely directed toward a specific eavesdropper. This assumption may be reasonable in controlled scenarios where the eavesdropper is an active or registered but untrusted node, so that its CSI can be estimated from pilot signals. However, for passive or

unknown eavesdroppers, perfect eavesdropper CSI is generally unavailable. In such cases, the proposed design should be interpreted as an ideal benchmark or upper-bound case.

**AN Model** The AN signal $s'$ is modeled as a complex circularly symmetric Gaussian random variable, i.e.,

$$s' \sim \mathscr{CN}(0,1), \tag{3.13}$$

and is assumed to be independent of the confidential information signal $s$.

This Gaussian assumption is commonly adopted in physical layer security, since Gaussian-distributed interference represents the worst-case noise from an information-theoretic perspective and maximally degrades the eavesdropper's decoding capability.

The AN is generated at the transmitter and further shaped by the IRS through the coefficient vector $\mathbf{z}$. As shown in (3.11) and (3.12), the AN component appears in the received signal as

$$\mathbf{z}^H s' \,\mathrm{diag}\{\mathbf{g}^H\}\mathbf{H}\mathbf{w}, \tag{3.14}$$

which indicates that the spatial distribution of the AN is controlled by $\mathbf{z}$ and the cascaded channel.

The role of AN is twofold. First, it introduces additional interference at the eavesdroppers, thereby reducing their received SINR. Second, its impact on the legitimate user is carefully controlled through the joint optimization of $\mathbf{v}$ and $\mathbf{z}$, such that the AN leakage toward Bob is minimized.

The artificial noise is assumed to occupy the same bandwidth as the information signal, such that it cannot be separated in the frequency domain and can effectively degrade the eavesdropper's reception.

Within this shared signal space, the impact of the AN is controlled through the beamforming vector $\mathbf{z}$, whose norm determines the power allocated to the AN component. The vector $\mathbf{z}$ is jointly optimized with the transmit beamforming vector $\mathbf{w}$ and the useful signal coefficient $\mathbf{v}$, so as to minimize the AN leakage toward the legitimate user while maximizing its interference effect on potential eavesdroppers.

## 3.4 Performance Analysis and Optimization Formulation

The performance analysis of the proposed IRS-backscatter security system requires the derivation of SINRs that account for the complex signal processing performed by the IRS. The SINR expressions provide the foundation for formulating the security optimization problem and establishing the fundamental trade-offs in the system design.

The SINR at Bob incorporates both the desired signal enhancement from the reflection beamforming vector $\mathbf{v}$ and the interference effect of the AN generated by the vector $\mathbf{z}$:

$$\gamma_{\mathbf{b}} = \frac{|\mathbf{h}_{\mathbf{b}}^H \mathbf{w} + \mathbf{v}^H \text{diag}\{\mathbf{g}_{\mathbf{b}}^H\}\mathbf{H}\mathbf{w}|^2}{\gamma_0 + |\mathbf{z}^H \text{diag}\{\mathbf{g}_{\mathbf{b}}^H\}\mathbf{H}\mathbf{w}|^2} \tag{3.15}$$

where $\gamma_0 = P/\sigma^2$ represents the normalized noise power. This expression reveals the fundamental trade-off in the system design: while the reflection beamforming vector $\mathbf{v}$ enhances the numerator by coherently combining the direct and reflected signal paths, the AN vector $\mathbf{z}$ introduces interference that appears in the denominator and potentially degrades Bob's reception quality.

The corresponding SINR at the $k$-th eavesdropper follows a parallel structure:

$$\gamma_k = \frac{|\mathbf{h}_k^H \mathbf{w} + \mathbf{v}^H \text{diag}\{\mathbf{g}_k^H\}\mathbf{H}\mathbf{w}|^2}{\gamma_0 + |\mathbf{z}^H \text{diag}\{\mathbf{g}_k^H\}\mathbf{H}\mathbf{w}|^2} \tag{3.16}$$

The optimization objective is to minimize the transmit power $P$ (equivalently, minimize $\gamma_0$) while ensuring that Bob can achieve reliable communication and that the eavesdroppers' signal quality is sufficiently degraded to prevent successful information extraction. It is worth noting that the parameter $\gamma_0$ is related to the transmit power $P$, i.e., $\gamma_0 = P/\sigma^2$. Since the transmit power is determined by the beamforming vectors, the objective function implicitly depends on the optimization variables $\mathbf{w}$, $\mathbf{v}$, and $\mathbf{z}$. This leads to the following constrained optimization problem:

$$
\begin{aligned}
(\text{P0}) \quad \min_{\mathbf{w},\mathbf{v},\mathbf{z}} \quad & \gamma_0 \\
\text{s.t.} \quad & \text{C1} : \gamma_{\mathbf{b}} \geq \Gamma_{\mathbf{b}}, \\
& \text{C2} : \gamma_k \leq \Gamma_e, \ \forall k \in \mathscr{K}, \\
& \text{C3} : \text{Tr}(\mathbf{w}\mathbf{w}^H) = 1, \\
& \text{C4} : [\mathbf{v}\mathbf{v}^H + \mathbf{z}\mathbf{z}^H]_{l,l} \leq 1, \quad \forall l \in \mathscr{L}
\end{aligned}
\tag{3.17}
$$

where $\Gamma_b$ represents the minimum acceptable SINR threshold for Bob to ensure reliable decoding of the confidential information, $\Gamma_e$ denotes the maximum allowable SINR for eavesdroppers to prevent successful information extraction, and $\mathscr{K} = \{1, 2, ..., K\}$ is the set of eavesdropper indices.

The transmit beamforming vector is normalized such that $\|\mathbf{w}\|^2 = 1$, and the total transmit power is controlled by $P$. The IRS-related vectors $\mathbf{v}$ and $\mathbf{z}$ do not introduce additional power, but instead control the spatial distribution of the reflected signal and artificial noise.

Constraint C1 makes sure that the quality of Bob's communication is above a certaing level, hence the security improvement of the wiretap communication does not deteriorate the quality of service of the legal communication. The security requirement is enforced by C2 since it can be used to reduce the SINR that the eavesdroppers can access and this may leave the eavesdroppers unable to decode the confidential information. The normalizing constraint C3 involves the scaling ambiguity in optimization variables, and C4 aims to confine the IRS operation in the passive condition of the elements physically.

The formulated optimization problem (P0) represents a challenging non-convex optimization problem due to the coupling between the optimization variables $\mathbf{w}$, $\mathbf{v}$, and $\mathbf{z}$ in both the objective function and the constraints. The non-convexity arises from the multiplicative terms in the SINR expressions and the quadratic nature of the power constraints, making direct solution approaches computationally intractable for realistic system dimensions.

## 3.5 Alternating Optimization Algorithm Development

The computational intractability and non-convexity in the joint optimization problem (P0), however, motivate to design an efficient algorithm for producing relatively high quality solutions within affordable time budget. The method used in this paper breaks down the problem of joint optimization into a series of intermediate suboptimal subproblems, the resolutions of which may have closed form solutions using existing convex optimization tools.

The AO framework divides the original problem into two main subproblems: the optimization of the beamforming vector **w** with fixed IRS coefficients **v** and **z**, and the optimization of the IRS vectors with fixed beamforming. This decomposition exploits the structure of the problem to enable the application of specialized optimization techniques to each subproblem.

### 3.5.1 Beamforming Vector Optimization

When the IRS reflection and AN vectors **v** and **z** are held fixed, the optimization of the transmit beamforming vector **w** becomes a more tractable problem that can be solved using SDR techniques. The vectors **v** and **z** are initialized with feasible IRS coefficients, where **v** adopts unit-modulus phase values and **z** is initialized as a normalized random complex vector satisfying the IRS constraints. The key insight is to introduce auxiliary variables and matrix representations that transform the problem into a convex form.

To facilitate the mathematical manipulation, several auxiliary matrices and vectors are defined:

$$\Phi_{\mathrm{b}} = \mathrm{diag}\{\mathbf{g}_{\mathrm{b}}^H\}\mathbf{H} \tag{3.18}$$

$$\Phi_k = \mathrm{diag}\{\mathbf{g}_k^H\}\mathbf{H} \tag{3.19}$$

$$\bar{\Phi}_{\mathrm{b}} = [\Phi_{\mathrm{b}}; \mathbf{h}_{\mathrm{b}}^H] \tag{3.20}$$

$$\bar{\Phi}_k = [\Phi_k; \mathbf{h}_k^H] \tag{3.21}$$

$$\bar{\mathbf{v}} = [\mathbf{v}; 1] \tag{3.22}$$

These definitions enable the compact representation of the signal power terms in the SINR expressions. The squared magnitude of the effective channel gain at Bob can be expressed as:

$$|\mathbf{h}_{\mathbf{b}}^H\mathbf{w} + \mathbf{v}^H\mathrm{diag}\{\mathbf{g}_{\mathbf{b}}^H\}\mathbf{H}\mathbf{w}|^2 = |\bar{\mathbf{v}}^H\bar{\Phi}_{\mathbf{b}}\mathbf{w}|^2 \tag{3.23}$$

$$= \mathrm{Tr}\left(\mathbf{W}\bar{\Phi}_{\mathbf{b}}^H\bar{\mathbf{V}}\bar{\Phi}_{\mathbf{b}}\right) \tag{3.24}$$

where $\mathbf{W} \triangleq \mathbf{w}\mathbf{w}^H$ and $\bar{\mathbf{V}} \triangleq \bar{\mathbf{v}}\bar{\mathbf{v}}^H$ are the rank-one matrices corresponding to the beamforming and reflection vectors.

The AN power terms can be similarly expressed using the trace formulation:

$$|\mathbf{z}^H\mathrm{diag}\{\mathbf{g}_{\mathbf{b}}^H\}\mathbf{H}\mathbf{w}|^2 = \mathrm{Tr}\left(\mathbf{W}\Phi_{\mathbf{b}}^H\mathbf{Z}\Phi_{\mathbf{b}}\right) \tag{3.25}$$

where $\mathbf{Z} \triangleq \mathbf{z}\mathbf{z}^H$ is the rank-one matrix associated with the AN vector.

Using these matrix representations, the optimization problem can be reformulated in terms of the matrix variables $\mathbf{W}$, $\bar{\mathbf{V}}$, and $\mathbf{Z}$:

$$
\begin{aligned}
(\mathrm{P2}) \quad \min_{\mathbf{W}} \quad & \gamma_0 \\
\text{s.t.} \quad & \mathrm{C5}: \frac{\mathrm{Tr}\left(\mathbf{W}\bar{\Phi}_{\mathbf{b}}^H \bar{\mathbf{V}} \bar{\Phi}_{\mathbf{b}}\right)}{\gamma_0 + \mathrm{Tr}\left(\mathbf{W}\Phi_{\mathbf{b}}^H \mathbf{Z} \Phi_{\mathbf{b}}\right)} \geq \Gamma_{\mathbf{b}}, \\
& \mathrm{C6}: \frac{\mathrm{Tr}\left(\mathbf{W}\bar{\Phi}_k^H \bar{\mathbf{V}} \bar{\Phi}_k\right)}{\gamma_0 + \mathrm{Tr}\left(\mathbf{W}\Phi_k^H \mathbf{Z} \Phi_k\right)} \leq \Gamma_e, \quad \forall k \in \mathscr{K} \\
& \mathrm{C7}: \mathrm{Tr}(\mathbf{W}) = 1, \quad \mathbf{W} \succeq \mathbf{0} \\
& \mathrm{C8}: \mathrm{rank}(\mathbf{W}) = 1
\end{aligned}
\tag{3.26}
$$

The fractional constraints C5 and C6 can be transformed into linear matrix inequalities by cross-multiplication, yielding:

$$
\mathrm{C9}: \mathrm{Tr}\left(\mathbf{W}\bar{\Phi}_{\mathbf{b}}^H \bar{\mathbf{V}} \bar{\Phi}_{\mathbf{b}}\right) - \Gamma_{\mathbf{b}} \mathrm{Tr}\left(\mathbf{W}\Phi_{\mathbf{b}}^H \mathbf{Z} \Phi_{\mathbf{b}}\right) \geq \Gamma_{\mathbf{b}} \gamma_0 \tag{3.27}
$$

$$
\mathrm{C10}: \mathrm{Tr}\left(\mathbf{W}\bar{\Phi}_k^H \bar{\mathbf{V}} \bar{\Phi}_k\right) - \Gamma_e \mathrm{Tr}\left(\mathbf{W}\Phi_k^H \mathbf{Z} \Phi_k\right) \leq \Gamma_e \gamma_0 \tag{3.28}
$$

By applying SDR and temporarily ignoring the rank constraint C8, the problem becomes a convex SDP:

$$
\begin{aligned}
(\mathrm{P3}) \quad \min_{\mathbf{W}} \quad & \gamma_0 \\
\text{s.t.} \quad & \mathrm{C7}, \mathrm{C9}, \mathrm{C10}
\end{aligned}
\tag{3.29}
$$

This convex problem is efficiently solvable via interior-point methods (IPM) that are readily available, for example in Convex optimization software (CVX). The original beamforming design problem involves a vector variable $\mathbf{w}$, which is reformulated into a matrix variable $\mathbf{W} = \mathbf{w}\mathbf{w}^H$ to enable convex relaxation. This introduces a rank-one constraint on $\mathbf{W}$, which ensures that it can be decomposed back into a beamforming vector.

If the optimal solution $\mathbf{W}^*$ is rank-one, it is also the optimal beamforming vector. In this case, $\mathbf{W}^* = \mathbf{w}^* \mathbf{w}^{*H}$ holds, and the beamforming vector $\mathbf{w}^*$ can be directly obtained via eigenvalue decomposition. Otherwise, if $\mathbf{W}^*$ has a rank higher than one, it cannot be expressed as a single beamforming vector, and thus does not directly correspond to a

feasible solution of the original problem. rank-one approximation methods like Gaussian randomization can be used to obtain a good quality beamforming solution. Specifically, candidate beamforming vectors are generated from the distribution defined by $\mathbf{W}^*$, and the one achieving the best objective value is selected as an approximate solution.

### 3.5.2 IRS Coefficient Optimization

The optimization of the IRS reflection and AN vectors $\mathbf{v}$ and $\mathbf{z}$ with fixed beamforming vector $\mathbf{w}$ presents similar challenges due to the non-convex nature of the constraints and objectives. The approach follows a parallel strategy to the beamforming optimization, utilizing matrix variable substitutions and SDR.

The optimization problem for the IRS coefficients can be formulated as:

$$\begin{aligned}
(\text{P4}) \quad \min_{\bar{\mathbf{V}},\mathbf{Z}} \quad & \gamma_0 \\
\text{s.t.} \quad & \text{C9}, \text{C10} \\
& \text{C11} : \bar{\mathbf{V}} \succeq \mathbf{0}, \text{rank}(\bar{\mathbf{V}}) = 1 \\
& \text{C12} : \mathbf{Z} \succeq \mathbf{0}, \text{rank}(\mathbf{Z}) = 1 \\
& \text{C13} : [\bar{\mathbf{V}}_{1:L,1:L} + \mathbf{Z}]_{l,l} \leq 1, \quad \forall l \in \mathscr{L} \\
& \text{C14} : [\bar{\mathbf{V}}]_{L+1,L+1} = 1 \\
& \text{C15} : [\bar{\mathbf{V}}_{1:L,1:L} + \mathbf{Z}]_{l,l} \geq 0, \quad \forall l \in \mathscr{L}
\end{aligned} \tag{3.30}$$

The constraints C13-C15 ensure that the IRS coefficients satisfy the physical limitations imposed by the passive nature of the elements, while constraints C14 accounts for the normalization of the direct channel component in the augmented vector formulation.

By relaxing the rank constraints C11 and C12, the problem becomes a convex SDP that can be solved efficiently. The rank-one solutions can be recovered using standard techniques if the relaxation is not tight.

The AO algorithm in Table 3.1 is designed to solve the non-convex joint beamforming and IRS coefficient optimization problem. The algorithm iteratively optimizes the beamforming and IRS coefficients until convergence is achieved, as measured by the relative change in

Table 3.1 Alternating Optimization Algorithm for IRS-Backscatter Security System

| **Alternating Optimization Algorithm for IRS-Backscatter Security System** | |
|---|---|
| 1 | **Initialize:** Set $t = 0$, $\gamma_0^{(0)} = 0$ |
| 2 | **Initialize:** $\mathbf{w}^{(0)} = \mathbf{h}_{\text{avg}} / \|\mathbf{h}_{\text{avg}}\|$ |
| 3 | **Initialize:** $\mathbf{v}^{(0)} = [1, 1, \ldots, 1]^H$ |
| 4 | **Initialize:** $\mathbf{z}^{(0)} = [0, 0, \ldots, 0]^H$ |
| 5 | **Repeat:** |
| 6 | Set $t = t + 1$ |
| 7 | **Solve Subproblem 1:** With given $\mathbf{v}^{(t-1)}$ and $\mathbf{z}^{(t-1)}$, solve problem (P3) and employ rank-one recovery to obtain $\mathbf{w}^{(t)}$ |
| 8 | **Solve Subproblem 2:** With given $\mathbf{w}^{(t)}$, solve problem (P4) and employ rank-one recovery to obtain $\mathbf{v}^{(t)}$ and $\mathbf{z}^{(t)}$ |
| 9 | Update $\gamma_0^{(t)}$ based on the current solution |
| 10 | **Until:** $\frac{\|\gamma_0^{(t)} - \gamma_0^{(t-1)}\|}{\|\gamma_0^{(t)}\|} < \varepsilon$ (convergence criterion) |
| 11 | **Return:** Optimal solution $(\mathbf{w}^{(t)}, \mathbf{v}^{(t)}, \mathbf{z}^{(t)}, \gamma_0^{(t)})$ |

the objective function value between successive iterations. This approach is widely adopted in IRS-related studies due to its effectiveness in handling coupled variables and achieving locally optimal solutions.

## 3.6 Complexity Analysis and Implementation Considerations

The complexity of the AO algorithm lies in the complexity of solving the semidefinite programming subproblems and the number of iterations to converge. Examination of this complexity is crucial for determining the feasibility of the scheme in practice, and in order to understand the prospects of extension of the idea to larger system dimensions.

The computational complexity of the first subproblem (P3) depends primarily on the dimensions of the optimization variables and constraints. Using the IPM framework, the complexity can be expressed as:

$$C_{\mathrm{P3}} = \frac{\sqrt{2N+K+2}}{\varepsilon}\left[8n_1N^3 + 4n_1^2N^2 + (n_1^2+n_1)(K+2)\right] \tag{3.31}$$

where $\varepsilon$ represents the desired solution accuracy, $n_1 = \mathcal{O}\{4N^2\}$ accounts for the number of scalar optimization variables, $N$ is the number of transmit antennas, and $K$ is the number of eavesdroppers.

Similarly, the computational complexity of the second subproblem (P4) can be characterized as:

$$C_{\mathrm{P4}} = \frac{\sqrt{6L+K+4}}{\varepsilon}\left[8n_2(L+1)^3 + 4n_2^2(L+1)^2\right. \tag{3.32}$$

$$\left. +8n_2L^3 + 4n_2^2L^2 + (2L+K+2)(n_2^2+n_2)\right] \tag{3.33}$$

where $n_2 = \mathcal{O}\{4(L+1)^2 + 4L^2\}$ and $L$ is the number of IRS elements.

The total computational complexity of the AO algorithm is approximately:

$$C_{\mathrm{total}} \approx T(C_{\mathrm{P3}} + C_{\mathrm{P4}}) \tag{3.34}$$

where $T$ represents the number of iterations required for convergence.

The complexity analysis reveals that the computational cost scales polynomially with the system dimensions, making the algorithm practical for realistic system sizes. The number of iterations $T$ typically ranges from 10 to 30 for most practical scenarios, depending on the initialization strategy and convergence tolerance.

Moreover, it is convenient and low-cost to incorporate the algorithm into practical wireless communications due to its easy hardware implementation. Simple control circuitry is only required by the IRS to realize the computed reflection and AN coefficients, whereas the BS needs the software updates to realize the joint optimization algorithm. Its backward compatibility with legacy systems and its low hardware needs are appealing for a potential implementation.

## 3.7 Simulation Results and Performance Evaluation

The performance evaluation of the proposed IRS-backscatter security system is conducted through numerical simulations, where both communication efficiency and security performance are assessed and compared with benchmark approaches. The simulation parameters are selected to reflect practical deployment scenarios while ensuring fair and consistent comparisons.

The simulation environment considers a typical indoor communication setup, where the locations of Alice, the IRS and Bob are assumed to be fixed. While the eavesdroppers are randomly located within a predefined area to capture location uncertainty in practical systems. This modeling approach reflects a more realistic scenario, where the exact positions of potential eavesdroppers are unknown. The detailed system parameters are summarized in Table 3.2.

Table 3.2 Simulation Parameters and System Configuration

| Parameter | Description | Value |
|---|---|---|
| $d_{\mathrm{sb}}$ | Distance Alice to Bob | 60 m |
| $d_{\mathrm{si}}$ | Distance Alice to IRS | 50 m |
| $d_{\mathrm{ib}}$ | Distance IRS to Bob | 12 m |
| $d_{\mathrm{ie}}$ | Distance IRS to Eves | $\mathscr{U}(d_{\mathrm{ib}}-2, d_{\mathrm{ib}}+2)$ m |
| $d_{\mathrm{se}}$ | Distance Alice to Eves | $\mathscr{U}(d_{\mathrm{sb}}-10, d_{\mathrm{sb}}+10)$ m |
| $N$ | Antenna number at Alice | 2 |
| $K$ | Number of eavesdroppers | 20 |
| $L$ | IRS element number | 30 |
| $\sigma^2$ | Noise variance | $10^{-10}$ W/Hz |
| $\kappa$ | Rician factor | 3 |
| $\alpha$ | Path loss exponent | 2.5 |
| $\Gamma_e$ | Maximum SINR at Eve | 2 or 5 dB |
| $\Gamma_b$ | Minimum SINR at Bob | 10 dB |
| $\mathrm{PL}_0$ | Reference path loss | $-30$ dB |

The performance evaluation encompasses three primary benchmark schemes that represent the current in IRS-assisted secure communications:

Reflection-IRS Baseline, This scheme implements a traditional IRS-assisted system where the IRS functions solely as a passive reflector to enhance the legitimate communication link.

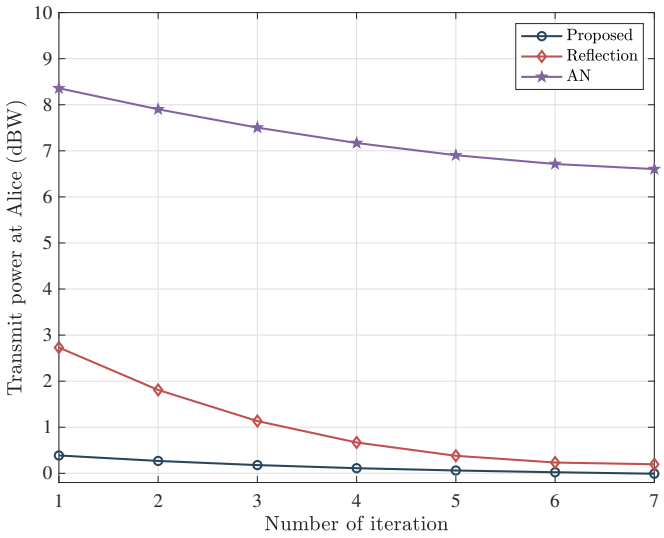


Fig. 3.2 Convergence behavior of the proposed AO algorithm, demonstrating rapid initial convergence followed by fine-tuning to achieve the optimal solution.

The optimization focuses on maximizing Bob's received signal quality without considering AN generation, representing the conventional approach to IRS-assisted communications.

AN-IRS Scheme, This approach utilizes the IRS exclusively for AN generation through backscatter techniques, directing interference towards eavesdroppers while the legitimate communication relies solely on the direct transmission path. This scheme represents the opposite extreme where security enhancement is prioritized over communication quality improvement.

Proposed Hybrid Scheme, The novel approach presented in this chapter that simultaneously optimizes both reflection beamforming for communication enhancement and AN generation for security improvement, representing the optimal balance between these competing objectives.

Fig. 3.2 illustrates the convergence behavior of the proposed AO algorithm for a representative system configuration. The algorithm demonstrates excellent convergence properties, achieving near-optimal performance within the first 7 iterations for the precision threshold of $\varepsilon = 10^{-9}$. The monotonic decrease in transmit power requirement with each iteration confirms the stability and effectiveness of the optimization approach.

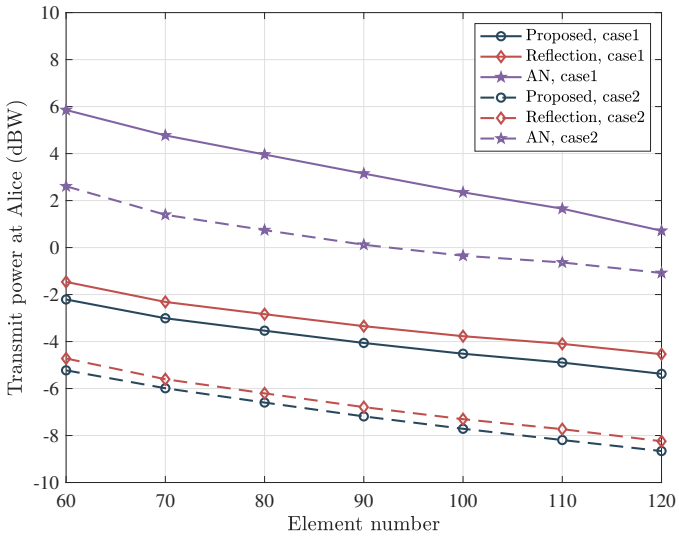


Fig. 3.3 Impact of IRS element count on minimum transmit power requirement, showing the superior scalability of the proposed hybrid approach compared to single-functionality baselines (Case 1: $\Gamma_e = 2$ dB; Case 2: $\Gamma_e = 5$ dB)

.

The reflection-only and AN-based schemes correspond to two commonly adopted baseline strategies in IRS-assisted physical layer security, and are used here as representative benchmarks to evaluate the effectiveness of the proposed hybrid design. The minimum transmit power required by other schemes compared into the proposed method shows the superiority of the proposed method. The hybrid policy outperforms the two single-functionality baselines in all scenarios in term of power when again both communication and security constraints are met. On the other hand, the AN-IRS scheme attains security performance gains at the expense of high transmit power because the AN-IRS scheme is unable to improve the legitimate link.

Although Fig. 3.3 primarily illustrates the reduction in transmit power, the improvement in security is reflected indirectly through the system design objective. Specifically, for a given secrecy constraint, a lower required transmit power indicates that the legitimate user's quality-of-service can be satisfied while maintaining the degradation of the eavesdropper's channel. This implies an improved secrecy performance, as the system can achieve the same security level with reduced power consumption.

Two cases are considered in the simulations. Case 1 corresponds to a relatively loose eavesdropper SINR constraint with $\Gamma_e = 2$ dB, while Case 2 corresponds to a stricter constraint with $\Gamma_e = 5$ dB.

The effect of IRS array size over the system performance for different approaches is shown in Fig. 3.3 The hybrid deployment achieves an excellent scalability property in terms of the number of IRS elements, as the transmit power requirements/right pathloss ratio decreases monotonically with the number of reflection/detection elements. This is consistent with the capability of the algorithm to perform better depending on more available degree of freedom by larger size arrays for the sake of both communication quality and degree of security.

The reflection-IRS baseline shows modest improvements with increasing array size, limited by its inability to actively counter eavesdropping attempts. This is because the reflection-only IRS enhances the signal propagation in a passive manner, without introducing additional interference to suppress the eavesdroppers. As a result, the reflected signal may also improve the channel conditions of unintended receivers. In contrast, schemes incorporating artificial noise can deliberately degrade the eavesdropper's channel, leading to a larger performance gain. This effect is reflected in Fig. 3.3, where the reflection-only scheme exhibits a slower reduction in transmit power compared to the hybrid approach. The AN-IRS scheme demonstrates the poorest scaling behavior, as the exclusive focus on interference generation prevents exploitation of the communication enhancement benefits offered by larger arrays.

The analysis of the IRS deployment scheme that is shown in Fig. 3.4 provides important information on where the IRS is to be placed to maximize security aspects. The considered hybrid scheme achieves better performance for all deployment distances, but the performance difference becomes more prominent as the distance between the IRS and the transmit or receive terminals becomes smaller. In particular, the performance degradation of the proposed scheme is more gradual, and the gap with the baseline approaches remains noticeable even under less favorable placement conditions. This suggests that the proposed design is less

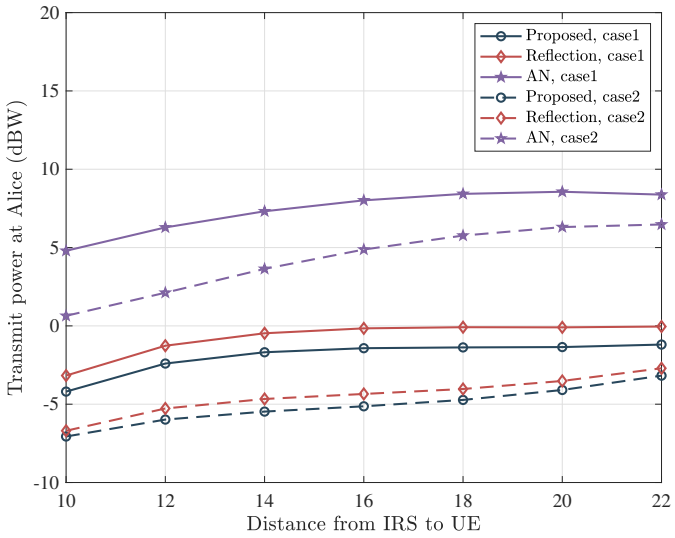


Fig. 3.4 Effect of IRS deployment distance on system performance, illustrating the importance of strategic positioning for optimal security and efficiency balance (Case 1: $\Gamma_e = 2$ dB; Case 2: $\Gamma_e = 5$ dB)

.

sensitive to IRS placement variations and is able to maintain relatively stable performance within the considered range.

## 3.8 Security Analysis and Robustness Evaluation

The underlying security premise is based on the spatial selectivity of the AN generation, which enhances the signal quality at the legitimate user while degrading the effective channels of the eavesdroppers. The performance of this approach depends on factors such as the relative distances between users and eavesdroppers, as well as the accuracy of the channel state information at the transmitter (CSIT).

Under the assumption of perfect CSI, the proposed scheme provides an upper-bound performance consistent with the wiretap channel formulation. The impact of channel estimation errors is not explicitly analyzed in this section and is instead investigated in Chapter 4, where additional simulations and discussions are provided.

The results presented in this section are therefore based on ideal CSI conditions and serve as a benchmark to illustrate the potential performance of the proposed design. A more detailed evaluation under imperfect CSI conditions is deferred to the later part of the thesis.

## 3.9 Chapter Summary and Key Insights

This chapter has presented a framework for IRS-backscatter based security enhancement in wireless communication systems. The proposed approach jointly considers communication quality and security performance within a unified optimization formulation.

Specifically, a mathematical model has been developed to characterize the interaction between IRS reflection beamforming and AN generation. This formulation reveals an inherent trade-off in the system design, where the available IRS resources are shared between enhancing the useful signal and generating interference. Increasing the emphasis on AN improves security performance but may reduce the signal enhancement capability, and vice versa. Based on this model, an optimization problem has been formulated to jointly design the transmit beamforming and IRS coefficients. An AO algorithm has been adopted to obtain a feasible solution with manageable computational complexity.

Simulation results demonstrate that the proposed hybrid scheme achieves improved performance compared to benchmark approaches in terms of transmit power and scalability with respect to the number of IRS elements. In addition, the proposed method maintains consistent performance advantages over a range of IRS deployment distances within the considered scenarios.

The analysis in this chapter is conducted under the assumption of perfect CSI and serves as a baseline to illustrate the potential performance of the proposed design. The impact of channel estimation errors and more practical considerations are further investigated in the subsequent chapter.

Overall, the results indicate that jointly exploiting signal enhancement and artificial noise generation provides additional flexibility in improving secrecy performance. The framework

developed in this chapter lays the foundation for the extensions presented in the following chapters, including multi-user scenarios and learning-based optimization methods.

# Chapter 4

# GNN-based STAR-RIS for Secure Indoor Multi-User Communications

## Overview

The need for selective precedence in multilayer networks has intensified with the evolution of wireless communication systems towards ubiquitous connectivity. As a result, intelligent solutions that meet diverse system performance demands-such as extended coverage, interference suppression, and security enhancement-are increasingly essential. This chapter presents an innovative indoor multi-user communication framework based on STAR-RIS. The design leverages the unique capability of STAR-RIS to simultaneously manage transmission and reflection, in conjunction with advanced GNN techniques. Unlike conventional approaches, the proposed system introduces a novel 2-in-1 architecture with a multi-timescale control mechanism. This enables significant performance gains and enhanced security, overcoming limitations of traditional methods.

## 4.1 Motivation and System Architecture Overview

The increasing use of indoor wireless systems has provided a unique set of challenges for the design of wireless communication systems, especially for applications that must support high

data rates, reliable conductivity and provable security simultaneously. Conventional solutions to the above problems tend to result in disparate solutions for each of the above, leading to increased system complexity, higher power consumption, and suboptimal performance.

The rationale for such an integrated approach can be deduced from several observations concerning the drawbacks inherent to existing solutions. Although conventional RISs are effective in signal enhancement, they are not flexible enough to address interference management and security provision jointly. Likewise, classical beamforming is unable to efficiently exploit the spatial diversity and environmental controllability offered by intelligent reflectors. In Chapter 3, conventional reflection-only RIS is considered as a baseline for comparison, while the main contribution lies in a backscatter-based hybrid IRS framework that enables joint signal enhancement and security-oriented interference generation. The development of STAR-RIS technology provides the opportunity to overcome these limitations; however, fully exploiting its potential remains challenging and requires advanced optimization tools capable of handling the significantly increased complexity of the joint design space.

The system architecture introduced in this chapter successfully tackles these issues by a well balance between hardware revolution and algorithm complexity. The STAR-RIS is assumed to be deployed at a representative position, such as on a wall or window, to enable both indoor coverage and interaction with the outdoor environment. The surface can be leveraged for legitimate indoor users by reflection and can also produce focused interference for potential outdoor eavesdroppers by transmission in the meantime. The two functions are leveraged in tandem by developing a novel two-timescale optimization framework which will decouple long-term channel adaptation from the short-term security enhancement, so that the two objectives can be achieved without conflicting with each other. We adopt a baseband-equivalent signal model, where the transmitted signal is represented in complex form. The specific modulation format (e.g., QAM/PSK) is not specified, as the analysis is based on SINR and achievable rate. No specific multiple access scheme (e.g., OFDMA) is assumed. Instead, a general multi-user beamforming framework is considered.

The introduction of GNNs to this architecture is a fundamental innovation without which the system would not be able to account for the complex dependencies between multiple

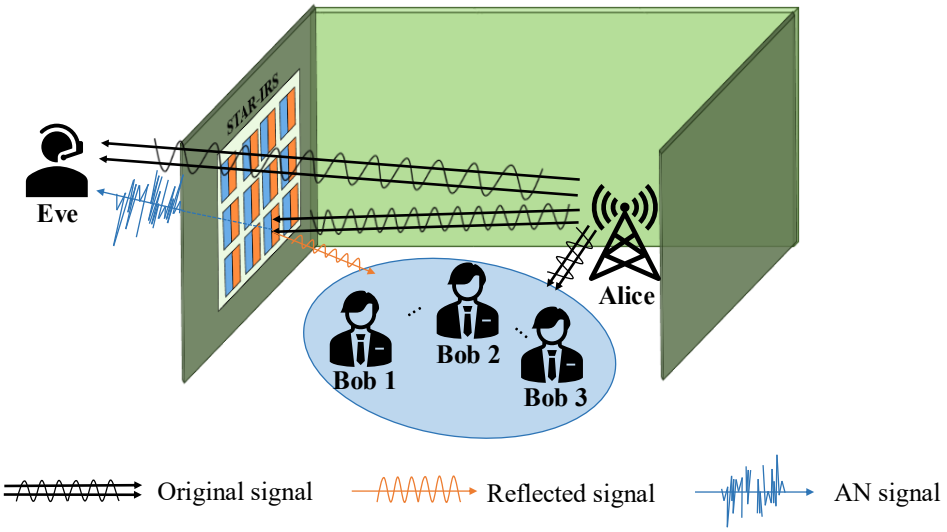


Fig. 4.1 Comprehensive system architecture showing the dual-functional STAR-RIS deployment for secure indoor multi-user communications, with reflection-based service for indoor users and transmission-based interference for outdoor eavesdroppers.

users, numerous surface elements, and various optimization goals. In contrast to conventional optimization methods that are inefficient for high-dimensional non-convex joint design problems, the GNN framework can learn effective optimization policies directly from system data, and adapt to varying system conditions and increasing system dimensions.

## 4.2 Multi-User Indoor Communication System Model

The mathematical theory of the system is established via a realistic model, which considers the complicated behaviors among the multiple primary users, multiple suspicious eavesdroppers, and the STAR-RIS. The system is comprised from a $N_a$-antenna BS Alice that aims to serve $K$ legitimate users Bob, each with $N_b$-antennas and indoor location-wise. The security risk is modeled by an $N_e$-antenna eavesdropper Eve located outside, who seeks to eavesdrop the confidential messages exchanged between legitimate users as shown in Fig. 4.1.

The STAR-RIS is deployed on the building envelope (e.g., walls or windows) at a representative location to enable its dual-functional operation, where the RIS consists of $L$ intelligent elements. Such a deployment allows the surface to enhance indoor communication

through reflection while interacting with the outdoor environment through transmission. The mathematical framework of such system demands a careful treatment of the multiple signal paths, the complex beamforming relations, and the intelligent signal processing at the STAR-RIS.

Alice transmits $K$ confidential data streams $\mathbf{s} = [s_1, s_2, \ldots, s_K]^T \in \mathbb{C}^{K\times 1}$ to the $K$ legitimate users, where each symbol $s_k$ represents the confidential information intended for the $k$-th user and satisfies $\mathbb{E}\{|s_k|^2\} = 1$. The transmission is accomplished through a sophisticated precoding matrix $\mathbf{W} = [\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_K] \in \mathbb{C}^{N_a\times K}$ that must satisfy the total transmit power constraint $\mathrm{Tr}(\mathbf{W}\mathbf{W}^H) = \sum_{k=1}^{K} \mathrm{Tr}(\mathbf{w}_k\mathbf{w}_k^H) \leq P_{\max}$.

The channel characterization in this system involves multiple distinct propagation paths that must be carefully modeled to enable effective optimization. The direct channels from Alice to the $k$-th legitimate user and to the eavesdropper are denoted by $\mathbf{H}_k \in \mathbb{C}^{N_b\times N_a}$ and $\mathbf{H}_e \in \mathbb{C}^{N_e\times N_a}$, respectively. The channels from the STAR-RIS to the users and eavesdropper are represented by $\mathbf{F}_k \in \mathbb{C}^{N_b\times L}$ and $\mathbf{F}_e \in \mathbb{C}^{N_e\times L}$, while the critical channel from Alice to the STAR-RIS is characterized by $\mathbf{G} \in \mathbb{C}^{L\times N_a}$.

The advanced signal processing capabilities of the STAR-RIS are characterised by two distinct coefficient matrices, which allow for independent control of its reflection and transmission functions. Specifically, the reflection behaviour is governed by the reflection coefficient matrix, defined as:

$$\Theta_r = \mathrm{diag}\{\sqrt{\alpha_1^r}e^{j\theta_1^r}, \sqrt{\alpha_2^r}e^{j\theta_2^r}, \ldots, \sqrt{\alpha_L^r}e^{j\theta_L^r}\} \tag{4.1}$$

while the transmission coefficient matrix is given by:

$$\Theta_t = \mathrm{diag}\{\sqrt{\alpha_1^t}e^{j\theta_1^t}, \sqrt{\alpha_2^t}e^{j\theta_2^t}, \ldots, \sqrt{\alpha_L^t}e^{j\theta_L^t}\} \tag{4.2}$$

where $\alpha_l^r \in [0,1]$ and $\alpha_l^t \in [0,1]$ represent the reflection and transmission amplitudes of the $l$-th element, respectively, with the fundamental constraint $\alpha_l^r + \alpha_l^t = 1$ ensuring energy conservation. The phase shifts $\theta_l^r \in [0, 2\pi)$ and $\theta_l^t \in [0, 2\pi)$ provide additional degrees of freedom for optimizing the signal processing characteristics of each element.

The signal received at the $k$-th legitimate user incorporates contributions from both the direct transmission path and the reflection-enhanced path through the STAR-RIS:

$$\mathbf{y}_k = (\mathbf{H}_k + \mathbf{F}_k \Theta_r \mathbf{G})\mathbf{W}\mathbf{s} + \mathbf{n}_k, \quad \forall k \in \mathscr{K} \tag{4.3}$$

where $\mathscr{K} = \{1, 2, \ldots, K\}$ denotes the set of legitimate user indices and $\mathbf{n}_k \sim \mathscr{CN}(0, \sigma_k^2 \mathbf{I}_{N_b})$ represents the additive white Gaussian noise at the $k$-th user.

The signal structure at the eavesdropper is fundamentally different due to the dual-functional design of the STAR-RIS. The eavesdropper receives signals through both the direct path from Alice and the transmission path from the STAR-RIS, but the transmitted signal is deliberately modulated to create AN rather than useful information:

$$\mathbf{y}_e = (\mathbf{H}_e + \mathbf{F}_e \bar{\Theta}_t \mathbf{G})\mathbf{W}\mathbf{s} + \mathbf{n}_e \tag{4.4}$$

where $\mathbf{n}_e \sim \mathscr{CN}(0, \sigma_e^2 \mathbf{I}_{N_e})$ is the noise at the eavesdropper and $\bar{\Theta}_t$ represents the modulated transmission coefficient matrix that implements the AN generation functionality. It is worth noting that the matrix $\bar{\Theta}_t$ is introduced as an intermediate representation to model the symbol-level random phase modulation applied at the STAR-RIS transmission side. This time-varying matrix differs from the deterministic transmission matrix $\Theta_t$, which characterizes the long-term channel-level transmission coefficients.

## 4.3 Dual-Functional STAR-RIS Design Principles

The novelty of the proposed system is the adoption of a dual-functional STAR-RIS design in which the proposed system adjusts its operating parameters on two time scales to optimally co-design its communication performance, as well as its security-enhancing capability. Such a multi-timescale framework allows the system to decouple the slow-evolving component of optimizing channel reuse from the fast-changing requirement of providing security, so that each objective can be optimally adapted with the tailored tools, via suitable time-scale separation.

### 4.3.1 Channel-Level Reflection Optimization

Regarding channel-level operation, the STAR-RIS reflection coefficient optimization to improve communication channels that cover intended users. This optimization is performed at a time scale corresponding to the coherence time of the wireless channels, for instance, which varies from some milliseconds to tens of milliseconds according to the users' mobility and environment dynamics.

Although this suggests frequent updates in time-varying channel conditions, such optimization remains feasible in practice. This is because the reflection coefficients are updated at a relatively slow time scale compared to symbol-level processing, and efficient algorithms (e.g., AO) can provide near-optimal solutions with manageable complexity. In addition, practical implementations may employ reduced-complexity or pre-trained approaches to avoid full re-optimization at every channel realization.

The reflection coefficient optimization aims to create constructive interference between the direct and reflected signal paths at each legitimate user's location while minimizing inter-user interference. The effective channel experienced by the $k$-th user can be expressed as:

$$\mathbf{D}_k = \mathbf{H}_k + \mathbf{F}_k \Theta_r \mathbf{G} \tag{4.5}$$

The optimization of the reflection coefficients is devoted to maximize the effective channel gains subject to the physical regulation due to the passive operation of the STAR-RIS elements. This optimal configuration must take into account the various interrelated channels of the different users, as well as limitations in the degrees of freedom achievable with the surface design.

The channel-level optimization problem can be formulated as maximizing the sum of effective channel gains subject to the energy conservation constraints:

$$\max_{\Theta_r} \sum_{k=1}^{K} \|\mathbf{D}_k\|_F^2 \quad \text{s.t.} \quad \alpha_l^r + \alpha_l^t = 1, \quad \alpha_l^r, \alpha_l^t \in [0,1], \quad \forall l \tag{4.6}$$

The solution to this optimization problem provides the foundation for the communication enhancement capabilities of the system, establishing the baseline performance levels that will be maintained while security enhancements are implemented through the transmission functionality.

### 4.3.2 Symbol-Level AN Generation

Symbol-level operation of the STAR-RIS results in more complex AN generation involving fast tuning of the transmission coefficients. This operation works on a timescale much faster than in the main protocol (actually at the symbol rate or above) and allows generating AN patterns to an eavesdropper that looks random while maintaining preferably known properties to the legitimate users.

The key innovation in this approach lies in the mathematical relationship between the confidential information signal and the AN generation process. The transmission coefficient matrix is dynamically modulated according to:

$$\mathbf{F}_e \bar{\Theta}_t \mathbf{G}\mathbf{W}\mathbf{s} = \sum_{k=1}^{K} \mathbf{F}_e \mathrm{diag}\{\mathbf{G}\mathbf{w}_k\} \bar{\theta}_t s_k \tag{4.7}$$

Through careful modulation of the transmission coefficients, this expression can be transformed to generate AN:

$$\sum_{k=1}^{K} \mathbf{F}_e \mathrm{diag}\{\mathbf{G}\mathbf{w}_k\} \theta_t z_k = \mathbf{F}_e \Theta_t \mathbf{G}\mathbf{W}\mathbf{z} \tag{4.8}$$

where $\mathbf{z}$ represents the AN signal vector with $\mathbf{z} \sim \mathscr{CN}(\mathbf{0}, \mathbf{I})$ and the transformation from $\bar{\theta}_t$ to $\theta_t$ implements the modulation process that converts the information-bearing signal into structured interference. It should be noted that $\mathbf{z}$ is not an independently generated signal, but an equivalent representation of the phase-randomized transmitted signal.

The use of $\bar{\Theta}_t$ enables a clear description of how symbol-level phase perturbations transform the structured transmitted signal into interference at the eavesdropper. This transformation allows the signal model at the eavesdropper to be expressed in a form consistent with the legitimate user model. For analytical tractability, the resulting signal

can be equivalently represented using the deterministic matrix $\Theta_t$ together with an artificial noise vector $\mathbf{z}$, while highlighting the distinct roles of reflection (signal enhancement) and transmission (interference generation).

This dual-timescale operation enables the STAR-RIS to maintain stable communication enhancement for legitimate users through reflection while simultaneously generating dynamic interference patterns for eavesdroppers through transmission. The separation of these functionalities across different timescales prevents conflicts between the optimization objectives and enables each to be pursued with appropriate techniques.

### 4.3.3 SINRs Analysis

In performance analysis the dual-functional STAR-RIS system should carefully derive the SINR, considering the enhanced reception of legitimate users and the degraded reception of eavesdroppers. The SINR experienced at the $k$-th legitimate user, including the favorable influence of the reflection enabled channel enhancement and the inter-user interference, is given by:

$$\gamma_k = \frac{\|\mathbf{D}_k \mathbf{w}_k\|^2}{\sigma_k^2 + \sum_{i=1, i\neq k}^{K} \|\mathbf{D}_k \mathbf{w}_i\|^2} \tag{4.9}$$

where $\mathbf{D}_k = \mathbf{H}_k + \mathbf{F}_k \Theta_r \mathbf{G}$ represents the effective channel incorporating both direct and reflected components.

The SINR at the eavesdropper must account for the AN generated through the transmission functionality:

$$\gamma_{e,k} = \frac{\|\mathbf{H}_e \mathbf{w}_k\|^2}{\sigma_e^2 + \sum_{i=1, i\neq k}^{K} \|\mathbf{H}_e \mathbf{w}_i\|^2 + \|\bar{\mathbf{F}}_e \mathbf{W}\|_F^2} \tag{4.10}$$

where $\bar{\mathbf{F}}_e = \mathbf{F}_e \Theta_t \mathbf{G}$ captures the AN contribution from the STAR-RIS transmission functionality.

The secrecy rate achieved for the $k$-th user is determined by the difference between the legitimate and eavesdropper channel capacities:

$$R_{s,k} = \left[\log_2(1+\gamma_k) - \log_2(1+\gamma_{e,k})\right]^+ \tag{4.11}$$

The operator $[x]^+ = \max(x,0)$ ensures that the secrecy rate is non-negative, since a negative value indicates that the eavesdropper's channel is stronger than that of the legitimate user, in which case secure communication is not achievable.

Based on the above definition, we aim to maximize the overall system performance by jointly optimizing the transmit beamforming at Alice and the STAR-RIS configuration. Specifically, the objective is to maximize the WSR, which accounts for both system throughput and user fairness. The corresponding optimization problem is formulated as

$$\begin{aligned}
(\text{P0}) \quad \max_{\mathbf{w}_k, \Theta_\text{r}, \Theta_\text{t}} \quad & \sum_{k=1}^{K} w_{s,k} R_{s,k} \\
s.t. \quad & \text{C1} : \sum_{k=1}^{K} \text{Tr}(\mathbf{w}_k \mathbf{w}_k^H) \leq P_\text{max}, \\
& \text{C2} : \alpha_l^r + \alpha_l^t = 1, \quad \forall l \in \mathscr{L}, \\
& \text{C3} : \alpha_l^r, \alpha_l^t \in [0,1], \quad \forall l \in \mathscr{L}, \\
& \text{C4} : 0 \leq \theta_l^\text{r} \leq 2\pi, \quad \forall l \in \mathscr{L}, \\
& \text{C5} : 0 \leq \theta_l^\text{t} \leq 2\pi, \quad \forall l \in \mathscr{L}.
\end{aligned} \tag{4.12}$$

where $P_\text{max}$ denotes the maximum transmit power at Alice, and $w_{s,k}$ represents the weight associated with the $k$-th user, which is used to control user fairness and priority in the system.

## 4.4 Graph Neural Network Optimization Framework

The challenge of co-designing the active beamforming at Alice and the dual-functional coefficients at the STAR-RIS calls for sophisticated optimization designs that can cope with high-dimensional, non-convex optimization problems, while achieving computational complexity in real time learning. The GNN framework we have proposed in this chapter is a

paradigm shift to this problem, in that it is founded on the strong ML which allows learning of efficient optimization directly from system data.

### 4.4.1 Graph Representation and Network Architecture

Common to all of these techniques is the observation that the multi-user STAR-RIS system can be conveniently modeled as a graph whose nodes are the various communication entities, and edges denote how these entities interact and communicate. In this way the GNN model is able to learn complex relationships between users and based elements in the system, and at the same time it achieves computational efficiency as it can flexibly scale to user and surface different numbers. Fig. 4.2 presents the GNN-based optimization framework, where the communication system is modeled as a graph structure.

The graph $G = (V, E)$ is constructed with the node set $V = \{v_0, v_1, \ldots, v_{K+1}\}$, where $v_0$ represents the STAR-RIS as the central coordinating entity, nodes $v_k$ for $k \in \{1, 2, \ldots, K\}$ represent the legitimate users, and node $v_{K+1}$ represents the eavesdropper. The edge set $E$ captures the communication links and interference relationships between these entities, forming a fully connected graph that reflects the broadcast nature of wireless communications.

The choice of a fully connected graph architecture is motivated by the recognition that in wireless systems, every transmitter can potentially affect every receiver, either beneficially or detrimentally. This complete connectivity ensures that the GNN can learn to exploit all available spatial relationships and interference patterns in its optimization decisions.

The input feature representation for each node is carefully designed to capture the essential CSI and system parameters that influence the optimization decisions. The STAR-RIS node $v_0$ incorporates aggregated channel information that reflects its central role in coordinating the system operation:

$$\mathbf{x}_0^0 = [\Re\{\bar{\mathbf{H}}^T\}, \Im\{\bar{\mathbf{H}}^T\}, \mathrm{vec}(\Re\{\bar{\mathbf{F}}\})^T, \mathrm{vec}(\Im\{\bar{\mathbf{F}}\})^T]^T \tag{4.13}$$

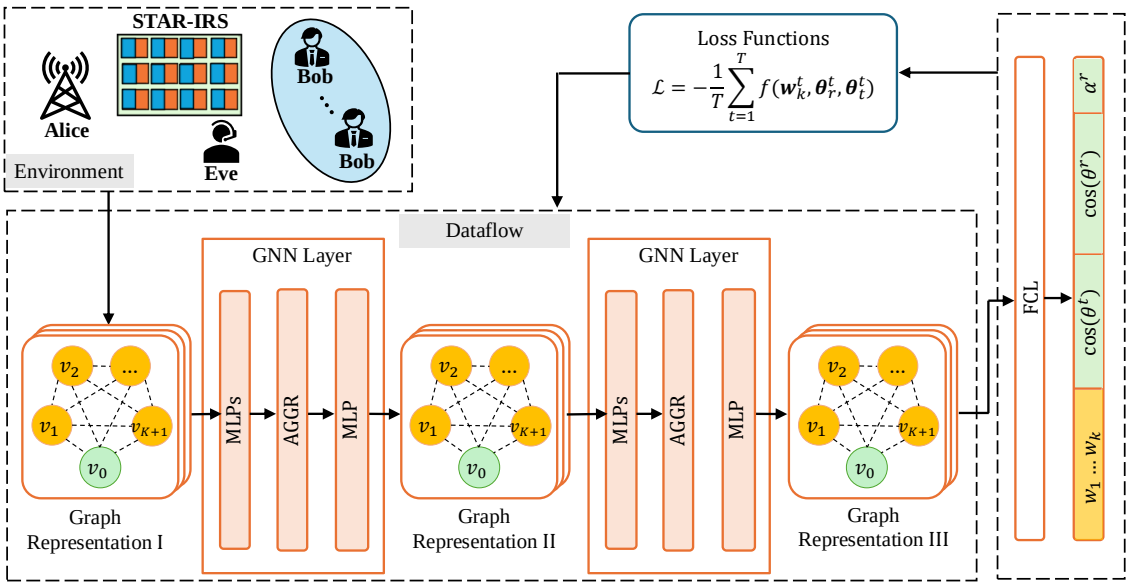


Fig. 4.2 Comprehensive GNN framework architecture showing the node feature representation, message passing mechanisms, and output generation for joint optimization of beamforming and STAR-RIS coefficients.

where $\bar{\mathbf{H}}$ and $\bar{\mathbf{F}}$ represent averaged channel matrices that capture the statistical properties of the propagation environment, and $\Re\{\cdot\}$ and $\Im\{\cdot\}$ denote the real and imaginary parts, respectively.

The feature vector for each legitimate user node $v_k$ incorporates the specific CSI relevant to that user:

$$\mathbf{x}_k^0 = [\Re\{\mathbf{H}_k^T\}, \Im\{\mathbf{H}_k^T\}, \text{vec}(\Re\{\bar{\mathbf{F}}_k\})^T, \text{vec}(\Im\{\bar{\mathbf{F}}_k\})^T]^T \tag{4.14}$$

where $\bar{\mathbf{F}}_k = \mathbf{F}_k \Theta_r \mathbf{G}$ represents the cascaded channel from Alice to the $k$-th user through the STAR-RIS reflection functionality.

The eavesdropper node $v_{K+1}$ is represented by features that capture the threat characteristics:

$$\mathbf{x}_{K+1}^0 = [\Re\{\mathbf{H}_e^T\}, \Im\{\mathbf{H}_e^T\}, \text{vec}(\Re\{\bar{\mathbf{F}}_e\})^T, \text{vec}(\Im\{\bar{\mathbf{F}}_e\})^T]^T \tag{4.15}$$

where $\bar{\mathbf{F}}_e = \mathbf{F}_e \Theta_t \mathbf{G}$ represents the cascaded channel from Alice to the eavesdropper through the STAR-RIS transmission functionality.

The separation of channel information into real and imaginary components is necessary because the GNN architecture operates on real-valued inputs, while the underlying wireless channels are inherently complex-valued. This representation preserves all the essential information while maintaining compatibility with the neural network processing requirements.

### 4.4.2 Message Passing and Feature Updates

At the heart of the GNN optimization paradigm is an intelligent how nodes communicate similar to how conversation propagates between individuals about their local experiences and constraints toward a globally optimal-contour. The message passing process is realized by multiple layers which iteratively update the node representations by aggregating information from their neighbors.

The update rule for node $v$ at the $n$-th layer is formulated as:

$$\mathbf{h}_v^{(n)} = \sigma\left(\mathrm{MLP}\left(\mathbf{h}_v^{(n-1)} \,\|\, \mathrm{AGGR}\left(\{\mathbf{h}_u^{(n-1)} | u \in \mathscr{N}(v)\}\right)\right)\right) \tag{4.16}$$

where $\mathbf{h}_v^{(n)}$ represents the feature vector of node $v$ at layer $n$, $\mathbf{h}_u^{(n-1)}$ represents the feature vector of neighboring node $u$ at layer $n-1$, $\mathscr{N}(v)$ denotes the neighborhood of node $v$, and $\|$ indicates the concatenation operation. In this work, the initial node features $\mathbf{h}_v^{(0)}$ are constructed from the system-specific feature vectors defined in Eqs. (4.13)–(4.15), such as channel coefficients, beamforming-related parameters, and IRS configuration variables. The neighboring features are aggregated to capture the interactions between different components in the system.

The aggregation function $\mathrm{AGGR}(\cdot)$ is specifically tailored to the characteristics of different nodes in the system. For the central STAR-RIS node $v_0$, which must coordinate information from all users and the eavesdropper, a mean aggregation function is employed:

$$\mathrm{AGGR}_{v_0}(\{\mathbf{h}_u^{(n-1)} | u \in \mathscr{N}(v_0)\}) = \frac{1}{|\mathscr{N}(v_0)|} \sum_{u \in \mathscr{N}(v_0)} \mathbf{h}_u^{(n-1)} \tag{4.17}$$

This choice ensures that the STAR-RIS node captures the average influence from all connected entities, reflecting its role as a global coordinator that must balance the requirements of all system participants.

For the user and eavesdropper nodes, a max aggregation function is employed to focus on the most significant influences:

$$\text{AGGR}_{v_k}(\{\mathbf{h}_u^{(n-1)} | u \in \mathcal{N}(v_k)\}) = \max_{u \in \mathcal{N}(v_k)} \mathbf{h}_u^{(n-1)} \tag{4.18}$$

This approach enables each node to prioritize the most important information from its neighbors, facilitating efficient processing in scenarios where multiple competing influences must be considered.

The MLP component in the update rule implements the learned transformation that combines the node's current state with the aggregated neighborhood information:

$$\text{MLP}(\mathbf{x}) = \mathbf{W}_2 \sigma(\mathbf{W}_1 \mathbf{x} + \mathbf{b}_1) + \mathbf{b}_2 \tag{4.19}$$

where $\mathbf{W}_1$, $\mathbf{W}_2$, $\mathbf{b}_1$, and $\mathbf{b}_2$ are learnable parameters that are optimized during the training process to capture the complex relationships between system states and optimal decisions.

### 4.4.3 Output Generation and Parameter Extraction

The last step in the GNN framework is to design the optimization parameters for Alice's active beamforming as well as STAR-RIS's dual-functional coefficients. The process of output generation needs to map the learned node representations to the physical parameters that comply with the constraints imposed by the system structures, and the characteristics of wireless propagation.

For each user node $v_k$, the output layer generates a real-valued vector that is subsequently converted to the complex-valued beamforming vector:

$$\mathbf{w}_k' = \text{FCL}_k(\mathbf{h}_k^{(N)}) \in \mathbb{R}^{2N_a \times 1} \tag{4.20}$$

where FCL denotes a fully connected layer and $N$ is the number of GNN layers. The conversion to complex form is accomplished through:

$$\mathbf{w}_k = \mathbf{w}'_k[1:N_a] + j \cdot \mathbf{w}'_k[N_a+1:2N_a] \tag{4.21}$$

The STAR-RIS node generates the parameters controlling both reflection and transmission functionalities:

$$\mathbf{v}' = \mathrm{FCL}_0(\mathbf{h}_0^{(N)}) \in \mathbb{R}^{3L\times 1} \tag{4.22}$$

The output vector $\mathbf{v}'$ is structured to contain three types of parameters: the reflection amplitude coefficients $\alpha_l^r$ in the first $L$ components, and the cosine representations of the reflection and transmission phase shifts in the remaining components:

$$\alpha_l^r = \sigma(\mathbf{v}'[l]) \tag{4.23}$$

$$\cos(\theta_l^r) = \tanh(\mathbf{v}'[L+l]) \tag{4.24}$$

$$\cos(\theta_l^t) = \tanh(\mathbf{v}'[2L+l]) \tag{4.25}$$

where $\sigma(\cdot)$ is the sigmoid function ensuring that the amplitude coefficients remain in the valid range $[0,1]$, and $\tanh(\cdot)$ constrains the cosine values to the appropriate range $[-1,1]$.

The transmission amplitude coefficients are automatically determined by the energy conservation constraint:

$$\alpha_l^t = 1 - \alpha_l^r \tag{4.26}$$

The phase angles are recovered from their cosine representations using appropriate inverse trigonometric functions, with care taken to ensure that the phase unwrapping process maintains consistency across optimization iterations.

### 4.4.4 Loss Function Design and Training Process

The training of the GNN optimization framework requires the design of a loss function that effectively captures the multi-objective nature of the system optimization problem while providing stable and efficient learning dynamics. The loss function must simultaneously encourage communication performance improvement for legitimate users and security enhancement through eavesdropper degradation.

The primary component of the loss function is based on the negative sum secrecy rate, ensuring that the training process maximizes the overall security performance of the system:

$$\mathscr{L}_{\text{secrecy}} = -\frac{1}{T}\sum_{t=1}^{T}\sum_{k=1}^{K} R_{s,k}^{(t)} \tag{4.27}$$

where $T$ represents the number of training samples and $R_{s,k}^{(t)}$ is the secrecy rate achieved for the $k$-th user in the $t$-th training sample.

Additional regularization terms are incorporated to ensure that the learned solutions satisfy the physical constraints and maintain reasonable parameter magnitudes:

$$\mathscr{L}_{\text{reg}} = \lambda_1 \sum_{k=1}^{K} \|\mathbf{w}_k\|^2 + \lambda_2 \sum_{l=1}^{L} (\alpha_l^r + \alpha_l^t - 1)^2 \tag{4.28}$$

where $\lambda_1$ and $\lambda_2$ are regularization coefficients that balance the different components of the loss function.

The complete loss function combines these components:

$$\mathscr{L} = \mathscr{L}_{\text{secrecy}} + \mathscr{L}_{\text{reg}} \tag{4.29}$$

The training process employs stochastic gradient descent with the Adam optimizer to efficiently navigate the complex optimization landscape. The learning rate is adaptively adjusted using a cosine annealing schedule to ensure stable convergence:

$$\eta_t = \eta_{\min} + \frac{1}{2}(\eta_{\max} - \eta_{\min})\left(1 + \cos\left(\frac{t}{T_{\max}}\pi\right)\right) \tag{4.30}$$

where $\eta_{\min}$ and $\eta_{\max}$ are the minimum and maximum learning rates, and $T_{\max}$ is the total number of training steps.

## 4.5 Simulation Environment and Performance Evaluation

The thorough performance validation of the proposed GNN-based STAR-RIS system also requires the simulator to be carefully designed such that the essential aspects of the realistic deployment conditions are taken into account, as well as the possibility of systematic comparison with the already existing benchmark methods. The simulation platform comprises of the detailed channel models, real system parameters and extensive performance measures in order to make us understand in-depth about the potential and constraints of the proposed scheme.

### 4.5.1 System Configuration and Parameters

The simulation layout represents a realistic indoor-outdoor communication with the BS Alice deployed inside a building to serve multiple indoor users and a potential eavesdropper that sensitive information may leak of located outdoors. The STAR-RIS is also placed on the building envelope at a position for optimum dual-functionality. In this chapter, the STAR-RIS is assumed to operate under the ES protocol, where each element simultaneously supports both reflection and transmission. This allows the incident signal to be partitioned into reflected and transmitted components, providing sufficient flexibility for joint beamforming and security design. The system parameters listed in Table 4.1 are selected based on commonly adopted configurations in the literature on IRS- and STAR-RIS-assisted wireless communications, e.g., [4, 28, 155].

In particular, the number of RIS elements, node locations, and channel parameters follow typical settings used in prior works, ,where the transmitter, STAR-RIS, and users are deployed within a limited area. The path loss model and Rician fading factor are chosen according to standard wireless channel assumptions in indoor environments [156, 157]. The Rician fading factor is chosen to capture the presence of both line-of-sight and scattered components. As

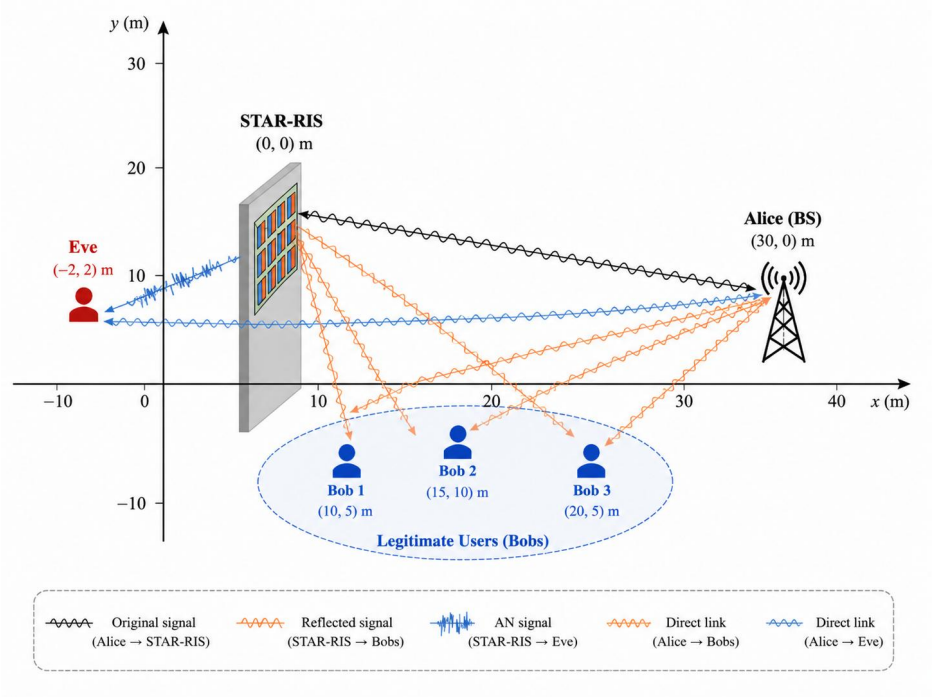


Fig. 4.3 Simulation scenario for the STAR-RIS-assisted secure indoor communication system.

shown in Fig. 4.3, the simulation scenario follows the coordinate settings summarized in Table 4.1.

The GNN-related parameters, including learning rate, batch size, and training epochs, are determined based on standard training practices to ensure stable convergence. In addition, multiple system configurations have been considered by varying key parameters such as the number of users and RIS elements, and the corresponding results are presented to demonstrate the robustness of the proposed scheme.

The channel modeling incorporates both large-scale and small-scale fading effects to provide realistic performance evaluation. The large-scale path loss follows the standard model:

$$\mathrm{PL}(d) = \mathrm{PL}_0 - 10\alpha \log_{10}(d/d_0) \tag{4.31}$$

where $d$ is the transmission distance, $d_0 = 1$ m is the reference distance, and $\alpha = 2.5$ is the path loss exponent. The small-scale fading follows a Rician distribution with factor $\varepsilon = 3$,

Table 4.1 Comprehensive System Parameters and Configuration Settings

| Parameter | Description | Value |
|---|---|---|
| $(x,y)_a$ | Alice spatial coordinates | $(30,0)$ m |
| $(x,y)_r$ | STAR-RIS spatial coordinates | $(0,0)$ m |
| $(x,y)_b$ | Bob spatial coordinates | $x,y \in [0,30]$ m |
| $(x,y)_e$ | Eve spatial coordinates | $(-2,2)$ m |
| $N_a$ | Alice antenna count | 4 |
| $N_b$ | Bob antenna count | 4 |
| $N_e$ | Eve antenna count | 4 |
| $L$ | STAR-RIS element count | 64 |
| $K$ | Number of legitimate users | 3 |
| $\varepsilon$ | Rician fading factor | 3 |
| $lr$ | GNN learning rate | 0.001 |
| $E$ | Training epochs | 600 |
| $\gamma$ | Learning rate decay factor | 0.995 |
| $B$ | Training batch size | 64 |
| $\alpha$ | Path loss exponent | 2.5 |
| $\mathrm{PL}_0$ | Reference path loss | $-30$ dB |

reflecting the mixed line-of-sight and multipath characteristics typical of indoor-outdoor communication scenarios.

The GNN architecture employs two layers of graph convolutions to balance representation capability with computational efficiency. The Adam optimizer is configured with an initial learning rate of 0.001 and a batch size of 64. Dropout regularization with a rate of 0.4 is applied to prevent overfitting and improve generalization performance.

### 4.5.2 Benchmark Algorithms and Comparison Framework

The performance evaluation considers several representative benchmark schemes to assess the effectiveness of the proposed GNN-based STAR-RIS framework under multi-user secure communication scenarios. These benchmarks are selected to reflect different beamforming strategies and system configurations commonly used in IRS-assisted systems.

**Traditional RIS**, This benchmark considers a conventional reflecting-only RIS architecture, where the surface only supports signal reflection without transmission capability. Compared with STAR-RIS, it lacks the additional degrees of freedom provided by simultaneous transmission and reflection, and therefore serves as a reference for evaluating the benefit of dual-functional surface design.

**MMSE Beamforming**, This scheme employs minimum mean square error (MMSE) beamforming at the transmitter, which aims to balance signal enhancement and interference suppression. It represents a widely used linear beamforming strategy in multi-user systems.

**Zero-Forcing (ZF) Beamforming**, This method applies zero-forcing beamforming to completely eliminate inter-user interference at the receiver side. While effective in interference suppression, it may lead to noise amplification, especially under limited transmit power.

**Maximum Ratio Transmission (MRT)**, This scheme focuses on maximizing the received signal power for each user without explicitly mitigating inter-user interference. It provides a performance lower bound in interference-limited scenarios.

**Proposed GNN-based STAR-RIS**, This scheme jointly optimizes active beamforming and STAR-RIS transmission and reflection coefficients using a GNN. It represents the proposed solution in this chapter and leverages both dual-functional surface capability and data-driven optimization.

The performance of these schemes is evaluated primarily in terms of the WSR, which is defined based on secrecy rate formulations and captures both communication efficiency and information leakage. Additional comparisons under different system configurations, such as varying numbers of users, transmit power levels, and RIS elements, are conducted to provide a comprehensive assessment of scalability and robustness.

In addition, comparisons with representative physical-layer security schemes, including Non-GNN STAR-RIS, AN-based beamforming, and random RIS configurations, are conducted to further validate the effectiveness of the proposed approach.

### 4.5.3 Learning Convergence and Training Dynamics

The analysis of GNN training dynamics provides crucial insights into the stability and efficiency of the proposed optimization approach. Fig. 4.4 illustrates the convergence behavior of the GNN training process over multiple epochs, demonstrating the algorithm's ability to effectively learn the complex optimization strategies required for joint beamforming and STAR-RIS control.

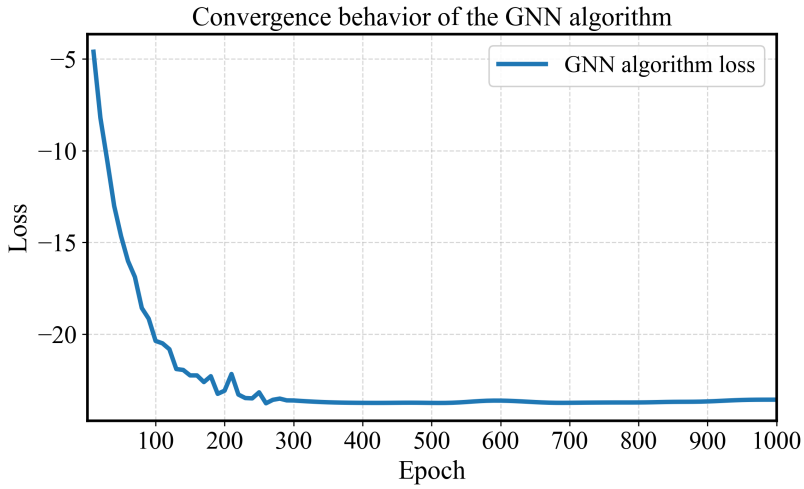


Fig. 4.4 GNN training convergence characteristics showing rapid initial learning followed by fine-tuning convergence to optimal performance levels.

The convergence analysis uncovers a number of key features of the learning. During the early stage of training, it is seen that significant progress has been made before the GNN learns simple optimizations and dependencies. There is then a long tail of refinement where the algorithm learns to deal with complex interactions and edge cases. The last convergence to a fixed optimum proves the convergence of training process and the rationality of the design of loss function.

The training dynamics also indicate the need to carefully choose the hyperparameters and schedule the learning rate. The adaptive learning rate process allows the algorithm to learn fast at the beginning and yet to be stable upon further fine-tuning. The dropout regularization is beneficial to inhibit overfitting and provide better generalization to channel conditions which are not seen.

### 4.5.4 Performance Comparison Analysis

This subsection evaluates the performance of the proposed GNN-based STAR-RIS scheme under different system configurations. The WSR is adopted as the main performance metric. The proposed method is compared with conventional RIS, MMSE, ZF, MRT, Non-GNN

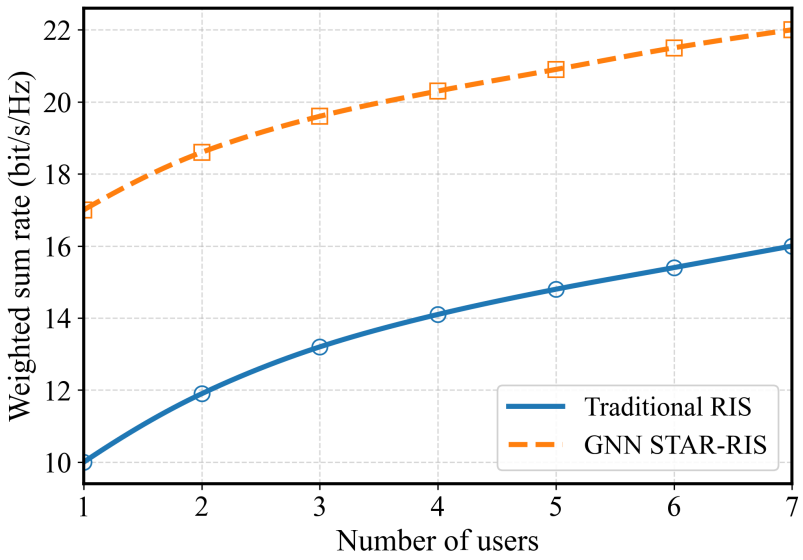


Fig. 4.5 Comparison between IRS and GNN-based STAR-RIS.

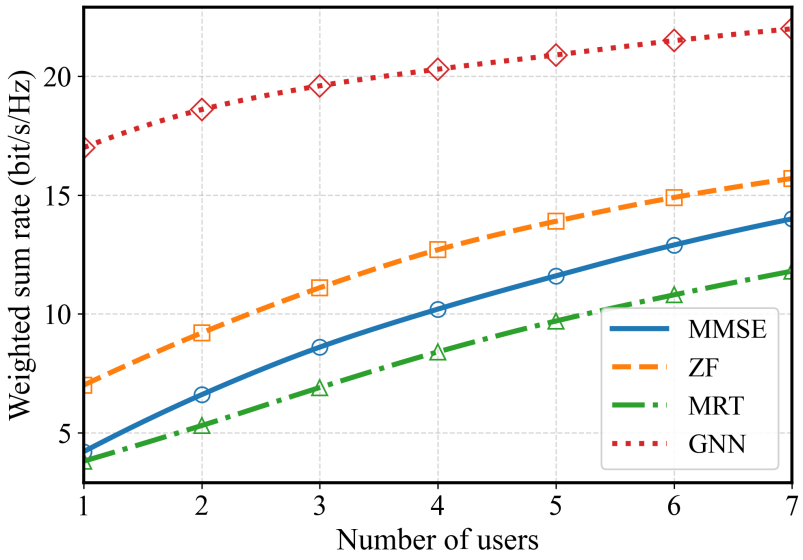


Fig. 4.6 WSR versus number of users under different beamforming schemes.

STAR-RIS, AN-based beamforming, and random RIS benchmarks to provide a comprehensive assessment of its effectiveness and scalability.

Fig. 4.5 compares the WSR performance of the proposed GNN-based STAR-RIS scheme with that of the traditional RIS scheme under different numbers of users. As shown in the figure, the WSR of both schemes increases as the number of users grows, since more users provide additional opportunities for multi-user resource allocation. However, the

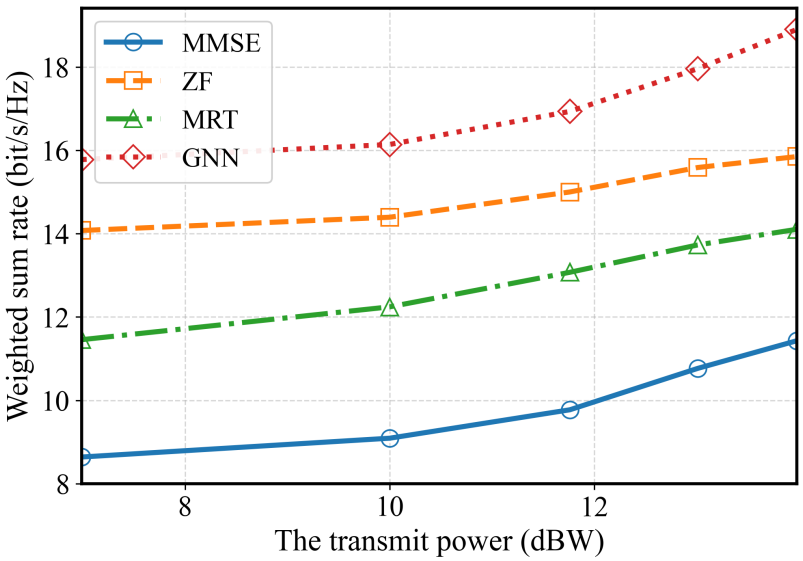


Fig. 4.7 WSR versus transmit power.

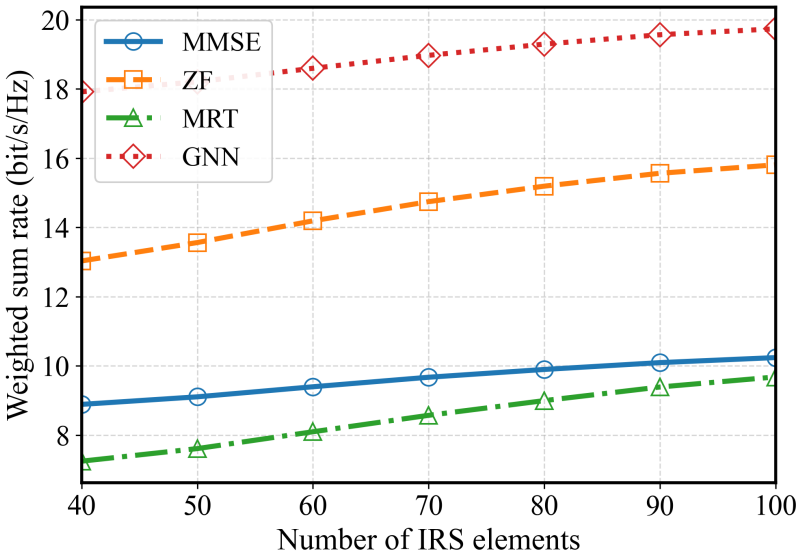


Fig. 4.8 WSR versus number of RIS elements.

proposed GNN-based STAR-RIS scheme consistently achieves a substantially higher WSR than the traditional RIS scheme across all values of $K$. This improvement is mainly due to the dual-functional transmission and reflection capability of STAR-RIS, which provides additional spatial degrees of freedom compared with the reflecting-only RIS. In addition, the GNN-based optimization can more effectively exploit the multi-user channel structure and

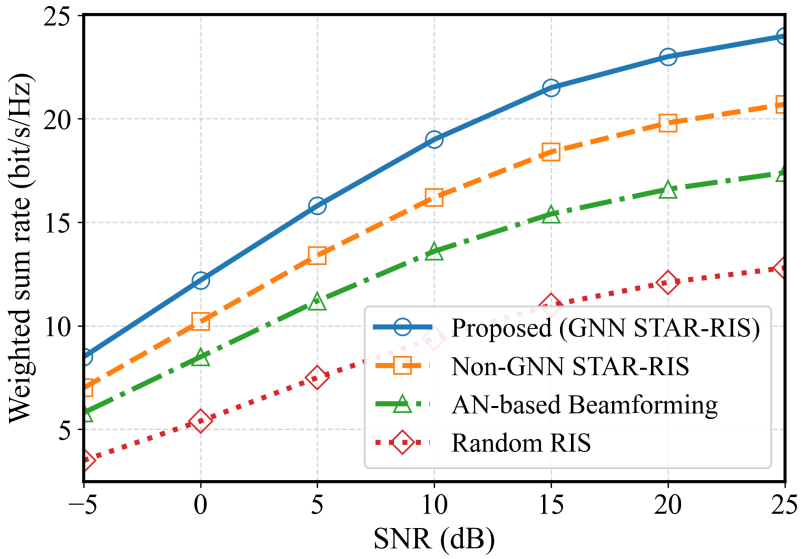


Fig. 4.9 WSR versus SNR for the proposed GNN-based STAR-RIS scheme and benchmark methods, including Non-GNN STAR-RIS, AN-based beamforming, and random RIS.

adjust the STAR-RIS coefficients accordingly. Therefore, the proposed scheme demonstrates better scalability and resource utilization in multi-user scenarios.

Fig. 4.6 further compares the proposed GNN-based method with conventional beamforming schemes, including MMSE, ZF, and MRT, under varying user loads. The GNN-based scheme achieves the highest WSR for all considered values of $K$, demonstrating its superior scalability and interference management capability. As $K$ increases, the system experiences stronger inter-user interference and more complex resource allocation requirements. Conventional schemes rely on fixed or analytically designed beamforming rules and therefore have limited flexibility in adapting to the joint STAR-RIS configuration. In contrast, the proposed GNN-based method learns the relationship between channel conditions, user distribution, and optimization variables, allowing it to better exploit the available spatial resources. Among the conventional methods, ZF generally outperforms MMSE and MRT due to its stronger interference suppression capability, while MRT shows lower performance because it prioritizes signal enhancement without sufficiently mitigating inter-user interference.

Fig. 4.7 shows the WSR versus the transmit power budget $P_{\max}$. The WSR of all methods increases with $P_{\max}$ because a larger power budget allows stronger signal transmission and

improved received SINR. However, the proposed GNN-based approach achieves consistently higher WSR than the conventional methods over the whole power range. This indicates that the proposed scheme can utilize the available transmit power more efficiently through joint optimization of active beamforming and STAR-RIS coefficients. The performance advantage becomes more pronounced at higher transmit power, where efficient interference control and spatial signal shaping become increasingly important. In comparison, MRT exhibits earlier performance saturation, suggesting inefficient power utilization under multi-user interference.

Fig. 4.8 illustrates the WSR versus the number of RIS elements. The WSR improves as the number of STAR-RIS elements increases, since more elements provide additional spatial degrees of freedom for signal enhancement and interference suppression. The proposed GNN-based method achieves the best performance across all values of $L$, showing that it can effectively scale with the size of the reconfigurable surface. This result also indicates that the GNN can learn to exploit the enlarged STAR-RIS configuration efficiently. By contrast, conventional beamforming methods obtain smaller gains as $L$ increases, because they cannot fully utilize the additional reflection and transmission resources provided by the STAR-RIS.

Fig. 4.9 compares the proposed method with representative physical-layer security benchmarks, including Non-GNN STAR-RIS, AN-based beamforming, and random RIS. The proposed GNN-based STAR-RIS scheme achieves the highest WSR over the entire SNR range. The gain over Non-GNN STAR-RIS demonstrates the benefit of learning-based optimization in handling the coupled active beamforming and passive STAR-RIS coefficient design. The improvement over AN-based beamforming highlights the advantage of using STAR-RIS to shape the wireless propagation environment and generate spatially selective interference. The significant gap between the proposed method and random RIS further confirms that optimized STAR-RIS control is essential for achieving high system performance.

Overall, the results demonstrate that the proposed GNN-based STAR-RIS framework provides clear performance advantages over both traditional RIS and conventional physical-layer security schemes. The proposed method achieves higher WSR under varying user numbers,

transmit power budgets, RIS sizes, and SNR levels. These results confirm its effectiveness in multi-user secure communication scenarios and show that the combination of STAR-RIS and GNN-based optimization offers improved scalability, interference management, and resource utilization.

## 4.6 Robustness Analysis under Practical Uncertainties

In practical systems, the acquisition of CSI for IRS/STAR-RIS-assisted links is challenging due to the cascaded nature of the channels. Typically, the overall BS-RIS-user channel is estimated rather than individual links.

Common approaches include pilot-based training with sequential ON/OFF reflection patterns, where the RIS elements are activated in predefined configurations to facilitate channel estimation. For high-dimensional systems, compressed sensing techniques can be employed to exploit channel sparsity and reduce training overhead. In addition, semi-passive RIS architectures, where a small number of elements are equipped with RF chains, can assist in more efficient channel acquisition.

Due to practical limitations, channel estimation errors are inevitable, which may degrade the system performance and the effectiveness of beamforming and RIS configuration. Therefore, it is essential to evaluate the robustness of the proposed scheme under these practical conditions.

### 4.6.1 Impact of Imperfect CSI

The assumption of perfect CSI is rarely satisfied due to channel estimation errors, pilot contamination, feedback delay, and hardware impairments in practical STAR-RIS-assisted wireless systems. These factors introduce uncertainty in the channel knowledge, which may significantly affect the performance of beamforming and STAR-RIS coefficient optimization.

To model channel estimation errors, the estimated channel is expressed as

$$\hat{\mathbf{H}} = \mathbf{H} + \Delta\mathbf{H}, \tag{4.32}$$

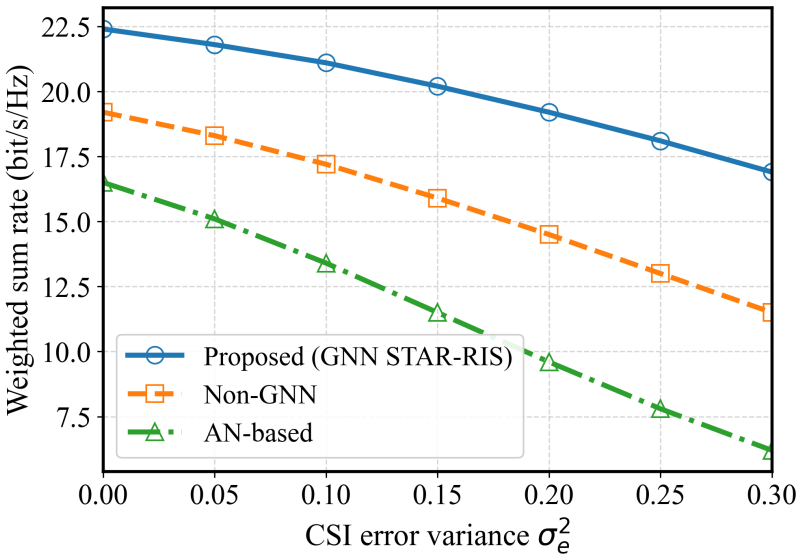


Fig. 4.10 WSR versus CSI error variance under different transmission schemes.

where $\mathbf{H}$ denotes the actual channel matrix, $\hat{\mathbf{H}}$ represents the estimated CSI used for optimization, and $\Delta\mathbf{H}$ is the estimation error. The error is modeled as a complex Gaussian random matrix:

$$\Delta\mathbf{H} \sim \mathscr{CN}(\mathbf{0}, \sigma_e^2\mathbf{I}), \tag{4.33}$$

where $\sigma_e^2$ is the CSI error variance. In this work, the beamforming vectors and STAR-RIS coefficients are designed based on $\hat{\mathbf{H}}$, while the system performance is evaluated using the true channel $\mathbf{H}$. This reflects a practical mismatch between design and operation.

Fig. 4.10 illustrates the WSR versus the CSI error variance. It can be observed that the WSR decreases monotonically as $\sigma_e^2$ increases. This degradation is mainly due to the mismatch between the optimized coefficients and the actual propagation environment. Specifically, CSI errors affect two critical aspects of the STAR-RIS system: (i) the coherent combination of the direct and STAR-RIS-assisted signal paths, and (ii) the spatial distribution of AN. As the CSI becomes less accurate, the phase alignment provided by the STAR-RIS becomes suboptimal, and the AN cannot be precisely directed toward the eavesdroppers, resulting in performance loss.

Nevertheless, the proposed GNN-based STAR-RIS scheme consistently achieves higher WSR than the Non-GNN and AN-based benchmark methods across all CSI error levels.

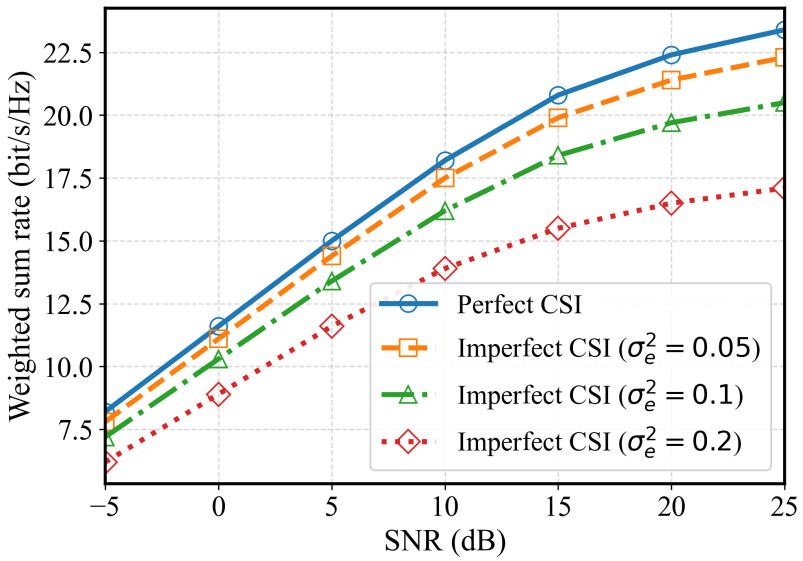


Fig. 4.11 WSR versus SNR under perfect and imperfect CSI conditions with different error variances.

This indicates that the learned optimization strategy is less sensitive to channel uncertainty and can better capture the underlying structure of the wireless environment compared to conventional iterative approaches. In contrast, the AN-based method suffers from more severe performance degradation, as it relies heavily on accurate CSI to place AN in the appropriate spatial directions.

Fig. 4.11 further presents the WSR versus SNR under different CSI error variances. As expected, increasing the SNR improves the WSR for all cases. However, the performance gap between perfect CSI and imperfect CSI becomes more pronounced at high SNR levels. This is because, in high-SNR regimes, the system performance is more dependent on precise beamforming and interference management, making it more sensitive to CSI inaccuracies.

Moreover, it is observed that moderate CSI errors (e.g., $\sigma_e^2 = 0.05$) lead to only limited performance degradation, while larger errors (e.g., $\sigma_e^2 = 0.2$) result in more noticeable performance loss. This demonstrates that the proposed scheme maintains a satisfactory level of robustness under realistic channel estimation conditions. The ability of the GNN-based approach to generalize across imperfect CSI scenarios can be attributed to its data-driven

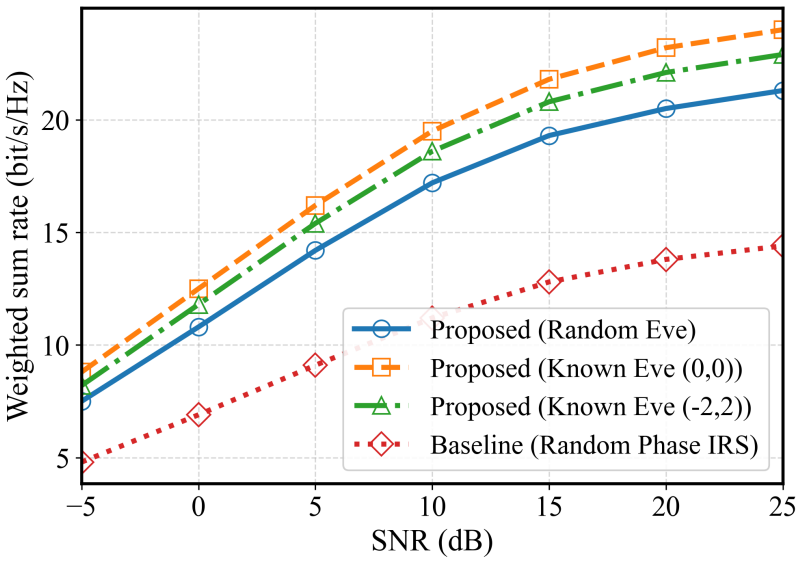


Fig. 4.12 WSR versus SNR under different eavesdropper location assumptions.

nature, which enables it to implicitly learn robust mappings between channel realizations and optimal control variables.

Overall, these results confirm that although imperfect CSI inevitably degrades system performance, the proposed GNN-based STAR-RIS framework remains effective and robust in practical environments, achieving superior performance compared to conventional methods under both perfect and imperfect CSI conditions.

### 4.6.2 Impact of Unknown or Mobile Eavesdroppers

In addition to CSI uncertainty, the uncertainty in the location of eavesdroppers is another important practical factor that affects system security performance. To model this uncertainty, the eavesdropper is assumed to be randomly distributed within a predefined region, and the performance is evaluated by averaging over multiple realizations.

Fig. 4.12 shows the WSR versus SNR under different eavesdropper location assumptions, including two known fixed locations and a randomly distributed case. This figure directly evaluates the impact of location uncertainty on the security performance of the proposed scheme.

It can be observed that the proposed scheme achieves the highest WSR when the eavesdropper location is perfectly known, as the system can more accurately suppress the corresponding eavesdropping channel. In particular, the curve corresponding to the known eavesdropper location consistently lies above the other cases across all SNR values.

When the eavesdropper is randomly distributed within a predefined region, the WSR decreases compared to the ideal case with known location. This performance loss is due to the fact that the AN cannot be precisely aligned to a specific eavesdropper channel. Instead, the interference must be distributed over a potential eavesdropping region, which reduces its effectiveness for any individual realization. Nevertheless, the degradation remains moderate, and the proposed scheme still achieves a steadily increasing WSR as the SNR increases, demonstrating robustness against location uncertainty.

Furthermore, the proposed scheme significantly outperforms the baseline method with random phase IRS across all SNR levels. The performance gap remains substantial, particularly in the medium- to high-SNR region, indicating that optimized STAR-RIS control is essential for maintaining security performance under uncertain eavesdropper conditions.

Overall, these results confirm that unknown or mobile eavesdroppers inevitably degrade system performance, but the proposed GNN-based STAR-RIS framework remains effective. By adaptively adjusting beamforming and interference patterns, the system can provide reliable security performance even when the exact eavesdropper location is unavailable.

## 4.7 Computational Complexity and Implementation Considerations

This section analyzes the computational complexity and discusses practical implementation aspects of the proposed GNN-based STAR-RIS system. In addition, deployment considerations of STAR-RIS are addressed to provide a more comprehensive view of real-world applicability.

### 4.7.1 Complexity Analysis

The computational complexity of the proposed framework mainly arises from the GNN inference process and the STAR-RIS coefficient generation.

The complexity of the GNN forward propagation scales linearly with the size of the graph, and can be expressed as

$$\mathcal{O}(L \cdot d \cdot H), \tag{4.34}$$

where $L$ is the number of GNN layers, $d$ is the feature dimension, and $H$ is the hidden layer size. This linear complexity makes the proposed approach scalable with respect to the number of users and STAR-RIS elements.

Compared with conventional optimization-based methods, which typically require solving non-convex problems via iterative algorithms, the proposed method significantly reduces online computational burden. Traditional approaches often involve matrix operations with cubic complexity and iterative updates, leading to high latency. In contrast, the proposed GNN-based method only requires a single forward pass during inference.

The training process has higher complexity, given by

$$\mathcal{O}(T \cdot B \cdot L \cdot d \cdot H), \tag{4.35}$$

where $T$ denotes the number of training epochs and $B$ is the batch size. However, this process is performed offline and does not affect real-time system operation.

### 4.7.2 Implementation Issues

From an implementation perspective, several practical factors need to be considered for deploying the proposed GNN-based STAR-RIS system.

First, the acquisition of CSI introduces overhead and estimation errors. In practical systems, imperfect CSI is unavoidable due to estimation inaccuracies and feedback delays. As discussed in Section 4.6, the proposed method maintains robust performance under such conditions.

Second, real-time adaptation is required due to dynamic channel variations. The proposed GNN-based approach is well-suited for this scenario, as the inference process involves only a forward pass through the network, enabling low-latency computation. This allows the system to update beamforming vectors and STAR-RIS coefficients within practical channel coherence times.

Third, the implementation of STAR-RIS control requires programmable hardware capable of adjusting transmission and reflection coefficients. Modern metasurface technologies support such programmable control via digital interfaces, enabling integration with BS controllers.

Finally, the computational tasks associated with GNN inference can be efficiently executed on standard processing platforms, such as GPUs or dedicated signal processing units. This makes the proposed approach feasible for practical deployment without requiring specialized hardware beyond current communication system capabilities.

### 4.7.3 STAR-RIS Deployment Considerations

In addition to algorithm design, the physical deployment of the STAR-RIS plays a critical role in determining system performance, particularly for secure communication scenarios.

As illustrated in Fig. 4.13, the STAR-RIS is deployed to strengthen signal coverage in the legitimate user region while limiting signal leakage toward a potential eavesdropping region. Instead of directing AN toward a specific eavesdropper, the interference is spatially distributed over a region where eavesdroppers may be located. This reflects a practical deployment scenario where the exact location of the eavesdropper is unknown or time-varying.

In this thesis, the STAR-RIS location is assumed to be fixed in order to focus on beamforming and system optimization. However, in practical deployments, the placement of the STAR-RIS should be carefully designed according to both communication efficiency and security requirements.

From a communication perspective, the STAR-RIS should be deployed to strengthen the propagation links between the BS and legitimate users, typically by ensuring favorable geometric positioning and strong line-of-sight components.

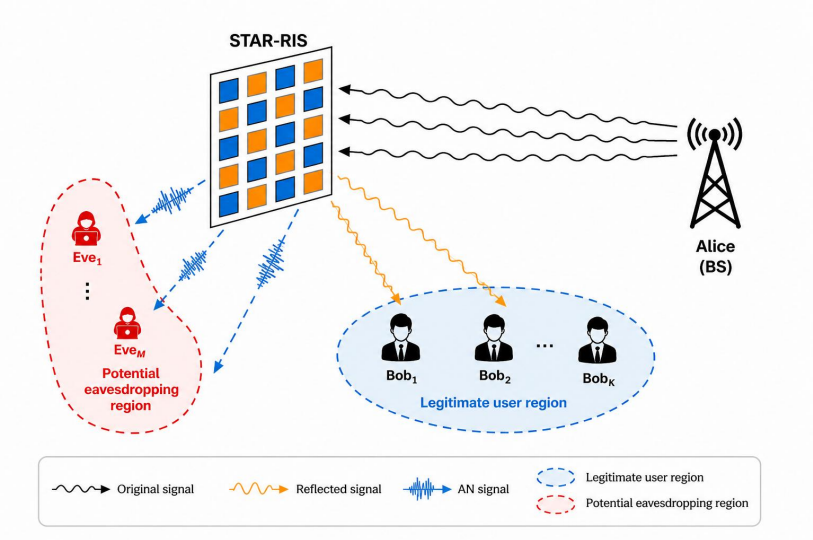


Fig. 4.13 Illustration of STAR-RIS deployment for secure communication under uncertain eavesdropper locations. The STAR-RIS enhances the legitimate user region while distributing AN over a potential eavesdropping region.

From a security perspective, deployment should consider potential eavesdropping regions. When the exact location of the eavesdropper is unknown or time-varying, a region-based deployment strategy is more appropriate. Specifically, the STAR-RIS can be positioned to enhance signal coverage within the legitimate user region while limiting signal leakage toward areas where eavesdroppers may exist.

Under such deployment, the AN is not directed toward a specific point but is spatially distributed over a potential eavesdropping region. This is achieved through the joint design of transmit beamforming and STAR-RIS coefficients, which shape the spatial distribution of interference.

Furthermore, the GNN-based optimization framework adapts to the deployment geometry and channel conditions, enabling effective interference distribution even under location uncertainty.

Overall, although optimal STAR-RIS placement is difficult to guarantee in dynamic environments, geometry-aware and region-based deployment strategies provide a practical and effective approach for secure STAR-RIS-assisted communication systems.

## 4.8 Chapter Summary and Future Directions

This chapter has presented a unified framework for GNN-empowered STAR-RIS optimization in secure indoor multi-user communication systems, aiming to bridge intelligent surface technology with learning-based optimization approaches. The proposed method addresses the joint design problem in a correlated MIMO wiretap channel by employing a scalable and structured optimization framework.

The main technical contributions include the design of a dual-functional STAR-RIS architecture, the development of a GNN-based optimization framework for joint active and passive beamforming, and a comprehensive performance evaluation under realistic system assumptions. The results demonstrate consistent performance gains over representative benchmark schemes in terms of WSR and system efficiency.

The dual-functional STAR-RIS enables simultaneous transmission and reflection, which provides additional spatial degrees of freedom compared to conventional reflecting-only RIS. This facilitates enhanced signal shaping for legitimate users while enabling the distribution of AN toward potential eavesdropping regions.

The proposed GNN-based optimization framework reduces the computational burden associated with conventional iterative algorithms. By learning the mapping between channel conditions and optimization variables, the GNN can efficiently approximate high-dimensional solutions with significantly reduced complexity. The graph-based representation captures the relationships among users and channels, enabling scalable optimization in multi-user scenarios.

Simulation results show that the proposed approach achieves higher WSR compared to conventional methods such as MMSE, ZF, MRT, and non-learning-based STAR-RIS schemes. In addition, the results demonstrate robustness under imperfect CSI and varying eavesdropper locations, indicating the effectiveness of the proposed design under practical uncertainties.

From a security perspective, the proposed framework enhances performance by combining spatial signal enhancement for legitimate users with AN distribution in uncertain regions. While the current evaluation considers randomly distributed eavesdroppers, more sophisticated adversarial models remain an important direction for future work.

In terms of practical implementation, the proposed framework is compatible with existing system architectures, as the optimization is primarily performed at the BS and the STAR-RIS operates through programmable coefficients. The GNN inference process introduces moderate computational overhead, making near real-time implementation feasible for typical system sizes.

Despite these advantages, several limitations remain. The current work assumes fixed deployment geometry, simplified channel estimation models, and ideal hardware conditions. Moreover, the GNN is trained under a specific indoor scenario and its generalization to different environments is not explicitly validated.

Future work should therefore focus on developing robust channel estimation methods, geometry-aware STAR-RIS deployment strategies, and learning frameworks with improved generalization across different scenarios. In addition, incorporating hardware constraints and more advanced eavesdropping models would further enhance the practical relevance of the proposed framework. Extending the current design toward integrated sensing, communication, and security systems also represents a promising research direction.

Overall, the findings of this chapter provide useful insights into the design of intelligent wireless systems that jointly consider communication performance, security, and computational efficiency, and offer a foundation for future research on practical STAR-RIS-assisted networks.

# Chapter 5

# IRS-Backscatter Downlink Multi-User Communications with Radar Sensing

## Overview

The increasing demand for spectrum efficiency and dual-functionality in next-generation wireless networks has accelerated research into ISAC. In this context, IRS technology offers a promising pathway by enabling RCC through passive backscatter operation. This chapter introduces a novel indoor multi-user downlink communication framework in which a colocated MIMO radar not only performs target detection but also serves as a carrier source for IRS-assisted backscatter transmission. By jointly optimizing radar transmit signals, IRS reflection coefficients, user scheduling, and radar receive processing, the system achieves efficient spectrum sharing and balanced performance between sensing and communications. A fractional programming-based AO algorithm is developed to address the inherent non-convexity of the design, offering convergence within a small number of iterations. Extensive simulations validate the feasibility of the framework, demonstrating significant gains over baseline schemes, as well as clear trade-offs between radar SINR and communication throughput. Compared with the confidential IRS-backscatter design in Chapter 3 and the STAR-RIS based optimization in Chapter 4, the present framework advances the role of IRS towards dual-functional operation, establishing it as a key enabler for 6G ISAC systems.

## 5.1 Motivation and System Architecture

With the continuous evolution of wireless networks towards fifth- and sixth-generation (5G/6G) systems, there has been a dramatic increase in demand for spectrum resources to accommodate high-capacity communications, pervasive connectivity, and low-latency applications. At the same time, radar systems remain indispensable for civilian, industrial, and defense applications, including target detection, tracking, and environmental sensing. The convergence of these two requirements has led to an urgent need for RCC solutions. Unlike traditional spectrum allocation, where dedicated frequency bands are exclusively reserved for either radar or communication, RCC aims to enable these two functionalities to operate simultaneously within shared spectral resources. Such integration is increasingly recognized as a fundamental enabler of ISAC in 6G systems [158, 159].

Chapters 3 and 4 of this thesis investigated two key frontiers in IRS technology. In Chapter 3, the concept of IRS-assisted backscatter confidential communication was developed, where IRS was leveraged to enhance secrecy performance in a multi-user system by jointly optimizing the reflection coefficients and confidential information signals. Chapter 4 extended this paradigm into STAR-RIS systems, where GNNs were designed to manage secure multi-user communications with reduced computational complexity. Building upon these results, the present chapter advances the analysis by considering the dual role of IRS in enabling both radar sensing and downlink communications through passive backscatter operation. This represents a significant departure from conventional IRS designs, where IRS is regarded purely as a programmable reflecting entity. Here, the IRS is reinterpreted as an active enabler of spectrum sharing and multi-user communication leveraging incident radar signals.

### 5.1.1 Motivation

The motivation for this research can be summarized as follows. First, spectrum scarcity in 6G has become a critical challenge. With mmWave and THz bands being targeted for 6G deployment, spectrum resources are increasingly contested, and sharing spectrum

between radar and communication systems provides a natural pathway to improve efficiency. Second, IRS technology offers unprecedented flexibility in shaping wireless propagation environments. By enabling IRS to operate in a backscatter mode, the incident radar waveform can be opportunistically re-purposed to support downlink communication without requiring additional active transmitters. It should be noted that the radar signal is not specifically designed to strengthen the communication link; rather, it is reused as an information carrier through IRS-based modulation, enabling dual functionality without additional transmission resources. Third, in RCC systems, a fundamental trade-off arises between maintaining high radar detection performance and ensuring sufficient throughput for communication users. Optimizing this trade-off is non-trivial, particularly in multi-user scenarios. Finally, as 6G envisions a fully converged communication-sensing paradigm, exploring IRS-based backscatter coexistence represents a crucial step toward low-cost and energy-efficient ISAC architectures.

### 5.1.2 System Architecture

Consider a dual-functional system comprising a colocated MIMO radar and an IRS deployed to serve multiple downlink users, as illustrated in Fig. 5.1. Such a system is representative of ISAC applications in scenarios such as smart environments, indoor coverage enhancement, and vehicular networks, where sensing and communication functionalities are required to coexist within the same spectral resources. The MIMO radar transmits probing signals to track a far-field target. These signals impinge upon the IRS, which is equipped with L reflecting elements. Instead of acting as a simple mirror, the IRS applies modulated phase shifts to the incident radar waveform, thereby backscattering information-bearing signals towards K user equipments (UEs). Each UE is equipped with N antennas and receives both direct signals from the radar and indirect signals via the IRS.

Simultaneously, the radar receiver processes the echoes reflected from both the target and the IRS-assisted communication paths. As a result, the radar must distinguish between target echoes and IRS-backscattered communication signals, which introduces a design challenge in beamforming and resource allocation. Specifically, the signals received at the radar consist

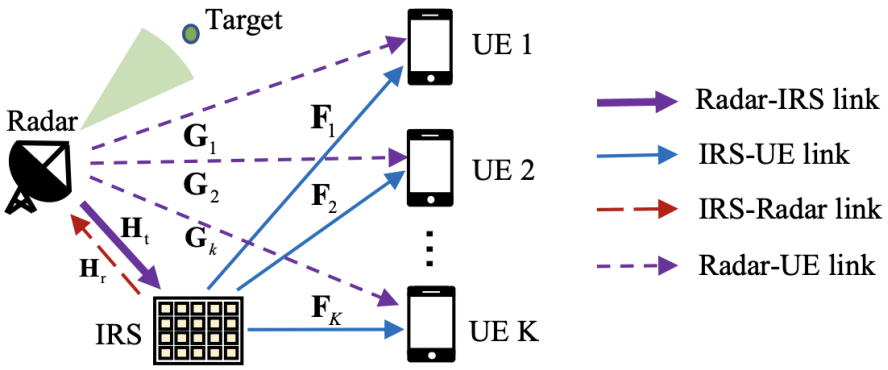


Fig. 5.1 Illustration of an IRS-assisted ISAC system, where a radar and a multi-user downlink communication system coexist.

of the desired target echoes as well as the signals reflected from the IRS, which may carry communication information. There is no direct transmission from the UEs to the radar in this model. The IRS is therefore required to balance between aligning reflections for improved downlink communications and avoiding destructive interference that may degrade radar sensing.

Mathematically, the IRS-assisted RCC system can be characterized by four critical design dimensions. The first concerns radar transmit signal design, which governs both detection quality and the signal available for backscatter modulation. The second involves the optimization of IRS reflection coefficients, which control the directionality and strength of the backscattered signals. The third dimension is user time allocation and scheduling, which ensures fairness and efficient utilization of resources across multiple UEs. Finally, the fourth dimension is radar receive beamforming, which enables effective separation of target echoes from communication-induced interference.

By jointly designing these components, the system seeks to maximize the WSR of communications while simultaneously maintaining the minimum SINR required for reliable radar sensing. This unified design problem forms the foundation of the optimization framework developed in this chapter.

## 5.2 Mathematical System Model

As illustrated in Fig. 5.1, we consider an IRS backscatter enabled time division duplex (TDD) downlink multi-user communication system coexisting with radar sensing. A colocated MIMO radar equipped with $M_t$ transmit antennas and $M_r$ receive antennas transmits a detection signal to track a far-field point-like target, while an $L$-element IRS is deployed to harvest the radar signal and enable downlink communications with $K$ users, each equipped with $N$ antennas, in a TDD manner. It should be clarified that the radar signal is reused as a communication carrier through IRS-based modulation, rather than being a dedicated downlink signal. Therefore, it is not inherently constructive or destructive to the communication users. The constructive effect is achieved through the design of IRS reflection coefficients, which align the reflected signal toward the intended users, while misalignment or improper design may result in interference. The considered system operates in a time-division manner. Specifically, the radar transmits a unified waveform, while the IRS serves multiple users sequentially over different time slots. During each time slot, the IRS modulates and reflects the incident radar signal to a specific user, enabling downlink communication. Therefore, different users are served in orthogonal time slots, and time allocation is introduced as an additional optimization variable. It is assumed that the control information between the radar and the IRS can be exchanged reliably and that the CSI of all links is perfectly known.

### 5.2.1 Dual-Function Signal Model

The radar transmits probing signal $\mathbf{x} \in \mathbb{C}^{M_t \times 1}$ for target detection, subject to the power constraint

$$\mathrm{Tr}\left(\mathbf{x}\mathbf{x}^T\right) \leq P, \tag{5.1}$$

where $P$ denotes the total radar transmit power budget. Specifically, $\mathbf{x}$ is used to illuminate the target for sensing, while simultaneously acting as the incident signal for IRS-based backscatter communication. In this work, the radar transmit signal $\mathbf{x}$ is treated as an optimization variable. Both its amplitude and phase are jointly optimized to enhance communication performance while satisfying the radar sensing requirements.

When the IRS communicates with the $k$-th UE, the received backscatter signal is given by

$$\mathbf{F}_k\Theta_k\mathbf{H}_t\mathbf{x} = \mathbf{F}_k\text{diag}\{\mathbf{H}_t\mathbf{x}\}\theta_k \overset{\text{modulate}}{=\!=\!=} \mathbf{F}_k\text{diag}\{\mathbf{H}_t\mathbf{x}\}\mathbf{v}_k s_k, \quad k \in \mathscr{K}, \tag{5.2}$$

where $\mathscr{K} = \{1,2,\ldots,K\}$, $\mathbf{H}_t \in \mathbb{C}^{L\times M_t}$ is the radar-IRS channel, and $\mathbf{F}_k \in \mathbb{C}^{N\times L}$ is the IRS-UE channel for user $k$. The backscatter coefficient vector is $\mathbf{v}_k \in \mathbb{C}^{L\times 1}$, which embeds the new symbol $s_k$. It should be noted that the received signal corresponds to the IRS-backscattered signal rather than a direct transmission. Specifically, the IRS encodes information by dynamically varying its reflection coefficients across symbols, such that each element multiplies the incident signal $\mathbf{H}_t\mathbf{x}$ by a modulation term. As a result, the new symbol $s_k$ is introduced through this modulation process. Therefore, the signal is not simply $\mathbf{v}_k\mathbf{x}$, but rather a modulated reflection of the incident waveform carrying additional information.

Due to the IRS reflection constraint, we must have

$$[\mathbf{v}_k\mathbf{v}_k^H]_{l,l} \leq 1, \quad \forall l, \tag{5.3}$$

where $[\cdot]_{l,l}$ denotes the $(l,l)$-th diagonal entry of a matrix. For analysis, $\{s_k\}$ are modeled as i.i.d. Gaussian random variables.

### 5.2.2 Received Signal at the Users

The received signal at the $k$-th UE is

$$\mathbf{y}_{c,k} = \mathbf{G}_k\mathbf{x} + \mathbf{F}_k\text{diag}(\mathbf{H}_t\mathbf{x})\,\mathbf{v}_k s_k + \mathbf{n}_{c,k}, \quad k \in \mathscr{K} \tag{5.4}$$

where $\mathbf{G}_k \in \mathbb{C}^{N\times M_t}$ represents the channel gain matrix from the radar to the $k$-th UE channel, and $\mathbf{n}_{c,k} \sim \mathscr{CN}(0,\sigma_c^2\mathbf{I}_N)$ is the white Gaussian noise vector. It should be noted that all users receive the same radar probing signal $\mathbf{x}$ through different channel realizations $\mathbf{G}_k$. However, the user-specific information is not conveyed by $\mathbf{x}$ itself, but is embedded through the IRS backscatter modulation term $\mathbf{v}_k s_k$. Here, $s_k$ represents the desired information symbol for the $k$-th user.

The SINR at the $k$-th user is given by

$$\gamma_{c,k} = \mathbf{v}_k^H \mathbf{T}_k^H \left(\sigma_{c,k}^2 \mathbf{I}_c + \mathbf{G}_k \mathbf{x}\mathbf{x}^H \mathbf{G}_k^H\right)^{-1} \mathbf{T}_k \mathbf{v}_k, \quad k \in \mathscr{K}, \tag{5.5}$$

where $\mathbf{T}_k = \mathbf{F}_k \text{diag}\{\mathbf{H}_t \mathbf{x}\}$. Thus, the communication rate at the $k$-th UE is given by

$$R_k = \log_2\left(1 + \gamma_{c,k}\right). \tag{5.6}$$

### 5.2.3 Received Signal at the Radar

At the radar receiver, the received signal is

$$\mathbf{y}_{r,k} = \eta \Lambda(\theta)\mathbf{x} + \mathbf{H}_r \text{diag}\{\mathbf{H}_t \mathbf{x}\}\mathbf{v}_k s_k + \mathbf{n}_{r,k}, \quad k \in \mathscr{K}, \tag{5.7}$$

where $\theta$ is the target azimuth, $\eta$ the path-loss coefficient, $\mathbf{H}_r \in \mathbb{C}^{M_r \times L}$ the IRS-radar channel, and $\mathbf{n}_{r,k} \sim \mathscr{CN}(0, \sigma_{r,k}^2 \mathbf{I}_r)$ is the noise vector. The steering matrix is $\Lambda(\theta) = \mathbf{a}_r(\theta)\mathbf{a}_t^T(\theta)$, with

$$\mathbf{a}_t(\theta) = \tfrac{1}{M_t}[1, e^{j2\pi d \sin\theta}, \ldots, e^{j2\pi(M_t-1)d\sin\theta}]^T, \tag{5.8}$$

$$\mathbf{a}_r(\theta) = \tfrac{1}{M_r}[1, e^{j2\pi d \sin\theta}, \ldots, e^{j2\pi(M_r-1)d\sin\theta}]^T. \tag{5.9}$$

Applying a normalized beamformer $\mathbf{w}_k \in \mathbb{C}^{M_r \times 1}$, the radar output is

$$\bar{\mathbf{y}}_{r,k} = \eta \mathbf{w}_k^H \Lambda(\theta)\mathbf{x} + \mathbf{w}_k^H \mathbf{H}_r \text{diag}\{\mathbf{H}_t \mathbf{x}\}\mathbf{v}_k s_k + \mathbf{w}_k^H \mathbf{n}_{r,k}. \tag{5.10}$$

Thus, the radar SINR is

$$\gamma_{r,k} = \frac{|\eta \mathbf{w}_k^H \Lambda(\theta)\mathbf{x}|^2}{|\mathbf{w}_k^H \mathbf{H}_r \text{diag}\{\mathbf{H}_t \mathbf{x}\}\mathbf{v}_k|^2 + \sigma_r^2 \|\mathbf{w}_k\|^2}, \quad k \in \mathscr{K}. \tag{5.11}$$

## 5.3 Problem Formulation and Proposed Optimization Algorithm

The objective is to maximize the weighted sum bits per unit bandwidth of all UEs by jointly optimizing the transmit beamforming signal $\mathbf{x}$, the IRS beamforming vectors $\mathbf{v}_k$, the time allocation $\{t_k\}$, and the radar receive beamforming $\mathbf{w}_k$. The optimization problem is formulated as

$$\text{(P1)} \quad \max_{\mathbf{x},\mathbf{v}_k,\mathbf{w}_k,t_k} \sum_{k\in\mathscr{K}} \omega_k t_k \log\left(1+\gamma_{c,k}\right), \tag{5.12}$$

subject to

$$\text{C1: } \mathrm{Tr}(\mathbf{x}\mathbf{x}^H) \le P, \tag{5.13}$$

$$\text{C2: } \left[\mathbf{v}_k\mathbf{v}_k^H\right]_{l,l} \le 1, \quad l \in \mathscr{L}, k \in \mathscr{K}, \tag{5.14}$$

$$\text{C3: } 0 \le t_k, \quad k \in \mathscr{K}, \tag{5.15}$$

$$\text{C4: } 0 \le \sum_{k\in\mathscr{K}} t_k \le T, \tag{5.16}$$

$$\text{C5: } \gamma_{r,k} \ge \Gamma_r, \quad k \in \mathscr{K}, \tag{5.17}$$

where $\omega_k$ is the weighting factor of the $k$-th UE, $T$ is the considered time block length, and $\Gamma_r$ is the minimum SINR required at the radar. The weighting factors $\omega_k$ are introduced to provide flexibility in prioritizing different users in the multi-user system.

### 5.3.1 Objective Transformation

By introducing auxiliary variables $\alpha_k \ge 0$, the weighted sum term can be equivalently expressed as

$$\omega_k t_k \log(1+\gamma_{c,k}) = \omega_k t_k \big[\log(1+\alpha_k) - \alpha_k + \frac{\omega_k t_k (1+\alpha_k)\gamma_{c,k}}{1+\gamma_{c,k}}\big]. \tag{5.18}$$

Applying the quadratic transform, we obtain

$$\frac{\omega_k t_k(1+\alpha_k)\gamma_{c,k}}{1+\gamma_{c,k}} = 2\sqrt{\omega_k t_k(1+\alpha_k)}\Re\{\beta_k^H \mathbf{a}_k\} - \beta_k^H \mathbf{B}_k \beta_k, \tag{5.19}$$

where $\beta_k$ is an auxiliary variable vector, and

$$\mathbf{a}_k = \mathbf{T}_k \mathbf{v}_k, \tag{5.20}$$

$$\mathbf{B}_k = \mathbf{T}_k \mathbf{v}_k \mathbf{v}_k^H \mathbf{T}_k^H + \sigma_{c,k}^2 \mathbf{I}_c + \mathbf{G}_k \mathbf{x}\mathbf{x}^H \mathbf{G}_k^H. \tag{5.21}$$

Thus, the problem (P1) is equivalently written as

$$\text{(P2)} \quad \max_{\mathbf{x},\mathbf{v}_k,\mathbf{w}_k,t_k,\alpha_k,\beta_k} f(\mathbf{x},\mathbf{v}_k,t_k,\alpha_k,\beta_k), \tag{5.22}$$

subject to C1-C5, and

$$\text{C6: } \alpha_k \geq 0, \quad k \in \mathscr{K}, \tag{5.23}$$

where

$$\begin{aligned} f(\mathbf{x},\mathbf{v}_k,t_k,\alpha_k,\beta_k) = &\sum_{k\in\mathscr{K}} \omega_k t_k \big[\log(1+\alpha_k) - \alpha_k\big] \\ &+ \sum_{k\in\mathscr{K}} 2\sqrt{\omega_k t_k(1+\alpha_k)}\Re\{\beta_k^H \mathbf{a}_k\} - \sum_{k\in\mathscr{K}} \beta_k^H \mathbf{B}_k \beta_k. \end{aligned} \tag{5.24}$$

### 5.3.2 AO Framework

Since the variables are coupled, we adopt an AO framework with the following update steps:

- **Step 1 (Update $\alpha_k, \beta_k$):** Given $\mathbf{x}, \mathbf{v}_k, \mathbf{w}_k, t_k$, the optimal $\alpha_k, \beta_k$ admit closed-form solutions:

$$\alpha_k^* = \gamma_{c,k}, \tag{5.25}$$

$$\beta_k^* = \mathbf{B}_k^{-1} \mathbf{a}_k. \tag{5.26}$$

- **Step 2 (Update x):** For fixed $\mathbf{v}_k, t_k, \mathbf{w}_k, \alpha_k, \beta_k$, optimizing $\mathbf{x}$ reduces to

$$\text{(P3)} \quad \max_{\mathbf{x}} \ f(\mathbf{x}), \quad \text{s.t. } \text{Tr}(\mathbf{x}\mathbf{x}^H) \leq P, \ \gamma_{r,k} \geq \Gamma_r. \tag{5.27}$$

(P3) is a convex SDP.

- **Step 3 (Update $\mathbf{v}_k$):** With other variables fixed, the subproblem for $\mathbf{v}_k$ is

$$\text{(P5)} \quad \max_{\mathbf{v}_k} \ f(\mathbf{v}_k), \quad \text{s.t. } [\mathbf{v}_k \mathbf{v}_k^H]_{l,l} \leq 1. \tag{5.28}$$

This is solved iteratively with SCA and rank-one recovery.

- **Step 4 (Update $t_k$):** For fixed $\mathbf{x}, \mathbf{v}_k, \mathbf{w}_k$, the allocation problem is

$$\text{(P6)} \quad \max_{t_k} \sum_{k \in \mathscr{K}} \omega_k t_k \log(1 + \gamma_{c,k}), \quad \text{s.t. } 0 \leq \sum_{k \in \mathscr{K}} t_k \leq T. \tag{5.29}$$

(P6) is a linear program.

- **Step 5 (Update $\mathbf{w}_k$):** The radar receive beamforming is obtained from

$$\text{(P7)} \quad \max_{\mathbf{w}_k} \ \gamma_{r,k}. \tag{5.30}$$

This can be reformulated as a generalized eigenvalue problem:

$$\text{(P8)} \quad \max_{\mathbf{w}_k} \frac{|\eta \mathbf{w}_k^H \Lambda(\theta) \mathbf{x}|^2}{\mathbf{w}_k^H \mathbf{C}_k \mathbf{w}_k}, \tag{5.31}$$

$$\text{(P9)} \quad \mathbf{w}_k^* = \arg\max_{\mathbf{w}_k} \frac{\mathbf{w}_k^H \mathbf{A}_k \mathbf{w}_k}{\mathbf{w}_k^H \mathbf{C}_k \mathbf{w}_k}, \tag{5.32}$$

where $\mathbf{A}_k = \eta^2 \Lambda(\theta) \mathbf{x}\mathbf{x}^H \Lambda^H(\theta)$ and $\mathbf{C}_k = \mathbf{H}_t \text{diag}\{\mathbf{H}_t \mathbf{x}\} \mathbf{v}_k \mathbf{v}_k^H \text{diag}\{\mathbf{H}_t \mathbf{x}\}^H \mathbf{H}_r^H + \sigma_r^2 \mathbf{I}_r$.

Table 5.1 Overall Algorithm for Solving Problem (P2)

| **Overall Algorithm for Solving Problem (P2)** |
|---|
| **Input:** Channel data, transmit power, and system parameters |
| **Initialize:** Set $j = 0$, tolerance $\varepsilon$, and initial values $\mathbf{x}^{(0)}$, $\mathbf{v}_k^{(0)}$, $\mathbf{w}_k^{(0)}$, $t_k^{(0)}$ |
| **Compute:** Initial objective value $f^{(0)}$ |
| **Repeat:** |
| Set $j = j+1$ |
| Update auxiliary variables $\alpha_k^{(j)}$ and $\beta_k^{(j)}$, $\forall k \in \mathscr{K}$ |
| **Solve Subproblem 1:** Solve (P3) without constraint C10 to obtain $\mathbf{X}^{(j)}$ |
| Recover $\mathbf{x}^{(j)}$ from $\mathbf{X}^{(j)}$ via SVD |
| **For each user** $k \in \mathscr{K}$**:** |
| Initialize $i = 0$, penalty parameter $\rho_k$, upper bound $\rho_{\max}$, scaling factor $c$, and objective value $g^{(0)}$ |
| **Repeat:** |
| Set $i = i+1$ |
| Solve (P5) to update $\mathbf{V}_k^{(i)}$ and $\eta_k^{(i)}$ |
| Update $\rho_k^{(i)} = \min\{c\,\rho_k^{(i-1)}, \rho_{\max}\}$ |
| **Until:** $\frac{\lvert g^{(i)} - g^{(i-1)}\rvert}{\lvert g^{(i)}\rvert} < \varepsilon$ |
| **End For** |
| **For each user** $k \in \mathscr{K}$**:** |
| Solve (P6) to update $t_k^{(j)}$ |
| Solve (P9) to update $\mathbf{w}_k^{(j)}$ |
| **End For** |
| Update objective value $f^{(j)}$ |
| **Until:** $\frac{\lvert f^{(j)} - f^{(j-1)}\rvert}{\lvert f^{(j)}\rvert} < \varepsilon$ |
| **Return:** Final solution $(\mathbf{x}^{(j)}, \mathbf{v}_k^{(j)}, \mathbf{w}_k^{(j)}, t_k^{(j)})$ |

### 5.3.3 Overall Algorithm

The overall iterative procedure for solving problem (P2) is summarized in Table 5.1. The proposed algorithm adopts an AO framework, where the original non-convex problem is decomposed into several tractable subproblems and solved iteratively.

Specifically, for given auxiliary variables, the transmit signal $\mathbf{x}$ is updated by solving problem (P3) using SDR followed by rank-one recovery. Then, for each user, an inner loop is employed to optimize the IRS-related variables by solving problem (P5) iteratively until

convergence. After that, the time allocation and receive beamforming variables are updated by solving problems (P6) and (P9), respectively.

The transmit signal $\mathbf{x}$ is optimized via a SDR approach. Specifically, by introducing the lifted variable $\mathbf{X} = \mathbf{x}\mathbf{x}^H$, the original non-convex problem is reformulated into a convex semidefinite program (P3) by relaxing the rank-one constraint. After solving (P3), if the obtained solution $\mathbf{X}$ is rank-one, the transmit beamforming vector $\mathbf{x}$ can be directly recovered via eigenvalue decomposition. Otherwise, Gaussian randomization is employed to obtain a feasible approximate solution.

The algorithm repeats the above steps until the objective value converges. Due to the monotonic improvement of the objective function in each iteration, the proposed algorithm is guaranteed to converge to a locally optimal solution.

## 5.4 Simulation Environment and Performance Evaluation

This section presents numerical results to validate the effectiveness of the proposed IRS-backscatter RCC framework. Unless otherwise specified, the simulation parameters follow Table 5.2. Each curve is averaged over 100 independent channel realizations. The analysis focuses on convergence, radar SINR, and the impact of system dimensions.

### 5.4.1 Simulation Setup

We consider an IRS-assisted downlink multi-user communication system coexisting with radar sensing, as described in Sections 5.2-5.3. The colocated MIMO radar is equipped with $M_t$ transmit and $M_r$ receive antennas, and the IRS has $L$ reflecting elements. The system serves $K$ users, each with $N$ antennas. The radar transmit power is $P$, and the noise variances at the radar and users are $\sigma_r^2$ and $\sigma_c^2$, respectively. Unless otherwise stated, the radar SINR threshold is $\Gamma_r$. Channel realizations follow a Rician fading model with factor $\varepsilon$, and the antenna spacing is normalized by the wavelength. Simulation parameters such as the block length $T$ and user weights $\omega_k$ follow the article.

Table 5.2 Simulation Parameters

| **Parameter** | **Value** |
|---|---|
| Channel model | Rician fading, factor $\kappa = 3$ |
| Path loss model | $PL = PL_0 - 25\log_{10}(d/d_0)$ |
| Reference path loss | $PL_0 = -30$ dB at $d_0 = 1$ m |
| Number of UEs | $K = 2$ |
| UE antennas | $N = 2$ |
| Radar transmit power | $P = -6$ dBW |
| Radar antennas | $M_t = M_r = 4$ |
| Target distance | $d_{rt} = 50$ m |
| Radar-IRS distance | $d_{ri} = 50$ m |
| IRS elements | $L = 40$ |
| User weight | $\omega_k = 1$ |
| Radar SINR threshold | $\Gamma_r = 1 \times 10^{-6}$ |
| Block length | $T = 1$ s |
| Noise variances | $\sigma_c^2 = \sigma_{r,k}^2 = 3 \times 10^{-6}$ W |
| Radar-UE distance range | $[d_{ru} - 10,\ d_{ru} + 10]$, $d_{ru} = 60$ m |
| IRS-UE distance range | $[d_{iu} - 10,\ d_{iu} + 10]$, $d_{iu} = 50$ m |

### 5.4.2 Baseline Schemes

The following schemes are considered for benchmarking:

**Proposed:** This scheme corresponds to the AO-based joint optimization method developed for problem (P1), as detailed in Section 5.3.

**MRT:** In this simplified design, the radar transmit vector and the receive beamforming are chosen according to the maximum ratio transmission (MRT) principle. Specifically, the normalized receive beamforming is fixed as

$$\mathbf{w}_k = \frac{1}{\sqrt{M_t}}, \tag{5.33}$$

while the dual-function radar waveform is aligned to the steering direction as

$$\mathbf{x} = \frac{\sqrt{P}\mathbf{w}^H \Lambda(\theta)}{|\mathbf{w}^H \Lambda(\theta)|}. \tag{5.34}$$

**Discrete:** This version adopts the same optimization procedure as the proposed scheme but constrains the phase shift of each IRS element to take values from a finite set of discrete

levels (phase quantization). The cases with 4 and 8 quantization levels are examined to demonstrate the impact of phase resolution.

**ZF:** In this approach, the IRS passive beamforming vector $v_k$ is designed within the null space of $\mathbf{H}_{\mathrm{r}}\mathrm{diag}\{\mathbf{H}_{\mathrm{t}}\mathbf{x}\}$, thereby eliminating interference to the radar receiver through a zero-forcing strategy.

## 5.5 Computational Complexity Analysis

The computational complexity of the proposed AO algorithm is dominated by the following subproblems:

Solving (P3) involves semidefinite programming with complexity on the order of $\mathscr{O}(M_t^3 + L^3)$, depending on the radar transmit dimension and IRS size.

Solving (P5) requires iterative convex approximation and rank-one recovery, whose complexity scales as $\mathscr{O}(L^3)$ due to the matrix operations involved in the IRS beamforming optimization.

Solving (P6) is a linear programming problem in $\{t_k\}$, whose complexity grows linearly with the number of users $K$.

Solving (P7)-(P9) reduces to a generalized eigenvalue decomposition of size $M_r$, leading to $\mathscr{O}(M_r^3)$.

Overall, the per-iteration complexity is $\mathscr{O}(M_t^3 + L^3 + M_r^3)$, and the AO algorithm converges in a small number of iterations (typically fewer than ten in simulations). This ensures practical feasibility for medium-scale IRS-assisted RCC systems.

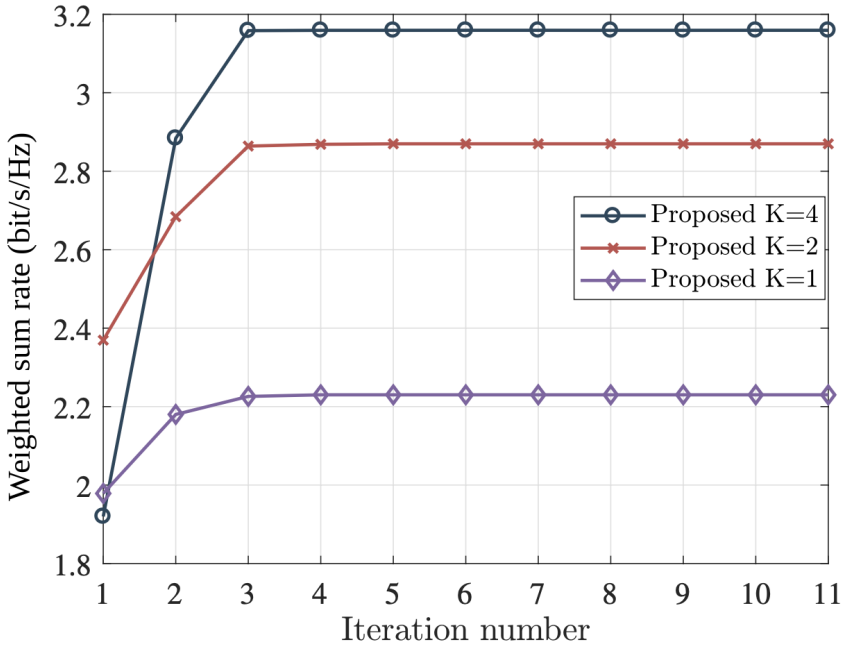


Fig. 5.2 Convergence behavior of the proposed AO algorithm in a representative observation.

## 5.6 Simulation Results and Performance Evaluation

### 5.6.1 Convergence of the AO Algorithm

Fig. 5.2 illustrates the WSR as a function of AO iterations in a representative observation. The results show that the AO algorithm converges monotonically within approximately 10 iterations, regardless of initialization, confirming robustness and efficiency.

### 5.6.2 Impact of Radar Transmit Power

Fig. 5.3 illustrates that higher $P$ consistently boosts the achievable WSR. The Proposed scheme attains the highest performance across all transmit powers, outperforming the other schemes. Discrete8 closely approaches Proposed and is superior to Discrete4, indicating the benefit of higher phase resolution. MRT yields moderate gains but remains below the IRS-optimized designs, while ZF performs the worst with only marginal improvement as P rises. Overall, the Proposed scheme exhibits the most favorable growth with P, confirming its advantage over the baselines.

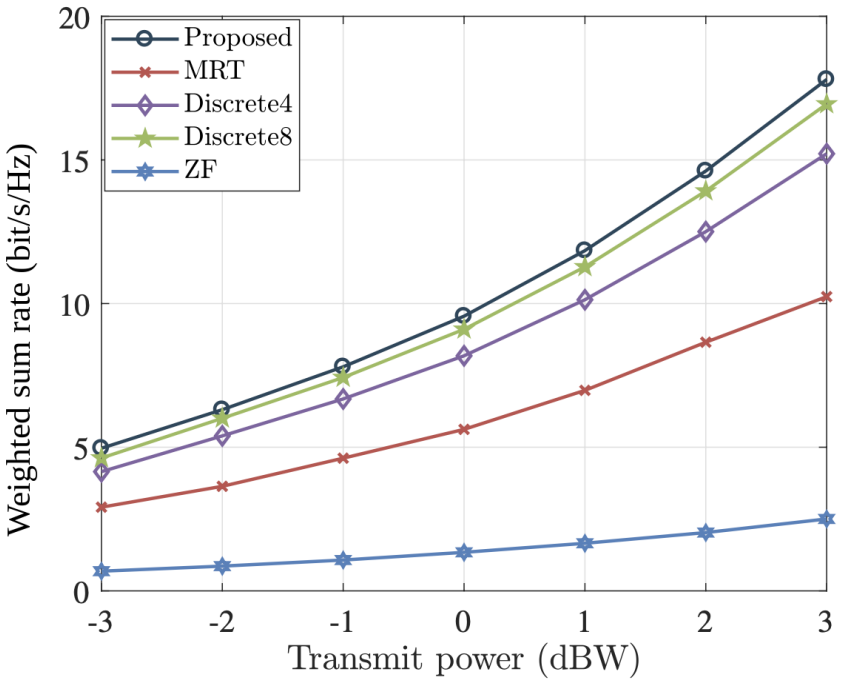


Fig. 5.3 Weighted sum rate versus radar transmit power under different schemes.

### 5.6.3 Impact of IRS Size

From Fig. 5.4, it is observed that the achievable WSR increase with the number of IRS elements. The Proposed scheme consistently provides the best performance across all $L$, confirming the effectiveness of the optimized IRS-assisted backscatter design. The Discrete8 scheme closely follows Proposed, while Discrete4 performs slightly worse, showing that higher phase resolution improves system throughput. In contrast, MRT yields limited improvement, and ZF exhibits the lowest performance with marginal gains as $L$ increases. These results demonstrate that enlarging the IRS size significantly enhances communication rates, especially when combined with optimized phase design.

### 5.6.4 Impact of Radar SINR Constraint

From Fig. 5.5, it is observed that the WSR decrease as the allowable minimum received SINR of the radar increases. This is because stricter radar SINR requirements reduce the degrees of freedom available for communication optimization. For all cases, larger transmit

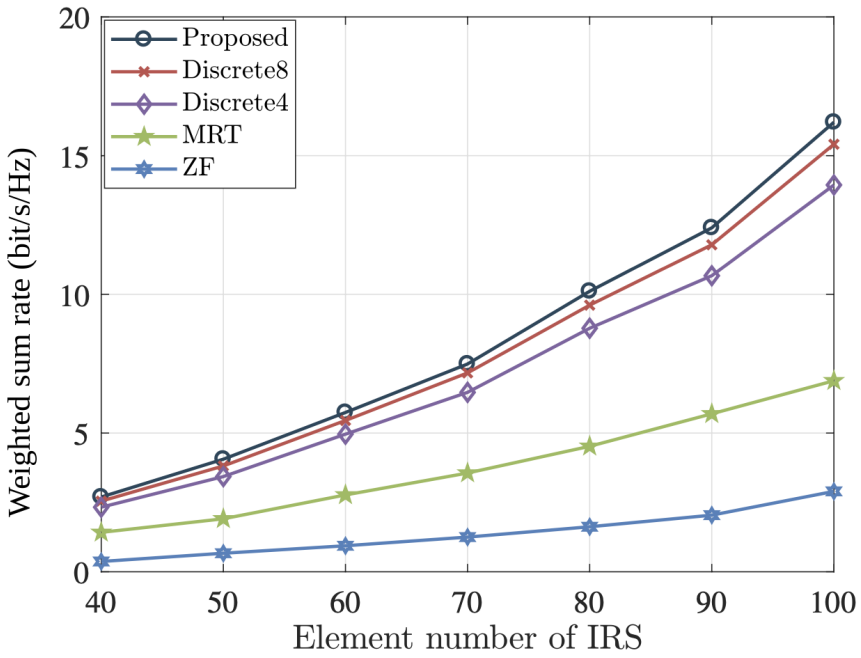


Fig. 5.4 Weighted sum rate and radar SINR versus IRS size $L$.

power $P$ and more IRS elements $L$ lead to higher achievable WSR. For instance, the case with $P = 0$ dBW and $L = 60$ achieves the best performance across the entire SINR range, while the case with $P = -6$ dBW and $L = 40$ shows the lowest throughput. These results confirm the fundamental trade-off between guaranteeing radar sensing performance and maintaining high communication rates.

### 5.6.5 Comparisons with Baseline Schemes

Across all settings, the proposed IRS-backscatter scheme significantly outperforms random IRS and no-IRS transmission. Ignoring radar constraints leads to higher throughput but fails to guarantee radar sensing performance. In contrast, the proposed algorithm achieves a favorable trade-off between communication throughput and radar SINR guarantees.

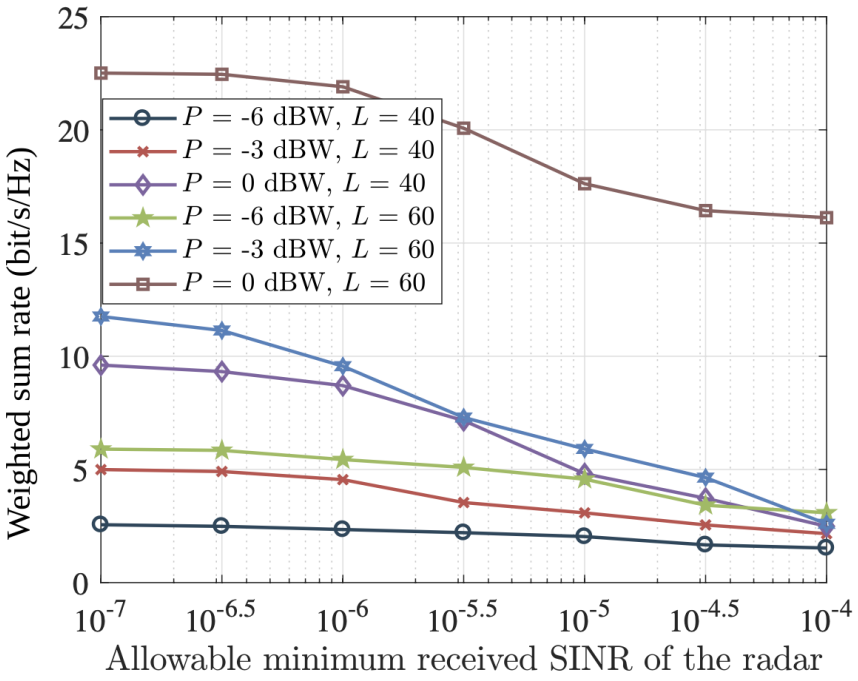


Fig. 5.5 Trade-off between communication throughput and radar SINR threshold $\Gamma_r$.

## 5.7 Chapter Summary and Key Insights

This chapter developed an IRS-backscatter enabled downlink multi-user communication framework coexisting with radar sensing. The proposed system builds upon the earlier chapters of this thesis by extending IRS from secrecy enhancement (Chapter 3) and STAR-RIS based secure communications (Chapter 4) towards dual-functional RCC.

### 5.7.1 Key Insights

The analysis and results of this chapter yield several key insights. IRS proves to be a powerful enabler of RCC, offering spectrum- and energy-efficient dual functionality. A fundamental trade-off exists between radar SINR and communication throughput, making explicit optimization essential to achieve balanced performance. While the AO algorithm provides a rigorous performance benchmark, it is computationally demanding, and scalable ML approaches, such as those explored in Chapter 4, represent a promising alternative for

large-scale systems. Overall, IRS-backscatter emerges as a viable pathway toward ISAC in 6G.

### 5.7.2 Concluding Remarks

In summary, this chapter has demonstrated the feasibility of IRS-backscatter systems for achieving efficient RCC. Together with the findings of Chapters 3 and 4, the results position IRS as a key enabling technology for integrated wireless systems in future 6G networks.

# Chapter 6

# Conclusions and Future Work

A further part of the research activities addressed in this thesis has focused on the promise of IRS technologies as a means for revolutionizing the field of PLS for wireless communications. Given three different but aligned system settings: the traditional reflective IRS, the backscatter-type hybrid systems, and the STAR-RIS, we have showed the great leaps equipped each wireless secure system design, analysis, and optimization. In the final chapter, we summarize the main results of our investigations, perform an extensive performance comparison between the proposed systems, and then outline a final vision of what is expected to be the evolution of intelligent, wireless environments.

The evolution process in this thesis showed that the traditional strategy of treating security as an overlay on top of the existed communication systems is no longer sufficient to satisfy the stringent demands of the next wireless generation. On the other hand, our work suggests that security needs to be inherently included in the physical layer designs, where one may begin to design the environment such that security will result from basic interaction of the network's elements, using the special properties of IRS to achieve this objective. This new perspective of reacting security responses has become pro-active security design, is a new age on the history of wireless communications.

This research is important not only for the specific technical contributions but, more importantly, for significant implications in the design and use secure wireless networks. The presented capability to deliver large security gains while preserving or even increasing energy

efficiency contrasts the classic trade-offs of security and performance. The scalability and flexibility of proposed solutions make them promising candidates for handling the varying security needs of new applications such as IoT networks to mission-critical communications.

With the advent of 6G, the fusion of PLS with key enablers such as artificial intelligence, blockchain, and quantum communications would open a new spectrum of possibilities to develop secure, intelligent wireless networks. The basis of this thesis discussed here are well suited to explore these exciting opportunities and will help in addressing the core challenges that will drive the future of wireless communications.

## 6.1 Conclusions

This thesis investigates the role of IRS in enhancing PLS for wireless communication systems. By considering progressively advanced architectures, including conventional reflective IRS, backscatter-based hybrid systems, and STAR-RIS, the work demonstrates how intelligent surfaces can be leveraged to actively shape the wireless environment for improved security and system performance.

The results show that conventional reflective IRS systems provide significant signal enhancement and energy efficiency benefits through passive beamforming, particularly in non-line-of-sight scenarios. However, their security capability is inherently limited, as the same reflection patterns that enhance legitimate communication may also benefit potential eavesdroppers.

To overcome this limitation, a backscatter-based hybrid IRS framework was developed, where artificial noise is generated via signal remodulation at the surface. This approach enables simultaneous communication enhancement and interference generation without requiring additional active transmission. The proposed design achieves improved secrecy performance and reduced transmit power, demonstrating the potential of passive security enhancement mechanisms.

Building on this, the STAR-RIS architecture introduces simultaneous transmission and reflection capabilities, providing additional degrees of freedom for multi-user systems. This

dual-functional design enables independent control of signal enhancement and interference generation, leading to improved secrecy performance in complex multi-user scenarios. Furthermore, the integration of GNN-based optimization provides an efficient solution to the high-dimensional joint design problem, offering scalability and adaptability to varying network configurations.

Finally, the extension to RCC demonstrates the applicability of IRS in ISAC systems. By incorporating radar SINR constraints into the optimization framework, the proposed approach ensures reliable sensing performance while maximizing communication throughput. The results highlight that IRS-assisted backscatter can effectively support spectrum sharing and enable dual-functional system operation.

Overall, this thesis presents a unified framework for IRS-enabled secure wireless systems, illustrating a clear progression from signal enhancement to joint communication, security, and sensing optimization. The findings indicate that intelligent surfaces can serve as a key enabler for future wireless networks, particularly in scenarios requiring secure, energy-efficient, and adaptive system design.

## 6.2 Limitations and Future Work

Although this thesis has investigated IRS/STAR-RIS-assisted secure communication systems from the perspectives of system design, optimization, and simulation-based performance evaluation, several limitations remain. These limitations are not weaknesses of the proposed framework itself, but rather indicate important directions for making IRS/STAR-RIS-assisted PLS systems more realistic, robust, and deployable in future wireless networks.

### 6.2.1 Robust Channel Estimation and Imperfect CSI Modeling

A major limitation of this thesis is that the proposed optimization frameworks rely on the availability of CSI. In Chapters 3 and 4, the beamforming vectors and IRS/STAR-RIS coefficients are designed based on known or estimated channel information. Although Chapter 4 introduces an imperfect CSI model to evaluate robustness, no dedicated channel

estimation method is developed. This is a critical limitation, since channel acquisition in IRS-assisted systems is significantly more challenging than in conventional wireless systems due to the passive nature of reflecting elements [160, 161].

Unlike traditional active antenna systems, IRS elements typically lack radio-frequency chains and cannot directly transmit or receive pilot signals. As a result, the cascaded BS–IRS–user channel must be estimated indirectly, which leads to increased pilot overhead and estimation complexity [162]. This challenge becomes even more severe in STAR-RIS systems, where both reflection and transmission links must be estimated simultaneously, further increasing system dimensionality [163].

Future work should focus on developing channel estimation schemes tailored to IRS- and STAR-RIS-assisted systems. Promising approaches include compressed sensing and learning-based estimation methods, which can reduce pilot overhead and improve estimation accuracy in high-dimensional environments [164]. In addition, robust optimization under statistical or partial CSI should be considered, especially for eavesdropper channels, which are typically unknown in practice.

### 6.2.2 Deployment Optimization and Geometry-Aware IRS Placement

Another limitation of this thesis is the assumption of fixed IRS/STAR-RIS deployment. In Chapters 3 and 4, the positions of the BS and IRS/STAR-RIS are predefined, and system performance is evaluated under this fixed geometry. While this assumption simplifies analysis, it does not capture the critical impact of deployment on system performance.

The placement of IRS/STAR-RIS strongly affects propagation paths, signal strength, and interference patterns. In particular, improper placement may result in weak reflected links or increased signal leakage toward potential eavesdroppers. Existing studies have shown that deployment plays a crucial role in determining the achievable gains of IRS-assisted systems [160, 165].

Future work should consider geometry-aware deployment optimization, including IRS location, orientation, and coverage region. For STAR-RIS systems, this problem becomes more complex due to full-space coverage capability. In addition, region-based deployment

strategies should be developed to enhance legitimate communication while suppressing signal leakage toward potential eavesdropping areas.

### 6.2.3 Generalization of GNN-Based Optimization Across Different Scenarios

The GNN-based optimization framework proposed in Chapter 4 demonstrates strong performance under varying system parameters, including user numbers, transmit power, and STAR-RIS size. However, the simulations are conducted under a fixed indoor deployment scenario, and do not explicitly consider different geometrical layouts or STAR-RIS placements.

Although GNNs are capable of capturing structural relationships through graph representations, their generalization ability across significantly different environments is not explicitly verified in this thesis. This is an important limitation, as real-world deployments may involve diverse indoor layouts, user distributions, and propagation conditions.

Future work should investigate training strategies that improve generalization, such as multi-scenario training, transfer learning, and domain adaptation. In addition, online learning mechanisms could be incorporated to enable real-time adaptation to dynamic environments. These directions are aligned with recent developments in learning-based wireless optimization [166].

### 6.2.4 Advanced Eavesdropper Models and Adaptive Security Strategies

This thesis considers eavesdroppers with either known or randomly distributed locations. While this is more realistic than assuming perfect knowledge, the model remains relatively simple and does not capture adaptive or intelligent adversaries.

In practical systems, eavesdroppers may employ advanced strategies, such as mobility, multi-antenna reception, or interference cancellation. These capabilities may significantly reduce the effectiveness of AN, especially when it is designed based on static assumptions. Therefore, the current security analysis may not fully reflect worst-case scenarios.

Future work should incorporate more sophisticated adversarial models, including mobile and cooperative eavesdroppers. Game-theoretic formulations can be used to model the interaction between the transmitter and eavesdropper, providing deeper insights into security performance. In addition, adaptive and learning-based security strategies can be explored, where AN patterns are dynamically adjusted based on environmental observations [167].

### 6.2.5 Hardware Impairments and Practical STAR-RIS Implementation

The system models in this thesis assume ideal IRS/STAR-RIS operation, with continuous phase shifts and perfect control. However, practical implementations are subject to hardware limitations, including discrete phase resolution, insertion loss, and imperfect reflection/transmission coefficients.

In particular, STAR-RIS elements must simultaneously control reflection and transmission, which introduces additional hardware constraints compared to conventional IRS. Ignoring these factors may lead to performance overestimation.

Future work should incorporate practical hardware models into the optimization framework. This includes discrete phase shifts, amplitude constraints, and efficiency losses. In addition, learning-based methods such as GNNs could be adapted to directly output hardware-feasible configurations, reducing the gap between theoretical design and practical implementation.

### 6.2.6 Integration of Sensing, Communication, and Security

Chapter 5 extends the framework to RCC, where a dual-functional radar waveform is used for both sensing and communication. While this demonstrates the feasibility of integrated systems, the current work primarily focuses on communication performance under sensing constraints.

In future wireless systems, sensing, communication, and security are expected to be deeply integrated. For example, sensing information can be used to detect potential eavesdrop-

pers or identify high-risk regions, which can then be incorporated into secure beamforming design.

Future work should develop unified frameworks that jointly optimize sensing accuracy, communication performance, and security. Multi-objective optimization techniques could be used to balance these competing requirements. In addition, IRS/STAR-RIS can be leveraged to simultaneously shape sensing and communication channels, enabling more intelligent and secure wireless environments [168, 169].

## 6.3 Final Reflections and Concluding Remarks

This thesis has established a systematic research framework for exploring the transformative potential of IRS technologies in secure wireless communications. From the initial investigation of backscatter-based hybrid systems to the development of advanced dual-functional STAR-RIS architectures, the results demonstrate that intelligent manipulation of the wireless propagation environment represents not merely an incremental evolution of wireless technology, but a fundamental shift toward secure, energy-efficient, and adaptive communication systems.

The evolution of wireless system design from conventional architectures, where security is treated as an additional feature layered on top of existing communication frameworks, toward integrated architectures in which security is embedded into the underlying signal propagation process represents an important step forward. The demonstrated capability of intelligent wireless environments to simultaneously improve security, energy efficiency, and communication performance challenges the traditional assumption of unavoidable trade-offs in wireless system design. These findings further suggest that future wireless systems should not be designed through isolated optimization of individual components, but rather through joint optimization that fully exploits the interactions among different system elements.

The incorporation of deep learning techniques, particularly the GNN-based optimization framework for STAR-RIS systems, represents an important step toward self-learning and adaptive wireless networks capable of improving performance over time. The possibility of

transferring computationally intensive optimization tasks from online processing to offline learning-based approaches provides a practical pathway for implementing intelligent wireless systems in real-world deployments. This transition from conventional algorithm-driven optimization to data-driven system design is aligned with the broader evolution of AI-enabled wireless communications.

The vision outlined in this thesis extends beyond the individual technical contributions and highlights a broader evolution toward secure and intelligent wireless environments. The integration of reflection, transmission, interference generation, and sensing within unified surface architectures suggests a future in which wireless propagation environments can be dynamically configured according to user and network requirements while simultaneously supporting secure and reliable communications.

The emphasis on energy efficiency, implementation simplicity, scalability, and multi-objective optimization throughout this work is motivated by the practical constraints associated with deploying next-generation wireless systems. The demonstrated ability to satisfy stringent security and performance requirements under realistic system assumptions provides strong evidence that IRS-enabled technologies can evolve from theoretical concepts into deployable communication solutions.

The future research directions identified in this thesis represent only a subset of the broader opportunities enabled by the integration of IRS with emerging technologies such as advanced machine learning, quantum communications, and future wireless architectures. The potential synergy among these technologies suggests that IRS will play a significant role not only in improving wireless performance, but also in shaping the future evolution of intelligent communication systems.

The work presented in this thesis constitutes foundational research for addressing security and performance challenges in next-generation wireless networks, including future 6G systems. These networks are expected to seamlessly integrate communication, sensing, intelligence, and connectivity across physical and digital environments. The demonstrated capability of IRS technologies to create secure and controllable electromagnetic environments

provides a promising foundation for the development of trustworthy wireless infrastructures for future connected societies.

This research also demonstrates that the future of wireless security should not rely solely on reactive approaches that address threats after they emerge, but should increasingly focus on proactive mechanisms capable of shaping the wireless environment itself to mitigate security vulnerabilities. The IRS technologies investigated in this thesis represent important building blocks toward such inherently secure wireless systems, while maintaining practical implementation complexity and communication efficiency.

In summary, this thesis has demonstrated the potential of IRS technologies as key enablers for next-generation secure wireless communications. The proposed systems and algorithms provide both immediate practical value and broader strategic insights for future research and development. As wireless systems continue to evolve toward increasingly intelligent and interconnected architectures, the principles and methodologies developed in this work are expected to contribute to the realization of secure, efficient, and adaptive wireless networks for future connected societies.

# References


[1] Y. Zheng, S. Bi, Y.-J. A. Zhang, Z. Quan, and H. Wang, "Intelligent reflecting surface enhanced user cooperation in wireless powered communication networks," *IEEE Wirel. Commun. Lett.*, vol. 9, no. 6, pp. 901–905, 2020.

[2] Y. Liu, X. Liu, X. Mu, T. Hou, J. Xu, M. Di Renzo, and N. Al-Dhahir, "Reconfigurable intelligent surfaces: Principles and opportunities," *IEEE Commun. Surv. Tutor.*, vol. 23, no. 3, pp. 1546–1577, 2021.

[3] S. Gong, X. Lu, D. T. Hoang, D. Niyato, L. Shu, D. I. Kim, and Y.-C. Liang, "Toward smart wireless communications via intelligent reflecting surfaces: A contemporary survey," *IEEE Commun. Surv. Tutor.*, vol. 22, no. 4, pp. 2283–2314, 2020.

[4] E. Başar, M. Di Renzo, J. de Rosny, M. Debbah, M.-S. Alouini, and R. Zhang, "Wireless communications through reconfigurable intelligent surfaces," *IEEE Access*, vol. 7, pp. 116 753–116 773, 2019.

[5] Q. Wu, S. Zhang, B. Zheng, C. You, and R. Zhang, "Intelligent reflecting surface-aided wireless communications: A tutorial," *IEEE Trans. Commun.*, vol. 69, no. 5, pp. 3313–3351, 2021.

[6] Q.-U.-A. Nadeem, A. Kammoun, A. Chaaban, M. Debbah, and M.-S. Alouini, "Intelligent reflecting surface assisted wireless communication: Modeling and channel estimation," *IEEE Access*, vol. 8, pp. 145 814–145 827, 2020.

[7] S. Asaad, Y. Wu, A. Bereyhi, R. R. Müller, R. F. Schaefer, and H. V. Poor, "Secure active and passive beamforming in irs-aided mimo systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 17, pp. 1300–1315, 2022.

[8] G. Chen, Q. Wu, R. Liu, J. Wu, and C. Fang, "Active irs aided multiple access for energy-constrained iot systems," *IEEE Trans. Wirel. Commun.*, vol. 22, no. 3, pp. 1677–1694, 2023.

[9] M. Di Renzo, M. Debbah, D.-T. Phan-Huy, A. Zappone, M.-S. Alouini, C. Yuen, V. Sciancalepore, G. C. Alexandropoulos, J. Hoydis, H. Gacanin *et al.*, "Smart radio environments empowered by reconfigurable ai meta-surfaces: An idea whose time has come," *EURASIP J. Wirel. Commun. Netw.*, vol. 2019, no. 1, pp. 1–20, 2019.

[10] Z. U. A. Tariq, E. Baccour, A. Erbad, and M. Hamdi, "A novel energy efficient irs-relay network for its with nakagami-m fading channels," *ICT Express*, vol. 9, no. 6, pp. 1042–1047, 2023.

[11] Ã. PepeoÄ§lu and L. Durak-Ata, "Comparative analysis of intelligent reflecting surfaces and af/df relaying for energy efficient wireless communication," *EURASIP Journal on Wireless Communications and Networking*, vol. 2024, no. 1, pp. 1–23, 2024.

[12] J. Kim, S. Hosseinalipour, T. Kim, D. J. Love, and C. G. Brinton, "Deep reinforcement learning-based adaptive irs control with limited feedback codebooks," *IEEE Trans. Wirel. Commun.*, vol. 21, no. 12, pp. 10 569–10 583, 2022.

[13] ——, "Learning-based adaptive irs control with limited feedback codebooks," *arXiv:2112.01874*, 2021.

[14] M. H. Alsharif, M. A. Albreem, A. A. Solyman, and S. Kim, "Machine learning for intelligent-reflecting-surface-based wireless communication towards 6g: A review," *Sensors*, vol. 22, no. 14, p. 5405, 2022.

[15] H. Xie, J. Xu, K. An, and D. W. K. Zhang, "Reflection coefficients optimization in irs-assisted communication: An evolutionary game approach," in *2021 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2021, pp. 1–6.

[16] Z. U. A. Tariq, E. Baccour, A. Erbad, and M. Hamdi, "Reinforcement learning for resilient aerial-irs assisted wireless communications networks in the presence of multiple jammers," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 15–37, 2024.

[17] M. A. Contreras-Cruz and J.-P. Ramírez-Paredes, "Channel-adaptive robust resource allocation for highly reliable irs-assisted v2x communications," *arXiv:2504.11871*, 2024.

[18] J. Yuan, Y.-C. Liang, J. Joung, G. Feng, and E. G. Larsson, "Intelligent reflecting surface-enhanced ofdm: Channel estimation and reflection optimization," *IEEE Wirel. Commun. Lett.*, vol. 9, no. 4, pp. 518–522, 2020.

[19] R. Kaur, B. Bansal, S. Majhi, S. Jain, C. Huang, and C. Yuen, "A survey on reconfigurable intelligent surface for physical layer security of next-generation wireless communications," *IEEE Open J. Veh. Technol.*, vol. 5, pp. 172–199, 2024.

[20] M. Di Renzo, J. Song *et al.*, "A review on intelligent reflecting surfaces: Challenges and opportunities towards secured communications," *Int. J. Commun. Syst.*, vol. 38, no. 3, p. e6024, 2025.

[21] X. Yu, D. Xu, and R. Schober, "Miso wireless communication systems via intelligent reflecting surfaces," *IEEE Transactions on Signal Process.*, vol. 68, pp. 2974–2987, 2020.

[22] Y. Liu, X. Mu, J. Xu, R. Schober, Y. Hao, H. V. Poor, and L. Hanzo, "Star-riss: Simultaneous transmitting and reflecting reconfigurable intelligent surfaces," *IEEE Commun. Lett.*, vol. 25, no. 9, pp. 3134–3138, 2021.

[23] J. Xu, Y. Liu, X. Mu, J. Zhou, and L. Song, "Simultaneously transmitting and reflecting (star) ris aided wireless communications," *IEEE Trans. Wirel. Commun.*, vol. 21, no. 5, pp. 3083–3098, 2022.

[24] Y. Liu, J. Xu, Z. Wang, X. Mu, J. Zhou, and L. Song, "Simultaneously transmitting and reflecting (star) riss for 6g: fundamentals, recent advances, and future directions," *Front. Inf. Technol. Electron. Eng.*, vol. 24, no. 12, pp. 1689–1707, 2023.

[25] M. Al-Humaidi, Z. Liu, L. Zou, Q. Wu, J. Xu, and Y. Liu, "Simultaneously transmitting and reflecting (star) ris enhanced covert transmission with noise uncertainty," *Signal Process.*, vol. 220, p. 109449, 2025.

[26] P. Zeng, Q. Wu, and D. Qiao, "Star-ris assisted uav communications with wireless energy harvesting," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 4, pp. 1320–1335, 2022.

[27] Z. Yang, M. Chen, W. Saad, W. Xu, M. Shikh-Bahaei, H. V. Poor, and L. Hanzo, "Simultaneously transmitting and reflecting reconfigurable intelligent surface (star-ris) assisted uav communications," *IEEE Trans. Wirel. Commun.*, vol. 21, no. 10, pp. 8800–8815, 2022.

[28] X. Mu, Y. Liu, L. Guo, J. Lin, and R. Schober, "Simultaneously transmitting and reflecting (star) ris aided downlink communications," *IEEE Trans. Wirel. Commun.*, vol. 21, no. 5, pp. 3114–3130, 2022.

[29] M. V. Katwe, J. Yaswanth, K. Singh, and A. Schmeink, "Towards green communication: Power-efficient beamforming for star-ris-aided swipt," *IEEE Trans. Green Commun. Netw.*, vol. 8, no. 2, pp. 789–803, 2024.

[30] B. Song and F. Wang, "Star-ris-aided secure communications for mec with delay/energy-constrained qos using multi-agent deep reinforcement learning," *Comput. Netw.*, vol. 238, p. 110114, 2024.

[31] R. Alhamad and H. Boujemaa, "Simultaneously transmitting and reflecting reconfigurable intelligent surfaces (star-ris) with hybrid solar, rf and wind energy harvesting," *Wirel. Pers. Commun.*, vol. 138, no. 3, pp. 1799–1813, 2024.

[32] W. Saad, H. Al-Hraishawi, M. Shokair *et al.*, "Beamforming design for star-ris assisted secure wireless communication system under hardware impairments," *EURASIP J. Wirel. Commun. Netw.*, vol. 2024, no. 1, pp. 1–25, 2024.

[33] W. Zhang, Y. Wu, A. Khisti *et al.*, "Weighted sum power maximization for star-ris-aided swipt systems with nonlinear energy harvesting," *Sci. China Inf. Sci.*, vol. 67, no. 8, p. 182301, 2024.

[34] X. Li, K. M. Rabie, B. Adebisi, H. Gacanin, and L. Wan, "Performance of star-ris-aided cooperative noma networks under nakagami-m fading," *Comput. Netw.*, vol. 240, p. 110168, 2024.

[35] S. Javed, O. Aziz, I. Ahmad *et al.*, "Robust beamforming design for star-ris aided rsma network with hardware impairments," *arXiv:2505.08642*, 2024.

[36] J. Kim, X. Liu, H. Chen *et al.*, "Star-ris-assisted key generation method in quasi-static environment," *EURASIP J. Wirel. Commun. Netw.*, vol. 2024, no. 1, pp. 1–28, 2024.

[37] Z. Liu, L. Zou, Q. Wu, J. Xu, and Y. Liu, "Star-ris-assisted multi-antenna covert communication: Analysis and optimization," *IEEE Trans. Wirel. Commun.*, vol. 22, no. 12, pp. 9450–9465, 2023.

[38] R. Alhamad and H. Boujemaa, "Simultaneously transmitting and reflecting reconfigurable intelligent surfaces (star-ris) with hybrid solar, rf and wind energy harvesting," *Wirel. Pers. Commun.*, vol. 138, no. 3, pp. 1799–1813, 2024.

[39] W. Zhang, Q. Li, Y. Wu *et al.*, "Design and prototyping of filtering active star-ris with adjustable power splitting," *arXiv:2501.11062*, 2025.

[40] Z. Yang, M. Chen, Y. Liu *et al.*, "Simultaneously transmitting and reflecting reconfigurable intelligent surfaces empowered cooperative rate splitting with user relaying," *Entropy*, vol. 26, no. 12, p. 1019, 2024.

[41] X. Li, F. Zhou, D. W. K. Ng *et al.*, "Joint design for simultaneously transmitting and reflecting (star) ris assisted noma systems," *IEEE Trans. Wirel. Commun.*, vol. 21, no. 9, pp. 7463–7479, 2022.

[42] G. Wang, F. Gao, R. Fan, and C. Tellambura, "Ambient backscatter communication systems: Detection and performance analysis," *IEEE Trans. Commun.*, vol. 64, no. 11, pp. 4836–4846, 2016.

[43] G. Yang, Y.-C. Liang, R. Zhang, and Y. Pei, "Modulation in the air: Backscatter communication over ambient OFDM carrier," *IEEE Trans. Commun.*, vol. 66, no. 3, pp. 1219–1233, 2018.

[44] A. Parks, A. Liu, S. Gollakota, and J. R. Smith, "Turbocharging ambient backscatter communication," in *Proceedings of the 2014 ACM Conference on SIGCOMM*, 2014, pp. 619–630.

[45] H. Guo, Q. Zhang, S. Xiao, and Y.-C. Liang, "Exploiting multiple antennas for cognitive ambient backscatter communication," *IEEE Internet Things Journal*, vol. 6, no. 1, pp. 765–775, 2019.

[46] M. Zhao, Q. Wu, M. Zhao, and R. Zhang, "Exploiting amplitude control in intelligent reflecting surface aided wireless communication with imperfect CSI," *IEEE Trans. Commun.*, vol. 69, no. 6, pp. 3653–3667, 2021.

[47] Q. Zhang, H. Guo, Y.-C. Liang, and X. Yuan, "Constellation learning-based signal detection for ambient backscatter communication systems," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 11, pp. 2427–2439, 2018.

[48] R. Kishore, S. Gurugopinath, P. C. Sofotasios, S. Muhaidat, and N. Al-Dhahir, "Opportunistic ambient backscatter communication in RF-powered cognitive radio networks," *IEEE Trans. Cogn. Commun. Netw.*, vol. 5, no. 2, pp. 413–426, 2019.

[49] S. Basharat, S. A. Hassan, H. Pervaiz, A. Mahmood, Z. Ding, and M. Gidlund, "Reconfigurable intelligent surface-assisted backscatter communication: A new frontier for enabling 6g iot networks," *Ad Hoc Netw.*, vol. 142, p. 103116, 2023.

[50] X. Jia and X. Zhou, "Irs-assisted ambient backscatter communications utilizing deep reinforcement learning," *IEEE Wirel. Commun. Lett.*, vol. 10, no. 10, pp. 2102–2106, 2021.

[51] M. T. Majeed, H. K. Qureshi, S. A. Hassan, and H. Jung, "Design of intelligent reflecting surface-boosted ambient backscatter systems," *IEEE Access*, vol. 10, pp. 77 866–77 878, 2022.

[52] F. H. Khoso, A. Lakhan, B. Das, Z. A. Nizamani *et al.*, "Intelligent reconfigurable surface enhanced ambient backscatter communication enabled wireless body area network," *ICT Express*, vol. 9, no. 4, pp. 675–681, 2023.

[53] S. Abeywickrama, R. Zhang, Q. Wu, and C. Yuen, "Channel estimation for intelligent reflecting surface assisted backscatter communication," *IEEE Wirel. Commun. Lett.*, vol. 10, no. 9, pp. 1932–1936, 2021.

[54] S. Xu, J. Liu, Y. Cao, J. Li, and S. Chatzinotas, "An irs backscatter enabled integrated sensing, communication and computation system," *IEEE Trans. Commun.*, vol. 70, no. 11, pp. 7537–7552, 2022.

[55] H. Yang, Z. Xiong, J. Zhao, D. Niyato, L. Xiao, and Q. Wu, "Intelligent reflecting surface-aided backscatter communications," *IEEE Wirel. Commun. Lett.*, vol. 9, no. 11, pp. 1884–1888, 2020.

[56] M. Jian, G. C. Alexandropoulos, E. Basar, C. Huang, R. Liu, and Y. Liu, "Analytical performance analysis of intelligent reflecting surface aided ambient backscatter

communication network," *IEEE Wirel. Commun. Lett.*, vol. 10, no. 12, pp. 2734–2738, 2021.

[57] D. Munir, S. T. Shah, and I. Koo, "Cooperative relay strategy for backscatter communication networks with rf energy harvesting," *Digit. Commun. Netw.*, vol. 5, no. 3, pp. 173–184, 2019.

[58] X. Zhou, R. Zhang, and C.-K. Ho, "Optimal resource allocation in backscatter assisted wpcn with practical energy harvesting model," *IEEE Commun. Lett.*, vol. 23, no. 12, pp. 2355–2359, 2019.

[59] X. He, K. Wang, W. Huang, N. Liu, and G. K. Karagiannidis, "Energy minimization for irs-assisted swipt-mec system," *Sensors*, vol. 24, no. 17, p. 5498, 2024.

[60] J. Lee, L. V. Tran, M. Juntti, M. Rasti, and T. Q. Duong, "Irs-enabled ultra-low-power wireless sensor networks: Scheduling and transmission schemes," *Sensors*, vol. 22, no. 23, p. 9135, 2022.

[61] A. M. T. Khel, K. Altuwairgi, and K. Hamdi, "Performance analysis of irs-assisted backscatter communications under hardware imperfections," in *2022 IEEE 95th Vehicular Technology Conference (VTC2022-Spring)*. IEEE, 2022, pp. 1–5.

[62] A. M. Tota Khel and K. Hamdi, "Irs backscatter enhancing against jamming and eavesdropping attacks," *IEEE Trans. Commun.*, vol. 71, no. 8, pp. 4710–4725, 2023.

[63] Q. Cai, J. Ma, B. Yao, X. Wu, and X. Xue, "A trade-off strategy and correlation analysis for secrecy rate and power consumption in irs-assisted cognitive radio networks," *Digit. Commun. Netw.*, vol. 10, no. 4, pp. 852–863, 2024.

[64] D. Korpi, O. Tirkkonen, K. Ruttik, and T. Riihonen, "Rate-energy tradeoffs of wireless powered backscatter communication with power splitting and time switching," *IEEE Trans. Commun.*, vol. 69, no. 3, pp. 1744–1759, 2021.

[65] A. Ranjha, G. Kaddoum *et al.*, "Trajectory optimization of uav-irs assisted 6g thz network using deep reinforcement learning approach," *Sci. Rep.*, vol. 14, no. 1, p. 18501, 2024.

[66] J. Wang and C. Liu, "Joint passive beamforming and deployment design for active intelligent reflecting surface-assisted energy harvesting-cognitive radio sensor networks," *Sci. Rep.*, vol. 14, no. 1, p. 21944, 2024.

[67] C. Zhai, J. Zhao, G. Zheng, Y. Li, and B. Vucetic, "Optimal resource allocation in backscatter assisted wireless powered communication networks with practical energy harvesting model," *IEEE Trans. Commun.*, vol. 67, no. 12, pp. 8837–8851, 2019.

[68] J. Yang and S. Ulukus, "Energy-harvesting wireless sensor networks: A review," *ACM Trans. Sens. Netw.*, vol. 14, no. 2, pp. 1–35, 2018.

[69] J. Wang and C. Liu, "Joint passive beamforming and deployment design for active intelligent reflecting surface-assisted energy harvesting-cognitive radio sensor networks," *Sci. Rep.*, vol. 14, no. 1, p. 21944, 2024.

[70] L. Jin, L. Lv, G. Chen, B. Ai, and C. Zhong, "Intelligent reflecting surface-aided covert ambient backscatter communication," *IEEE Trans. Veh. Technol.*, vol. 73, no. 2, pp. 2018–2032, 2024.

[71] F. Jameel, W. U. Khan *et al.*, "Energy efficient irs assisted 6g network for industry 5.0," *Sci. Rep.*, vol. 13, no. 1, p. 14329, 2023.

[72] X. He, K. Wang, W. Huang, N. Liu, and G. K. Karagiannidis, "Irs-enabled ultra-low-power wireless sensor networks: Scheduling and transmission schemes," *Sensors*, vol. 22, no. 23, p. 9135, 2022.

[73] S. Daidakulov, A. Yerlan *et al.*, "Energy-harvesting wireless sensor networks: A review," *ACM Trans. Sens. Netw.*, vol. 14, no. 2, pp. 1–35, 2018.

[74] Q. H. Ahmed, L. L. Yang, Y. Chen, and Y. J. Guo, "Next generation backscatter communication: systems, techniques, and applications," *EURASIP J. Wirel. Commun. Netw.*, vol. 2019, no. 1, pp. 1–20, 2019.

[75] A. Salem, K. M. Rabie, K. A. Hamdi, E. Alsusa, and X. Li, "Intelligent reflecting surface-aided phase-shift backscatter communication," in *2020 IEEE International Conference on Communications (ICC)*. IEEE, 2020, pp. 1–6.

[76] Z. Wei, C. Zhao, X. Li, K. M. Rabie, and R. Kharel, "Backscatter-assisted wireless powered communication networks empowered by intelligent reflecting surface," *IEEE Trans. Green Commun. Netw.*, vol. 5, no. 2, pp. 986–1001, 2021.

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

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

[79] W. Zhang, J. Chen, Y. Kuo, and Y. Zhou, "Artificial-noise-aided optimal beamforming in layered physical layer security," *IEEE Commun. Lett.*, vol. 23, no. 1, pp. 72–75, 2019.

[80] B. Xie and R. Zhou, "Robust artificial-noise-aided beamforming in physical layer security," in *2020 Information Technology and Networking (ITN)*. IEEE, 2020, pp. 84–88.

[81] F. Nizam, S. Ahmed, P. Kumar, A. Tsetse, R. Kumar, B. Shanker, and N. Sohu, "Enhancing physical layer security in MIMO systems through beamforming and artificial noise techniques," *J. Internet Serv. Inf. Secur.*, vol. 13, no. 2, pp. 34–53, 2023.

[82] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Physical layer security of MIMO–OFDM systems by beamforming and artificial noise generation," *Phys. Commun.*, vol. 4, no. 4, pp. 313–324, 2011.

[83] G. Jang, D. Kim, I.-H. Lee, and H. Jung, "Cooperative beamforming with artificial noise injection for physical-layer security," *IEEE Access*, vol. 11, pp. 24 304–24 320, 2023.

[84] M. H. Yılmaz, E. Güvenkaya, H. M. Furqan, S. Köse, and H. Arslan, "Cognitive security of wireless communication systems in the physical layer," *Secur. Commun. Netw.*, vol. 2017, pp. 1–14, 2017.

[85] A. Pittolo and A. M. Tonello, "Physical layer security in power line communication networks: an emerging scenario, other than wireless," *IET Commun.*, vol. 8, no. 8, pp. 1239–1247, 2014.

[86] M. Obeed, A. M. Salhab, M.-S. Alouini, and S. A. Zummo, "Survey on physical layer security in optical wireless communication systems," *IEEE Commun. Netw. Serv. Manag.*, 2018.

[87] X. Li, J. Jiang, H. Wang, C. Han, G. Chen, J. Du, C. Hu, and S. Mumtaz, "Physical layer security for wireless-powered ambient backscatter cooperative communication networks," *IEEE Trans. Cogn. Commun. Netw.*, vol. 9, no. 3, pp. 665–680, 2023.

[88] C. Zhang, J. Ge, F. Gong, Y. Ji, and J. Li, "Improving physical-layer security for wireless communication systems using duality-aware two-way relay cooperation," *IEEE Syst. J.*, vol. 13, no. 1, pp. 896–907, 2019.

[89] Q. Xiao, J. Zhao, S. Feng, G. Li, and A. Hu, "Securing nextg networks with physical-layer key generation: A survey," *Secur. Saf.*, vol. 3, p. 2023021, 2024.

[90] R. Liu, X. Chen, Q. Wu, and R. Zhang, "Pilot spoofing attack detection and channel estimation for secure massive mimo," *Electron. Lett.*, vol. 60, no. 4, p. e13156, 2024.

[91] B. Akgun, M. Krunz, and O. O. Koyluoglu, "Vulnerabilities of massive mimo systems to pilot contamination attacks," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 5, pp. 1251–1263, 2018.

[92] F. Choudhury, A. Ikhlef, W. Saad, and M. Debbah, "Deep learning for detection and identification of asynchronous pilot spoofing attacks in massive mimo networks," *IEEE Trans. Wirel. Commun.*, vol. 23, no. 8, pp. 8945–8960, 2024.

[93] W. Xu, R. Wang, Y. Zhang, H. Q. Ngo, and W. Xiang, "Pilot spoofing attack on the downlink of cell-free massive mimo: From the perspective of adversaries," *IEEE Trans. Inf. Forensics Secur.*, vol. 19, pp. 5641–5654, 2024.

[94] M. Meenalakshmi, S. Chaturvedi, and V. K. Dwivedi, "Enhancing 6g network security: Gans for pilot contamination attack detection in massive mimo systems," *AEU-Int. J. Electron. Commun.*, vol. 175, p. 155085, 2024.

[95] M. K. Saeed, I. Ahmad *et al.*, "Pilot contamination in massive mimo systems: Challenges and future prospects," *arXiv:2404.19238*, 2024.

[96] S. Wang, Q. Deng, X. Fu, and P. Li, "Statistical-based detection of pilot contamination attack for noma in 5g networks," *Sci. Rep.*, vol. 15, no. 1, p. 2485, 2025.

[97] H. Guerboukha, R. Shrestha, Z. Fang, E. Knightly, and D. M. Mittleman, "Wireless communications sensing and security above 100 ghz," *Nat. Commun.*, vol. 14, no. 1, p. 841, 2023.

[98] R. Shrestha, H. Guerboukha, Z. Fang, E. W. Knightly, and D. M. Mittleman, "Jamming a terahertz wireless link," *Nat. Commun.*, vol. 13, no. 1, p. 3045, 2022.

[99] J. Ma, R. Shrestha, J. Adelberg, C.-Y. Yeh, Z. Hossain, E. Knightly, J. M. Jornet, and D. M. Mittleman, "Security and eavesdropping in terahertz wireless links," *Nature*, vol. 563, no. 7729, pp. 89–93, 2018.

[100] V. Petrov, D. Moltchanov, J. M. Jornet, and Y. Koucheryavy, "Exploiting multipath terahertz communications for physical layer security in beyond 5g networks," pp. 865–872, 2019.

[101] C.-Y. Yeh, Y. Ghasempour, Y. Amarasinghe, D. M. Mittleman, and E. W. Knightly, "Security in terahertz wlans with leaky wave antennas," in *Proceedings of the 13th*

*ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2020, pp. 317–327.

[102] J. Qiao and M.-S. Alouini, "Secure transmission for intelligent reflecting surface-assisted mmwave and terahertz systems," *IEEE Wirel. Commun. Lett.*, vol. 9, no. 10, pp. 1743–1747, 2020.

[103] S. Badran, Z. Shaikhanov, H. Guerboukha, J. M. Jornet, D. M. Mittleman, and E. W. Knightly, "Metafly: Aerial "metasurface-in-the-middle" attacks on wireless backhaul links," in *GetMobile: Mobile Computing and Communications*, vol. 27, no. 1. ACM, 2023, pp. 5–11.

[104] N. Thawdar, A. Singh, and J. M. Jornet, "Terahertz communications, sensing and security," *IEEE MILCOM*, 2024.

[105] Z. Shaikhanov, S. Badran, J. M. Jornet, D. M. Mittleman, and E. W. Knightly, "Remotely positioned metasurface-drone attack," in *Proceedings of the 24th International Workshop on Mobile Computing Systems and Applications*, 2023, pp. 110–116.

[106] R. Kumar, M. Singh *et al.*, "A review of lightweight security and privacy for resource-constrained iot devices," *Comput. Mater. Continua*, vol. 78, no. 1, pp. 31–63, 2024.

[107] I. W. Damaj, H. Al-Mubasher, and M. Saadeh, "Efficiency and security evaluation of lightweight cryptographic algorithms for resource-constrained iot devices," *Sensors*, vol. 24, no. 12, p. 4008, 2024.

[108] A. Sevin and A. A. O. Mohammed, "A survey on software implementation of lightweight block ciphers for iot devices," *J. Ambient Intell. Humaniz. Comput.*, vol. 14, no. 2, pp. 1801–1815, 2023.

[109] I. Abubakar, M. Sani, and Y. Surajo, "A new lightweight cryptographic cipher for detection and prevention of replay attacks in wireless sensor networks," *Int. J. Sci. Global Sustain.*, vol. 10, pp. 33–40, 2024.

[110] A. M. Rasheed and R. M. S. Kumar, "Efficient lightweight cryptographic solutions for enhancing data security in healthcare systems based on iot," *Front. Comput. Sci.*, vol. 7, p. 1522184, 2025.

[111] F. Thabit, O. Can, A. O. Aljahdali, G. H. Al-Gaphari, and H. A. Alkhzaimi, "Cryptography algorithms for enhancing iot security," *Internet Things*, vol. 22, p. 100759, 2023.

[112] N. Kapalova, K. Algazy, and A. Haumen, "Development of a new lightweight encryption algorithm," *East.-Eur. J. Enterp. Technol.*, vol. 3, no. 9, pp. 6–19, 2023.

[113] N. Ibrahim and J. Agbinya, "Design of a lightweight cryptographic scheme for resource-constrained internet of things devices," *Appl. Sci.*, vol. 13, no. 7, p. 4398, 2023.

[114] F. Mendoza-Cardenas, A. J. Aparcana-Tasayco, R. S. Leon-Aguilar, and J. L. Quiroz-Arroyo, "Cryptography for privacy in a resource-constrained iot: A systematic literature review," *IEIE Trans. Smart Process. Comput.*, vol. 11, no. 5, pp. 351–360, 2022.

[115] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, "Advanced lightweight encryption algorithms for iot devices: Survey, challenges and solutions," *J. Ambient Intell. Humaniz. Comput.*, vol. 14, no. 1, pp. 123–141, 2023.

[116] S. Ghosh, S. P. Maity, and C. Chakraborty, "Secrecy outage probability and strictly positive secrecy capacity of uav assisted cooperative noma system with two untrusted destinations," *Sci. Rep.*, vol. 15, no. 1, p. 4321, 2025.

[117] T. H. Vu and S. Kim, "Enhancing covert communication in noma systems with joint security and covert design," *PLOS ONE*, vol. 19, no. 12, p. e0317289, 2024.

[118] W. Huang, X. Chen, and R. Zhang, "Secure transmission design for cooperative noma in the presence of internal eavesdropping," *IEEE Commun. Lett.*, vol. 26, no. 6, pp. 1387–1391, 2022.

[119] Q. Li, D. Xu, K. Navaie, and Z. Ding, "Covert and secure communications in noma networks with internal eavesdropping," *IEEE Wirel. Commun. Lett.*, vol. 12, no. 12, pp. 2154–2158, 2023.

[120] X. Liu, W. Chen, H. Zhang *et al.*, "Secure user pairing and power allocation for downlink non-orthogonal multiple access against external eavesdropping," *Entropy*, vol. 26, no. 1, p. 64, 2024.

[121] X. Chen, W. Liu, R. Zhang *et al.*, "A survey of deep learning based noma: State of the art, key aspects, open challenges and future trends," *Sensors*, vol. 23, no. 6, p. 3069, 2023.

[122] S. A. Abbas, S. A. Hassan *et al.*, "Dynamic ris partitioning in noma systems using deep reinforcement learning," *Front. Antennas Propag.*, vol. 2, p. 1418412, 2024.

[123] T. H. Vu and S. Kim, "Performance evaluation of power-beacon-assisted wireless-powered noma iot-based systems," *IEEE Internet Things Journal*, vol. 8, no. 14, pp. 11 655–11 665, 2021.

[124] R. Kumar, M. Singh *et al.*, "Combat hybrid eavesdropping in power-domain noma: Joint design of timing channel and symbol transformation," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 1234–1248, 2018.

[125] W. Chen, X. Liu *et al.*, "Noma decoding: Successive interference cancellation or maximum likelihood detection?" *IEEE Trans. Veh. Technol.*, 2024.

[126] C. Zhang, P. Patras, and H. Haddadi, "Deep learning in mobile and wireless networking: A survey," *IEEE Commun. Surv. Tutor.*, vol. 21, no. 3, pp. 2224–2287, 2019.

[127] N. C. Luong, D. T. Hoang, S. Gong, D. Niyato, P. Wang, Y.-C. Liang, and D. I. Kim, "Applications of deep reinforcement learning in communications and networking: A survey," *IEEE Commun. Surv. Tutor.*, vol. 21, no. 4, pp. 3133–3174, 2019.

[128] P. Veličković, G. Cucurull, A. Casanova, A. Romero, P. Lio, and Y. Bengio, "Graph attention networks," *arXiv:1710.10903*, 2017.

[129] S. Mohamed Ali, M. N. Jaidhan, Q. Abbas *et al.*, "Network anomaly detection using channel boosted and residual learning based deep convolutional neural network," *Appl. Soft Comput.*, vol. 83, p. 105645, 2020, dOI: 10.1016/j.asoc.2019.105645.

[130] T. N. Kipf and M. Welling, "Semi-supervised classification with graph convolutional networks," *arXiv:1609.02907*, 2016.

[131] V. Mnih, K. Kavukcuoglu, D. Silver, A. A. Rusu, J. Veness, M. G. Bellemare, A. Graves, M. Riedmiller, A. K. Fidjeland, G. Ostrovski *et al.*, "Human-level control through deep reinforcement learning," *Nature*, vol. 518, no. 7540, pp. 529–533, 2015.

[132] R. S. Sutton, D. A. McAllester, S. P. Singh, and Y. Mansour, "Policy gradient methods for reinforcement learning with function approximation," *Adv. Neural Inf. Process. Syst.*, vol. 12, pp. 1057–1063, 2000.

[133] R. Manche, "Decentralized federated reinforcement learning for multi-agent systems: A scalable approach," *Gen. Purpose Res. Publ. Rev.*, vol. 5, no. 12, pp. 1867–1879, 2024, dOI: 10.55248/gengpi.5.1224.3512.

[134] Y. Zhou, J. Guo, H. Li *et al.*, "Efficient federated learning in 6g-satellite systems: Deep reinforcement learning based multi-objective optimization," *IEEE WCNC*, pp. 1–6, 2024.

[135] S. Kumari, P. Rathore *et al.*, "A comprehensive investigation of anomaly detection methods in deep learning and machine learning: 2019-2023," *IET Inf. Secur.*, vol. 18, p. 8821891, 2024, dOI: 10.1049/2024/8821891.

[136] M. Sarfraz, M. Jamil *et al.*, "Distributed rate optimization for intelligent reflecting surface with federated learning," *IEEE Conf. Publ.*, pp. 1–6, 2020, dOI: 10.1109/ICCT46805.2020.9145388.

[137] M. Di Renzo, A. Zappone, M. Debbah, M.-S. Alouini, C. Yuen, J. de Rosny, and S. Tretyakov, "Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and the road ahead," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 11, pp. 2450–2525, 2020.

[138] M. Cui, G. Zhang, and R. Zhang, "Secure wireless communication via intelligent reflecting surface," *IEEE Wirel. Commun. Lett.*, vol. 8, no. 5, pp. 1410–1414, 2019.

[139] C. You and R. Zhang, "Wireless communication aided by intelligent reflecting surface: Active or passive?" *IEEE Wirel. Commun. Lett.*, vol. 10, no. 12, pp. 2659–2663, 2021.

[140] N. V. Huynh, D. T. Hoang, X. Lu, D. Niyato, P. Wang, and D. I. Kim, "Ambient backscatter communications: A contemporary survey," *IEEE Commun. Surv. Tutor.*, vol. 20, no. 4, pp. 2889–2922, 2018.

[141] G. Yang, D. Yuan, Y.-C. Liang, R. Zhang, and V. C. Leung, "Optimal resource allocation in full-duplex ambient backscatter communication networks for wireless-powered IoT," *IEEE Internet Things Journal*, vol. 6, no. 2, pp. 2612–2625, 2019.

[142] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, and J. R. Smith, "Ambient backscatter: Wireless communication out of thin air," *ACM SIGCOMM Computer Communication Review*, vol. 43, no. 4, pp. 39–50, 2013.

[143] N. Van Huynh *et al.*, "Ambient backscatter communications: A contemporary survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 2889–2922, 2018.

[144] J. Zhao, Y. Zhu, X. Mu, K. Cai, Y. Liu, and L. Hanzo, "Simultaneously transmitting and reflecting reconfigurable intelligent surface (STAR-RIS) assisted UAV communications," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 10, pp. 3041–3056, 2022.

[145] T. D. P. Perera, D. N. K. Jayakody, S. K. Sharma, S. Chatzinotas, and J. Li, "Simultaneous wireless information and power transfer (SWIPT): Recent advances and future challenges," *IEEE Commun. Surv. Tutor.*, vol. 20, no. 1, pp. 264–302, 2018.

[146] S. R. Shahcheragh and K. Mohamed-Pour, "Beamforming design for star-ris assisted secure wireless communication system under hardware impairments," *EURASIP J. Wirel. Commun. Netw.*, vol. 2024, no. 59, pp. 1–20, 2024, dOI: 10.1186/s13638-024-02389-x.

[147] F. Liu, Y. Cui, C. Masouros, J. Xu, T. X. Han, Y. C. Eldar, and S. Buzzi, "Integrated sensing and communications: Toward dual-functional wireless networks for 6g and beyond," *IEEE J. Sel. Areas Commun.*, vol. 40, no. 6, pp. 1728–1767, 2022.

[148] Z. Zhang, L. Dai *et al.*, "Joint beamforming optimization for active star-ris-assisted isac systems," *IEEE Trans. Wirel. Commun.*, vol. 23, pp. 8234–8249, 2024, dOI: 10.1109/TWC.2024.3434963.

[149] C. Wang, Z. Li *et al.*, "Securing star-fc-ris empowered integrated sensing and multiuser communications against target eavesdropping," *Sci. China Inf. Sci.*, vol. 68, pp. 1–15, 2024, dOI: 10.1007/s11432-024-4151-8.

[150] M. Hua, Q. Wu, W. Chen *et al.*, "Secure intelligent reflecting surface-aided integrated sensing and communication," *IEEE Trans. Wirel. Commun.*, vol. 23, pp. 575–591, 2024, dOI: 10.1109/TWC.2023.3241943.

[151] A. Al-Hubaishi, M. Alrabeiah, and A. Alkhateeb, "Deep reinforcement learning for intelligent reflecting surfaces: Towards standalone operation," *IEEE Commun. Lett.*, vol. 24, no. 12, pp. 2836–2840, 2020, dOI: 10.1109/LCOMM.2020.3017882.

[152] S. Zhang, J. Lin, and Q. Zhang, "A multi-agent reinforcement learning approach for efficient client selection in federated learning," *Proc. AAAI Conf. Artif. Intell.*, vol. 36, no. 8, pp. 9091–9099, 2022, dOI: 10.1609/aaai.v36i8.20894.

[153] Z. U. A. Tariq, E. Baccour, A. Erbad, and M. Hamdi, "Reinforcement learning for resilient aerial-irs assisted wireless communications networks in the presence of multiple jammers," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 15–37, 2024, dOI: 10.1109/OJCOMS.2023.3334489.

[154] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

[155] Q. Wu and R. Zhang, "Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming," *IEEE Transactions on Wireless Communications*, vol. 18, no. 11, pp. 5394–5409, 2019.

[156] E. Björnson, Ö. T. Özdogan, and E. G. Larsson, "Intelligent reflecting surface versus decode-and-forward: How large surfaces are needed to beat relaying?" *IEEE Wireless Communications Letters*, vol. 9, no. 2, pp. 244–248, 2020.

[157] J. Chen, Y.-C. Liang, Y. Pei, and H. Guo, "Reconfigurable intelligent surface assisted secure wireless communications," *IEEE Wireless Communications Letters*, vol. 9, no. 10, pp. 1651–1655, 2020.

[158] J. Chen, X. Liu *et al.*, "Ris-empowered satellite-aerial-terrestrial networks with pd-noma," *arXiv:2404.12987*, 2024.

[159] X. Liu, J. Chen *et al.*, "Ris-empowered satellite-aerial-terrestrial networks with power-domain noma: A comprehensive survey," *IEEE Commun. Surv. Tutor.*, vol. 25, pp. 2764–2807, 2023, dOI: 10.1109/COMST.2023.3287352.

[160] Q. Wu and R. Zhang, "Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network," *IEEE Communications Magazine*, vol. 58, no. 1, pp. 106–112, 2020.

[161] M. Di Renzo, A. Zappone, M. Debbah *et al.*, "Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and the road ahead," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 11, pp. 2450–2525, 2020.

[162] S. Gong, X. Lu, D. W. K. Ho *et al.*, "Toward smart wireless communications via intelligent reflecting surfaces: A contemporary survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2283–2314, 2020.

[163] J. Zhang, Y. Zhang, C. Zhong, and Z. Zhang, "Simultaneously transmitting and reflecting reconfigurable intelligent surface (star-ris): Fundamentals and applications," *IEEE Communications Magazine*, vol. 61, no. 4, pp. 84–90, 2023.

[164] C. Huang, A. Zappone, M. Debbah, and C. Yuen, "Achievable rate maximization by passive intelligent mirrors," *IEEE Transactions on Wireless Communications*, vol. 18, no. 8, pp. 3711–3725, 2019.

[165] E. Björnson, Ö. T. Özdogan, and E. G. Larsson, "Intelligent reflecting surface versus decode-and-forward: How large surfaces are needed to beat relaying?" *IEEE Wireless Communications Letters*, vol. 9, no. 2, pp. 244–248, 2020.

[166] K. Shen and W. Yu, "Fractional programming for communication systemsâĂŤpart i: Power control and beamforming," *IEEE Transactions on Signal Processing*, vol. 66, no. 10, pp. 2616–2630, 2018.

[167] M. Ji, J. Chen, L. Lv, Q. Wu, Z. Ding, and N. Al-Dhahir, "Secure noma systems with a dual-functional ris: Simultaneous information relaying and jamming," *IEEE Transactions on Communications*, vol. 71, no. 11, pp. 6514–6528, 2023.

[168] Y. Du, S. Xu, G. Zhang, B. Wu, and J. Zhang, "Intelligent reflecting surface backscatter downlink multi-user communications with radar sensing," *IEEE Transactions on Vehicular Technology*, vol. 74, no. 5, pp. 8351–8356, 2025.

[169] W. Liu, S. Shen, D. H. K. Tsang, and R. Murch, "Mimo ambient backscatter communications: Capacity maximization and beamforming optimization," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 12, pp. 15 829–15 843, 2023.

[170] S. Ma, G. Wang, R. Fan, and C. Tellambura, "Blind channel estimation for ambient backscatter communication systems," *IEEE Commun. Lett.*, vol. 22, no. 6, pp. 1296–1299, 2018.

[171] D. Li and Y.-C. Liang, "Adaptive ambient backscatter communication systems with MRC," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 12 304–12 316, 2018.

[172] P. Singh, P. Pawar, and A. Trivedi, "Physical layer security approaches in 5g wireless communication networks," in *2018 International Conference on Smart City and Emerging Technology (ICSCET)*. IEEE, 2018, pp. 1–5.

[173] F. Scarselli, M. Gori, A. C. Tsoi, M. Hagenbuchner, and G. Monfardini, "The graph neural network model," *IEEE Transactions on Neural Networks*, vol. 20, no. 1, pp. 61–80, 2008.

[174] T. N. Kipf and M. Welling, "Semi-supervised classification with graph convolutional networks," *International Conference on Learning Representations (ICLR)*, 2017.

[175] Z. Wu, S. Pan, F. Chen, G. Long, C. Zhang, and P. S. Yu, "A comprehensive survey on graph neural networks," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 32, no. 1, pp. 4–24, 2020.

[176] V. Liu, A. Parks, and V. Talla, "Backscatter communications for wireless powered sensor networks with energy harvesting," *IEEE Communications Magazine*, vol. 57, no. 7, pp. 85–91, 2019.

[177] G. Wang *et al.*, "Backcom: Backscatter communication for internet of things," *IEEE Wireless Communications*, vol. 27, no. 2, pp. 152–157, 2020.

# Appendix A

# Supplementary Background on Backscatter and ISAC Systems

## A.1 Backscatter Channel Estimation and Signal Processing

Effective channel estimation is crucial for optimal detection in backscatter communication systems. However, the unique characteristics of backscatter channels, including the multiplicative nature of the backscatter-link channel and the presence of direct-link interference, pose significant challenges [176, 177, 143].

The composite channel in a backscatter system can be written as

$$h_{\text{composite}} = h_d + h_t h_r \rho \tag{A.1}$$

where $h_t$ is the channel from the RF source to the tag, $h_r$ is the channel from the tag to the receiver, and their product $h_t h_r$ is referred to as the cascaded backscatter channel.

Conventional channel estimation approaches cannot be directly applied because passive backscatter nodes are unable to actively transmit pilot signals. Several estimation approaches have therefore been developed:

- **Pilot-assisted estimation:** The backscatter device modulates pilot symbols onto the reflected signal to facilitate channel estimation at the receiver.

- **Blind estimation:** Statistical properties of ambient signals and backscatter modulation structures are exploited to estimate the channel without explicit pilots.
- **Semi-blind estimation:** Partial pilot information is combined with statistical signal processing methods to balance estimation accuracy and signaling overhead.

The maximum likelihood (ML) estimator for the backscatter channel can be expressed as

$$\hat{h}_b = \arg\max_{h_b} \sum_{n=1}^{N} \log p(y[n]|h_b, \rho[n]) \tag{A.2}$$

where $p(y[n]|h_b, \rho[n])$ denotes the conditional probability density function of the received signal given the channel and reflection coefficient.

## A.2 Waveform Design for ISAC Systems

Dual-functional waveform design is a key challenge in ISAC systems, where radar sensing and wireless communication functionalities must coexist within shared spectral and hardware resources.

### A.2.1 OFDM-Based ISAC Waveforms

OFDM-based waveforms provide a flexible framework for ISAC by enabling independent allocation of subcarriers for radar sensing and communication:

$$s(t) = \sum_{k=0}^{K-1} X_k e^{j2\pi k\Delta f t}, \quad 0 \le t \le T \tag{A.3}$$

where $X_k$ represents the complex symbol on the $k$-th subcarrier and $\Delta f$ is the subcarrier spacing.

### A.2.2 Spread Spectrum ISAC Waveforms

Code-division multiple access (CDMA)-based spread spectrum techniques enable coexistence between radar and communication signals through orthogonal spreading codes:

$$s_c(t) = \sum_n d_n c_n(t) p(t - nT_c) \tag{A.4}$$

where $d_n$ is the data symbol, $c_n(t)$ is the spreading code, and $p(t)$ is the chip pulse shape.

### A.2.3 Chirp-Based ISAC Waveforms

Linear frequency modulated (LFM) chirp signals provide desirable radar sensing performance while simultaneously supporting communications through phase or amplitude modulation:

$$s(t) = Ae^{j(\omega_0 t + \frac{1}{2}\mu t^2 + \phi(t))} \tag{A.5}$$

where $A$ is the amplitude, $\omega_0$ is the carrier frequency, $\mu$ is the chirp rate, and $\phi(t)$ carries the communication information.