Secrecy Performance of RIS-enhanced Communication under Imperfect CSI

By

Khawaja Muhammad Hamza

Fall-2021-MS-EE-TCN 363504 SEECS

Supervisor

Dr. Syed Ali Hassan

Department of Electrical Engineering

A thesis submitted in partial fulfillment of the requirements for the degree of Masters of Science in Electrical Engineering (MS EE)

In

School of Electrical Engineering & Computer Science (SEECS) ,
National University of Sciences and Technology (NUST),
Islamabad, Pakistan.

(August 2023)

Thesis Acceptance Certificate

Certified that final copy of MS/MPhil thesis entitled "**Secrecy Performance of RIS-enhanced Communication under Imperfect CSI**" written by **Khawaja Muhammad Hamza**, (Registration No **Fall-2021-MS-EE-TCN 363504 SEECS**), of School of Electrical Engineering & Computer Science (SEECS) has been vetted by the undersigned, found complete in all respects as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial fulfillment for award of MS/M Phil degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have also been incorporated in the said thesis.

Signature. ____________________

Name of Advisor: **Dr. Syed Ali Hassan**

Date: ____________________

Signature (HoD): ____________________

Date: ____________________

Signature (Dean/Principal): ____________________

Date: ____________________

Approval

It is certified that the contents and form of the thesis entitled “**Secrecy Performance of RIS-enhanced Communication under Imperfect CSI**" submitted by **Khawaja Muhammad Hamza** have been found satisfactory for the requirement of the degree.

Advisor: **Dr. Syed Ali Hassan**

Signature: ____________________

Date: ____________________

Committee Member 1: **Dr. Humma Gafoor**

Signature: ____________________

Date: ____________________

Committee Member 2: **Dr. Mohaira Ahmad**

Signature: ____________________

Date: ____________________

Dedication

I am humbled and honored to dedicate this thesis book to the most important people in my life, my beloved family. Throughout this challenging yet rewarding journey, your unwavering support, love, and understanding have been my constant pillars of strength. From the early days of my academic pursuits to the late nights of writing and research, you have been there, cheering me on and believing in my abilities even when I doubted myself. Your sacrifices, patience, and encouragement have been the fuel that kept me going, and I am forever grateful for everything you have done.

To my esteemed supervisor **Dr. Syed Ali Hassan**, I extend my deepest gratitude for your exceptional guidance and mentorship. Your profound knowledge, passion for research, and dedication to your field have shaped the outcome of this thesis in ways I could not have imagined. Your constructive feedback, patience, and unwavering belief in my potential have inspired me to strive for excellence. Working under your guidance has been an honor and a privilege, and I am proud to dedicate this thesis to you as a token of my appreciation.

To my esteemed co-supervisors **Dr. Humma Gafoor**, **Dr. Mohaira Ahmad**, I am immensely grateful for your invaluable contributions to this work. Your expertise and insights have enriched the research and broadened my perspective. Your unwavering support and encouragement have motivated me to delve deeper into my studies and explore new avenues of knowledge. I am indebted to each of you for your mentorship and dedication to my academic growth, and I proudly dedicate this thesis to all of my co-supervisors.

Certificate of Originality

I hereby declare that this submission is my own work and to the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at Department of Electrical Engineering at School of Electrical Engineering & Computer Science (SEECS) or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at School of Electrical Engineering & Computer Science (SEECS) or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics which has been acknowledged.

Author Name: **Khawaja Muhammad Hamza**

Signature: __________________

Acknowledgments

Glory be to Allah (S.W.A), the Creator, the Sustainer of the Universe. Who only has the power to honour whom He please, and to abase whom He please. Verily no one can do anything without His will. From the day, I came to NUST till the day of my departure, He was the only one Who blessed me and opened ways for me, and showed me the path of success. Their is nothing which can payback for His bounties throughout my research period to complete it successfully.

Khawaja Muhammad Hamza

Contents

List of Figures

List of Tables

Abstract

In this work, we consider an reconfigurable intelligent surface (RIS) enhanced aerial communication system and reconfigurable intelligent surface (RIS) aided uplink noma communication system, in RIS-enhanced aerial communication system we have an unmanned aerial vehicle (UAV) intends to deliver confidential information to the legitimate user in the presence of an eavesdropper with the aid of an RIS. For an accurate performance analysis, we consider the practical constraints of imperfect channel state information (CSI) and discrete phase shifts for the RIS-enhanced system. Furthermore, in order to compensate for the secrecy loss due to the practical constraints, we formulate a secrecy rate maximization problem under the target secrecy rate constraint to optimize the number of RIS elements. Our extensive simulation results demonstrate the impact of various factors, namely the channel estimation error, RIS phase shift design, number of RIS elements, and transmit power, on the secrecy performance of the considered system. Moreover, the simulation results reveal that the secrecy performance degrades to a great extent in the case of imperfect channel estimation of the RIS to a legitimate user's link. In case of RIS-aided uplink noma communication system, the UE's wants to transmit confidential information to the base station (BS) in presence of an eavesdropper. We evaluate the impact of transmit power, distance of UE's and eavesdropper from RIS and split factor on secrecy performance under Nakagami-m fading channels of the considered system. The simulation results reveal that the secrecy rate increases with increase in the trasnmit power of UE's and the distance of eavesdropper from RIS, while secrecy rate degrades with increase in the distance of UE's from the RIS. Moreover, there is an increase in the secrecy rate of UE1 and decrease in the secrecy rate of UE2 with an increase in the split ratio as the number of RIS elements for the far user imcreases with increase in the split ratio.

Chapter 1

Introduction and Motivation

Reconfigurable intelligent surface (RIS), is made up of a massive number of low-cost reflecting components with adjustable phase shifts has lately been promoted as a practical way to greatly improve the performance of wireless communication [32], [39]. The RIS performs the functions of signal enhancement and interference reduction through smart reflectors without the need of active transmitters. One alluring benefit of using the RIS over the well-known massive multiple input multiple-output (MIMO) approach is to reduce the system's energy consumption and realize the sustainable green sixth-generation (6G) wireless networks. Conventional reflection arrays [9], liquid crystal meta-surfaces [19], and software-defined meta-materials [23] can be used to realize RIS. Different from the active relay systems, RIS is passive, operates in a full-duplex mode without self-interference, and doesn't amplify noise. Additionally, RIS varies from the active large intelligent surface (LIS) [22] by employing passive reflecting elements for the signal reflection rather than the entire surface for transmitting and receiving signals.

On the other hand, unmanned aerial vehicles (UAVs) have drawn a lot of interest over the past 10 years due to their affordability, ease of deployment, and ability to hover over a certain region. The main applications of UAV-assisted systems include real-time data collecting, traffic monitoring, surveillance, delivery of commodities, precision agriculture, and rescue missions. UAVs, often known as drones, can access places where there is no infrastructure and where it is not practicable for a human to visit. In its initial deployment, the UAV operated independently without any Internet-of-Things (IoT) or communication-related technology integration. UAVs can build better communication linkages with a variety of IoT devices by changing their position.

On the other hand, in order to provide secure wireless communications and prevent eavesdropping by unauthorized users, physical-layer security has drawn a lot of attention [4], [2]. Secure communication is conventionally accomplished via application layer implementation of traditional cryptographic techniques. However, the nature of wireless transmission presents a number of difficulties for key management and distribution when creating secured communication channels [7].In this regard, physical layer security has been developed based on information theory to improve the security of wireless communication [1].

Non-orthogonal multiple access (NOMA) will be crucial in 5G and beyond because of its improved spectrum efficiency [10]. NOMA has an exceptional capacity to strengthen the SE and user connection in comparison to the traditional orthogonal multiple access (OMA) network topology [13]. In wireless communication networks, where signals are broadcast, it is crucial to ensure the privacy of any conversations between the base station (BS) and legitimate users (LUs).

Due to the broadcast nature of radio propagation and the instability of the transmission connection, wireless communication networks have been experiencing significant information leakage caused by eavesdropping assaults. Physical layer security (PLS), which aims to establish information-theoretic security against hacking, is emerging as a potential method of safeguarding wireless communications. Secure communication is conventionally accomplished via traditional techniques, such as cooperative jamming, collaborating relays, and beamforming assisted by artificial noise. The fundamental obstacle still exists, especially at higher frequencies, despite the fact that the aforementioned methods have greatly improved the PLS of wireless systems. These methods need the deployment of a large number of relays and other helpers, which is expensive and requires more power.

Different from the aforementioned works, the main contributions of this work are summarized as follows.

- We consider an RIS-enhanced downlink aerial communication system, where an RIS assists the communication between a UAV and a legitimate user in the presence of an eavesdropper and an RIS-enhanced uplink NOMA communication system, where two UEs communicate with the BS with the aid of an RIS in the presence of an eavesdropper.

- The secrecy rate performance of the RIS-enhanced downlink aerial communication system is studied under imperfect channel state information (CSI) using discrete phases. Moreover, to compensate for the secrecy loss due to the practical constraints, we formulate a secrecy rate maximization problem under the target secrecy rate to optimize the number of RIS elements.

- Our extensive simulation results demonstrate the impact of various factors, namely the channel estimation error, RIS phase shift design, number of RIS elements, and transmit power, on the secrecy performance of the RIS-enhanced downlink aerial communication system. Moreover, the simulation results reveal that the secrecy performance degrades to a great extent in the case of imperfect channel estimation of the RIS to a legitimate user's link.

- The secrecy rate and secrecy outage probability of the RIS-enhanced uplink NOMA communication system is studied under Nakagami-m fading channels. Moreover, our simulation results demonstrate the impact of transmit power, distance of UEs from the RIS, split factor on the secrecy rate and the impact of transmit power on the secrecy outage probability with different threshold of the considered system.

Chapter 2

Literature Review

In recent years, the convergence of cutting-edge technologies has spurred a transformative shift in the field of wireless communication. As we delve into the literature review of this thesis, we embark on an exploration at the crossroads of three dynamic areas: reconfigurable intelligent surfaces (RIS), physical layer security (PLS), and non-orthogonal multiple access (NOMA). These realms of research, each offering distinct and groundbreaking contributions to the wireless landscape, now find themselves intricately intertwined, forming a nexus of innovation. RIS, with its ability to control and manipulate electromagnetic waves, promises to revolutionize wireless networks by enhancing signal strength and mitigating interference. In parallel, PLS strategies aim to safeguard the confidentiality of information transmitted over the airwaves, fostering trust in communication systems. Meanwhile, NOMA introduces a paradigm shift in multiple access schemes, allowing simultaneous transmission by multiple users over the same resources. As we delve deeper into the following sections, we embark on a journey to uncover the synergies, challenges, and transformative potentials that arise at this remarkable intersection of RIS, PLS, and NOMA in wireless communication systems.

Yuanwei Liu [41] provides a comprehensive overview of the working principle, beamforming design and performance analysis of reconfigurable intelligent surfaces.The author in [36] describes the working principle and the challenges like channel conditions in RIS-enhanced communication networks.Basar [36] explores the theoretical limitations of RIS-enhanced communication networks using mathematical techniques.The authors in [29] design solutions for non-convex problem for transmit power allocation and the phase shifts of the surface reflecting elements for the RIS-enhanced downlink communication system.

Cunhua Pan [43] reviews the application, challenges and future direction of reconfigurable intelligent surfaces. The author in [34] illustrates numerical results that highlight the spectral efficiency gains of RISs when their size is sufficiently large as compared with the wavelength of the radio waves.State of the artwork of smart radio environment for reconfigurable intelligent surface is reviewed in [35]. The design and evaluation of reconfigurable intelligent surface in real-world environment is reviewed by Georgios C. Trichopoulos [55]. Xiaojun Yuan [50] reviews the challenges and opportunities for RIS-enhanced communication systems.

Yi-Sheng Shiu [3] reviews different methods to enhance the physical layer security of wireless communication systems.The authors [16] propose diversity techniques like artificial noise and beamforming to enhance the physical layer security of the system. Amal Hyadi [17] overview the physical layer security of the wireless communication system with imperfect channel state information (CSI) at the transmitter. The physical layer security of the smart grid system is reviewed by Eun-Kyu Lee [6].

Junqing Zhang [18] proposes a secret key generation method for the physical layer security of the wireless communication system. Efficient hardware architecture is proposed in order to improve the physical layer security of the communication system[44].Nan Yang [15] explores different opportunities and challenges in order to create the secure 5G wireless communication network.The challenges in the physical layer security for a unmanned aerial vehicle (UAV) enhanced communication system is proposed in [31].

LJ Rodriguez [14] reviews different techniques for Physical layer security in wireless cooperative relay networks. Physical layer security of a wireless sensor network is reviewed by J Choi in [8].Kun Wang [21] proposed a relay and jamming technique for the secure communication issues of wireless cooperative networks in the presence of multiple friendly but selfish intermediate nodes.The impact of mobility on physical layer security of the wireless communication system under fading channel is explored in [24]. Saad [11] explores the physical layer security of the back-scatter wireless communication system.

Yongpeng Wu [26] proposed different physical layer security techniques for wireless communication systems. The Physical layer security for wireless implantable medical devices is studied in [12]. Zhang [18] proposed the two-relay cooperative system in order to increase the physical layer security of the wireless communication system. Chorti

[5] explores the physical layer security of the wireless communication system under active and passive eavesdropping. Different jamming techniques are explored in order to enhance the physical layer security of the wireless system in [20].

SK Das [57] reviews different machine learning techniques for RIS-enhanced IOT systems. The performance of RIS-enhanced two way orthogonal frequency division multiplexing (OFDM) is reviewed in [38].This articles [53] provides the proper functioning of future integrated terrestrial/non-terrestrial (INTENT) networks. The authors [49] explores optimization methods to increase the energy efficiency of downlink RIS-assisted wireless-powered communication network.A novel concept called simultaneously transmitting and reflecting RIS (STAR-RIS) is introduced into the wireless-powered mobile edge computing (MEC) systems to improve the efficiency of energy transfer and task offloading is proposed in [60].

Despite the research achievements, the RIS-aided systems are prone to eavesdropping since wireless media has a broadcasting nature. As a result, secure communication is a crucial concern. In this regard, Shen et al. explored the methods to enhance the secrecy rate for IRS-assisted multi-antenna systems [30]. The authors in [33] proposed a novel design for the secrecy beamforming optimization in an RIS-aided system.

In [37], the authors put forth the strategies to improve the secrecy rate of the RIS-assisted multiple-input single-output (MISO) system. The secure non-orthogonal multiple access (NOMA)- assisted SWIPT systems has been examined by Tang et al. in [25]. In [56], the authors proposed a novel RIS-aided IoT system for secure communication. In [54] the authors evaluated the physical-layer security of RIS-aided NOMA network under Nakagami-m fading.

RIS-assisted NOMA systems create a secure signal zone for the intended user by coherent phase shifting from RIS elements and by discrete phase shifting the signal is attenuated for the unauthorized users which eventually improves the secrecy performance. In this regard, Zhiqing Tang proposes a novel design of reconfigurable intelligent surface (RIS) to enhance the physical layer security (PLS) in the RIS-aided non-orthogonal multiple access (NOMA) network [27].

The authors [47] investigated the impact of Residual Hardware Impairment on the IoT Secrecy Performance of RIS-Assisted NOMA Networks.In [40], authors investigate network secrecy performance of RIS-assisted various emerging multi-user communication techniques, such as Unmanned Aerial Vehicles (UAVs), Non-Orthogonal Multiple Access (NOMA), Millimeter Wave (mmWave) and Terahertz (THz) communications. The secrecy performance of a RIS-aided NOMA 6G networks is investigated for two two "dead zone" NOMA users for both internal and external eavesdropping by Zhe Zhang [42]

Yasin Khan [58] evaluates the effect of phase error of RIS in a RIS-aided non-orthogonal multiple access communication system under Nakagami and Rayleigh fading. The requirements and issues of RIS-aided NOMA communication system is viewed in comparison with the orthogonal multiple access (OMA) schemes [59]. Qian Zhang [62] proposed the robust beamforming design for a RIS-aided NOMA communication system under hardware limitations.

The analytical expression of secrecy outage probability (SOP) under nakamgami-m fading is evaluated for the STAR-RIS NOMA system [52]. The paper [61] investigates a non-orthogonal multiple access (NOMA) and rate-splitting (RS) covert communication system employing a reconfigurable intelligent surface (RIS), concentrating on detection error probability and covert communication rate. Defining secrecy outage probability (SOP) expressions, doing an asymptotic analysis, and protecting against eavesdropping are all covered. Some of the important paper used as a base for this work is summarized in the table below.

After brief literature review, we considered two system models RIS-assisted downlink aerial communication system and RIS-enhanced Uplink NOMA communication system for the secrecy performance analysis.

Year	**Ref.**	**Paper Title**	**Working**
2021	[51]	User Cooperation for RIS-aided Secure SWIPT MIMO Systems under passive eavesdropping	Average secrecy rate maximization problem is formulated, which is addressed by a low complexity algorithm.
2021	[48]	Secrecy Outage Probability and Average Rate of RIS-Aided Communications Using Quantized Phases	Secrecy outage probability in the presence of non-colluding and colluding eavesdroppers is obtained with the analytical expressions of the average secrecy rate.
2019	[28]	Secure Wireless Communication via Intelligent Reflecting Surface	HMaximize the secrecy rate of the legitimate communication link by jointly designing the AP's transmit beamforming and the RIS's reflect beamforming.
2019	[33]	Enabling Secure Wireless Communications via Intelligent Reflecting Surfaces	In order to increase the secrecy rate, block coordinate descent and minimization maximization techniques are used to optimize the beamformer at the transmitter and the RIS phase shifts.

Table 2.1: Review of RIS-aided Communication Systems

Chapter 3

RIS-assisted downlink aerial communication system

As illustrated in Fig. 3.1, we consider an RIS-assisted downlink communication system, where an aerial BS intends to deliver the confidential information to a legitimate user in the presence of an eavesdropper with the aid of an RIS. We assume that each of the aerial BS, legitimate user, and eavesdropper are equipped with a single antenna, while the RIS consists of N passive reconfigurable elements, denoted by $\mathcal{N} = \{1, 2, \ldots., N\}$.

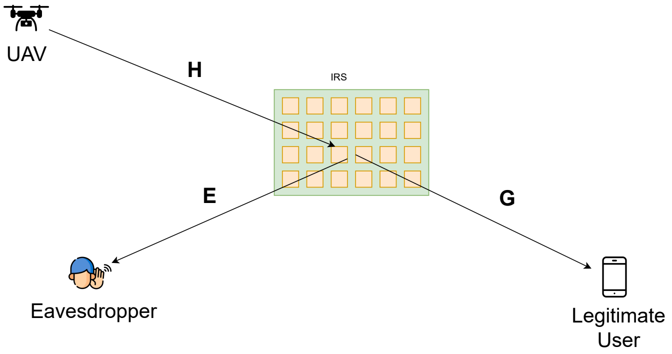


Figure 3.1: An illustration of RIS-enhanced downlink aerial communication system

3.0.1 Signal Model

The received signals at the legitimate user and eavesdropper are given by

$$y_l = \sqrt{P_t}(\mathbf{g}_l^H \Theta \mathbf{G})x + n_l, \tag{3.0.1}$$

and

$$y_e = \sqrt{P_t}(\mathbf{g}_e^H \Theta \mathbf{G})x + n_e, \tag{3.0.2}$$

respectively, P_t denote the transmit power of the UAV, $\mathbf{G} \in \mathbb{C}^{N\times 1}$, $\mathbf{g}_l \in \mathbb{C}^{N\times 1}$ and $\mathbf{g}_e \in \mathbb{C}^{N\times 1}$, are the channel vectors from the RIS to the legitimate user, RIS to the eavesdropper, and UAV to the RIS, respectively, x is the confidential information intended for the BS from legitimate user $n_l \sim \mathcal{CN}(0, \sigma_b^2)$ and $n_e \sim \mathcal{CN}\left(0, \sigma_e^2\right)$ are the additive white Gaussian noise (AWGN) with zero mean and variances σ_l^2 at legitimate user and σ_e^2 at eavesdropper, respectively, and $\mathbf{G}^H$ denotes the Hermitian transpose of $\mathbf{G}$. Similarly in (1) and (2), $\Theta = \text{diag}\left(\xi_1 e^{j\theta_1}, \xi_2 e^{j\theta_2}, \ldots, \xi_N e^{j\theta_N}\right) \in \mathbb{C}^{N\times N}$, is a diagonal matrix, $\xi_n \in [0,1]$ and $\theta_n \in \mathcal{F}_i$ denote both the continuous and discrete phase shifts of the n-th reflecting element of the RIS.Where $\mathcal{F}_1 = [0, 2\pi)$ is the set of *continuous phase shifts* and $F2 = \{0, \Delta\theta, \ldots, (M-1)\Delta\theta\}$ is the set of *discrete phase shifts*, obtained by uniformly quantizing the interval $[0, 2\pi)$, where $\Delta\theta = \frac{2\pi}{M}$, and $M = 2^\alpha$ denotes the discrete phase shift levels with an α-bit resolution. All wireless channels are assumed to be mutually independent and follow complex Gaussian distribution with zero mean and unit variance.

3.0.2 RIS Configuration and Effective Channel Gain

The RIS reconfigures the phase-shift $\theta_n = -\angle g_{l,n} \cdot g_{u,n}$ to maximize the received signal strength at the legitimate user, where $g_{l,n}$ and $g_{u,n}$ denote the n-th elements of g_l and G, respectively. Consequently, the effective channel gains of the legitimate user and eavesdropper are given by

$$\mathcal{G}_l = |g_l \Theta G|^2 = \left(\sum_{n=1}^{N} |g_{l,n}||G_n|\right)^2 \tag{3.0.3}$$

$$\mathcal{G}_e = |g_e \Theta G|^2 = \left(\sum_{n=1}^{N} g_{e,n} G_n e^{j\theta_n}\right)^2, \tag{3.0.4}$$

respectively. In the case of discrete phase shifts, the optimal phase shift θ_n is defined as

$$\theta_n = \arg\min_{\psi \in F2} |\psi - \theta_n|. \quad (5) \tag{3.0.5}$$

3.0.3 SNR and Achievable Rate

The signal-to-noise ratio (SNR) of the legitimate user and eavesdropper can be expressed as

$$\gamma_l = \frac{P_t \sum_{n=1}^{N} (|g_{l,n}||G_n|)^2}{\sigma_1^2}, \tag{3.0.6}$$

$$\gamma_e = \frac{P_t \sum_{n=1}^{N} |g_{e,n} G_n e^{j\theta_n}|^2}{\sigma_2^2}, \tag{3.0.7}$$

respectively. The achievable rates at the legitimate user and eavesdropper are given by

$$R_l = \log_2(1+\gamma_l) = \log_2\left(1 + \frac{P_t \sum_{n=1}^{N} |g_{l,n}|^2 |G_n|^2}{\sigma_1^2}\right), \tag{3.0.8}$$

$$R_e = \log_2(1+\gamma_e) = \log_2\left(1 + \frac{P_t \sum_{n=1}^{N} |g_{e,n} G_n e^{j\theta_n}|^2}{\sigma_2^2}\right), \tag{3.0.9}$$

3.0.4 Secrecy Rate and Outage Probability

The secrecy rate for transmitting confidential information to the UEs in the presence of an eavesdropper can be expressed as [45]

$$C_s = [R_l \,\breve{}\, R_e]^+ = \left[\log_2 (1+\gamma_l) - \log_2 (1+\gamma_e)\right]^+, \tag{3.0.10}$$

where $[z]^+ \triangleq \max(0, z)$.The secrecy outage probability (SOP) [37]is defined as

$$P_{out} = \mathbb{P}(C_s \leq \tau_s) \tag{3.0.11}$$

where τ_s is defined as the threshold rate under which the secure communication cannot be achieved.

3.0.5 Imperfect CSI

In order to achieve the optimal secrecy rate, perfect channel conditions are required; however, obtaining channel state information (CSI) of the eavesdropper is challenging in practice. Furthermore, the massive number of passive reconfigurable intelligent surface (RIS) elements without signal processing capability limits perfect CSI acquisition in an RIS-assisted system. Therefore, for accurate performance analysis, in this work, we assume imperfect CSI [[**ref21**]] [[**ref22**]], where the estimated channels G_b, b_{ge}, and b_{gl}

are modeled as follows:

$$G = \hat{G} + \epsilon_o, \tag{3.0.12}$$

$$g_l = \hat{g}_l + \epsilon_l, \tag{3.0.13}$$

$$g_e = \hat{g}_e + \epsilon_e, \tag{3.0.14}$$

where ϵ_μ is the channel estimation error of the respective links with $\mu \in \{o, l, e\}$, following the complex Gaussian distribution with mean 0 and variance σ_e^2, denoted by $\epsilon_\mu \sim \mathcal{CN}(0, \sigma_e^2)$.

3.0.6 Optimal Number of RIS Elements Given Practical Constraints

We formulate the secrecy rate maximization problem to evaluate the optimal number of RIS elements subject to two constraints, i.e. the secrecy rate should be greater than a threshold τ_s, and the number of RIS elements should be less than the maximum number of RIS elements N available.

$$\begin{aligned} \textbf{P:} \quad & \text{Maximize} \quad [R_l - R_e]^+ \\ \textbf{subject to:} \quad & \\ & \textbf{C1:} \quad [R_l - R_e]^+ \geq \tau_s \\ & \textbf{C2:} \quad N \leq N \end{aligned}$$

3.1 Performance Analysis of RIS-assisted downlink communication system

The simulation results demonstrate the impact of channel estimation error, RIS phase shift design, number of RIS elements, and transmit power on the secrecy rate of the proposed system. Unless mentioned otherwise, the simulation parameters are enlisted in Table 3.1

Fig.3.1 illustrates the secrecy rate with the change in number of RIS elements for the following cases: (i) Case-1: imperfect RIS-eavesdropper channel; (ii) Case-2: imperfect UAV-RIS and RIS-eavesdropper channels; (iii) Case-3: imperfect RISeavesdropper and RIS-legitimate user channels; (iv) Case-4: imperfect UAV-RIS, RIS-eavesdropper

Table 3.1: Simulation Parameters

Parameters	Values
UAV's transmit power P_t	50 dBm
Channel estimation error variance	$\sigma_{\epsilon o}$ 0.1
Channel estimation error variance	$\sigma_{\epsilon l}$ 0.1
Channel estimation error variance	$\sigma_{\epsilon e}$ 1
Number of RIS elements	N 50
Discrete phase shift level	M 32
Noise power	$\sigma_1 = \sigma_2$ -60 dBm

and RIS-legitimate user channels. It can be observed as the number of RIS elements increases, the secrecy rate increases for all four cases. Moreover, the highest secrecy rate is achieved when only the RIS-eavesdropper's channel is imperfect, and the secrecy performance degrades as the number of imperfect channels increases. In addition, the Case-2 achieves better secrecy rate than the Case-3, which indicates that the interference due to the imperfect RIS to legitimate user's channel is more than the interference due to the imperfect UAV to RIS channel. Hence, to achieve a higher secrecy rate, the RIS to legitimate user's channel must be estimated accurately.

Fig.3.2 illustrates the secrecy rate with increase in transmit power for imperfect RIS-eavesdropper channel, imperfect RISlegitimate user and RIS-eavesdropper channels, imperfect UAVRIS, RIS-eavesdropper and RIS-legitimate user channels. It can be observed that with an increase in transmit power the secrecy rate will be increase. Secrecy rate for the imperfect RIS-eavesdropper channel will be highest as compared to the imperfect RIS-legitimate user and RIS-eavesdropper channels, imperfect UAV-RIS, RIS-eavesdropper and RIS-legitimate user channels. It can be observed that if the channel estimation between the RIS- legitimate user is not accurate then increasing the transmit power will not enhance the system performance.

Fig.3.3 illustrates the impact of increasing the variance of estimation channel on the secrecy rate with imperfect channel conditions on the eavesdropper and legitimate user respectively. This result proves the claim that the the estimation of the channel between the RIS and legitimate user must be accurate in order to acheive high secrecy rate.

Fig.3.4 illustrates the impact of increasing the number of RIS elements and transmit

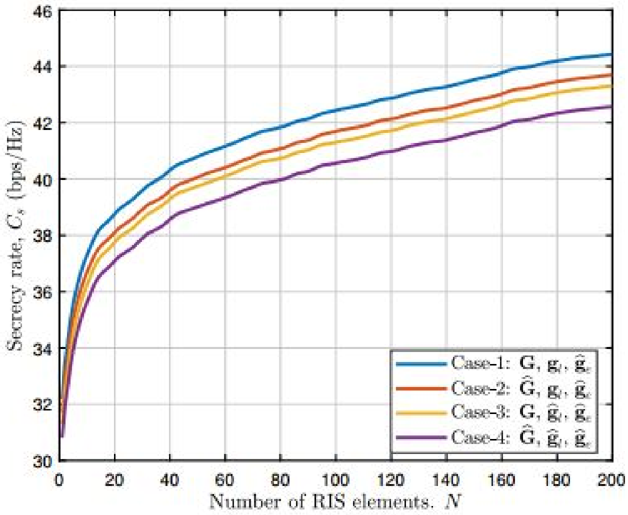


Figure 3.2: Secrecy rate versus the number of RIS elements with different cases of imperfect CSI.

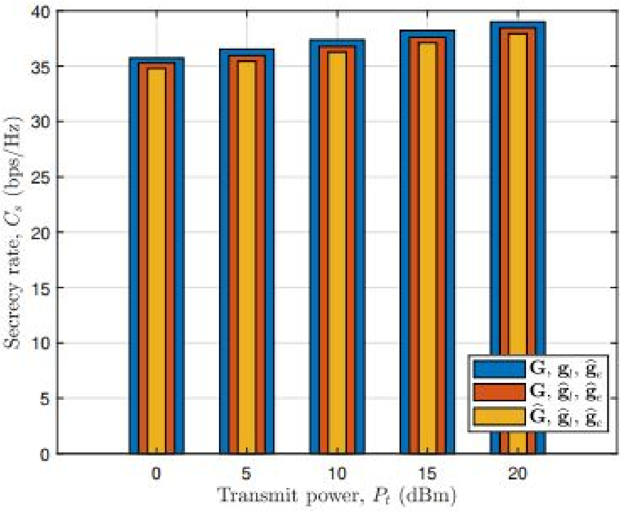


Figure 3.3: Secrecy rate for varying transmit power under different cases of imperfect CSI for N=10

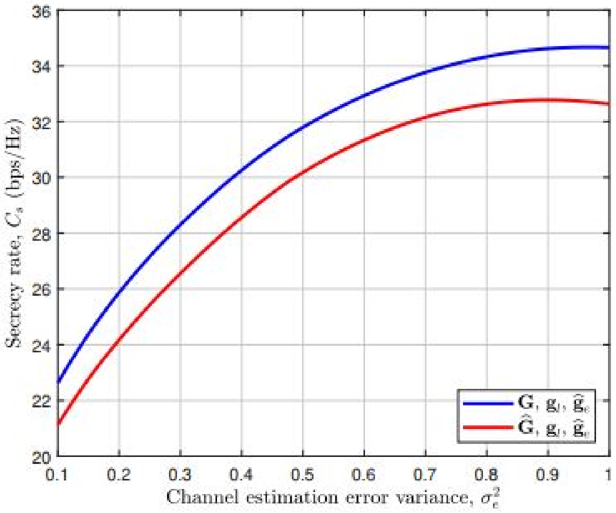


Figure 3.4: Secrecy rate versus variance of estimated channel.

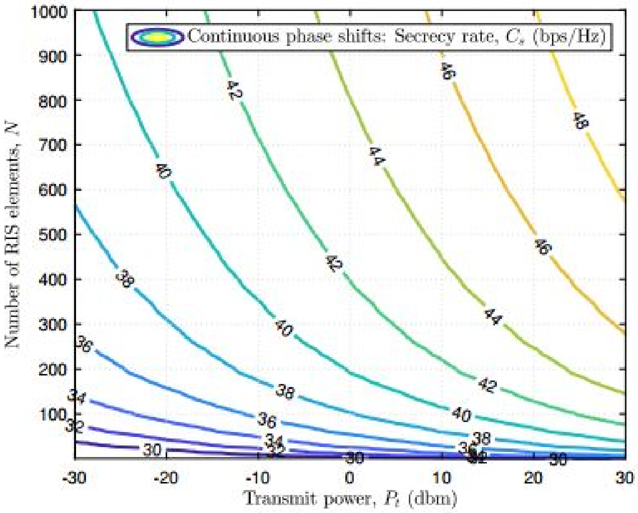


Figure 3.5: Secrecy rate for varying number of elements and transmit power under imperfect RIS to eavesdropper channel.

power on the secrecy rate for the imperfect channel conditions at the RIS-eavesdropper link. First, it can be observed that for a given transmit power, the secrecy rate increases with the increase in the number of RIS elements. Second, the required secrecy rate can be achieved at a reduced transmit power by increasing the number of RIS elements. For instance, for the secrecy rate requirement of 40 bps/Hz, a transmit power of -10 dBm is required for 300 RIS elements, while this value reduces to about -20 dBm for 500 elements.

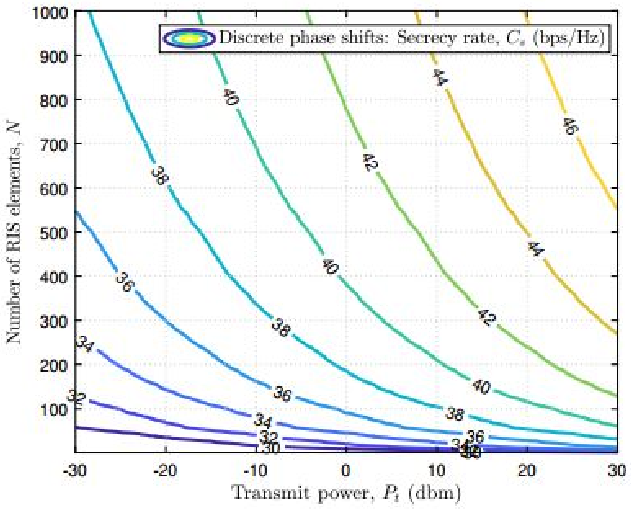


Figure 3.6: Secrecy rate for varying number of elements and transmit power under imperfect RIS to eavesdropper channel with discrete phase.

Fig.3.5 illustrates the impact of increasing the number of RIS elements and transmit power on the secrecy rate for the imperfect channel conditions at the RIS-eavesdropper link with discrete phase shifts. In comparison with the continuous phase shifts illustrated in Fig.2 for the secrecy rate requirement of 40 bps/Hz, a transmit power of 0 dBm is required for 400 RIS elements, while this value reduces to about -10 dBm for 700 elements.

Fig.3.6 illustrates the impact of increasing the variance of estimation channel on the secrecy rate with imperfect RISeavesdropper channel and imperfect UAV-RIS channel with continuous and discrete phase shifts respectively. The result proves that the secrecy rate with discrete phase shifts decrease in comparison with the continuous phase shifts.

Fig.3.7 illustrates the secrecy rate with the change in number of RIS elements for imperfect RIS-eavesdropper channel, imperfect UAV-RIS, RIS-eavesdropper and RIS-

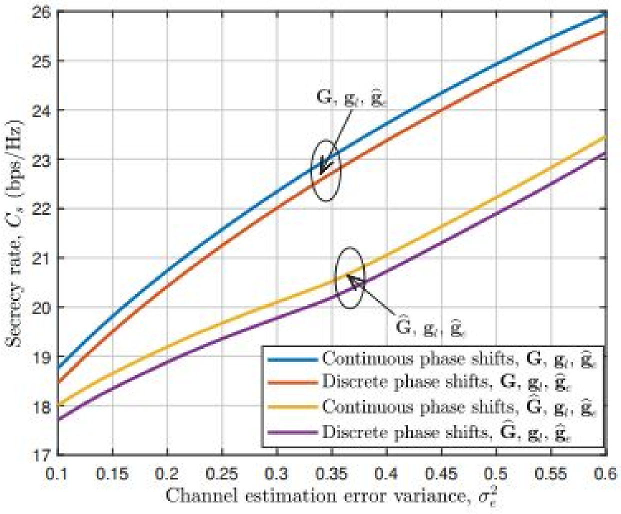


Figure 3.7: Secrecy rate versus variance of estimated channel with discrete phase shifts.

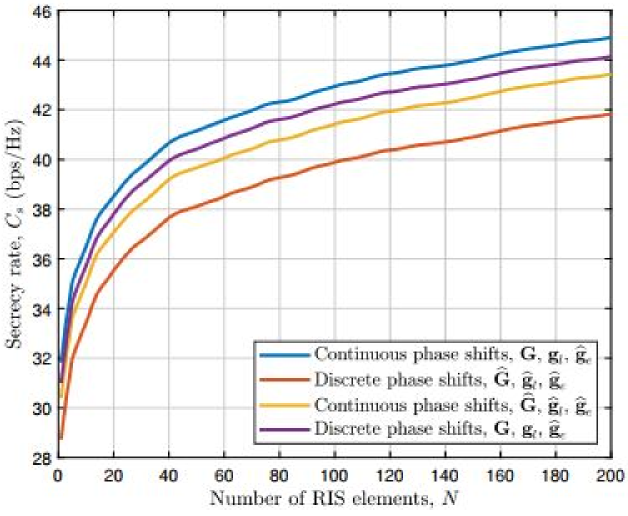


Figure 3.8: Secrecy rate versus the number of RIS elements with different cases of imperfect CSI with discrete phase shifts.

legitimate user channels under continuous and discrete phase shifts. It can be observed that the secrecy rate decrease with discrete phase shifts in comparison with the continuous phase shifts for imperfect RIS-eavesdropper channel and for imperfect UAV-RIS, RIS-eavesdropper and RIS-legitimate user channels. Hence the discrete phase shifts decrease the system performance.

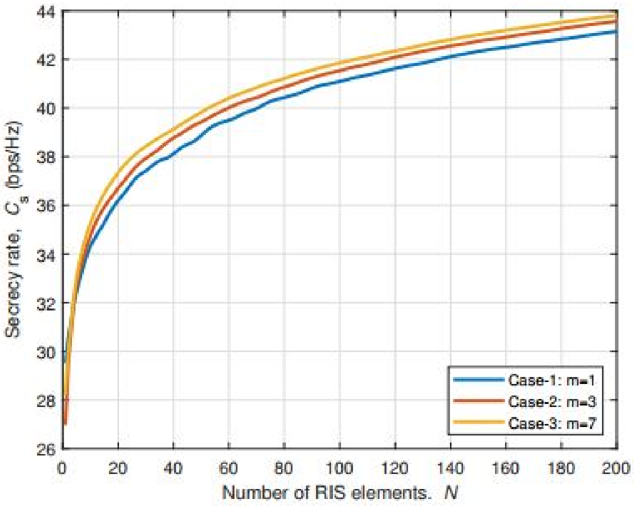


Figure 3.9: Secrecy rate versus the number of RIS elements under Nakagami-m fading.

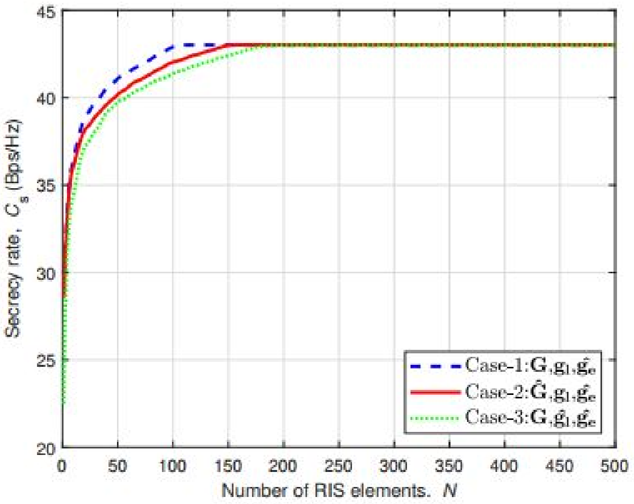
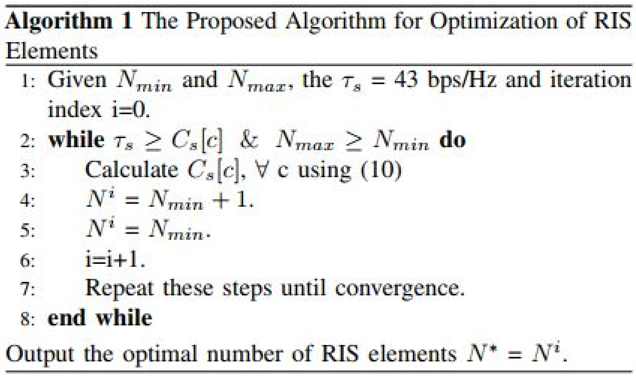


Figure 3.10: Convergence of the proposed algorithm under different cases of imperfect CSI for $\sigma_{\epsilon o} = \sigma_{\epsilon l} = 0.5$.

Fig.3.8 illustrates the secrecy rate with change in number of RIS elements for imperfect RIS-eavesdropper's channel under Nakagami-m fading. It can be observed that for m=1 i.e., for Rayleigh the secrecy rate will be less as compared to m¿1 because of the increase in Line of Sight (LOS) components.



Algorithm 1 The Proposed Algorithm for Optimization of RIS Elements

```
Given $N_{min}$ and $N_{max}$, the $\tau_s$ = 43 bps/Hz and iteration
index i=0.
while $\tau_s \geq C_s[c]$ & $N_{max} \geq N_{min}$ do
    Calculate $C_s[c]$, $\forall$ c using (10)
    $N^i = N_{min} + 1$.
    $N^i = N_{min}$.
    i=i+1.
    Repeat these steps until convergence.
end while
Output the optimal number of RIS elements $N^* = N^i$.
```

Figure 3.11: Algorithm to Solve Maximization Problem

Fig.3.9 illustrates the Convergence of the proposed algorithm for imperfect RIS-eavesdropper channel, imperfect UAVRIS and RIS-eavesdropper channels, imperfect RIS-legitimate user and RIS-eavesdropper channels. It can be observed that for a given secrecy rate of 43 bps/Hz the optimal number of RIS elements required are 105 for imperfect RIS-eavesdropper channel while the number of RIS elements are increased to 152 for imperfect UAV-RIS and RIS-eavesdropper channels.Moreover, 190 RIS elements are required imperfect RIS legitimate user and RIS-eavesdropper channels. This result also proof the claim that the estimation of the channel between the RIS and legitimate user must be accurate to have better secrecy rate.

Chapter 4

RIS-enhanced Uplink NOMA communication system

As illustrated in Fig. 4.1, we consider an RIS-assisted uplink NOMA network, where two single antenna UEs, denoted by UE1 and UE2, intend to deliver confidential information,x_1 and x_2, respectively, to a single antenna BS in the presence of an eavesdropper with the aid of N passive reconfigurable elements of an RIS, denoted by $\mathcal{N} = \{1, 2, \ldots, N\}$.

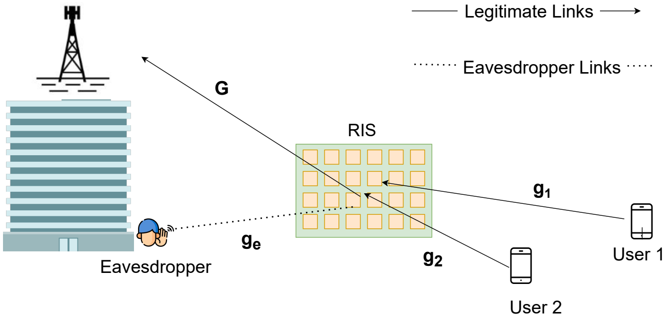


Figure 4.1: An illustration of secure RIS-enhanced uplink communication system.

4.0.1 Channel Model

Without the loss of generality, all channels are characterized by distance-dependent path loss and small-scale fading. The distance-dependent path loss is modeled as $L(d_x) = d_x^{-\alpha}$ where $\epsilon = \{G, g_1, g_2, g_e\}$, d_x and α denotes the distance and path loss exponent of the corresponding links respectively. In order to incorporate the small-scale fading we assume Nakagami-m fading distribution with fading parameter m. The probability desnsity function (PDF) for Nakagami-m fading is given as

$$f(y;m) = \frac{m^m y^{m-1}}{\Gamma(m)} e^{-my}, \forall y > 0, \tag{4.0.1}$$

where $\Gamma(u) = \int_0^\infty \nu^{u-1} e^{-\nu}\, d\nu$ denotes the Gamma function.

4.0.2 SINR and Achievable Rate

Based on the conventional uplink NOMA scheme, the BS first decodes the signal of strong UE in the NOMA pair. Without loss of generality, in this work, we assume that the UE1 is stronger than the UE2. Thus, the received signal-to-interference-plus-noise ratio at the BS and eavesdropper to decode x_1 can be expressed as

$$\gamma_1 = \frac{\frac{P_1}{(d_G d_{g_l})^\alpha} \left(\sum_{n=1}^N |G_n|\,|g_{l,n}|\right)^2}{\frac{P_o}{(d_G d_{g_l})^\alpha} \left(\sum_{n=1}^N |G_n|\,|g_{o,n}|\right)^2 + \sigma_l^2}, \tag{4.0.2}$$

and

$$\gamma_{l_e} = \frac{\frac{P_1}{(d_G d_{g_e})^\alpha} \left|\sum_{n=1}^N G_n g_{e,n} e^{j\theta_n}\right|^2}{\frac{P_o}{(d_G d_{g_e})^\alpha} \left|\sum_{n=1}^N G_n g_{e,n} e^{j\theta_n}\right|^2 + \sigma_e^2}, \tag{4.0.3}$$

respectively. Then, the BS and eavesdropper can eliminate the x_1 and decode x_2 without interference. The received signal to noise ratio the BS and eavesdropper to decode x_2 can be expressed as

$$\gamma_o = \frac{\frac{P_1}{(d_G d_{g_o})^{-\alpha}} \left(\sum_{n=1}^N |G_n|\,|g_{o,n}|\right)^2}{\sigma_l^2}, \tag{4.0.4}$$

and

$$\gamma_{o_e} = \frac{\frac{P_1}{(d_G d_{g_e})^{-\alpha}} \left|\sum_{n=1}^N G_n g_{e,n} e^{j\theta_n}\right|^2}{\sigma_e^2}, \tag{4.0.5}$$

The achievable rates at the UEs and eavesdropper are given by

$$R_l = \log_2\left(1 + \frac{\frac{P_1}{(d_G d_{g_l})^\alpha} \left(\sum_{n=1}^N |G_n|\,|g_{l,n}|\right)^2}{\frac{P_o}{(d_G d_{g_l})^\alpha} \left(\sum_{n=1}^N |G_n|\,|g_{o,n}|\right)^2 + \sigma_l^2}\right), \tag{4.0.6}$$

$$R_o = \log_2\left(1 + \frac{\frac{P_1}{(d_G d_{g_o})^\alpha} \left(\sum_{n=1}^N |G_n|\,|g_{o,n}|\right)^2}{\sigma_l^2}\right), \tag{4.0.7}$$

and

$$R_{l_e} = \log_2\left(1 + \frac{\frac{P_1}{(d_G d_{g_e})^\alpha} \left|\sum_{n=1}^N G_n g_{e,n} e^{j\theta_n}\right|^2}{\frac{P_o}{(d_G d_{g_e})^\alpha} \left|\sum_{n=1}^N G_n g_{e,n} e^{j\theta_n}\right|^2 + \sigma_e^2}\right), \tag{4.0.8}$$

,

$$R_{l_e} = \log_2 \left(1 + \frac{\frac{P_1}{(d_G d_{g_e})^{\alpha}} \left| \sum_{n=1}^{N} G_n g_{e,n} e^{j\theta_n} \right|^2}{\sigma_e^2} \right). \tag{4.0.9}$$

4.0.3 Secrecy Rate and Outage Probability

The secrecy rate for transmitting confidential information to the UEs in the presence of an eavesdropper can be expressed as [46].

$$C_{\rho_s} = [R_{\rho}\,\check{}\,R_{\rho_e}]^{+} = \left[\log_2 (1 + \gamma_{\rho}) - \log_2 (1 + \gamma_{\rho e})\right]^{+}, \tag{4.0.10}$$

where $[z]^{+} \triangleq \max(0, z)$ and $\rho \in \{1, 2, e\}$. The secrecy outage probability (SOP) [37] is defined as

$$P_{out} = \mathbb{P}\left(C_s \leq \tau_s\right) \tag{4.0.11}$$

where τ_s is defined as the threshold rate under which the secure communication cannot be achieved.

4.0.4 RIS configuration and Element Splitting

We assume that N RIS elements are split [30] between two UEs, i.e., a total of N_1 elements coherently combine the signal of UE1, based on that we can define the split factor γ as,

$$\gamma = \frac{N_1}{N} \tag{4.0.12}$$

while a total of N_2 elements coherently combine the signal of UE2,

$$N_2 = N - [\gamma N] \tag{4.0.13}$$

Therefore, the RIS terms for UEs can be written as

$$\left| \mathbf{G}^{H} \Theta \mathbf{g}_{\rho} \right|^2 = \underbrace{\left(\sum_{n=1}^{N_1} |G_n| \, |g_{\rho,n}| \right)^2}_{\text{Coherently Combined}} + \underbrace{\left| \sum_{n=N_2}^{N} g_{\rho,n} G_n e^{j\theta_n} \right|^2}_{\text{Randomly Combined}}, \tag{4.0.14}$$

where $\rho \in \{1, 2\}$.The set of elements which are not configured for ρ^{th}-UE will result in the random combining of its phases.

4.1 Performance analysis of RIS-enhanced Uplink NOMA communication system

In this section, we evaluate the secrecy performance of the RIS-enhanced uplink-NOMA communication system under Nakagami-m fading via monte carlo simulations. The simulation results demonstrate the impact of transmit power of UE's, distances of eavesdropper and UE's and the split factor on the secrecy rate and secrecy outage of the system. The simulation parameters, unless otherwise specified, are presented in Table 4.1.

Table 4.1: Simulation Parameters

Parameters	**Values**
Transmit power for far user UE1	P_1 = 40 dBm
Transmit power for near user UE2	P_2 = 40 dBm
Distance of base station from RIS	$d_b = 15$
Distance of eavesdropper from RIS	$d_e = 15$
Distance of far user from RIS	$d_1 = 15$
Distance of near user from RIS	$d_2 = 5$
Split factor	$\gamma = 0.28$
Path Loss exponent	$\alpha = 2.4$
Noise power	$\sigma_b^2 = \sigma_e^2$ = -1 dBm

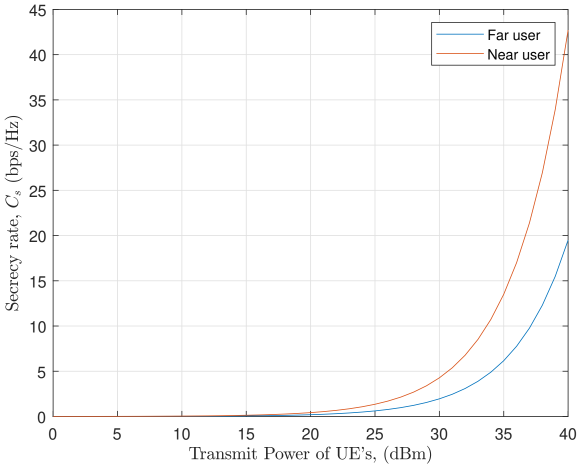


Figure 4.2: Secrecy rate under split factor = 0.28.

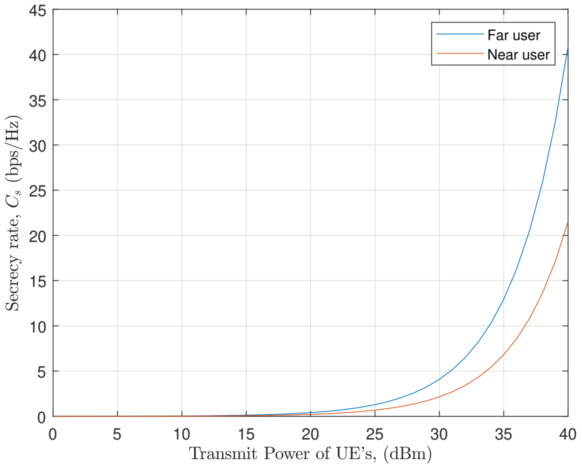


Figure 4.3: Secrecy rate under split factor = 0.64.

4.1.1 Impact of Transmit Power of UEs

Fig. 4.2 and Fig. 4.3 illustrates the secrecy rate with an increase in transmit power of UE's with different number of RIS elements for near and far user. First, it can be observed with an increase in transmit power of UE's the secrecy rate will increase. Second, if the number of RIS elements for near user is greater than the far user the secrecy rate for the near user will be greater than far user illustrated in fig. 4.2 while secrecy rate for the far user will be greater than near user if the RIS elements for far user is greater then near user illustrated in fig. 4.3.

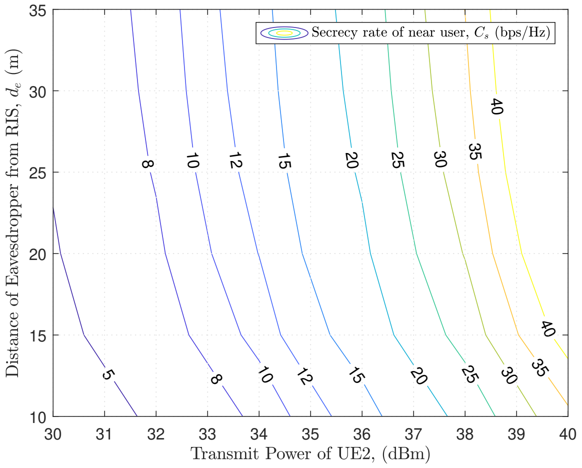


Figure 4.4: Secrecy rate for varying transmit power of UE's and distance of eavesdropper from RIS..

4.1.2 Impact of Transmit Power of UEs and distance of eavesdropper and far user from RIS

Fig. 4.4 and Fig. 4.5 illustrates the impact of transmit power of UE's and distance of the eavesdropper from RIS on the secrecy rate of near and far user respectively. It can be observed that with an increase in the transmit power of UE's and distance of the eavesdropper from RIS the secrecy rate will increase for both users.

Fig. 4.6 illustrates the impact of transmit power for UE2 and distance of the far user from RIS on the secrecy rate of the far user. First, we can observe that the secrecy rate for the far user will decrease with an increase in the distance of far user from the RIS. Second, if want to achieve a particular secrecy rate with increase in distance of far user

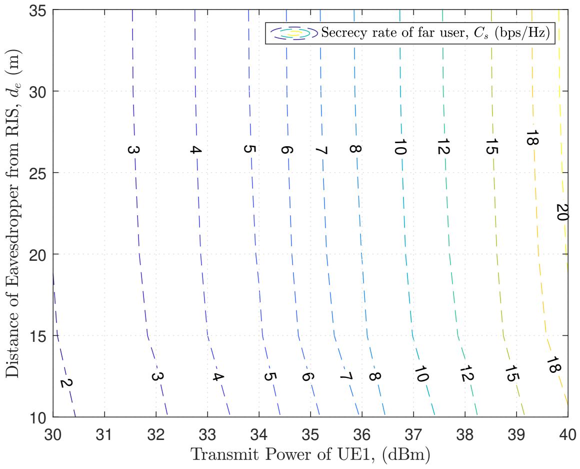


Figure 4.5: Secrecy rate for varying transmit power of UE's and distance of eavesdropper from RIS.

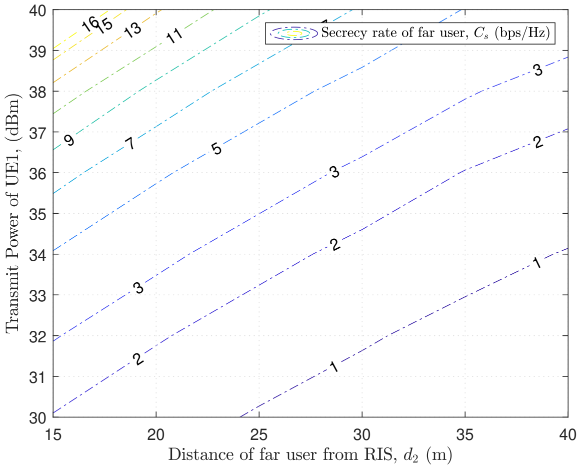


Figure 4.6: Secrecy rate for varying transmit power of UE's and distance of far user from RIS.

we have to increase the transmit power of UE2. For instance, we have secrecy rate of 9 bps/Hz for transmit power of 37 dBm at distance of 15 m from RIS, we have to increase the transmit power to 40 dBm to achieve the same secrecy rate at 25 m.

4.1.3 Impact of split factor and transmit power of UE's

Fig. 4.7 illustrates the impact of split factor on the secrecy rate of UE's. We can observe that with an increase in the split factor the number of elements for the far user is greater than the number of elements for the near user, the secrecy rate of the far user is greater than the secrecy rate of the near user.

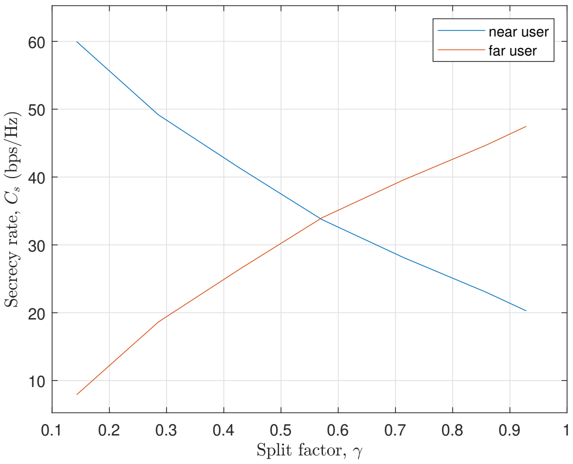


Figure 4.7: Secrecy rate for varying split factor.

Fig. 4.8 illustrates the impact of split factor and transmit power of UE's on the secrecy rate of near and far user. We can observe that with an increase in the split factor, we have to increase the power to achieve the particular secrecy rate for near user. For instance, we can achieve secrecy rate of 15 bps/Hz for near user and 10 bps/Hz for far user at split factor of 0.4 and transmit power of 36 dBm while if we have to achieve the secrecy rate of 15 bps/Hz for the near user at split factor of 0.8 we have to increase the transmit power to 38 dBm at which the secrecy rate of far user will be 30 bps/Hz.

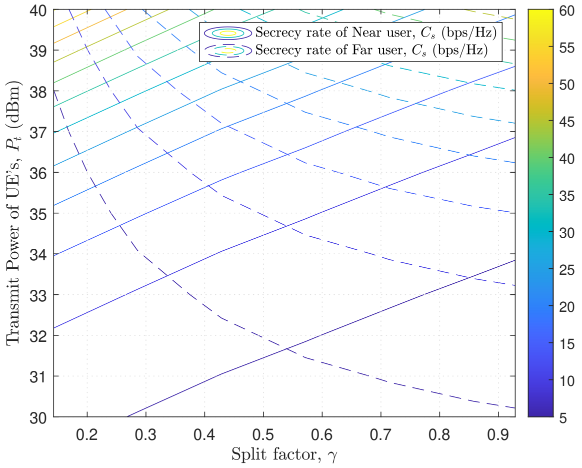


Figure 4.8: Secrecy rate for varying split factor of transmit power of UE's.

4.1.4 Impact of transmit power of UE's on Secrecy Outage Probability (SOP)

Fig. 4.9 illustrates the impact of transmit power of UE's on secrecy outage probability (SOP) of UE's at threshold of 5 bps/Hz and 15 bps/Hz respectively. First, we can observe that with the increase in the threshold τ_s the outage probability increases, second the outage probability of the near user is less than far user as the number of RIS elements for the near user is greater than far user.

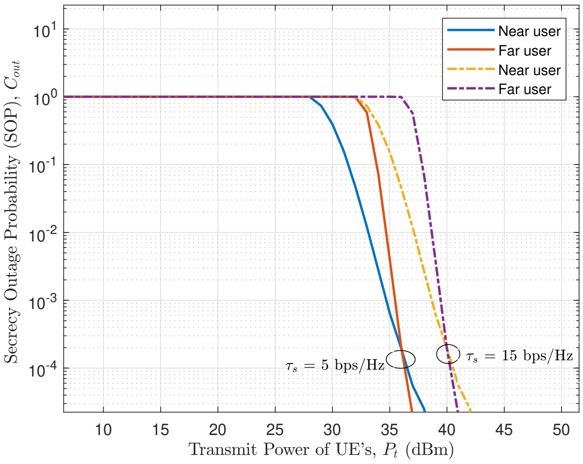


Figure 4.9: Secrecy outage for varying transmit power of UE's.

Chapter 5

Conclusion and Future Directions

In RIS-enhanced aerial communication system, we investigated the secrecy performance of an RIS-assisted aerial communication system under imperfect channel conditions at UAV to RIS link, RIS to eavesdropper link, and RIS to legitimate user link. Our simulation results demonstrated that the secrecy rate can be improved through better channel estimation, and increasing the number of RIS elements or transmit power. Moreover, our results revealed that the errors due to the imperfect channel estimation of the RISlegitimate user's link and discrete phase shifts highly reduce the secrecy rate, thus highlighting the importance of better channel estimation of particularly RIS to legitimate user's channel.

Whereas, in case of RIS-enhanced uplink NOMA communication system, our simulation result demonstrated the impact of transmit power with different split factor, distance between the RIS and eavesdropper, distance of UEs from RIS, path loss exponent, split factor on secrecy rate and the impact of transmit power on the secrecy outage probability. Moreover, our results revealed that with the increase in the distance of the eavesdropper from RIS the secrecy rate will increase and with the decrease in the distance of UEs and RIS the secrecy rate will decrease, also if we increase the path loss exponent for UEs we have to increase the transmit power to achieve a good secrecy rate.

In the future, theoretical expressions of the secrecy rate and secrecy outage probability (SOP) can be evaluated to evaluate the system performance.

Bibliography

[1] Ashish Khisti and Gregory W Wornell. "Secure transmission with multiple antennas—Part II: The MIMOME wiretap channel". In: *IEEE Transactions on Information Theory* 56.11 (2010), pp. 5515–5532.

[2] Rongqing Zhang et al. "Physical layer security for two way relay communications with friendly jammers". In: *2010 IEEE global telecommunications conference GLOBECOM 2010*. IEEE. 2010, pp. 1–6.

[3] Yi-Sheng Shiu et al. "Physical layer security in wireless networks: A tutorial". In: *IEEE wireless Communications* 18.2 (2011), pp. 66–74.

[4] Xiaojun Tang et al. "Interference assisted secret communication". In: *IEEE Transactions on Information Theory* 57.5 (2011), pp. 3153–3167.

[5] Arsenia Chorti et al. "Physical layer security in wireless networks with passive and active eavesdroppers". In: *2012 IEEE Global Communications Conference (GLOBECOM)*. IEEE. 2012, pp. 4868–4873.

[6] Eun-Kyu Lee, Mario Gerla, and Soon Y Oh. "Physical layer security in wireless smart grid". In: *IEEE Communications Magazine* 50.8 (2012), pp. 46–52.

[7] Xiaojun Sun et al. "Performance of secure communications over correlated fading channels". In: *IEEE Signal Processing Letters* 19.8 (2012), pp. 479–482.

[8] Jinho Choi, Jeongseok Ha, and Hyoungsuk Jeon. "Physical layer security for wireless sensor networks". In: *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. IEEE. 2013, pp. 1–6.

[9] Sean Victor Hum and Julien Perruisseau-Carrier. "Reconfigurable reflectarrays and array lenses for dynamic antenna beam control: A review". In: *IEEE transactions on antennas and propagation* 62.1 (2013), pp. 183–198.

[10] Nobuhide Nonaka, Yoshihisa Kishiyama, and Kenichi Higuchi. "Non-orthogonal multiple access using intra-beam superposition coding and SIC in base station cooperative MIMO cellular downlink". In: *2014 IEEE 80th vehicular technology conference (VTC2014-Fall)*. IEEE. 2014, pp. 1–5.

[11] Walid Saad et al. "On the physical layer security of backscatter wireless systems". In: *IEEE transactions on wireless communications* 13.6 (2014), pp. 3442–3451.

[12] Z Esat Ankaralı et al. "Physical layer security for wireless implantable medical devices". In: *2015 IEEE 20th International Workshop on Computer Aided Modelling and Design of Communication Links and Networks (CAMAD)*. IEEE. 2015, pp. 144–147.

[13] Johannes Richter et al. "Weak secrecy in the multiway untrusted relay channel with compute-and-forward". In: *IEEE Transactions on Information Forensics and Security* 10.6 (2015), pp. 1262–1273.

[14] Leonardo Jimenez Rodriguez et al. "Physical layer security in wireless cooperative relay networks: State of the art and beyond". In: *IEEE Communications Magazine* 53.12 (2015), pp. 32–39.

[15] Nan Yang et al. "Safeguarding 5G wireless communication networks using physical layer security". In: *IEEE Communications Magazine* 53.4 (2015), pp. 20–27.

[16] Yulong Zou et al. "Improving physical-layer security in wireless communications using diversity techniques". In: *IEEE Network* 29.1 (2015), pp. 42–48.

[17] Amal Hyadi, Zouheir Rezki, and Mohamed-Slim Alouini. "An overview of physical layer security in wireless communication systems with CSIT uncertainty". In: *IEEE Access* 4 (2016), pp. 6121–6132.

[18] Junqing Zhang et al. "Experimental study on key generation for physical layer security in wireless communications". In: *IEEE Access* 4 (2016), pp. 4464–4477.

[19] Senglee Foo. "Liquid-crystal reconfigurable metasurface reflectors". In: *2017 IEEE International Symposium on Antennas and Propagation & USNC/URSI National Radio Science Meeting*. IEEE. 2017, pp. 2069–2070.

[20] Yan Huo et al. "Jamming strategies for physical layer security". In: *IEEE Wireless Communications* 25.1 (2017), pp. 148–153.

[21] Kun Wang et al. “Strategic antieavesdropping game for physical layer security in wireless cooperative networks”. In: *IEEE Transactions on Vehicular Technology* 66.10 (2017), pp. 9448–9457.

[22] Sha Hu, Fredrik Rusek, and Ove Edfors. “Beyond massive MIMO: The potential of data transmission with large intelligent surfaces”. In: *IEEE Transactions on Signal Processing* 66.10 (2018), pp. 2746–2758.

[23] Christos Liaskos et al. “A new wireless communication paradigm through software-controlled metasurfaces”. In: *IEEE Communications Magazine* 56.9 (2018), pp. 162–169.

[24] Jie Tang et al. “Impact of mobility on physical layer security over wireless fading channels”. In: *IEEE Transactions on Wireless Communications* 17.12 (2018), pp. 7849–7864.

[25] Jie Tang et al. “Optimization for maximizing sum secrecy rate in SWIPT-enabled NOMA systems”. In: *IEEE Access* 6 (2018), pp. 43440–43449.

[26] Yongpeng Wu et al. “A survey of physical layer security techniques for 5G wireless networks and challenges ahead”. In: *IEEE Journal on Selected Areas in Communications* 36.4 (2018), pp. 679–695.

[27] Wei Zhang et al. “Artificial-noise-aided optimal beamforming in layered physical layer security”. In: *IEEE Communications Letters* 23.1 (2018), pp. 72–75.

[28] Miao Cui, Guangchi Zhang, and Rui Zhang. “Secure wireless communication via intelligent reflecting surface”. In: *IEEE Wireless Communications Letters* 8.5 (2019), pp. 1410–1414.

[29] Chongwen Huang et al. “Reconfigurable intelligent surfaces for energy efficiency in wireless communication”. In: *IEEE transactions on wireless communications* 18.8 (2019), pp. 4157–4170.

[30] Hong Shen et al. “Secrecy rate maximization for intelligent reflecting surface assisted multi-antenna communications”. In: *IEEE Communications Letters* 23.9 (2019), pp. 1488–1492.

[31] Xiaofang Sun et al. “Physical layer security in UAV systems: Challenges and opportunities”. In: *IEEE Wireless Communications* 26.5 (2019), pp. 40–47.

[32] Qingqing Wu and Rui Zhang. “Towards smart and reconfigurable environment: Intelligent reflecting surface aided wireless network”. In: *IEEE communications magazine* 58.1 (2019), pp. 106–112.

[33] Xianghao Yu, Dongfang Xu, and Robert Schober. “Enabling secure wireless communications via intelligent reflecting surfaces”. In: *2019 IEEE Global Communications Conference (GLOBECOM)*. IEEE. 2019, pp. 1–6.

[34] Marco Di Renzo et al. “Reconfigurable intelligent surfaces vs. relaying: Differences, similarities, and performance comparison”. In: *IEEE Open Journal of the Communications Society* 1 (2020), pp. 798–807.

[35] Marco Di Renzo et al. “Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and the road ahead”. In: *IEEE journal on selected areas in communications* 38.11 (2020), pp. 2450–2525.

[36] Mohamed A ElMossallamy et al. “Reconfigurable intelligent surfaces for wireless communications: Principles, challenges, and opportunities”. In: *IEEE Transactions on Cognitive Communications and Networking* 6.3 (2020), pp. 990–1002.

[37] Keming Feng et al. “Physical layer security enhancement exploiting intelligent reflecting surface”. In: *IEEE Communications Letters* 25.3 (2020), pp. 734–738.

[38] Chandan Pradhan et al. “Reconfigurable intelligent surface (RIS)-enhanced two-way OFDM communications”. In: *IEEE Transactions on Vehicular Technology* 69.12 (2020), pp. 16270–16275.

[39] Sarah Basharat et al. “Reconfigurable intelligent surfaces: Potentials, applications, and challenges for 6G wireless networks”. In: *IEEE Wireless Communications* 28.6 (2021), pp. 184–191.

[40] Qin Chen et al. “Impact of residual hardware impairment on the IoT secrecy performance of RIS-assisted NOMA networks”. In: *IEEE Access* 9 (2021), pp. 42583–42592.

[41] Yuanwei Liu et al. “Reconfigurable Intelligent Surfaces: Principles and Opportunities”. In: *IEEE Communications Surveys Tutorials* 23.3 (2021), pp. 1546–1577. doi: 10.1109/COMST.2021.3077737.

[42] Munyaradzi Munochiveyi et al. “Reconfigurable intelligent surface aided multi-user communications: State-of-the-art techniques and open issues”. In: *IEEE Access* 9 (2021), pp. 118584–118605.

[43] Cunhua Pan et al. “Reconfigurable intelligent surfaces for 6G systems: Principles, applications, and research directions”. In: *IEEE Communications Magazine* 59.6 (2021), pp. 14–20.

[44] R Pradeep and R Kanimozhi. “Hardware Efficient Architectural Design for Physical Layer Security in Wireless Communication”. In: *Wireless Personal Communications* 120.2 (2021), pp. 1821–1836.

[45] Feng Shu et al. “Enhanced secrecy rate maximization for directional modulation networks via IRS”. In: *IEEE Transactions on Communications* 69.12 (2021), pp. 8388–8401.

[46] Bashar Tahir, Stefan Schwarz, and Markus Rupp. “Outage analysis of uplink IRS-assisted NOMA under elements splitting”. In: *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*. IEEE. 2021, pp. 1–5.

[47] Zhiqing Tang et al. “A novel design of RIS for enhancing the physical layer security for RIS-aided NOMA networks”. In: *IEEE Wireless Communications Letters* 10.11 (2021), pp. 2398–2401.

[48] Imène Trigui, Wessam Ajib, and Wei-Ping Zhu. “Secrecy outage probability and average rate of RIS-aided communications using quantized phases”. In: *IEEE Communications Letters* 25.6 (2021), pp. 1820–1824.

[49] Yongjun Xu et al. “RIS-enhanced WPCNs: Joint radio resource allocation and passive beamforming optimization”. In: *IEEE Transactions on Vehicular Technology* 70.8 (2021), pp. 7980–7991.

[50] Xiaojun Yuan et al. “Reconfigurable-intelligent-surface empowered wireless communications: Challenges and opportunities”. In: *IEEE wireless communications* 28.2 (2021), pp. 136–143.

[51] Gui Zhou et al. “User cooperation for RIS-aided secure SWIPT MIMO systems under the passive eavesdropping”. In: *2021 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*. IEEE. 2021, pp. 171–176.

[52] Xingwang Li et al. “Enhancing secrecy performance for STAR-RIS NOMA networks”. In: *IEEE Transactions on Vehicular Technology* 72.2 (2022), pp. 2684–2688.

[53] Parisa Ramezani, Bin Lyu, and Abbas Jamalipour. “Toward RIS-enhanced integrated terrestrial/non-terrestrial connectivity in 6G”. In: *IEEE Network* (2022).

[54] Zhiqing Tang et al. “Physical layer security of intelligent reflective surface aided NOMA networks”. In: *IEEE Transactions on Vehicular Technology* 71.7 (2022), pp. 7821–7834.

[55] Georgios C Trichopoulos et al. “Design and evaluation of reconfigurable intelligent surfaces in real-world environment”. In: *IEEE Open Journal of the Communications Society* 3 (2022), pp. 462–474.

[56] Yuhong Wang and Jingyi Peng. “Physical-Layer Secure Wireless Transmission via Active Reconfigurable Intelligent Surfaces”. In: *2022 IEEE 4th International Conference on Power, Intelligent Computing and Systems (ICPICS)*. IEEE. 2022, pp. 285–289.

[57] Sree Krishna Das et al. “Comprehensive review on ML-based RIS-enhanced IoT systems: basics, research progress and future challenges”. In: *Computer Networks* 224 (2023), p. 109581.

[58] Yasin Khan and Ankit Dubey. “On the Effect of Phase Error on Physical Layer Security of RIS-Aided NOMA Network”. In: *2023 National Conference on Communications (NCC)*. IEEE. 2023, pp. 1–6.

[59] Saeid Pakravan et al. “Physical Layer Security for NOMA Systems: Requirements, Issues, and Recommendations”. In: *IEEE Internet of Things Journal* (2023).

[60] Xintong Qin et al. “Joint Resource Allocation and Configuration Design for STAR-RIS-Enhanced Wireless-Powered MEC”. In: *IEEE Transactions on Communications* 71.4 (2023), pp. 2381–2395.

[61] Liang Yang et al. “Covert Transmission and Secrecy Analysis of RS-RIS-NOMA-Aided 6 G Wireless Communication Systems”. In: *IEEE Transactions on Vehicular Technology* (2023).

[62] Qian Zhang et al. “Robust Beamforming Design for RIS-Aided NOMA Secure Networks with Transceiver Hardware Impairments”. In: *IEEE Transactions on Communications* (2023).