Department of Information Engineering and Computer Science

Master's Degree in
Computer Science

Final Dissertation

MIMO physical layer security using multiple Reconfigurable Intelligence Surfaces

A study in vehicular environments

Supervisor
Segata Michele

Co-Supervisor
Casari Paolo

Student
Marrocco Simone

Academic year 2024/2025

Acknowledgements

...thanks to...

Contents

Abstract

This paper presents an extension of physical layer security techniques using Reconfigurable Intelligent Surfaces (RISs) in Multiple-Input Multiple-Output (MIMO) communications. Building upon previous work on secure transmissions, we generalize the mathematical framework to support multiple legitimate receivers and complex RIS configurations and combinations, including parallel and in-series reflections. Our approach maintains low error rates for legitimate users while ensuring high levels of artificial noise for eavesdroppers, preserving security through Space Shift Keying (SSK) modulation. Extensive simulations analyze Bit Error Rate (BER) performance across various scenarios and demonstrate that our framework achieves robust security and reliability. Our simulations include realistic channel modeling, incorporating Rician fading and different path loss calculations, and present them through BER heatmaps. The proposed framework offers promising applications for emerging technologies requiring secure communication, such as vehicular networks and Internet of Things, without introducing the latency overhead of complex encryption schemes.

1 Introduction

Every day, more and more people and objects connect, communicate and transfer data with each other. In today's world, we need both speed and security for our communications, even if both were considered two opposite ends of a spectrum. By adding error correction and encryption to our data, we can increase reliability and privacy at the expense of latency.

Modern technologies, like the Internet of Things (IOT) and the Cooperative Autonomous Driving (CAV), are becoming more and more popular and necessary in our society. But they are highly demanding advancements, needing real-time communication and defense against dangerous disruptions.

Every day we interact with smart devices, capable of coordinating with each other in real time to reach a common goal. Multiple applications exist in wildfire prevention, logistics, home control and many more fields. These devices include sensors, cameras, agents, controllers and robotics. An important advantage we gain from these intricate, deeply connected networks is high efficiency and low error and incident rates.

With a declining population that gets more productive by the day, we are moving towards a future where technology can help us in a lot of mundane, repetitive and sometimes dangerous tasks, allowing people to express more freely their potential and contribute more to the well-being and advancement of humankind. Imagine a world where the house is cleaned automatically, the electricity bill is reduced by automatic control based on necessities, and autonomous driving vehicles move you wherever needed while you work on your most important objectives. This is a promising future, but there are a lot of obstacles to overcome first.

The load on our infrastructure grows faster than ever. Every day, more people and devices alike connect to the internet or with each other, sending and receiving even more data. Cable communications cost too much in terms of space and maintenance, and wireless communication challenges increase as the number of connected machines multiply. But at the same time, we need reliability and speed.

With our lives dependent on technology, we also need way more security. We cannot risk attacks from malicious users, because of the damage they may cause. Appliances may be hacked to spy or short-circuited, cars could be deceived and cause fatal crashes. Critical infrastructure like hospitals are breached every day, exposing sensitive and crucial data to all malicious actors there could be.

But at the same time, the rate of progress forbids us to choose between fast but unsecure commu-

nications, or encrypted and slow to capture ones. We need new ways, new paradigms to ensure safe data transfer with low latency and high accuracy.

Reconfigurable Intelligent Surfaces (RIS) are a new proposal that may help in this context. They are a low-power, low-cost solution to transform reflection from passive noise in our communications into active parameters we can fine-tune to redirect, expand and propagate our communication signals into more complex scenarios, for example by helping in situations without direct Line of Sight (LOS).

RIS may help us expand our networks significantly, reaching more users, ensuring more speed and helping us with the reliability of the received signals.

In this thesis, we aid the research by expanding current literature and studying how to use RIS not only for the aforementioned reason, but also to protect our communication privacy against malicious eavesdroppers. We can modulate the reflection signal to make sure only the legitimate receivers can understand the message, while making the reflected signal be undecipherable and act as artificial noise to protect against unwanted listeners.

This is called Physical Layer Security (PLS): our objective is supporting higher levels of security, like encryption, to protect ourselves against adversary actors even when they have bigger resources than us, or reduce the complexity of it by ensuring less probability of capturing the signal in the first place.

Our plan is to serve as many users as needed, in complex scenarios without clear direct path between all the actors, while making the exchanged data unreadable for unwanted users. With our proposal, the signal is not undecipherable for anyone else, but it is completely unreadable from the start.

Imagine that instead of sending to everyone random letters, where only the legitimate receivers can understand what is written, we can also make sure that all the other unwanted listeners get not random letters, but random strikes. Even if they had unlimited resources and computational power, for example quantum computers, they would not be able to do anything because they have nothing to work on.

By adding this extra layer of security, we can then reduce the encryption power on the higher levels of communications, making messages faster to parse and understand. In critical high-speed communication like CAV, having a bigger throughput with lower latency can be critical in expanding the possible speed of every car in the network from scientific interest to usable, everyday technology.

1.1 Our contribution

The specific contributions of this work are:

- a general explanation of the current advancements in Physical Layer Security and Reconfigurable Intelligent Surfaces
- a detailed explanation of a proposed signal modulation, called Space Shift Keying (SSK), and a proposed framework for RIS-aided encryption made by prominent researchers in the field
- generalize the framework to support multiple legitimate users, multiple RIS in series, and multiple signal paths in parallel, while keeping the same level of security and complexity
- carry out Bit Error Rate (BER) simulation analysis to prove the efficacy of our proposed solution
- model a realistic communication system to include channel gain matrix calculations, Rician fading and path loss
- in particular, study different configurations of path losses to give a better general vision of the applicability of our solution
- heatmap graphs to show the behavior in various practical scenarios

We will provide detailed mathematical explanation and extensive simulation code to better help the research in more future application studies about the application in real-life communications between physical actors.

1.2 Notation

We will use the following notations in this work:

- Variables are written as capital italic letters X
- Vectors are written as italic letters x
- Matrices are written as bold capital italic letters $\boldsymbol{X}$
- $\mathbb{C}$ defines the Complex set, C^X a complex vector of length X, and C^{XxY} a complex matrix of dimension X rows and Y columns
- given $x \in \mathbb{C}^Y$, we define $\boldsymbol{X} = diag\{p\} \in \mathbb{C}^{YxY}$ a matrix with all zeros, except in the diagonal where position y, y is equal to x_y
- given $\boldsymbol{X} \in \mathbb{C}^{YxY}$, we define $x = diag(\boldsymbol{X}) \in C^Y$ the vector of the elements in the diagonal of $\boldsymbol{X}$
- given $\boldsymbol{X} \in \mathbb{C}^{YxY}$, we define $\boldsymbol{X}_{diag} \in \mathbb{C}^{YxY}$ the matrix with all zeros, except in the diagonal where position y, y is equal to $\boldsymbol{X}_{y,y}$
- given $\boldsymbol{X} \in \mathbb{C}^{YxZ}$, we define $[\boldsymbol{X}]_{:,1:Y} \in \mathbb{C}^{YxY}$ the first Y columns of $\boldsymbol{X}$
- $\odot$ is the Hadamard product
- A Hermitian transpose of $\boldsymbol{V}$ ($\boldsymbol{V}^H$), means we first transpose the matrix ($\boldsymbol{V} \rightarrow \boldsymbol{V}^T$), then take the conjugate of every element (so invert the sign of the imaginary part).
- The Frobenius norm of a matrix $\boldsymbol{X}$, denoted as $\|\boldsymbol{X}\|$, is defined as $\|\boldsymbol{X}\| = \sqrt{\sum_i \sum_j |x_{ij}|^2}$

2 Related works

2.1 Physical Layer Security

The essential premise of physical layer security is to enable the exchange of confidential messages over a wireless medium in the presence of unauthorized eavesdroppers, without relying on higher-layer encryption. [24]

Physical layer security is much lighter than complex secret key-based cryptographic techniques [26]. It ensures high reliability and security at less computational cost. Being much quicker than the higher layer counterparts, it ensures low latency in higher bands, like 5G or 6G. Ultra-reliable low latency communication (URLLC) may help critical infrastructure in delivering high privacy and data speed capabilities. The ability to combine both lower and higher layer security will also enhance the general capabilities of everyday applications.

We have two types of threats we need to protect against. Active attacks, like jamming a frequency, disrupt and block the flow of information; while passive attacks, like eavesdropping, are more subtle and we need to make our signals undecipherable with encryption or noise [29]. In particular, passive hearing could expose sensitive data, and even encryption may still leak location, traffic load and other sensitive information.

Modern communication needs multiple requirements in order to guarantee the efficacy and security of communications:

- legitimate users should be authenticated
- access control must be implemented to ensure confidentiality of the messages
- integrity of the communication, to ensure the message is correctly delivered
- availability of the channel link, to ensure jamming attacks do not influence negatively the flow of information
- defense and encryption against eavesdroppers

There are different methods we can use to mask our communications: we can fingerprint the legitimate users, as explained in the paper [31], use directional antennas to reduce the area where it is possible to capture the signal [11], or add artificial noise schemes to disrupt unwanted hearers [10].

Different error correction strategies can also mitigate the effect of active attacks. We can use some of the passed bits to ensure the data received is correct, and sometimes even fix the errors. We can also use *Spread Spectrum Coding* to rapidly change the frequency used to deliver the message, ensuring difficulties in disrupting all of the available ones.

Modeling the threats of adversaries can be quite challenging [33]. Many research papers include assumptions that we need to be careful about. For example, eavesdroppers may not just be passive listeners, but may actually collect data to later transform into active attackers.

The adversaries may also have better resources, both in computer power and signal reception, and it is difficult to model all possible threats we may face. We may have multiple stations collaborating together in deciphering the signal, or even be backed up by national agencies. Some work has already been done addressing these issues: in [12], the authors study a universal coding scheme to protect against eavesdroppers changing constantly channels. In [17] a statistical model is created to calculate the probability of achieving secrecy from eavesdroppers in unknown locations.

Achieving perfect communication secrecy is not really possible for all cases, given that we need the secret key to be at least as big as the secret message [28], but there are some practical strategies we can implement.

In particular to eavesdropping, there is a huge opportunity for improvements. While disruptions have been studied for long, especially in military communications, message encryption is usually

delegated to the higher levels [24]. However, the physical layer can assist by hiding or masking the signal, making it harder for the eavesdropper to capture it. Given the advances in quantum computing and encryption breaking algorithms [30], it is important to be protected at all layers.

2.2 Reconfigurable Intelligent Surface

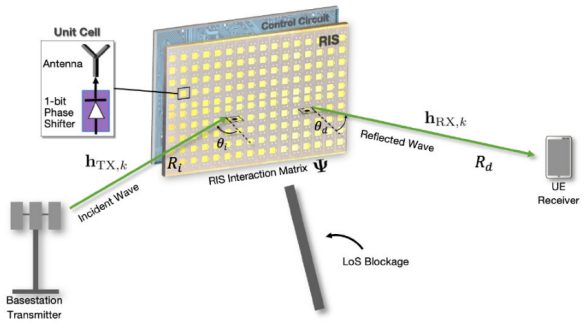

Figure 2.1: An example of possible design of a Reconfigurable Intelligent Surface [From [34]]

Reconfigurable Intelligent Surfaces (RISs) are a new technology that can help in improving the security and reach of wireless communications. They are made of a large number of passive elements that can reflect the signals in a way that can be controlled and optimized.

With RISs, it is possible to control the propagation and reflection of radio waves, making it possible to transform the environment, in which the waves need to travel, from an uncontrollable phenomenon to a programmable variable that is possible to (partially) control and optimize.

RISs can help in particular in two scenarios. In the first one, two nodes which are not in the line of sight (LOS) can communicate with the help of the RIS; in the second one, being in the LOS means an inability to take advantage of delayed reflections (especially for new technologies like 5G and 6G), which can be used to improve the signal quality and robustness, but we can create them with RISs [7].

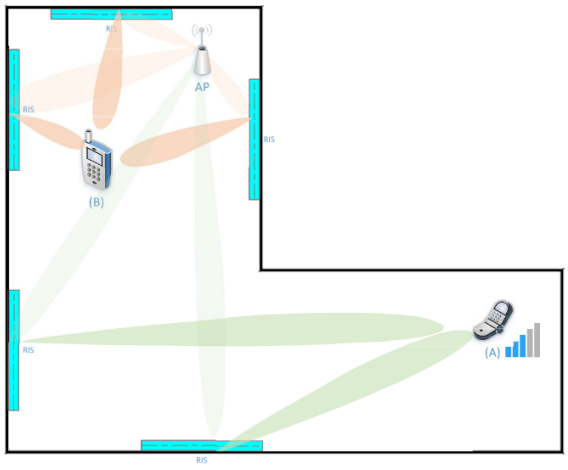

Figure 2.2: *A smart radio environment with multiple RISs. User A is far away from the AP and suffers from low received signal strength, while user B has ample received power but a low-rank ill-conditioned channel. The RISs can be optimized to help in both scenarios.* [From [7]]

The main advantages of RISs are the low cost, the low power consumption and the easy deployment, which makes them a good candidate for the future of wireless communications. They do not require a dedicated energy source, they do not suffer from noise amplification, they can work with any frequency and can be easily put on any surface like walls or ceilings [3].

A specific controller is used to modify dynamically the reflecting elements of the RIS, giving huge margins for custom configurations in complex scenarios and new communications frameworks.

Numerous applications are being studied to this day. For example, in [16] the authors study the modeling of path loss for a reflected signal; they then recreate a RIS using an Arduino to validate the mathematical calculations.

RIS can also be included in more general smart cities projects [19]: in a more interconnected world, they can be used for everyday streets and personal homes; huge, unused building surfaces may aid the general population in getting better connectivity; smart factories and the industry 4.0 could be assisted in dense IoT device places, by countering the negative effects of metals for signal strength.

Active RIS can also be deployed [21], which can amplify the received signal before reflecting it, ensuring an even higher power output and reach for a similar design. Beamforming can also be used to redirect the signal towards a specific direction, increasing the signal strength for the receiver in that specific area.

2.3 Using RISs for Physical Layer Security

RISs can be used to greatly increase not only the network performance but also its security [18]. By using RISs, we can make the signal quality better, reduce the signal degradation and make the signal more difficult to intercept by eavesdroppers.

For example, the reflection can be used as multiplicative randomness to make the transmission not understandable from eavesdroppers, while having a decoding for the legitimate user linear [22].

There is the possibility for attackers to also use RIS as an assistance tool to spy on communications, and even propagate jamming attacks in multiple directions [2].

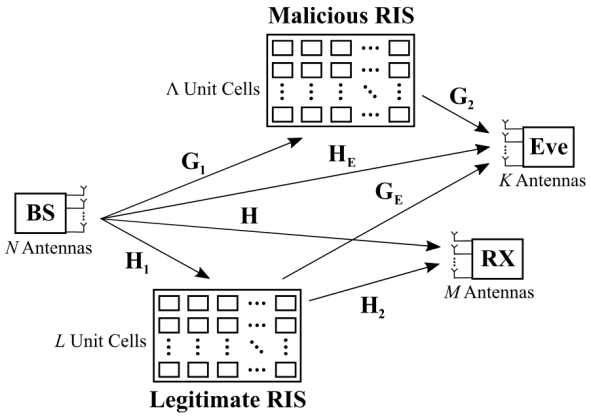

Figure 2.3: Eavesdroppers could not only listen from the transmitter or the legitimate RIS, but even deploy a malicious one, possibility for passive and active attacks [From [2]]

Another paper [40] studied how to use a novel RIS based channel randomization technique to improve the secrecy rate, and another one [5] shows an iterative efficient algorithm to maximize the minimum secrecy rate by optimizing the reflecting coefficients of the RIS.

RISs can also be used to protect against jamming attacks: for example, in [32] an aerial RIS is used to mitigate the effects of the disturbance and increase the transmission power and reliability.

2.4 RISs and Physical Layer Security for Vehicular Networks

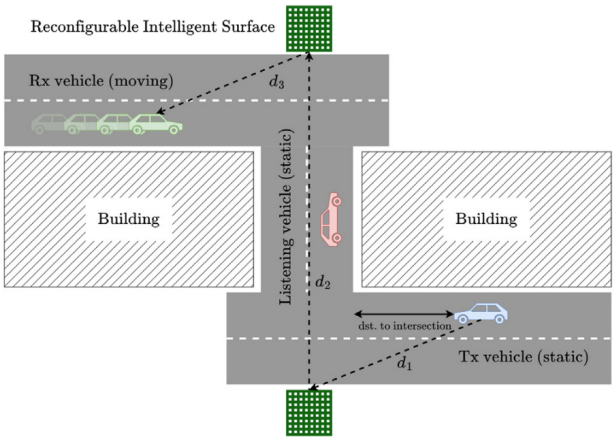

Figure 2.4: An example of usage of RIS for vehicle communications [From [27]]

Cooperative autonomous driving can bring many benefits, like reducing traffic congestion, improving road safety and reducing the environmental impact of the vehicles. Cars and other vehicles can communicate with each other and with the infrastructure to share information and coordinate their movements. However, it also brings new security concerns, especially in the wireless communications.

It is clear that it is necessary to have a secure and fast way to communicate, and 6G network technologies plus RISs can help in this regard. By reflecting the signals, we can overcome the limitations of LOS and improve the signal quality by reducing signal degradation [6].

The sector is just starting to be studied, but there are already some promising results. Network simulators made specific, like CoopeRIS, allow to study and progress in this field [27].

Vehicular networks need low latency and high security. Active attacks may jeopardize drivers' and people's safety, while also slowing down the information exchange rate. Being moving agents, it is more difficult to correctly model this type of network, but also way more necessary: complex upper layer encryption may slow down data processing enough to render it useless [1].

Passive attackers may instead use vehicles' geolocation and traffic data for malicious activity. A way to detect and filter out intruders is discussed in [20].

Recent studies show how RISs can be used to protect the vehicular network against illegitimate users. In [23] the authors study how RISs can improve the average secrecy capacity and secrecy outage probability.

3 Hidden communication by targeted reflections

3.1 RIS Diagonalization

We will start from the paper *Reconfigurable Intelligent Surface: Reflection Design Against Passive Eavesdropping* [22], explaining how to hide communication between two actors from eavesdroppers using Reconfigurable Intelligent Surfaces, then expanding it to multiple receiving users at the same time.

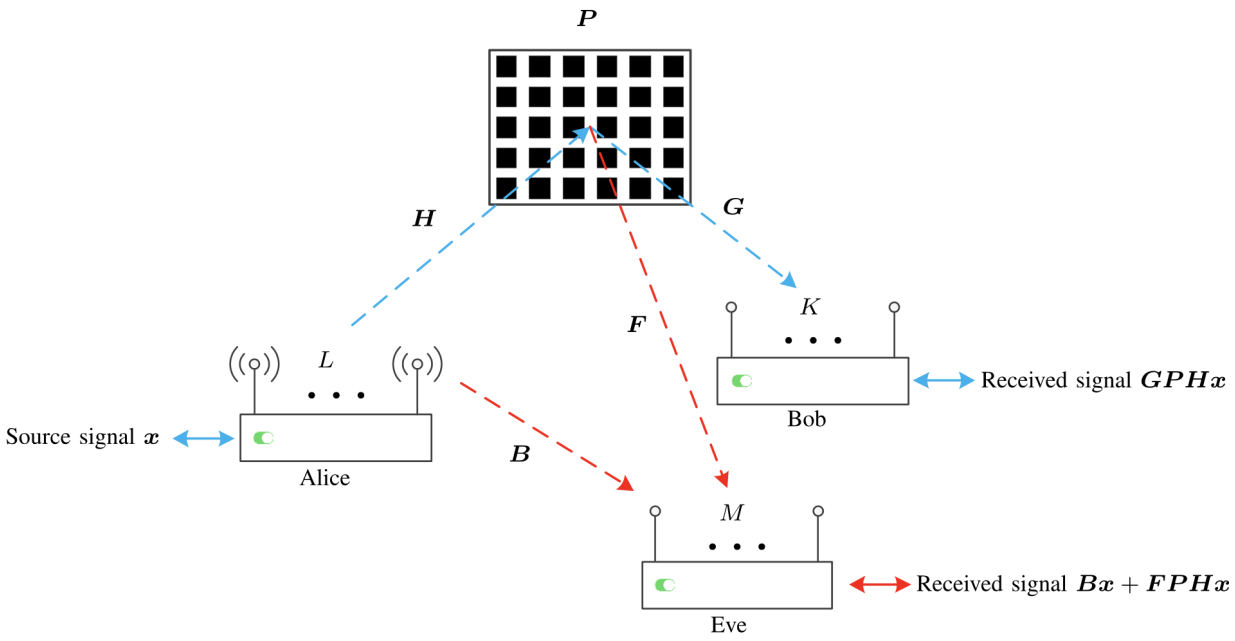

Figure 3.1: Setup of the system [From [22]]

In [22], the authors studied how to use RISs to allow communications between two users without LOS, while making the signal undecipherable for eavesdroppers. We call L the transmitter's antennas, K the receiver's antennas, M the eavesdropper's antennas, and N the RIS reflecting elements. We assume $L \geq K \geq 2$.

We define $\boldsymbol{H} \in \mathbb{C}^{N \times L}$ the channel response [1] from the transmitter to the RIS, $\boldsymbol{G} \in \mathbb{C}^{K \times N}$ the channel response from the RIS to the receiver, $\boldsymbol{P} = diag\{p\} \in \mathbb{C}^{N \times N}$ a diagonal matrix in which the nth diagonal element represents the reflection coefficient of the nth unit at the RIS.

The objective is making the receiver's final signal $\boldsymbol{GPH}$ a diagonal matrix, while making every possible eavesdropper's final signal a full matrix.

We will leave for later the technical details of why this would achieve secrecy for the legitimate users or how the actors communicate with each other, and will just focus on the mathematics behind the calculation. It is possible to read more in the paper *Space shift keying modulation for MIMO channels* [15], which we will summarize in a later chapter.

[1] A channel response for a MIMO communication is a matrix made of complex numbers, where the position i, j indicates the signal received from antenna j to antenna i

Our contribution to the field will be to generalize these calculations to J receiving users and M RISs used in parallel and in sequence.

Formally, the condition we want to satisfy is:

$$||[\boldsymbol{GPH}]_{:,1:K} - [[\boldsymbol{GPH}]_{:,1:K}]_{diag}||^2 = 0 \tag{3.1}$$

Where $[GPH]_{:,1:K} \in \mathbb{C}^{K\times K}$ denotes the first K columns of the matrix $\boldsymbol{GPH} \in \mathbb{C}^{K\times L}$.

Given

$$\boldsymbol{W} = \sum_{i,j=1,i\neq j}^{K} (g_{j,:} \odot h_i^T)^H (g_{j,:} \odot h_i^T) \tag{3.2}$$

$$\text{rank}(\boldsymbol{W}) = K(K-1) \tag{3.3}$$

$$\text{rank}(\boldsymbol{W}) + \text{null}(\boldsymbol{W}) = N \tag{3.4}$$

Where null refers to the dimension of the null space.

$$\text{null}(\boldsymbol{W}) = N - (K^2 - K) \tag{3.5}$$

The formula (3.1) can be rewritten as

$$Wp = 0 \tag{3.6}$$

and the solutions of p can be found in the null space of $\boldsymbol{W}$. Using singular value decomposition (SVD), we can decompose

$$\boldsymbol{W} = \boldsymbol{R\Sigma V}^H \tag{3.7}$$

With SVD, we have $\boldsymbol{\Sigma} = diag(\sigma) \in \mathbb{C}^{N\times N}$ a diagonal matrix. The first $\text{rank}(\boldsymbol{W}) = K^2 - K$ elements of σ are non-zero, while the last $\text{null}(\boldsymbol{W}) = N - (K^2 - K)$ elements are zero [8].

Given a more generic $\boldsymbol{A} \in \mathbb{C}^{m\times n} = \boldsymbol{R'\Sigma' V'}^H$, we have the column vectors of R' being an orthonormal span of $\mathbb{C}^m$, and the row vectors of V' being an orthonormal span of $\mathbb{C}^n$.

Suppose $\boldsymbol{A}$ is a Hermitian matrix (meaning $\boldsymbol{A} = \boldsymbol{A}^H$). This will be useful later, as $\boldsymbol{W}$ is also a Hermitian matrix by construction. Let's call k the null space dimension of $\boldsymbol{A}$, and, by the property above, the null space dimension of $\boldsymbol{A}^H$ too.

The last k columns of $\boldsymbol{R'}$ are a span of the null space

$$N(\boldsymbol{A}^H) = [r_{m-k}, ..., r_m] \in \mathbb{C}^{m\times k} \tag{3.8}$$

while the last k rows of V'^H are a span of the null space

$$N(\boldsymbol{A}) = \begin{bmatrix} v'^H_{n-k} \\ ... \\ v'^H_n \end{bmatrix} \in \mathbb{C}^{k\times n} \tag{3.9}$$

Being $\boldsymbol{A}$ a Hermitian matrix, the two null spaces are both solutions to $\boldsymbol{A}x = 0$.

Consider now $\boldsymbol{W} \in \mathbb{C}^{N\times N}$. The paper in question uses equation (3.8) to find the solutions, since W is Hermitian and square. Taking $\boldsymbol{U} \in \mathbb{C}^{N\times(N-(K^2-K))}$ as the last $N - (K^2 - K)$ columns of the left singular matrix $\boldsymbol{R}$. $\boldsymbol{U} \in \boldsymbol{N}(\boldsymbol{W})$ for the explanation above. We then have

$$\boldsymbol{WU} = 0 \tag{3.10}$$

$$p = \boldsymbol{U}q \tag{3.11}$$

$$\boldsymbol{WU}q = 0 \tag{3.12}$$

being true, and $q \in \mathbb{C}^{N-(K^2-K)}$ can be a random vector.

3.2 Space Shift Keying Modulation

How can the actors communicate if the result is a diagonal matrix with random values?

We will use a technique called *Space Shift Keying* (SSK) Modulation [15], where *antenna indices are used as the only means to relay information.* Given K the number of antennas of the actors in the system, we can send $log_2(K)$ bits by mapping each combination of bits to a specific antenna. [2]

Table 3.1: Example of the SSK mapper rule [From [15]]

$\mathbf{b} = [b_1 \quad b_2]$	symbol	antenna index j	$\mathbf{x} = [x_1 \quad \cdots \quad x_4]^T$
$\begin{bmatrix}0 & 0\end{bmatrix}$	0	1	$\begin{bmatrix}1 & 0 & 0 & 0\end{bmatrix}^T$
$\begin{bmatrix}0 & 1\end{bmatrix}$	1	2	$\begin{bmatrix}0 & 1 & 0 & 0\end{bmatrix}^T$
$\begin{bmatrix}1 & 0\end{bmatrix}$	2	3	$\begin{bmatrix}0 & 0 & 1 & 0\end{bmatrix}^T$
$\begin{bmatrix}1 & 1\end{bmatrix}$	3	4	$\begin{bmatrix}0 & 0 & 0 & 1\end{bmatrix}^T$

3.2.1 Direct Detection

Given a channel gain matrix $\boldsymbol{B} \in \mathbb{C}^{K \times K}$ and the input vector $x \in \mathbb{C}^K$ with only one element equal to 1, the signal received is

$$y = \boldsymbol{B}x + \sigma^2 \tag{3.13}$$

To understand the antenna index which sent the message, we need to find the column b_j which is most similar to y.

$$j = \arg\max_j \; p_y(y|x_j, \boldsymbol{B}) = \arg\min_j \; ||y - b_j||^2 \tag{3.14}$$

3.2.2 Diagonalized Reflection Detection

Following [22], for a reflected signal we have

$$y = \boldsymbol{GPH}x + \sigma^2 \tag{3.15}$$

Given that $\boldsymbol{GPH}$ is a diagonal matrix and x has only one element equal to 1, the resulting vector $\boldsymbol{GPH}x$ will still be a vector with only one element non-zero. Adding noise, to find the antenna index we search for the biggest value in the vector.

$$j = \arg\max_j \; y_j \tag{3.16}$$

[2] This may seem rather unoptimized, as we use only one antenna instead of combinations of them. To see a more general approach, the authors also wrote the paper [14], where they discuss a more general approach using multiple active antennas at the same time. The general approach will also work with our proposed solution.

3.3 Cascaded Channel Estimation

To understand how the actors (and in particular the RISs controller) estimate the channel gain between them, we redirect to the paper *Cascaded Channel Estimation for Large Intelligent Metasurface Assisted Massive MIMO* [13]. While we will not summarize the content here, we will still give a general idea of how to use the algorithm in the paper to estimate $\boldsymbol{G}$ and $\boldsymbol{H}$.

- The transmitter communicates to the RIS controller a setup message x' that it will send to the receiver;
- The RIS will set a random $\boldsymbol{P'}$;
- The receiver gets a signal y' (which will mean nothing), and sends it back to the RIS controller;
- Based on $x', y', \boldsymbol{P'}$ the RIS controller estimates $\boldsymbol{G}, \boldsymbol{H}$ and correctly sets up $\boldsymbol{P}$;
- The transmitter sends x, and the receiver gets y which it can correctly convert back;
- If transmitter and receiver are moving, the procedure will start all over. Otherwise, $\boldsymbol{G}$ and $\boldsymbol{H}$ remain the same, and the RIS controller can just create a new $\boldsymbol{P}$ for the next messages.

4 Expanding to multiple users

In real life scenarios, we deal with more than two communicating actors. We want to expand the findings of this paper by having it support multiple RISs in series and multiple receivers from the same transmitter. Once we have those, we can generalize it to also have receivers getting signals from multiple independent reflections of RISs.

We will first, however, make some simplifications about the actors by having $L = K$ for all of them[1]. We will still consider one transmitter, with $J \geq 1$ receivers.

4.1 Reflecting to multiple users

We consider the case where the transmitter wants to send the signal to J receivers without LOS. The condition we want to satisfy is

$$\forall j \in [1...J] \rightarrow ||\boldsymbol{G}_j\boldsymbol{P}\boldsymbol{H} - [\boldsymbol{G}_j\boldsymbol{P}\boldsymbol{H}]_{diag}||^2 = 0 \tag{4.1}$$

$$\forall j \in [1...J] \rightarrow \boldsymbol{W}_j p = 0 \tag{4.2}$$

$$\begin{bmatrix} \boldsymbol{W}_1 \\ \boldsymbol{W}_2 \\ ... \\ \boldsymbol{W}_j \end{bmatrix} p = 0 \tag{4.3}$$

$$\begin{bmatrix} \boldsymbol{W}_1 \\ \boldsymbol{W}_2 \\ ... \\ \boldsymbol{W}_j \end{bmatrix} = \boldsymbol{W} \in \mathbb{C}^{JNxN}, \boldsymbol{W} = \boldsymbol{R}\boldsymbol{\Sigma}\boldsymbol{V}^H \tag{4.4}$$

The problem we have now is that $\boldsymbol{W}$ is not a square matrix anymore, so we cannot use the last $N - (K^2 - K)$ columns of $\boldsymbol{R}$ to calculate the null space and p with its linear combination, by using formula (3.8). The null space would have dimension $N(\boldsymbol{W}) \in \mathbb{C}^{JNx(N-(K^2-K))}$, but that would require a $p \in C^{JN}$ instead of $p \in C^N$.

We can, however, use the last $N-(K^2-K)$ rows of $\boldsymbol{V}^H$, then apply again the hermitian transposition to get our desired solution. Remember that $N(\boldsymbol{W})$ can also be calculated using the left singular matrix, by using formula (3.9). $\boldsymbol{W}$ is not a square matrix, so $\boldsymbol{W} \neq \boldsymbol{W}^H$,

$$N(\boldsymbol{W}) = \begin{bmatrix} v^H_{N-J(K^2-K)} \\ ... \\ v^H_N \end{bmatrix}^H \tag{4.5}$$

Take $\boldsymbol{U}_1 \in \mathbb{C}^{N-J(K^2-K)xN}$ the last $N-(K^2-K)$ rows of $\boldsymbol{V}^H$, and

$$\boldsymbol{U} = \boldsymbol{U}_1^H \in \mathbb{C}^{NxN-J(K^2-K)} \tag{4.6}$$

We now can apply the same method as before

[1] We want the actors to be able to communicate with each other. Since the transmitter needs to have an equal or greater number of antennas than the receiver, but the roles may later switch, it follows that the number of antennas must be equal for the calculation. Using more antennas can still be done, by not considering the values coming from them (like the original paper did as well).

$$p = \boldsymbol{U}q \tag{4.7}$$

$$\boldsymbol{W}\boldsymbol{U} = 0 \tag{4.8}$$

$$\boldsymbol{W}\boldsymbol{U}q = 0 \tag{4.9}$$

4.2 RISs in parallel

Given the previous property, it follows that we can use M independent RIS, each one reflecting the signal to J multiple receivers, and without LOS from each other. For the receiver $j \in [1, J]$, we have

$$\sum_{m=1}^{M} \boldsymbol{G}_j \boldsymbol{P}_m \boldsymbol{H}_m x = (\sum_{m=1}^{M} \boldsymbol{G}_j \boldsymbol{P}_m \boldsymbol{H}_m)x \tag{4.10}$$

The sum of diagonal matrices is still a diagonal matrix, so the property still holds. Remember that we only care about the indexes of the active antennas and not their values, so there is no problem in adding them together.

4.3 RISs in series

We consider the case where the signal is bounced between M RISs in this way:

$$\text{Transmitter} \rightarrow \text{RIS 1} \rightarrow ... \rightarrow \text{RIS M} \rightarrow \text{Receiver} \tag{4.11}$$

We call $\boldsymbol{C}_i \in \mathbb{C}^{NxN}$ the channel gain between $\boldsymbol{P}_i$ and $\boldsymbol{P}_{i+1}$. We need to solve

$$||\boldsymbol{G}\boldsymbol{P}_1\boldsymbol{C}_1...\boldsymbol{P}_M\boldsymbol{H} - [\boldsymbol{G}\boldsymbol{P}_1\boldsymbol{C}_1...\boldsymbol{P}_M\boldsymbol{H}]_{diag}||^2 = 0 \tag{4.12}$$

We can generate $p_1, ..., p_{M-1}$ as random reflections, and calculate the last one based on the previous. An advantage we get is that eavesdroppers listening from a middle RIS will not be able to decipher the signal either.

Given $r_i \in [0, 1]$ the absorption coefficient, and $\theta_i \in [0, 2\pi]$ the phase shift, we can choose them randomly for all RIS p_m vectors, but the last one.

$$\forall m \in [1, M-1] : p_m[i] = \eta * r_i * e^{j\theta_i} \tag{4.13}$$

Given now

$$\boldsymbol{G}' = \boldsymbol{G}\boldsymbol{P}_1\boldsymbol{C}_1...\boldsymbol{P}_{M-1}\boldsymbol{C}_{M-1} \in \mathbb{C}^{KxN} \tag{4.14}$$

We can consider now the problem of solving

$$||\boldsymbol{G}'\boldsymbol{P}_M\boldsymbol{H} - [\boldsymbol{G}'\boldsymbol{P}_M\boldsymbol{H}]_{diag}||^2 = 0 \tag{4.15}$$

Which can be solved as before. [2] [3]

If we have multiple $\boldsymbol{G}_j$, it will be enough to calculate all the $\boldsymbol{G}'_j$ and proceed as before, allowing us to combine these properties in more complicated scenarios.

[2] It is also possible to set up randomly the last $M-1$ RIS and calculate the first one using $\boldsymbol{G}$ and $\boldsymbol{H}' = \boldsymbol{C}_1\boldsymbol{P}_2\boldsymbol{C}_2...\boldsymbol{P}_M$. The properties still hold.

[3] Estimating the channel gains $\boldsymbol{G}$ and $\boldsymbol{H}$, based on [13], could be more difficult, given that we do not have full control on $\boldsymbol{P} = \boldsymbol{P}_1\boldsymbol{C}_1...\boldsymbol{P}_M$ anymore. We can however estimate directly G' by keeping the same random $\boldsymbol{P}_1, ..., \boldsymbol{P}_{M-1}$ in both the acknowledgment round and the message transmission round, and just modify $\boldsymbol{P}_M$ after estimating $\boldsymbol{G}'$ and $\boldsymbol{H}$ to correctly deliver the message.

4.4 Complex reflections

The receiver could also get the signal from all the RISs in series, if in the right position.

For example, let's say it receives the signals $\boldsymbol{GP}_1\boldsymbol{H}_1x$ and $GP_1C_1P_2H_2x$. To solve this system, instead of setting $\boldsymbol{P}_1$ randomly, we would need first to solve it using $\boldsymbol{G}$ and $\boldsymbol{H}_1$, then solve $\boldsymbol{P}_2$ using $\boldsymbol{G}' = \boldsymbol{GP}_1\boldsymbol{C}_1$ and $\boldsymbol{H}_2$. The sum of the two signals would still be readable for the receiver correctly.

While the calculations of $\boldsymbol{P}_1$ depend on $\boldsymbol{G}$ and $\boldsymbol{H}_1$, the signal would still be random and undecipherable for an eavesdropper receiving it.

5 Simulation Results

In this chapter, we will evaluate the performance of the proposed framework through extensive simulations of different scopes and scenarios.

In section 5.1, we perform Bit Error Rate (BER) analysis using stochastic simulations to show the relation between correct capture of the signal depending on the Signal to Noise Ratio (SNR). This will allow a direct comparison to the results obtained from the paper [22], to show the efficacy of our expansion.

In section 5.2, we will simulate more realistic scenarios by considering path loss and spatial deployment, creating BER heatmaps to show the validity of the framework in physical environments and the security offered for all possible locations of an eavesdropper.

5.1 BER stochastic simulation

In this section, we consider the scenario illustrated in Figure 5.1, where a single transmitter Alice and multiple receivers exist. Frank is a direct receiver in line of sight. Bob and Charlie receive the signal from two double RIS reflections. Eve receives both the direct signal and the reflecting signal from all RISs. [1]

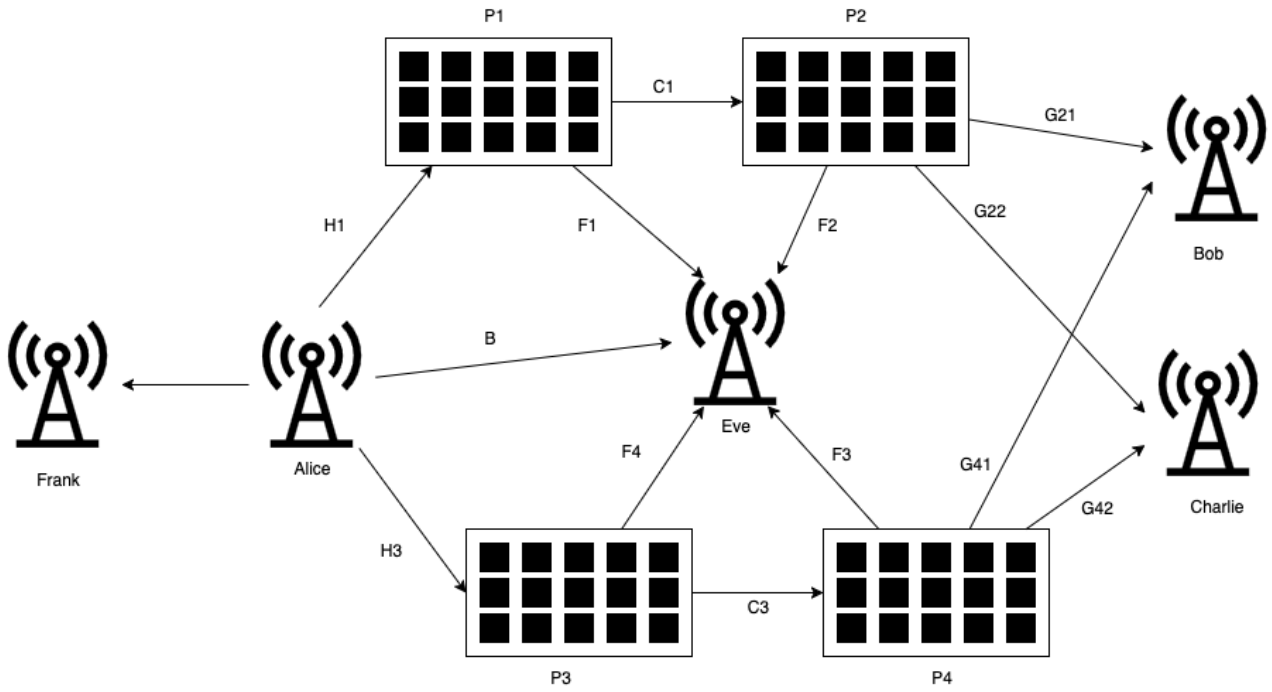

Figure 5.1: Complex setup for secure message transmission

More generally, we would have M consecutive RIS (in series) that reflect a signal, J legitimate receivers and Q different paths of RIS (in parallel) to send the signal at the same time. [2]

[1] It should be noted that if *Eve* is in the same position as *Frank* and receives just the direct signal, our particular framework would not give us physical layer security, and higher layer security would be needed. If instead *Eve* has no line of sight, the message would be completely unreadable from the start, since it would receive random matrices.

[2] The paths could have a different number of RIS (for example, a path of three and another of two). The results would still hold.

We will show simulation results for different combinations of (M, J), both with a single and double path. In all scenarios, $K = 2, N = 16, \eta = 0.9$ will be the number of antennas for all actors, the number of reflecting surfaces and the reflection coefficients. We take these parameters to compare the results to the original paper [22].

The direct link and the eavesdropper will try to understand the message by following the equation (3.14), while the receivers will try to understand it by following the equation (3.16).

5.1.1 Single RIS reflection (M=1)

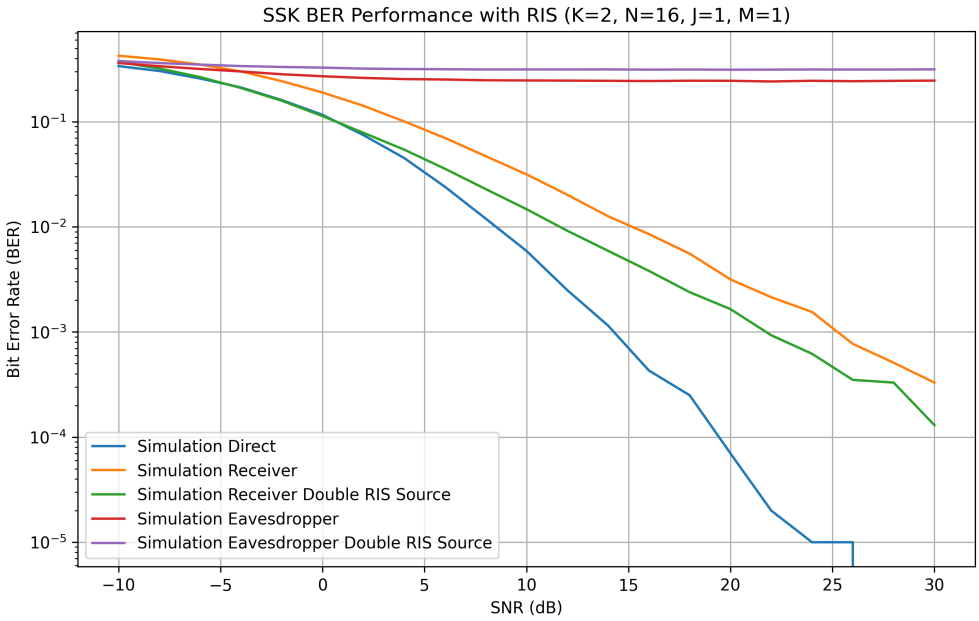

Figure 5.2: SSK BER Performance with RIS (K=2, N=16, J=1, M=1)

We can see in $(M = 1, J = 1)$ the results match with [22], for both *Simulation Receiver* and *Simulation Eavesdropper*. *Simulation Direct* is the strongest possible path, mainly because of the reflection loss due to η. Combining two different RIS in parallel (*Double RIS Source*) gives better signal to the receiver, while disturbing more the signal to the eavesdropper.

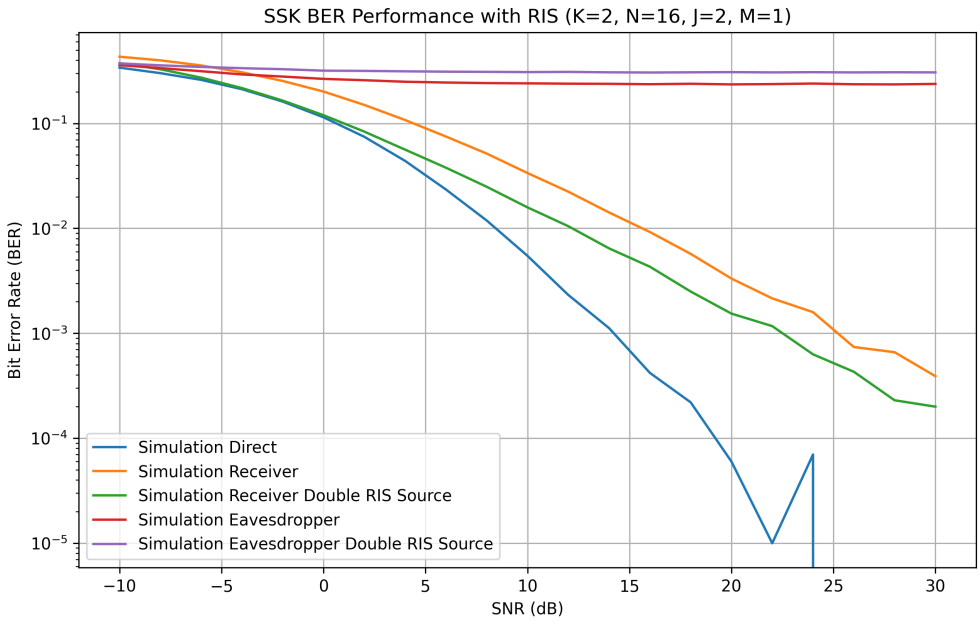

Figure 5.3: SSK BER Performance with RIS (K=2, N=16, J=2, M=1)

Increasing the number of receivers does not influence the result of our framework: the receivers still get a good signal depending on the SNR, while the eavesdropper is not getting an advantage in understanding the message.

5.1.2 Double RIS reflection (M=2)

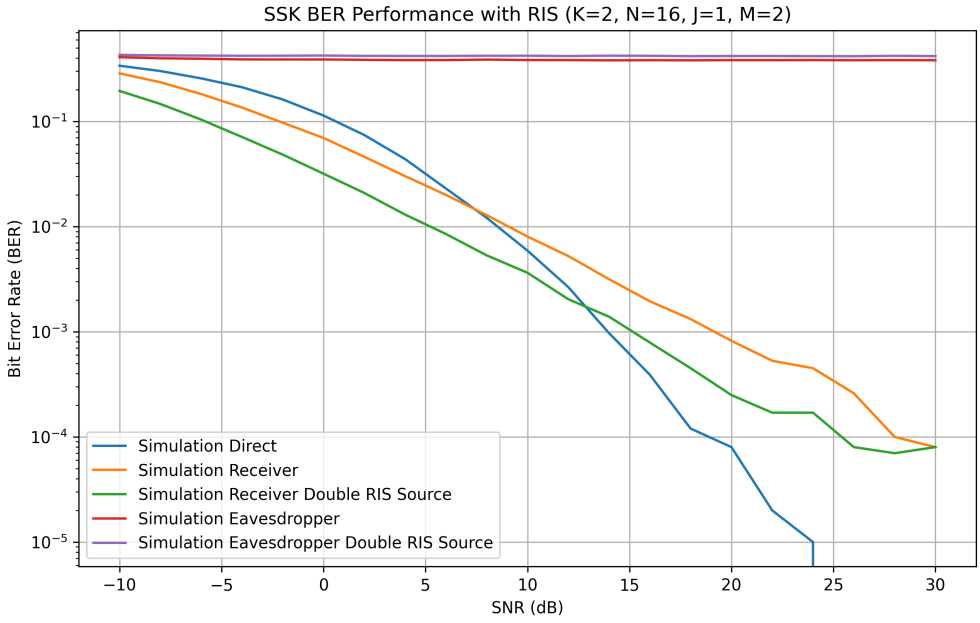

Figure 5.4: SSK BER Performance with RIS (K=2, N=16, J=1, M=2)

With multiple RIS in series, the eavesdropper get a worse signal because of the double interference of the 2 RIS.

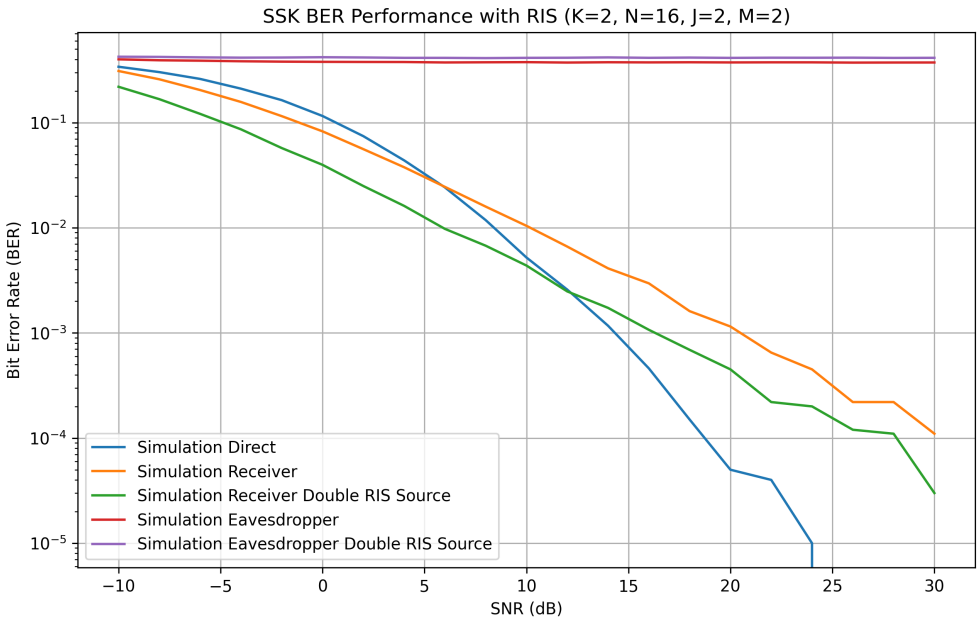

Figure 5.5: SSK BER Performance with RIS (K=2, N=16, J=2, M=2)

Combining all together with two paths and double reflection to two receivers, our properties still hold strong.

5.1.3 Theoretical conclusions

From the graphs we can see that changes in the Signal to Noise Ratio (SNR) do not help the eavesdropper in understanding better the message. When there is a lot of noise, the performance is similar to the legitimate receivers, because no one is able to decipher the message.

When the noise level is much lower, and the signal strength much higher in comparison, the legitimate user understands the message much better, while the eavesdroppers do not. This is because even if the natural noise is reduced, the artificial noise caused by the unreadable RIS signal distorts the received communication for unwanted hearing users, and at the end the BER remains constant.

From 5.2, we can already notice a lot of useful information. Firstly, the resulting graph comes out very similar to the one made by [22]. This is good, because now we have confirmation of our base work, useful to also be confident about our extension and mathematical modifications. In their graph Fig 5.a, they show different lines based on multiple reflection coefficients η, while we used only $\eta = 0.9$, and different Rician Factors to model the power difference between the direct signal and the reflected one, while we used only the eavesdropper with value equal to 1. Comparing those two particular lines to ours "Simulation Receiver" and "Simulation Eavesdropper".

We can focus better on our additions. Firstly, by adding the raw performance of the direct link, we can see that our reflected signal still gives for our legitimate users a solid link to communicate, that offers great performance even when considering the reflection coefficient loss η. Second, we can see that by adding a second reflection path with a double RIS source, our users get better signal while eavesdroppers get even more noise.

In the next graph 5.3 we can see how adding a second legitimate user does not influence the performance of our proposed general solution. This is great: our solution is more scalable, with the same capability to serve data securely. Adding more user constraints does not make our system more vulnerable or less understandable.

In 5.4 and 5.5 we can make similar considerations. Even by adding more reflections for each single path, our framework still shows high promises. We can see, however, that the legitimate receivers BER falls much faster. This is because without considering signal strength reductions due to path loss, multiplying the related matrices improves the overall signal calculated. This is why we also added a new type of simulation to our research, to test our framework with more realistic and specific

scenarios.

5.2 BER realistic scenario simulation

In this section, we evaluate our framework in more realistic spatial environments by creating BER heatmaps that show security performance across different physical locations. We model various path loss scenarios and analyze how they affect the security properties of our system.

We model the channel gain H and the path loss based on the distance between the actors. We will define λ as the wavelength of the signal, and d as the distance between two actors.

5.2.1 Channel gain calculation

We model the Rician fading [38] matrix $\boldsymbol{\Xi}$, to consider possible fading due to multipath interference. Using the Shape Parameter τ, defined as the ratio of the power contributions by line-of-sight path to the remaining multipaths, and the Scale parameter ξ, defined as the total power received in all paths, we can calculate

$$\nu^2 = \frac{\tau\xi}{1+\tau} \tag{5.1}$$

$$\sigma^2 = \frac{\xi}{2(1+\tau)} \tag{5.2}$$

and we can generate $\boldsymbol{\Xi}$ by creating a random complex matrix where the real and the imaginary values are extracted from a gaussian distribution $C(\frac{\nu}{\sqrt{2}}, \sigma)$ [37]

Then, given an actor r with n_r antennas disposed as a *uniform linear array*, we can define the *unit spatial signature in the directional cosine* $\Omega = cos\phi$ [35] as

$$e_r(\Omega) = \frac{1}{\sqrt{n_r}} \begin{bmatrix} 1 \\ exp(-j2\pi\Delta\Omega) \\ exp(-j2\pi 2\Delta\Omega) \\ \vdots \\ exp(-j2\pi(n_r-1)\Delta\Omega) \end{bmatrix} \tag{5.3}$$

where

- Δ is the distance between the antennas (usually $\lambda/2$)
- ϕ is the angle of incidence of the line-of-sight onto the actor antenna

and we can model the channel gain matrix [35] as

$$\boldsymbol{H} = \boldsymbol{\Xi} \odot \sqrt{n_t n_r} exp(-j2\pi d/\lambda) e_r(\Omega_r) e_t(\Omega_t)^H \tag{5.4}$$

We will use this equation both for a direct transmission between two actors, or between an actor and a RIS.

5.2.2 Path loss calculation

We begin by modeling the free space path loss [36] between two points as

$$\boldsymbol{PL} = ((4\pi/\lambda)^2 d^k)^{-\frac{1}{2}} \tag{5.5}$$

where k is equal to 2 when the antennas are isotropic, meaning they radiate power uniformly in all directions in three dimensional space. We will use $k = 2$ for our simulations, even if it is only a theoretical concept.

For a direct LOS communication between the transmitter and another actor (either a legitimate receiver or an eavesdropper), the signal received from input x would be

$$y = \boldsymbol{PL}_B * \boldsymbol{B}x \tag{5.6}$$

Given a reflected signal with channel gain GPH, where

- $\boldsymbol{G}$ is the communication transmitter-RIS

- $\boldsymbol{H}$ is the communication RIS-actors

- $\boldsymbol{P}$ is the RIS reflection coefficient diagonal matrix

we have two different LOS communications. We have different ways of calculating the total path loss:

- we consider the RISs to be active, meaning they amplify the signal received before reflecting it and so they negate the path loss reduction. The signal received would be $y = PL_H * GPHx$. As a result, in case of multiple RISs, only the last connection path loss is considered. We will call this as a *active path loss*

- we consider two separate path losses, one for each LOS. The signal received would be $y = PL_G * PL_H * \boldsymbol{GPH}x$. In case of multiple RISs, we multiply the path loss of all connections. We will call this as a *product path loss*. This usually represents a non directional, isotropic RIS, where the reflected signal is scattered uniformly across all directions and the path loss is significant.

- we consider one single path loss from the sum of the two distances ($d = d_{t-RIS} + d_{RIS-r}$). The signal received would be $y = PL_{G+H} * \boldsymbol{GPH}x$. In case of multiple RISs, we add all the distances. We will call this as a *sum path loss*. This is a simplification of a much more complex type of RIS, called directional RIS, which modulates the phase and magnitude of its elements to redirect the signal in a single direction. This regulation reduces the path loss caused by the second reflection, in relation to the number of elements N of the RIS. It is possible to read more in the paper [4]. It is important to note that, while we are showing results of how a scenario with this type of path loss may act, we will just vary the calculation of the path loss for each point in the map, and will not make any calculations of directional phases themselves. The RIS would still look like an uniform sending relay, and it is included in the document to show the potentiality of our framework in that condition. So for the *sum path loss*, it is important to remember this theoretical limitation. For example, we will show the BER for two different receivers in different locations and various situations, but of course it not be possible to serve in multiple direction for that type of RIS. Mathematically, you could see our graphs of this kind as showing the situation where we have $\lim_{X\to\infty} X$ RIS, all in the same position, each one directed to a different point of the map, with none interfering with each other. It is most certainly an interesting topic for a later research, the actual implementation of our framework with the constraint of directionality of the RIS. This could be done by putting more constraints on the vector q in (3.12).

We will show the main graph, showing the heatmap of the BER for each square, and two or three graphs, showing the logarithmic heatmap of the power received in that point from the transmitter of from a reflection passing through a RIS. For the BER, you could consider all spots not signed by a label as a possible eavesdropper location. **T** represents the transmitter, **P*** are the RIS and **R*** the legitimate receivers.

5.2.3 Single angle of reflection, aided by 1 RIS

Here we have a standard scenario where the transmitter has only a conical view between two buildings, and the receivers do not have direct LOS. What we want to show is that without LOS the message is completely unreadable except for the legitimate users, while the spots in LOS with the transmitter still receive various levels of noise.

For all of the three kinds of path loss, we will have the following parameters: $\lambda = 0.08m$, as standard for 5G connections, $\tau = 0.6, \xi = 1, \eta = 0.9, SNR = 10db, K = 4, N = 25$. In particular, we want to use for this scenario a higher number of antennas per actor and reflecting elements per RIS to show: 1) a bit more complex configuration that the standard $K = 2, N = 16$; 2) show that the BER does have an upper limit on 0.5, the value of random guessing. This is because, even if a higher K could make one suppose you have only $1/K$ probability of guessing the turned on antenna, the actual bit representation is only made of 0 and 1, and thus the probability of error for each bit is 0.5.

Path loss: active We can see here how this type of path loss ensures that in the vicinity of the RIS the Bit Error Rate remains very high, thanks to the active power component of the RIS itself.

We can see the reflected signal from the RIS has the RIS itself as the center.

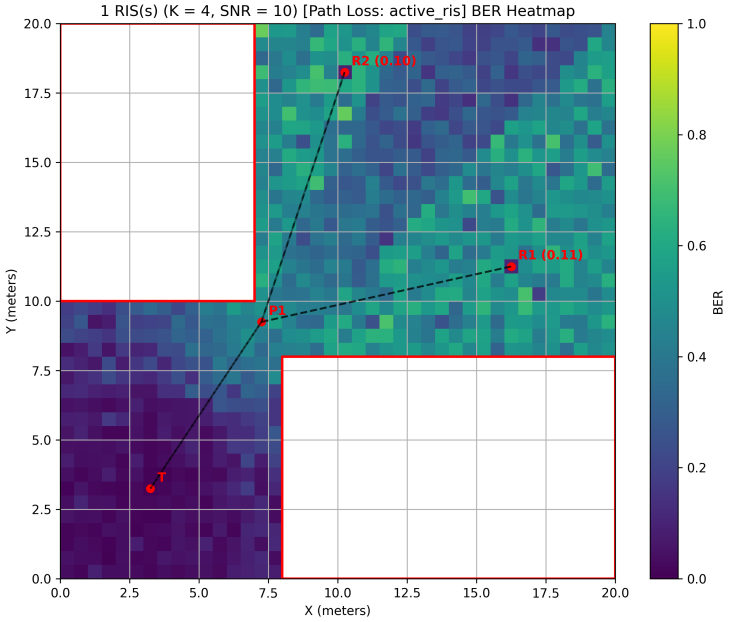

Figure 5.6: 1 RIS(s) [Path Loss: active ris] BER Heatmap

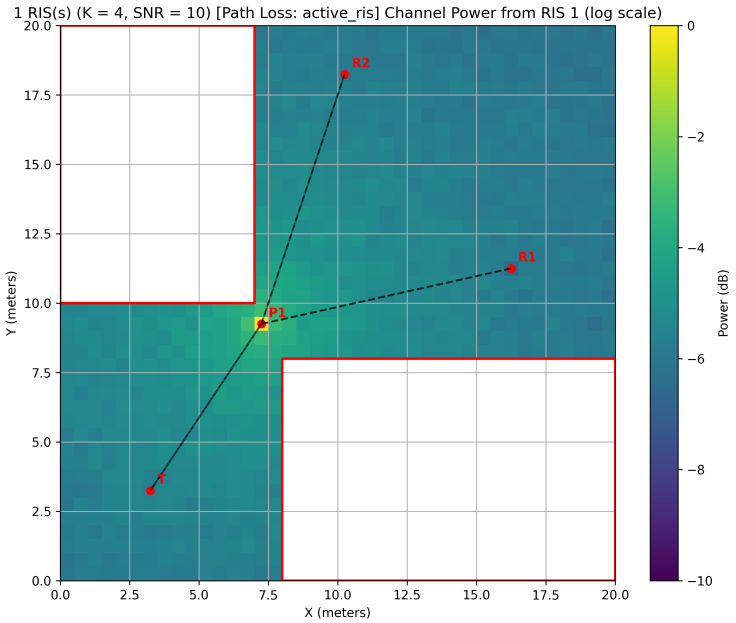

Figure 5.7: 1 RIS(s) [Path Loss: active ris] Channel Power from RIS 1 (log scale)

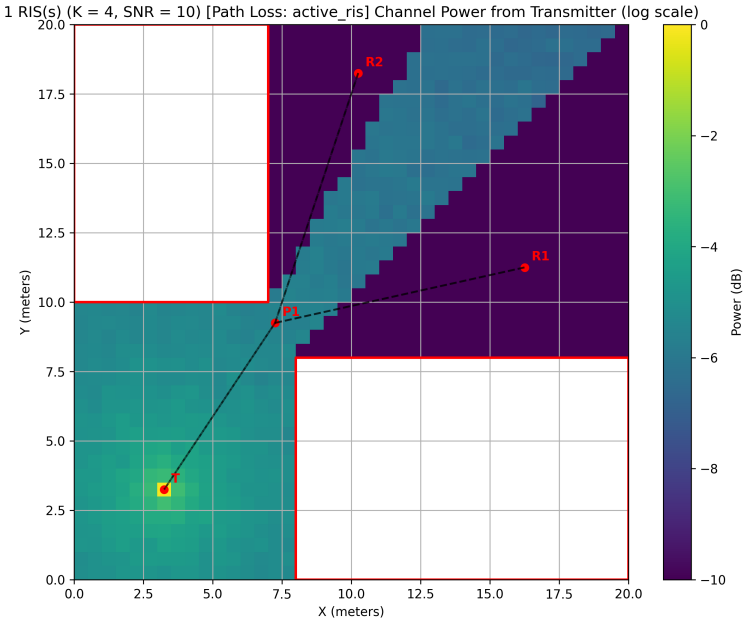

Figure 5.8: 1 RIS(s) [Path Loss: active ris] Channel Power from Transmitter (log scale)

Path loss: product With this type of path loss, the signal coming from the RIS has significantly less power than the direct link from the transmitter, and cannot influence significantly the outcome. Outside LOS, the framework still works as expected.

The power of the signal reflected from the RIS is so low, it does not show in the heatmap, as it is lower than $1e-10$.

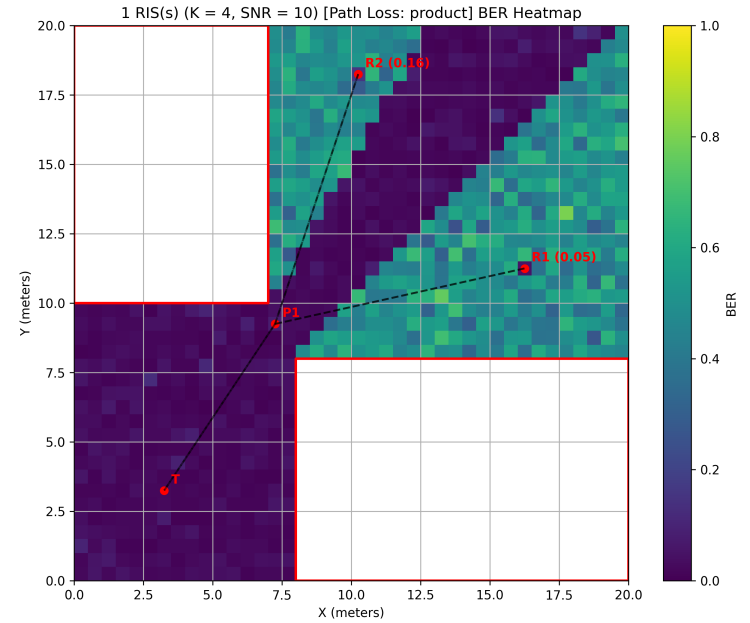

Figure 5.9: 1 RIS(s) [Path Loss: product] BER Heatmap

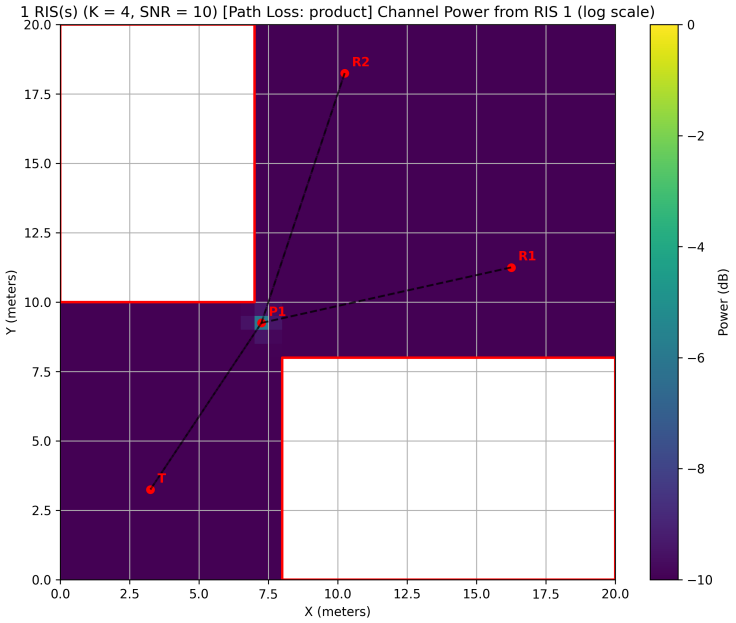

Figure 5.10: 1 RIS(s) [Path Loss: product] Channel Power from RIS 1 (log scale)

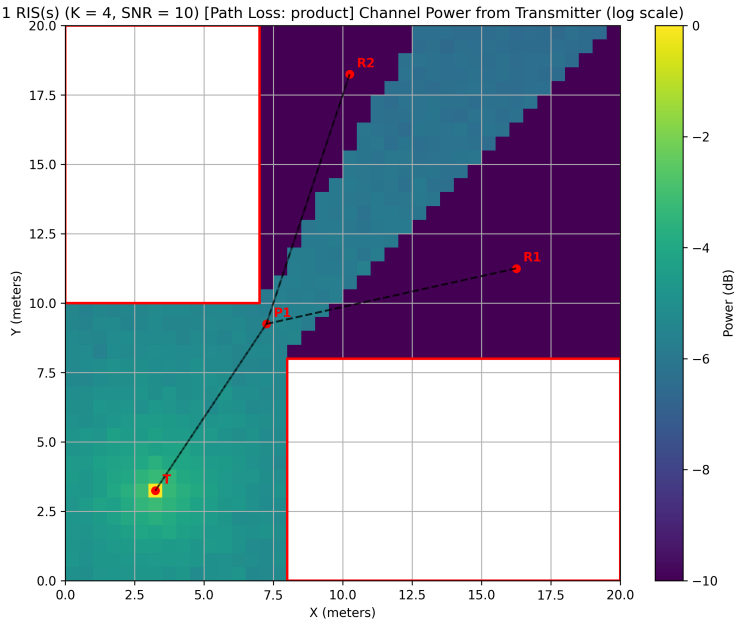

Figure 5.11: 1 RIS(s) [Path Loss: product] Channel Power from Transmitter (log scale)

Path loss: sum This is the path loss that better confirms our previous BER analysis. Without LOS, the BER for eavesdropper is stable at 0.5, the same as random guessing. With LOS, the RIS is still able to influence significantly the outcome, with more noise that reduces the BER at 0.3

We can see how the power coming from the RIS reflection looks more uniform than the others. This is because, as we said before, this type of path loss actually models a directional RIS. The total result of this graph does not exist. You could see them as the union of all the possible graphs considering a single direction of the reflection.

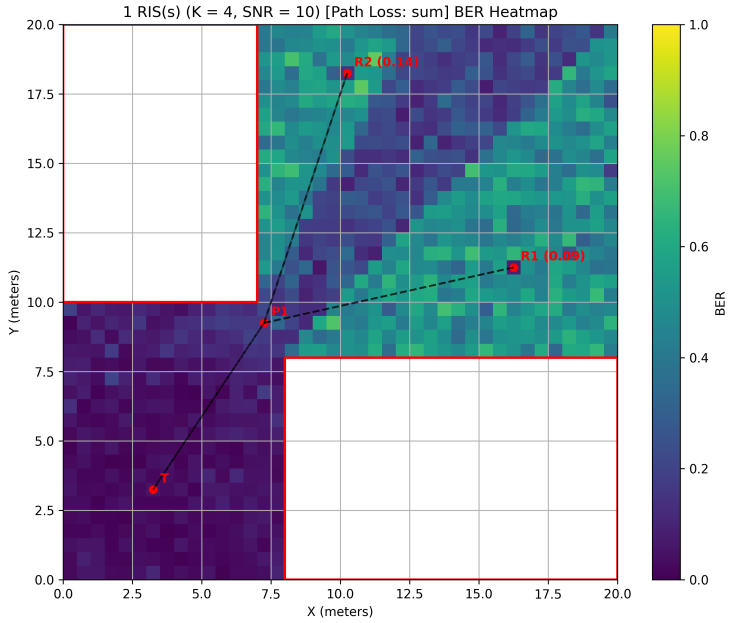

Figure 5.12: 1 RIS(s) [Path Loss: sum] BER Heatmap

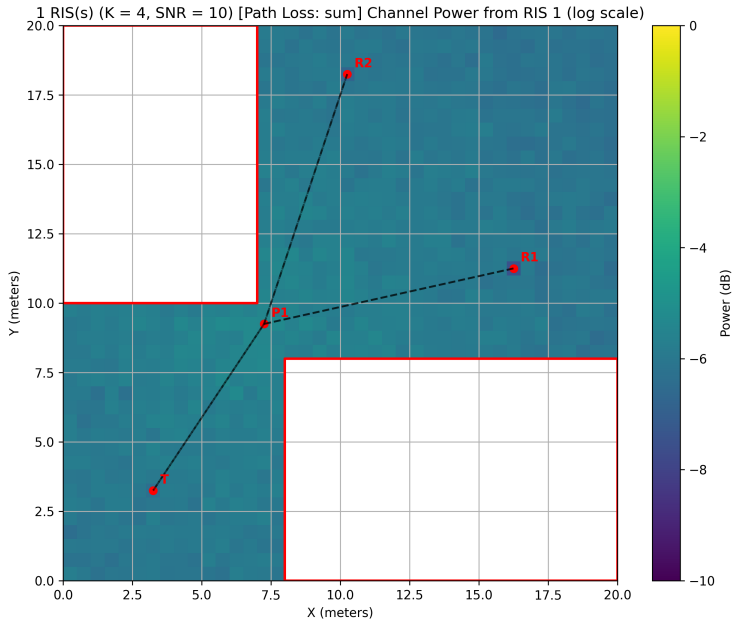

Figure 5.13: 1 RIS(s) [Path Loss: sum] Channel Power from RIS 1 (log scale)

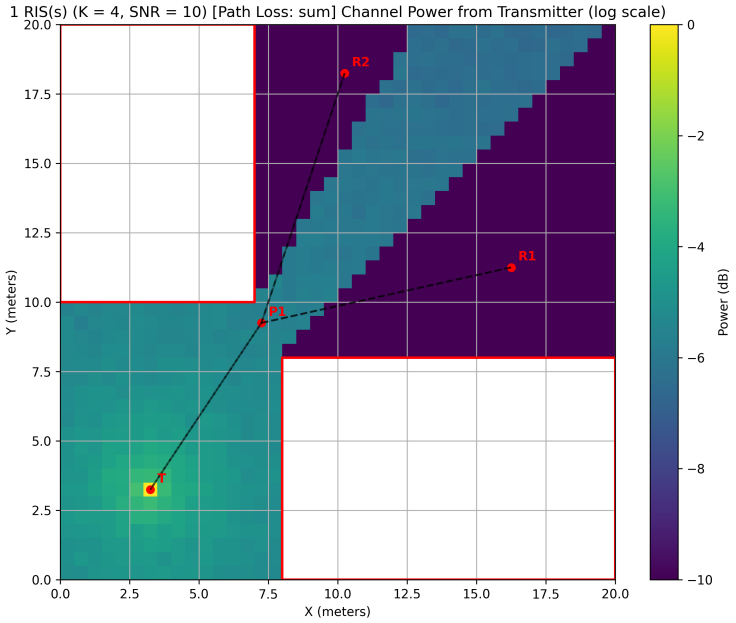

Figure 5.14: 1 RIS(s) [Path Loss: sum] Channel Power from Transmitter (log scale)

5.2.4 Double reflection from 2 RIS in series

It is certainly interesting to also study what would happen if we concatenate two RIS in series in relation to their combined path loss. For these tests, we used $\lambda = 0.08m, \tau = 0.6, \xi = 1, \eta = 0.9, SNR = 10db, K = 2, N = 16$.

All scenarios suppose the RIS use the same kind of path loss, meaning they are of different kind (active, passive uniform, passive directional). Of course, it would be an interesting case studying combining different variations of them to reach the most cost and power - efficient configuration.

Additional scenarios with RIS in parallel would also be valuable for future research, as they would likely show promising security characteristics based on our preliminary analysis.

Path loss: active Similar to the previous scenario, we can clearly see where the RIS have significant power to influence the signal reception, and where without LOS the signal is undecipherable for eavesdroppers.

As said before, it is slightly visible where the direct signal from **T** is and is not present. It is not visible however the difference where only **P2** creates interference from where both **P1** and **P2** contribute to the noise. You could imagine the area by selecting the intersection between the two RIS Channel Power graphs.

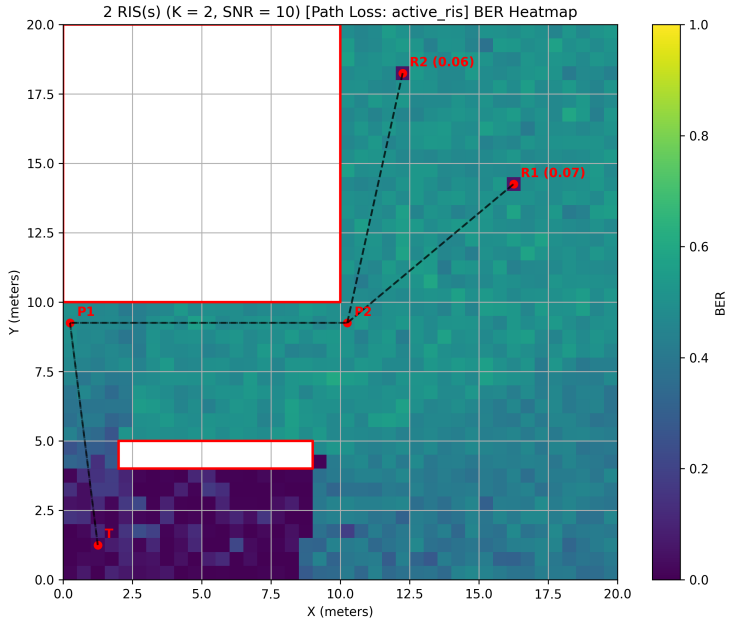

Figure 5.15: 2 RIS(s) [Path Loss: active ris] BER Heatmap

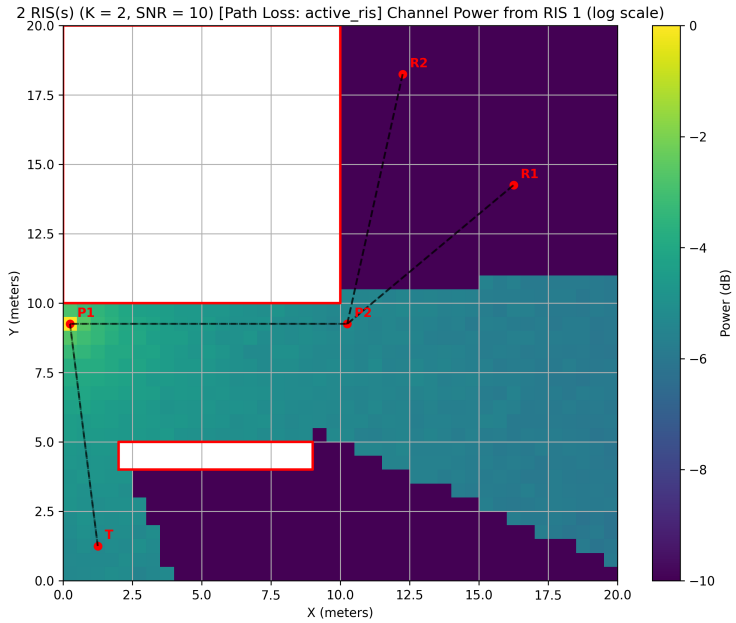

Figure 5.16: 2 RIS(s) [Path Loss: active ris] Channel Power from RIS 1 (log scale)

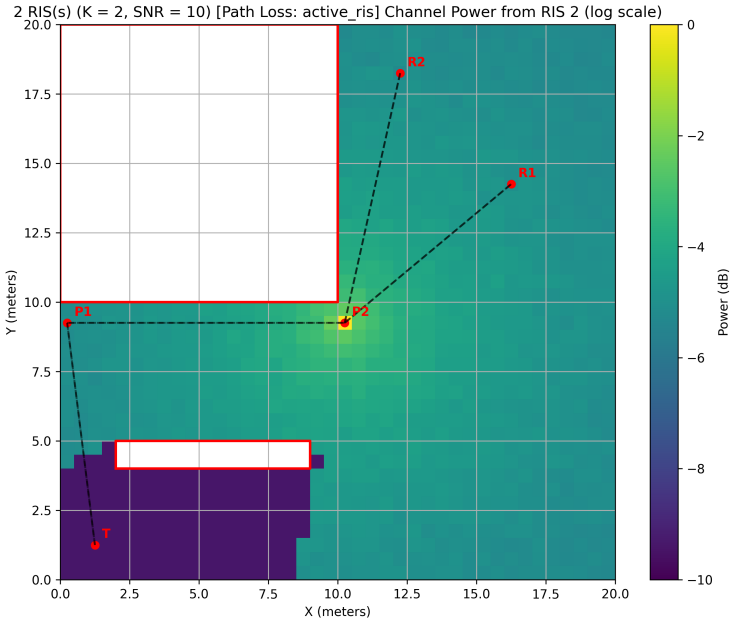

Figure 5.17: 2 RIS(s) [Path Loss: active ris] Channel Power from RIS 2 (log scale)

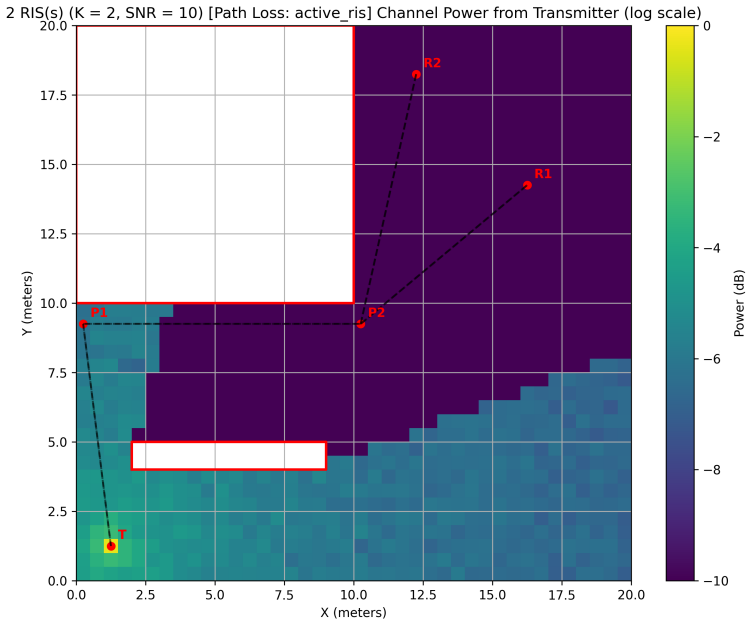

Figure 5.18: 2 RIS(s) [Path Loss: active ris] Channel Power from Transmitter (log scale)

Path loss: product We can draw similar conclusions as before for the product path loss. As we can see, the direct signal is not disturbed, and the reflection from **P2** after being already reflected from **P1** is so low, it does not even show on the **P2** position itself.

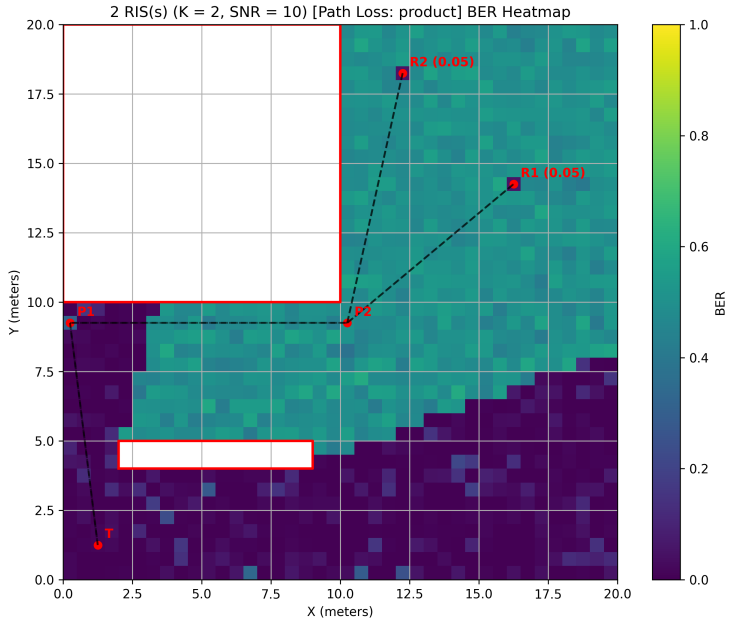

Figure 5.19: 2 RIS(s) [Path Loss: product] BER Heatmap

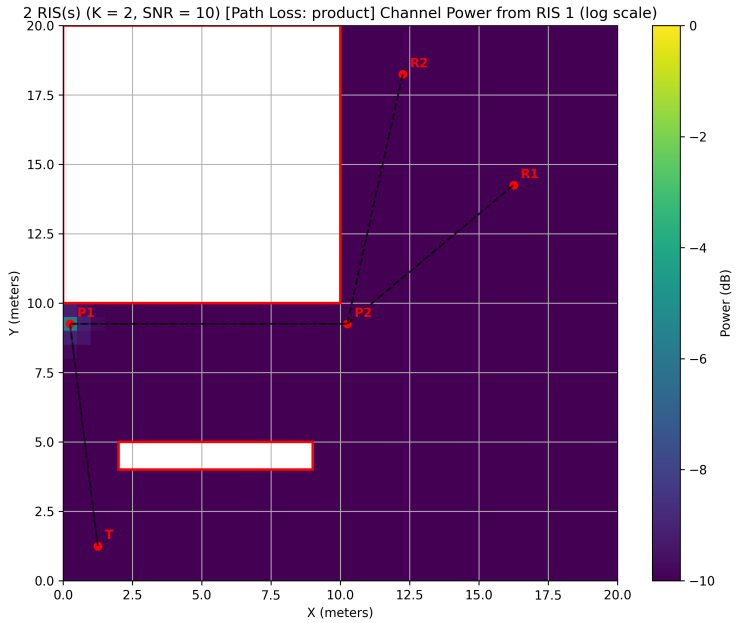

Figure 5.20: 2 RIS(s) [Path Loss: product] Channel Power from RIS 1 (log scale)

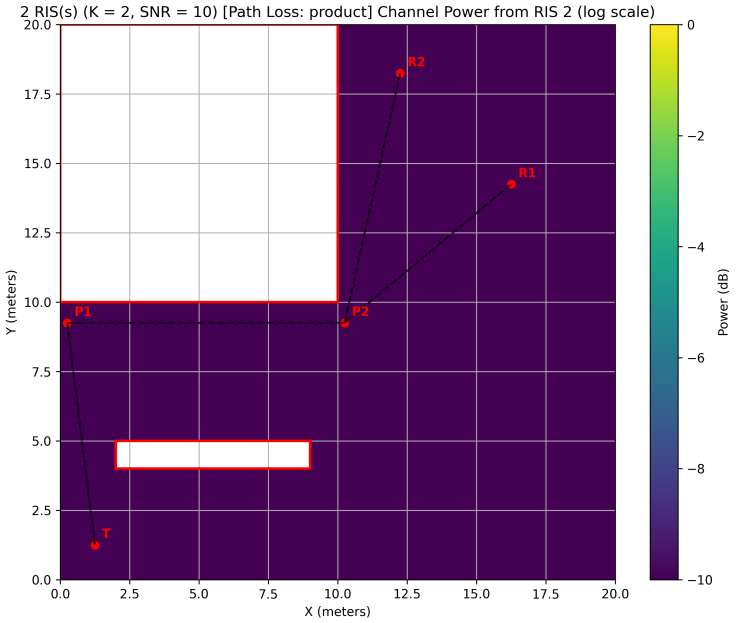

Figure 5.21: 2 RIS(s) [Path Loss: product] Channel Power from RIS 2 (log scale)

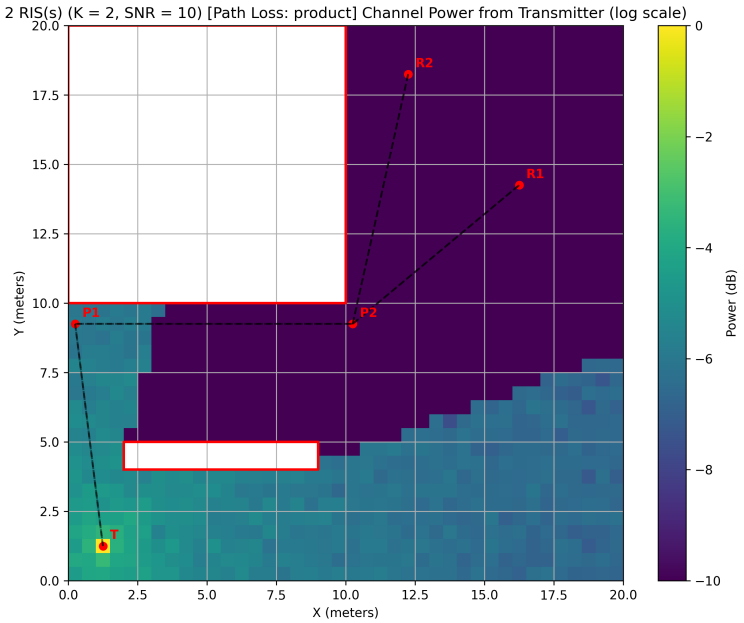

Figure 5.22: 2 RIS(s) [Path Loss: product] Channel Power from Transmitter (log scale)

Path loss: sum The distinction between having or not LOS are very visible here. The displayed values for the BER are in line with the previous graph on the same kind of path loss.

Like the active path loss, here there is no difference in having a single disturbance from **P2** versus from both **P1** and **P2**.

We do remember also here that this graph is not realistic, as RIS should be directional. Again, we invite you to consider this as the sum of all possible direction the RIS could take.

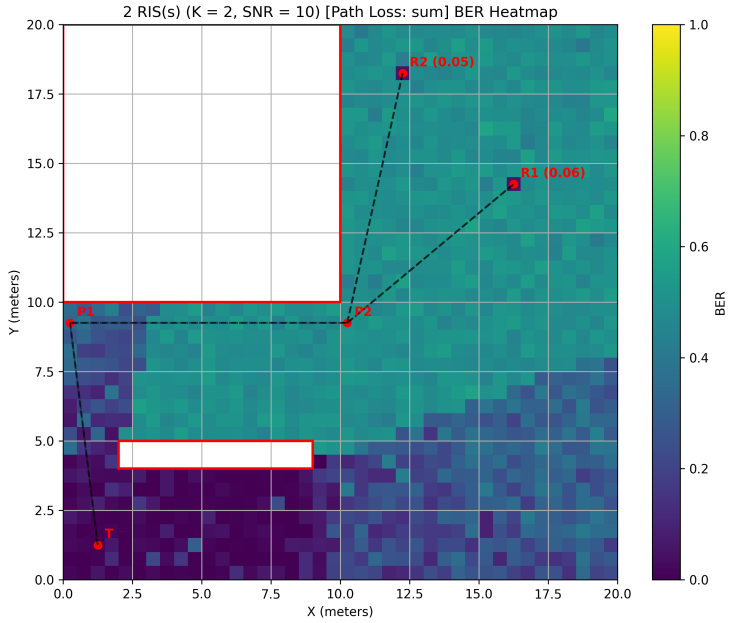

Figure 5.23: 2 RIS(s) [Path Loss: sum] BER Heatmap

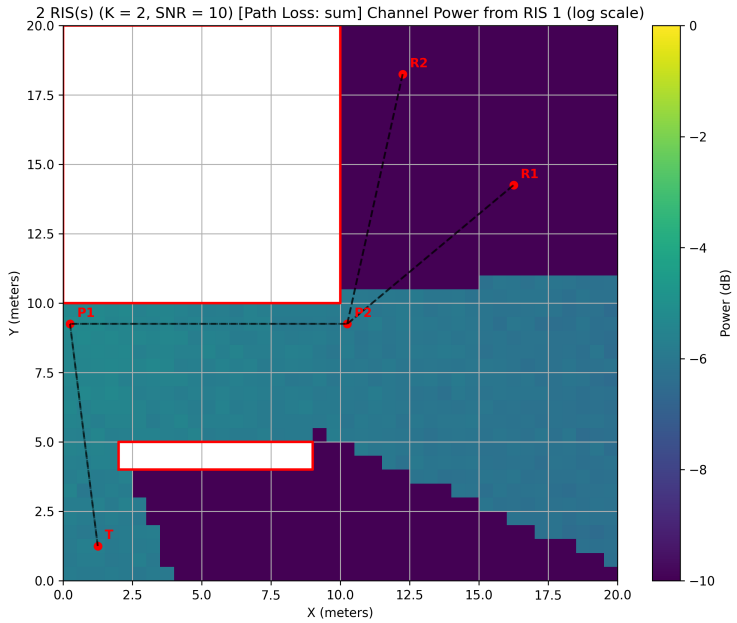

Figure 5.24: 2 RIS(s) [Path Loss: sum] Channel Power from RIS 1 (log scale)

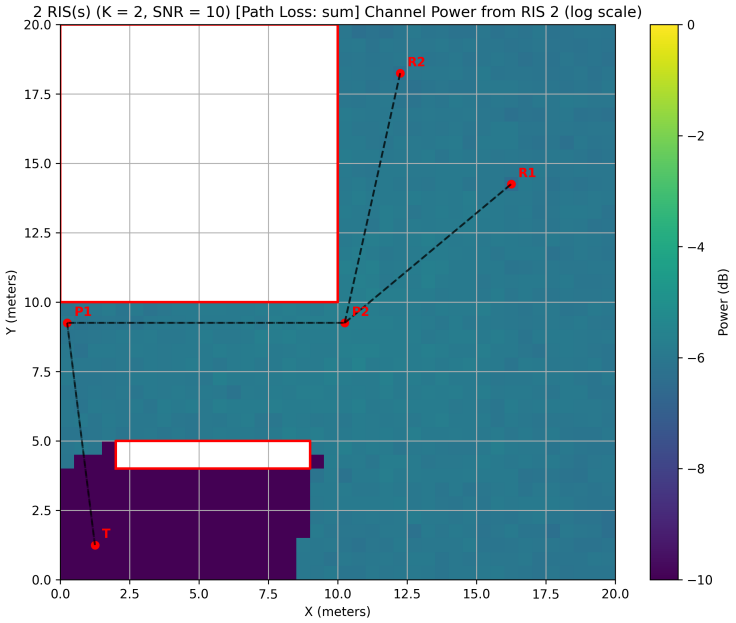

Figure 5.25: 2 RIS(s) [Path Loss: sum] Channel Power from RIS 2 (log scale)

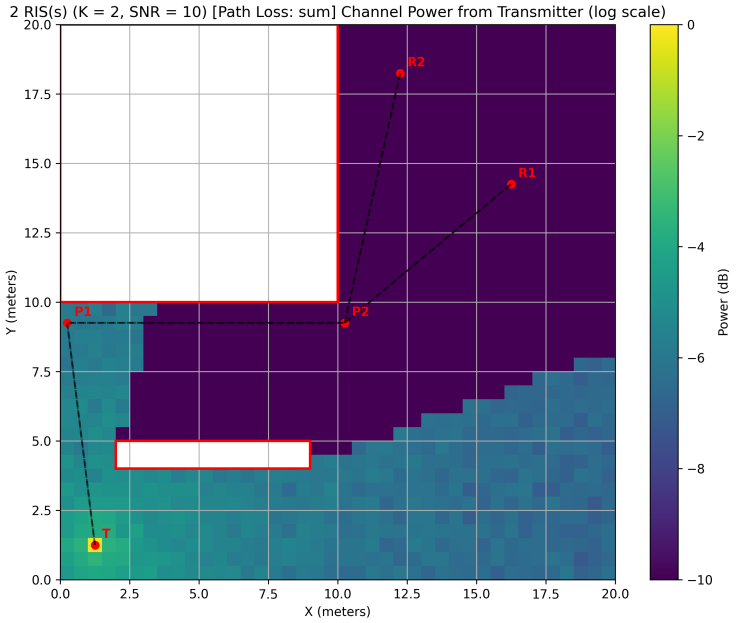

Figure 5.26: 2 RIS(s) [Path Loss: sum] Channel Power from Transmitter (log scale)

5.2.5 Heatmap conclusions

We can see from the proposed path loss common properties:

- with *active path loss*, the RIS channel power is of the same order of magnitude as the transmitter channel power, so the direct signal receives significant noise. The problem is that, being an active RIS, it costs way more in both the deployment and the maintenance;
- with *product path loss*, the RIS channel power is orders of magnitude smaller. The message

remains hidden in areas without direct line of sight to the transmitter. If the budget is tight, or the direct LOS security is less needed compared to the non LOS security (for example, if the space in LOS with the transmitter is completely under control), this is an excellent possibility;

- with *sum path loss*, the disturbance effect is still visible, although less effective. It also the one with the results most similar to the theoretical simulation we made in the previous section. Of course, the results must be considered keeping in mind that the RIS would be directional. It is an optimal choice for example to provide noise in a specific area, or if the scenario is composed of tight hallways.

Depending on the scenario, the budget and the level of security and obscuration needed, our framework provides an excellent choice for different kinds of situations and contexts.

Unfortunately, for specific vehicular applications, our framework is not really flexible due to the specific relation between the position, the distance and the channel gain matrix which then influence the readability of the signal. Our framework is still usable and highly recommended for static antennas and actors. For example, in a crossroad fixed antennas could communicate with the cars in the LOS using standard communication protocols, and with each other using RIS and our framework. The autonomous cars could also implement a traffic light - free crossroad queue system, when they would stop, communicate and coordinate with each other for who can go first. Common distributed algorithms for leader election could be used, like the *Bully Algorithm* [9].

It should be noted that the main difficulty in using our framework in conjunction with high speed moving vehicles is because of the channel gain estimation, since we do not only need the current one, but predict the next one where the car would go. Promising results are already coming in like in the paper "*Adaptive Massive MIMO for fast moving connected vehicles: It will work with Predictor Antennas!*" [25], which studies how to use a different set of antennas, called Predictor Antennas, used to predict the main one channel gain with great accuracy. Similar literature can be found, showing a great interest in the field. For example, we also cite "*Channel Estimation for Reconfigurable Intelligent Surface Assisted High-Mobility Wireless Systems*" [39], which proposes a new way to mitigate the error deriving from the movement speed, *achieving substantial power efficiency improvements* at speeds up to 90 mph and with as few as $N = 16$ RIS elements.

6 Conclusion

In this paper, we have expanded on the work presented in [22] regarding Physical Layer Security using Reconfigurable Intelligent Surfaces (RISs). We generalized the framework to support multiple receiving users and multiple RIS configurations, both in parallel and in series. By mathematically proving the formulas, and physically simulating realistic scenarios, we demonstrated the validity and usefulness of the proposed work.

With our contribution, the framework is now able to manage:

- Multiple receivers in different positions
- Multiple RISs in parallel that increase signal quality and security
- Multiple RISs working in series to accommodate complex situations
- A wide combination of these properties in realistic network conditions

With our Bit Error Rate (BER) simulations, we proved and demonstrated how the receivers are able to receive correctly the messages with a low error percentage, while ensuring no other malicious actor can decipher the signal when not having direct Line of Sight (LOS) from the transmitter. Even when this link is present, our configurations ensure the RIS disrupt the interception of the signal with significant noise, even at high Signal to Noise Ratio (SNR).

We also showed the realistic application of our framework in a simulated scenario including realistic channel gain calculations, adding Rician fading and considering signal strength using path loss. These added simulations will aid exporting our solution from a mathematical proof to an effective implementation usable for real life communication. We modeled different possibilities of path loss and RIS implementation to cover all possible variables, showing promising results even in the worst scenarios.

The implications of this work are particularly relevant for emerging technologies such as vehicular networks, Internet of Things, and other applications requiring secure wireless communications. Thanks to modern technologies, we are able to increase the security and privacy even at lower layers of communication, helping to reduce the load on higher layers which could impact negatively the usefulness of communications when latency and frequency of communication are crucial.

6.1 Future directions

Future research directions could include:

- Further optimization of RIS configurations for dynamic environments with mobile nodes
- Integration with existing security protocols at higher network layers
- Usage of more complex communication protocols, like GSSK [14] instead of the proposed SSK [15]
- Implementation and testing in real-world scenarios, particularly in vehicular networks
- Extension to even more complex network topologies with multiple transmitters and heterogeneous receiver capabilities

In particular, there is ample work that is possible to do in the heatmap simulations. For example, parallelization and the introduction of multiple RIS paths could be added, and a GUI to graphically set up the environment could be the start of a complex simulation environment.

The different types of path loss could be expanded in a more complete study of the different kinds of RIS: what would be the mathematical differences in applying our framework for active and passive

RIS, for uniform and directional ones? A simulation tool that could combine all these characteristics could be a great addition to the field of futuristic telecommunications.

Also, the entire field of Channel State Information (CSI), which here was introduced only in the part about Channel Gain matrix estimation, could also be simulated in our proposed tool and framework. Instead of using the physically calculated CSI, actors and RIS could try to communicate using estimations of it and then verify the actual realistic results, including in our software estimation simulation functions.

The implementation of our research in vehicular networks is also an interesting topic directly linked to the CSI one. Expanding the context here with modern research on channel estimation of moving actors could transform our proposed work into a promising candidate for the future of autonomous telecommunications.

In conclusion, our extended framework for physical layer security using RISs provides a promising approach to secure modern wireless communication systems, especially in scenarios where traditional encryption methods may introduce unacceptable computational overhead or latency. The flexibility to support multiple users and complex reflection paths makes it adaptable to various practical deployment scenarios while maintaining strong security guarantees.

Bibliography

[1] Yun Ai, Michael Cheffena, Aashish Mathur, and Hongjiang Lei. On physical layer security of double rayleigh fading channels for vehicular communications. *IEEE Wireless Communications Letters*, 7(6):1038–1041, Dec 2018.

[2] George C. Alexandropoulos, Konstantinos D. Katsanos, Miaowen Wen, and Daniel B. Da Costa. Counteracting eavesdropper attacks through reconfigurable intelligent surfaces: A new threat model and secrecy rate optimization. *IEEE Open Journal of the Communications Society*, 4:1285–1302, 2023.

[3] Ertugrul Basar, Marco Di Renzo, Julien De Rosny, Merouane Debbah, Mohamed-Slim Alouini, and Rui Zhang. Wireless communications through reconfigurable intelligent surfaces. *IEEE Access*, 7:116753–116773, 2019.

[4] Emil Björnson, Özgecan Özdogan, and Erik G. Larsson. Intelligent reflecting surface versus decode-and-forward: How large surfaces are needed to beat relaying? *IEEE Wireless Communications Letters*, 9(2):244–248, Feb 2020.

[5] Jie Chen, Ying-Chang Liang, Yiyang Pei, and Huayan Guo. Intelligent reflecting surface: A programmable wireless environment for physical layer security. *IEEE Access*, 7:82599–82612, 2019.

[6] Min Deng, Manzoor Ahmed, Abdul Wahid, Aized Amin Soofi, Wali Ullah Khan, Fang Xu, Muhammad Asif, and Zhu Han. Reconfigurable intelligent surfaces enabled vehicular communications: A comprehensive survey of recent advances and future challenges. *IEEE Transactions on Intelligent Vehicles*, pages 1–28, 2024.

[7] Mohamed A. ElMossallamy, Hongliang Zhang, Lingyang Song, Karim G. Seddik, Zhu Han, and Geoffrey Ye Li. Reconfigurable intelligent surfaces for wireless communications: Principles, challenges, and opportunities. *IEEE Transactions on Cognitive Communications and Networking*, 6(3):990–1002, Sep. 2020.

[8] Math Stack Exchange. How is the null space related to singular value decomposition? `https://math.stackexchange.com/questions/1771013/how-is-the-null-space-related-to-singular-value-decomposition`.

[9] Geeks for Geeks. Bully algorithm in distributed system. `https://www.geeksforgeeks.org/bully-algorithm-in-distributed-system/`.

[10] S. Goel and R. Negi. Secret communication in presence of colluding eavesdroppers. In *MILCOM 2005 - 2005 IEEE Military Communications Conference*, pages 1501–1506 Vol. 3, Oct 2005.

[11] Satashu Goel and Rohit Negi. Guaranteeing secrecy using artificial noise. *IEEE Transactions on Wireless Communications*, 7(6):2180–2189, June 2008.

[12] Xiang He and Aylin Yener. Providing secrecy when the eavesdropper channel is arbitrarily varying: A case for multiple antennas. In *2010 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 1228–1235, Sep. 2010.

[13] Zhen-Qing He and Xiaojun Yuan. Cascaded channel estimation for large intelligent metasurface assisted massive mimo. *IEEE Wireless Communications Letters*, 9(2):210–214, Feb 2020.

[14] Jeyadeepan Jeganathan, Ali Ghrayeb, and Leszek Szczecinski. Generalized space shift keying modulation for mimo channels. In *2008 IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications*, pages 1–5, Sep. 2008.

[15] Jeyadeepan Jeganathan, Ali Ghrayeb, Leszek Szczecinski, and Andres Ceron. Space shift keying modulation for mimo channels. *IEEE Transactions on Wireless Communications*, 8(7):3692–3703, July 2009.

[16] Jungi Jeong, Jun Hwa Oh, Seung Yoon Lee, Yuntae Park, and Sang-Hyuk Wi. An improved path-loss model for reconfigurable-intelligent-surface-aided wireless communications and experimental validation. *IEEE Access*, 10:98065–98078, 2022.

[17] Dimitrios S. Karas, Alexandros–Apostolos A. Boulogeorgos, and George K. Karagiannidis. Physical layer security with uncertainty on the location of the eavesdropper. *IEEE Wireless Communications Letters*, 5(5):540–543, Oct 2016.

[18] Ravneet Kaur, Bajrang Bansal, Sudhan Majhi, Sandesh Jain, Chongwen Huang, and Chau Yuen. A survey on reconfigurable intelligent surface for physical layer security of next-generation wireless communications. *IEEE Open Journal of Vehicular Technology*, 5:172–199, 2024.

[19] Steven Kisseleff, Wallace A. Martins, Hayder Al-Hraishawi, Symeon Chatzinotas, and Björn Ottersten. Reconfigurable intelligent surfaces for smart cities: Research challenges and opportunities. *IEEE Open Journal of the Communications Society*, 1:1781–1797, 2020.

[20] Sushil Kumar, Upasana Dohare, Kirshna Kumar, Durga Prasad Dora, Kashif Naseer Qureshi, and Rupak Kharel. Cybersecurity measures for geocasting in vehicular cyber physical system environments. *IEEE Internet of Things Journal*, 6(4):5916–5926, Aug 2019.

[21] Ruizhe Long, Ying-Chang Liang, Yiyang Pei, and Erik G. Larsson. Active reconfigurable intelligent surface-aided wireless communications. *IEEE Transactions on Wireless Communications*, 20(8):4962–4975, Aug 2021.

[22] Junshan Luo, Fanggang Wang, Shilian Wang, Hao Wang, and Dong Wang. Reconfigurable intelligent surface: Reflection design against passive eavesdropping. *IEEE Transactions on Wireless Communications*, 20(5):3350–3364, May 2021.

[23] Abubakar U. Makarfi, Khaled M. Rabie, Omprakash Kaiwartya, Kabita Adhikari, Xingwang Li, Marcela Quiroz-Castellanos, and Rupak Kharel. Reconfigurable intelligent surfaces-enabled vehicular networks: A physical layer security perspective, 2020.

[24] Amitav Mukherjee, S. Ali A. Fakoorian, Jing Huang, and A. Lee Swindlehurst. Principles of physical layer security in multiuser wireless networks: A survey. *IEEE Communications Surveys and Tutorials*, 16(3):1550–1573, Third 2014.

[25] Dinh-Thuy Phan-Huy, Stefan Wesemann, Joachim Bjoersell, and Mikael Sternad. Adaptive massive mimo for fast moving connected vehicles: It will work with predictor antennas! In *WSA 2018; 22nd International ITG Workshop on Smart Antennas*, pages 1–8, March 2018.

[26] Annapurna Pradhan, Susmita Das, Md Jalil Piran, and Zhu Han. A survey on physical layer security of ultra/hyper reliable low latency communication in 5g and 6g networks: Recent advancements, challenges, and future directions. *IEEE Access*, 12:112320–112353, 2024.

[27] Michele Segata, Paolo Casari, Marios Lestas, Alexandros Papadopoulos, Dimitrios Tyrovolas, Taqwa Saeed, George Karagiannidis, and Christos Liaskos. Cooperis: A framework for the simulation of reconfigurable intelligent surfaces in cooperative driving environments. *Computer Networks*, 248:110443, 2024.

[28] C. E. Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715, Oct 1949.

[29] Yi-Sheng Shiu, Shih Yu Chang, Hsiao-Chun Wu, Scott C.-H. Huang, and Hsiao-Hwa Chen. Physical layer security in wireless networks: a tutorial. *IEEE Wireless Communications*, 18(2):66–74, April 2011.

[30] P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, Nov 1994.

[31] Chris Sperandio and Paul G. Flikkema. Wireless physical-layer security via transmit precoding over dispersive channels: Optimum linear eavesdropping. pages 1113–1117, 2002. 2002 MILCOM Proceedings; Global Information GRID - Enabling Transformation Through 21st Century Communications ; Conference date: 07-10-2002 Through 10-10-2002.

[32] Xiao Tang, Dawei Wang, Ruonan Zhang, Zheng Chu, and Zhu Han. Jamming mitigation via aerial reconfigurable intelligent surface: Passive beamforming and deployment optimization. *IEEE Transactions on Vehicular Technology*, 70(6):6232–6237, June 2021.

[33] Wade Trappe. The challenges facing physical layer security. *IEEE Communications Magazine*, 53(6):16–20, June 2015.

[34] Georgios C. Trichopoulos, Panagiotis Theofanopoulos, Bharath Kashyap, Aditya Shekhawat, Anuj Modi, Tawfik Osman, Sanjay Kumar, Anand Sengar, Arkajyoti Chang, and Ahmed Alkhateeb. Design and evaluation of reconfigurable intelligent surfaces in real-world environment. *IEEE Open Journal of the Communications Society*, 3:462–474, 2022.

[35] David Tse and Pramod Viswanath. Fundamentals of wireless communication. `https://web.stanford.edu/~dntse/Chapters_PDF/Fundamentals_Wireless_Communication_chapter7.pdf`, 2005.

[36] Wikipedia. Free space path loss. `https://en.wikipedia.org/wiki/Free-space_path_loss`.

[37] Wikipedia. Rice distribution. `https://en.wikipedia.org/wiki/Rice_distribution`.

[38] Wikipedia. Rician fading. `https://en.wikipedia.org/wiki/Rician_fading`.

[39] Chao Xu, Jiancheng An, Tong Bai, Shinya Sugiura, Robert G. Maunder, Zhaocheng Wang, Lie-Liang Yang, and Lajos Hanzo. Channel estimation for reconfigurable intelligent surface assisted high-mobility wireless systems. *IEEE Transactions on Vehicular Technology*, 72(1):718–734, Jan 2023.

[40] Janghyuk Youn, Woong Son, and Bang Chul Jung. Physical-layer security improvement with reconfigurable intelligent surfaces for 6g wireless communication systems. *Sensors*, 21(4), 2021.

Appendix A Code Implementation

To validate our theoretical framework, we have implemented a simulation environment in Python that allows us to test both our mathematical models and their real-world applicability. The codebase consists of three main modules: diagonalization, bit error rate (BER) analysis, and a heatmap generator to visualize the spatial distribution of signal quality.

A.1 Diagonalization Module

The diagonalization module implements the core mathematical concepts of our RIS reflection framework, following the theoretical foundation presented in Section 3 and 4.

A.1.1 Null Space Calculation

We first start by making the calculation of reflection matrices, which ensure the effective channel between the transmitter and receiver is diagonalized. We implement this through the `calculate_W_single` and `calculate_W_multiple` functions:

```python
def calculate_W_single(K: int, N: int, G: np.ndarray, H: np.ndarray) -> np.ndarray:
    """
    Calculate W matrix for a single receiver.

    Args:
        K: Number of antennas
        N: Number of reflecting elements
        G: Channel matrix from RIS to receiver (KxN)
        H: Channel matrix from transmitter to RIS (NxK)

    Returns:
        W: The W matrix as defined in equation (8) of the paper
    """
    W = np.zeros((N, N), dtype=complex)

    for i in range(K):
        for j in range(K):
            if i != j:
                temp = np.multiply(G[j, :], H[:, i].T)
                W += np.outer(temp.conj(), temp)

    return W
```

Code A.1: Calculation of W matrices

This function calculates the W matrix for a single receiver. For multiple receivers, we stack these matrices:

```python
def calculate_W_multiple(K: int, N: int, J: int, Gs: List[np.ndarray], H: np.
    ndarray) -> np.ndarray:
    """
    Calculate combined W matrix for multiple receivers.
    """
    W_combined = np.zeros((J * N, N), dtype=complex)

    for j in range(J):
```

```
        W_j = calculate_W_single(K, N, Gs[j], H)
        W_combined[j*N:(j+1)*N, :] = W_j

    return W_combined
```

Code A.2: W matrix for multiple receivers

A.1.2 RIS Reflection Matrix Calculation

With the W matrix defined, we can calculate the reflection matrices using Singular Value Decomposition (SVD) to find the null space:

```
def calculate_ris_reflection_matrice(
    K: int,
    N: int,
    J: int,
    Gs: List[np.ndarray],
    H: np.ndarray,
    eta: float,
) -> Tuple[np.ndarray, float]:
    """
    Calculate reflection matrices for RIS surfaces.
    """
    W = calculate_W_multiple(K, N, J, Gs, H)
    U, sigma, Vh = np.linalg.svd(W)

    null_space_dim = N - J*K**2 + J*K
    if null_space_dim <= 0:
        raise ValueError(f"No solution exists. Need more reflecting elements.")

    first_singular_values = sigma[:N - null_space_dim]
    last_singular_values = sigma[-null_space_dim:]

    null_space_basis = Vh[-null_space_dim:, :].T.conj()

    if null_space_basis.shape != (N, null_space_dim):
        raise ValueError(f"Invalid null space basis shape.")

    a = np.random.normal(0, 1, (null_space_dim,)) + 1j * np.random.normal(0, 1, (
    null_space_dim,))

    p_unnormalized = null_space_basis @ a
    p = eta * p_unnormalized / np.max(np.abs(p_unnormalized))
    P = np.diag(p)
    dor = 2 * null_space_dim
    return P, dor
```

Code A.3: RIS Reflection Matrix Calculation

This function implements the theoretical approach described in Section 4.1, where we find the null space of W and then generate a random vector in this space to ensure randomness in our reflection coefficients.

A.1.3 Multiple RIS Support

To support multiple RIS surfaces in series, we implemented:

```
def calculate_multi_ris_reflection_matrices(
    K: int,
    N: int,
    J: int,
    M: int,
    Gs: List[np.ndarray],
    H: np.ndarray,
    eta: float,
    Cs: List[np.ndarray]
```

```
) -> Tuple[List[np.ndarray], float]:
    """
    Calculate reflection matrices for M RIS surfaces.
    """
    if len(Cs) != M-1:
        raise ValueError(f"Expected {M-1} inter-RIS channel matrices.")

    ps = []
    S = np.eye(N)

    # Generate M-1 random reflection vectors
    for i in range(M-1):
        absorptions = np.random.uniform(0, 1, N)
        phases = np.random.uniform(0, 2*np.pi, N)
        # p_m[i] = eta * r_i * exp(j*theta_i)
        p_m = absorptions * np.exp(1j * phases)
        ps.append(p_m)
        S = S @ np.diag(p_m) @ Cs[i]

    Gs_prime = [G @ S for G in Gs]

    # Calculate the last reflection matrix
    P_final, dor = calculate_ris_reflection_matrice(K, N, J, Gs_prime, H, eta)
    p_final = np.diag(P_final)
    ps.append(p_final)

    Ps = []
    for pm in ps:
        Ps.append(np.diag(pm))

    return Ps, dor
```

Code A.4: Multiple RIS calculation

This implements our approach from Section 4.3, where we generate random reflection coefficients for all but the last RIS, then calculate the last one to ensure diagonalization.

A.1.4 Unified Reflection Matrix

For convenience in calculations, we provide a function to unify multiple reflection matrices into a single effective matrix:

```
def unify_ris_reflection_matrices(Ps: List[np.ndarray], Cs: List[np.ndarray]) -> np
    .ndarray:
    """
    Unify reflection matrices into a single matrix.
    """
    P = Ps[0]
    for i in range(len(Ps)-1):
        P = P @ Cs[i] @ Ps[i+1]
    return P
```

Code A.5: Unifying RIS matrices

A.1.5 Verification

We also implement verification functions to ensure our theoretical expectations match the implementation:

```
def verify_multi_ris_diagonalization(
    Ps: List[np.ndarray],
    Gs: List[np.ndarray],
    H: np.ndarray,
    Cs: List[np.ndarray]
) -> List[bool]:
    """
```

```
    Verify that G(P_1C_1P_2C_2...P_M)H is diagonal for all receivers.
    """
    results = []

    P = unify_ris_reflection_matrices(Ps, Cs)
    for G in Gs:
        effective_channel = G @ P @ H
        off_diag_sum = np.sum(np.abs(effective_channel - np.diag(np.diag(
    effective_channel))))
        results.append(off_diag_sum < tolerance)
    return results
```

Code A.6: Verification of diagonalization

A.2 BER Module

The BER (Bit Error Rate) module implements the simulation of space shift keying (SSK) transmissions and calculates the error rates under different scenarios.

A.2.1 SSK Transmission Simulation

We simulate SSK transmission with the following core functions:

```
def simulate_ssk_transmission(K: int, sigma_sq: float, calculate_detected_id:
    Callable[[np.ndarray, np.ndarray], float]):
    n_bits = int(np.log2(K))
    if 2**n_bits != K:
        raise ValueError(f"K must be a power of 2, got {K}")
    bit_mappings = np.array([format(i, f'0{n_bits}b') for i in range(K)])
    true_bits = np.random.randint(0, 2, n_bits)
    true_bits_str = ''.join(map(str, true_bits))
    true_idx = np.where(bit_mappings == true_bits_str)[0][0]

    x = np.zeros(K)
    x[true_idx] = 1

    noise = create_random_noise_vector(K, sigma_sq)
    detected_idx = calculate_detected_id(x, noise)

    detected_bits = np.array(list(bit_mappings[detected_idx])).astype(int)
    errors = np.sum(detected_bits != true_bits)
    return errors / n_bits
```

Code A.7: SSK Transmission Simulation

This function implements the common core of our SSK transmission simulation. It maps bits to antenna indices, simulates transmission with noise, and calculates the error rate.

We then implement specialized versions for reflection and direct transmission:

```
def simulate_ssk_transmission_reflection(K: int, effective_channel: np.ndarray,
    sigma_sq: float):
    if effective_channel.shape != (K, K):
        raise ValueError(f"Reflection: Effective channel shape must be ({K}, {K})")

    def calculate_detected_id(x: np.ndarray, noise: np.ndarray):
        y = effective_channel @ x + noise
        return np.argmax(np.abs(y)**2)

    return simulate_ssk_transmission(K, sigma_sq, calculate_detected_id)
```

Code A.8: SSK Transmission with Reflection

```
def simulate_ssk_transmission_direct(K: int, B: np.ndarray, effective_channel: np.
    ndarray, sigma_sq: float):
    if B.shape != (K, K):
```

```
        raise ValueError(f"Direct: B shape must be ({K}, {K})")

    if effective_channel.shape != (K, K):
        raise ValueError(f"Direct: Effective channel shape must be ({K}, {K})")

    def calculate_detected_id(x: np.ndarray, noise: np.ndarray):
        y = (B + effective_channel) @ x + noise
        distances = np.array([np.linalg.norm(y - B[:, i]) for i in range(B.shape[1])])
        return np.argmin(distances)

    return simulate_ssk_transmission(K, sigma_sq, calculate_detected_id)
```

Code A.9: SSK Transmission with Direct Path

These functions implement the detection methods described in Section 3.2, where the legitimate receiver can detect the signal through the diagonalized channel, while the eavesdropper hears from the direct path and receives interference from the reflection.

A.2.2 BER Simulation

We also implement a comprehensive BER simulation function that evaluates performance across different SNR values:

```
def calculate_ber_simulation(snr_db, K, N, J, M, eta=0.9, num_symbols=10000):
    sigma_sq = snr_db_to_sigma_sq(snr_db)
    errors_receiver = 0
    errors_eavesdropper = 0
    errors_direct = 0

    errors_receiver_double = 0
    errors_eavesdropper_double = 0

    for _ in range(num_symbols):
        # Generate channel matrices
        H = generate_random_channel_matrix(N, K)
        Gs = [generate_random_channel_matrix(K, N) for _ in range(J)]
        G = random.choice(Gs)
        Fs = [generate_random_channel_matrix(K, N) for _ in range(M)]
        B = generate_random_channel_matrix(K, K)
        Cs = [generate_random_channel_matrix(N, N) for _ in range(M-1)]

        # Calculate reflection matrices
        Ps, _ = calculate_multi_ris_reflection_matrices(K, N, J, M, Gs, H, eta, Cs)
        P = unify_ris_reflection_matrices(Ps, Cs)

        # Calculate effective channels
        effective_channel_receiver = G @ P @ H
        effective_channel_eavesdropper = np.zeros((K, K), dtype=np.complex128)
        for i in range(M):
            P_to_i = unify_ris_reflection_matrices(Ps[:i+1], Cs[:i])
            effective_channel_eavesdropper += Fs[i] @ P_to_i @ H
        effective_channel_direct = np.zeros((K, K))

        # Simulate transmissions
        errors_receiver += simulate_ssk_transmission_reflection(K, effective_channel_receiver, sigma_sq)
        errors_eavesdropper += simulate_ssk_transmission_direct(K, B, effective_channel_eavesdropper, sigma_sq)
        errors_direct += simulate_ssk_transmission_direct(K, B, effective_channel_direct, sigma_sq)

        H2 = generate_random_channel_matrix(N, K)
        Gs2 = [generate_random_channel_matrix(K, N) for _ in range(J)]
        G2 = random.choice(Gs2)
        Fs2 = [generate_random_channel_matrix(K, N) for _ in range(M)]
```

```
        Cs2 = [generate_random_channel_matrix(N, N) for _ in range(M-1)]
        Ps2, _ = calculate_multi_ris_reflection_matrices(
            K, N, J, M, Gs2, H2, eta, Cs2
        )
        P2 = unify_ris_reflection_matrices(Ps2, Cs2)

        effective_channel_receiver_2 = G2 @ P2 @ H2
        effective_channel_eavesdropper_2 = np.zeros((K, K), dtype=np.complex128) # F @ P @ H
        for i in range(M):
            P_to_i = unify_ris_reflection_matrices(Ps2[:i+1], Cs2[:i])
            effective_channel_eavesdropper_2 += Fs2[i] @ P_to_i @ H2

        effective_channel_receiver_double = effective_channel_receiver + effective_channel_receiver_2
        effective_channel_eavesdropper_double = effective_channel_eavesdropper + effective_channel_eavesdropper_2

        errors_receiver_double += simulate_ssk_transmission_reflection(K, effective_channel_receiver_double, sigma_sq)
        errors_eavesdropper_double += simulate_ssk_transmission_direct(K, B, effective_channel_eavesdropper_double, sigma_sq)

    result_receiver = errors_receiver / num_symbols
    result_eavesdropper = errors_eavesdropper / num_symbols
    result_direct = errors_direct / num_symbols
    result_receiver_double = errors_receiver_double / num_symbols
    result_eavesdropper_double = errors_eavesdropper_double / num_symbols

    return result_receiver, result_eavesdropper, result_direct, result_receiver_double, result_eavesdropper_double
```

Code A.10: BER Simulation

This function simulates BER performance across legitimate receivers and eavesdroppers, including scenarios with multiple RIS surfaces and different path configurations.

A.3 Heatmap Generator

To visualize our results in a spatial context, we implemented a heatmap generator that simulates signal quality across a 2D space:

A.3.1 Core Heatmap Class

```
class HeatmapGenerator:
    def __init__(self, width: int, height: int, resolution: float = 0.5):
        """
        Initialize the heatmap generator with given dimensions.
        """
        self.width = width
        self.height = height
        self.resolution = resolution

        # Calculate grid dimensions based on resolution
        self.grid_width = int(width / resolution)
        self.grid_height = int(height / resolution)
        self.grid = np.zeros((self.grid_height, self.grid_width))
        self.buildings = []
        # Dictionary to store points with their labels and coordinates
        self.points = {}
```

Code A.11: Heatmap Generator Class

The heatmap generator creates a grid-based representation of a physical space, where we can place transmitters, receivers, and obstacles.

A.3.2 Building and Point Management

```python
def add_building(self, x: int, y: int, width: int, height: int):
    """
    Add a building to the map. Buildings are excluded from the heatmap calculation.
    """
    self.buildings.append((x, y, width, height))
    grid_x, grid_y = self._meters_to_grid(x, y)
    grid_width = int(width / self.resolution)
    grid_height = int(height / self.resolution)

    # Mark building area as NaN to exclude from heatmap
    self.grid[grid_y:grid_y+grid_height, grid_x:grid_x+grid_width] = np.nan

def add_point(self, label: str, x: float, y: float):
    """
    Add a point of interest to the map with a specific label.
    """
    if not (0 <= x < self.width and 0 <= y < self.height):
        raise ValueError(f"Point {label} coordinates ({x}, {y}) are outside the map boundaries")
    self.points[label] = (x, y)
```

Code A.12: Buildings and Points in Heatmap

These functions allow us to define the simulation environment with buildings (which block signals) and points representing transmitters, RIS surfaces, and receivers.

A.3.3 Line of Sight Checking

An important aspect of our simulation is determining whether two points have line-of-sight:

```python
def _line_intersects_building(self, x1: float, y1: float, x2: float, y2: float) -> bool:
    """
    Check if line between two points intersects any building.
    Uses line segment intersection algorithm.
    """
    def ccw(A: tuple, B: tuple, C: tuple) -> bool:
        """Returns True if points are counter-clockwise oriented"""
        return (C[1] - A[1]) * (B[0] - A[0]) > (B[1] - A[1]) * (C[0] - A[0])

    def intersect(A: tuple, B: tuple, C: tuple, D: tuple) -> bool:
        """Returns True if line segments AB and CD intersect"""
        return ccw(A, C, D) != ccw(B, C, D) and ccw(A, B, C) != ccw(A, B, D)

    for bx, by, bw, bh in self.buildings:
        building_corners = [
            (bx, by), (bx + bw, by),
            (bx + bw, by + bh), (bx, by + bh)
        ]

        for i in range(4):
            if intersect(
                (x1, y1), (x2, y2),
                building_corners[i], building_corners[(i + 1) % 4]
            ):
                return True
    return False
```

Code A.13: Line of Sight Checking

This function allows us to determine if buildings block the line-of-sight between points, which is crucial for accurate path loss simulation.

A.3.4 Distance Calculation

To model path loss, we calculate distances between points:

```python
def calculate_distance_from_point(self, point: str) -> np.ndarray:
    """
    Calculate the minimum distance from each grid cell to the specified point.
    """
    distances = np.full_like(self.grid, np.inf)
    px, py = self.points[point]

    for grid_y in range(self.grid_height):
        for grid_x in range(self.grid_width):
            if np.isnan(self.grid[grid_y, grid_x]):
                continue

            x, y = self._grid_to_meters(grid_x, grid_y)
            if self._line_intersects_building(x, y, px, py):
                continue

            distance = np.sqrt((x - px)**2 + (y - py)**2)
            distances[grid_y, grid_x] = distance

    return distances
```

Code A.14: Distance Calculation

This function creates a grid where each cell contains the distance to a specified point, setting infinite distance for points without line-of-sight due to buildings.

A.3.5 Channel Model Functions

We implement realistic channel models for our simulations:

```python
def calculate_free_space_path_loss(d: float, lam = 0.08, k = 2) -> float:
    """
    Calculate free space path loss between transmitter and receiver
    """
    if d == 0: d = 0.01
    return 1 / np.sqrt((4 * np.pi / lam) ** 2 * d ** k)

def calculate_unit_spatial_signature(incidence: float, K: int, delta: float):
    """
    Calculate the unit spatial signature vector for a given angle of incidence
    """
    directional_cosine = np.cos(incidence)
    e = np.array([(1 / np.sqrt(K)) * np.exp(-1j * 2 * np.pi * (k - 1) * delta *
    directional_cosine) for k in range(K)])
    return e.reshape(-1, 1)

def generate_rice_faiding_channel(L: int, K: int, ratio: float, total_power = 1.0)
    -> np.ndarray:
    """
    Generate a Ricean fading channel matrix
    """
    nu = np.sqrt(ratio * total_power / (1 + ratio))
    sigma = np.sqrt(total_power / (2 * (1 + ratio)))
    return generate_rice_matrix(L, K, nu, sigma)

def calculate_mimo_channel_gain(d: float, L: int, K: int, lam = 0.08, k = 2) ->
    tuple[np.ndarray, float]:
    """
    Calculate MIMO channel gains between transmitter and receiver
    """
    if d == np.inf:
        return np.zeros((K, L), dtype=complex)
    if d == 0:
```

```
        d = 0.5

    delta = lam / 2
    c = np.sqrt(L * K) * np.exp(-1j * 2 * np.pi * d / lam)
    e_r = calculate_unit_spatial_signature(0, K, delta)
    e_t = calculate_unit_spatial_signature(0, L, delta)
    H = c * (e_r @ e_t.T.conj())

    ratio = 0.6
    total_power = 1.0
    H = H * generate_rice_faiding_channel(L, K, ratio, total_power)
    return H
```

Code A.15: Channel Modeling Functions

These functions implement the channel models described in Section 5.2, including free space path loss, spatial signatures, and Ricean fading.

A.3.6 BER Heatmap Simulation

Finally, we put everything together in a function that simulates BER across the entire space:

```
def ber_heatmap_reflection_simulation(
    width: int,
    height: int,
    buildings: List[Tuple[int, int, int, int]],
    transmitter: Tuple[int, int],
    ris_points: List[Tuple[int, int]],
    receivers: List[Tuple[int, int]],
    num_symbols: int,
    N: int = 16,
    K: int = 2,
    eta: float = 0.9,
    snr_db: int = 10,
    path_loss_calculation_type: Literal['sum', 'product', 'active_ris'] = 'sum'
):
    """
    Run RIS reflection simulation with given parameters
    """
    ber_heatmap = HeatmapGenerator(width, height)

    # Setup environment
    for building in buildings:
        ber_heatmap.add_building(*building)

    tx, ty = transmitter
    ber_heatmap.add_point('T', tx, ty)

    M = len(ris_points)
    for i, (px, py) in enumerate(ris_points):
        ber_heatmap.add_point(f'P{i+1}', px, py)

    J = len(receivers)
    for i, (rx, ry) in enumerate(receivers):
        ber_heatmap.add_point(f'R{i+1}', rx, ry)

    # Calculate distance matrices
    distances_from_T = ber_heatmap.calculate_distance_from_point('T')
    distances_from_Ps = [ber_heatmap.calculate_distance_from_point(f'P{i+1}') for i
     in range(M)]

    # Create heatmaps for power analysis
    power_heatmap_from_T = HeatmapGenerator.copy_from(ber_heatmap)
    power_heatmap_from_Ps = [HeatmapGenerator.copy_from(ber_heatmap) for _ in range
    (M)]

```

```
    # Calculate channel matrices
    tx_grid_y, tx_grid_x = ber_heatmap._meters_to_grid(tx, ty)
    H = calculate_mimo_channel_gain(distances_from_Ps[0][tx_grid_y, tx_grid_x], K, N)

     if M > 1:
        receiver_grid_coords = [(ber_heatmap._meters_to_grid(rx, ry)) for rx, ry in receivers]
        Gs = [calculate_mimo_channel_gain(distances_from_Ps[-1][ry, rx], N, K)
              for ry, rx in receiver_grid_coords]

        ris_grid_coords = [ber_heatmap._meters_to_grid(px, py) for px, py in ris_points]
        Cs = [calculate_mimo_channel_gain(
            distances_from_Ps[i+1][ris_grid_coords[i][1], ris_grid_coords[i][0]],
            N, N
        ) for i in range(M-1)]
    else:
        receiver_grid_coords = [(ber_heatmap._meters_to_grid(rx, ry)) for rx, ry in receivers]
        Gs = [calculate_mimo_channel_gain(distances_from_Ps[0][ry, rx], N, K)
              for ry, rx in receiver_grid_coords]
        Cs = []

    print(f"Channel matrix from transmitter to RIS: Power {calculate_channel_power(H):.1e}")
    print(f"Channel matrix from RIS to receiver: Power {calculate_channel_power(Gs[0]):.1e}")

    Ps, _ = calculate_multi_ris_reflection_matrices(K, N, J, M, Gs, H, eta, Cs)
    P = unify_ris_reflection_matrices(Ps, Cs)
    print(f"Reflection matrix: Power {calculate_channel_power(P):.1e}")
    print(f"Effective channel matrix: Power {calculate_channel_power(Gs[0] @ P @ H):.1e}")
    print()

    # * Calculate cumulative path distances
    ris_path_distances = []
    for i in range(M):
        if i == 0:
            # * Distance from T to first RIS
            ris_path_distances.append(distances_from_Ps[0][ty, tx])
        else:
            # * Distance between consecutive RIS points
            ris_path_distances.append(
                distances_from_Ps[i][ris_points[i-1][1], ris_points[i-1][0]]
            )

    # Define BER calculation function for each point
    def calculate_ber_per_point(x: int, y: int) -> float:
        grid_x, grid_y = ber_heatmap._meters_to_grid(x, y)
        distance_from_T = distances_from_T[grid_y, grid_x]
        B = calculate_mimo_channel_gain(distance_from_T, K, K) * calculate_free_space_path_loss(distance_from_T)
        B_power = calculate_channel_power(B)
        power_heatmap_from_T.grid[grid_y, grid_x] = B_power

        distances_from_Ps_current = [distances_from_Ps[i][grid_y, grid_x] for i in range(M)]
        Fs = [calculate_mimo_channel_gain(d, N, K) for d in distances_from_Ps_current]

        # * Override channel matrices for receiver positions
        for j in range(J):
            if x == receivers[j][0] and y == receivers[j][1]:
                Fs[-1] = Gs[j]
```

```
99
100         errors = 0
101         for _ in range(num_symbols):
102             Ps, _ = calculate_multi_ris_reflection_matrices(K, N, J, M, Gs, H, eta,
     Cs)
103             P = unify_ris_reflection_matrices(Ps, Cs)
104 
105             effective_channel = np.zeros((K, K), dtype=complex)
106 
107             # Handle different path loss types
108             for i in range(M):
109                 if i == 0:
110                     P_to_i = Ps[0]
111                 else:
112                     P_to_i = unify_ris_reflection_matrices(Ps[:i+1], Cs[:i])
113 
114                 if path_loss_calculation_type == 'sum':
115                     total_distance = sum(ris_path_distances[:i+1]) +
    distances_from_Ps_current[i]
116                     total_path_loss = calculate_free_space_path_loss(total_distance
    )
117                     new_effective_channel = Fs[i] @ P_to_i @ H * total_path_loss
118                 elif path_loss_calculation_type == 'product':
119                     total_path_loss = 1
120                     for j in range(i+1):
121                         total_path_loss *= calculate_free_space_path_loss(
    ris_path_distances[j])
122                     total_path_loss *= calculate_free_space_path_loss(
    distances_from_Ps_current[i])
123                     new_effective_channel = Fs[i] @ P_to_i @ H * total_path_loss
124                 elif path_loss_calculation_type == 'active_ris':
125                     total_path_loss = calculate_free_space_path_loss(
    distances_from_Ps_current[i])
126                     new_effective_channel = Fs[i] @ P_to_i @ H * total_path_loss
127                 else:
128                     raise ValueError(f"Invalid path loss calculation type: {
    path_loss_calculation_type}")
129 
130                 effective_channel += new_effective_channel
131 
132             # Determine signal power and calculate BER
133             power = B_power if distance_from_T != np.inf else
    calculate_channel_power(effective_channel)
134             sigma_sq = snr_db_to_sigma_sq(snr_db, power)
135 
136             if distance_from_T == np.inf:
137                 errors += simulate_ssk_transmission_reflection(K, effective_channel
    , sigma_sq)
138             else:
139                 errors += simulate_ssk_transmission_direct(K, B, effective_channel,
     sigma_sq)
140 
141         return errors / num_symbols
142 
143     # Apply BER calculation to each point in the grid
144     ber_heatmap.apply_function(calculate_ber_per_point)
145 
146     # Visualize results
147     title = f'{M} RIS(s) (K = {K}, SNR = {snr_db}) [Path Loss: {
    path_loss_calculation_type}]'
148     ber_heatmap.visualize(title + ' BER Heatmap', vmin=0.0, vmax=1.0, label='BER',
    show_receivers_values=True)
149     ber_heatmap.visualize(title + ' BER Heatmap', log_scale=True, vmin=-10.0, vmax
    =0.0, label='BER', show_receivers_values=True)
150 
```

```
    power_heatmap_from_T.visualize(title + ' Channel Power from Transmitter',
    log_scale=True, vmin=-10.0, vmax=0.0, label='Power (dB)')
    for i in range(M):
        power_heatmap_from_Ps[i].visualize(title + f' Channel Power from RIS {i+1}'
    , log_scale=True, vmin=-10.0, vmax=0.0, label='Power (dB)')
```

Code A.16: BER Heatmap Simulation

This function implements our full simulation, calculating BER at each point in the space based on our theoretical framework and the different path loss models discussed in Section 5.2.

A.4 Main Simulation Scenarios

The main function in the heatmap.py file demonstrates how we use these components to evaluate different scenarios:

```
def main():
    # One reflection simulation
    buildings_single = [
        (0, 10, 7, 10),
        (8, 0, 12, 8)
    ]
    transmitter_single = (3, 3)
    ris_points_single = [(7, 9)]
    receivers_single = [(16, 11), (10, 18)]

    for path_loss_calculation_type in PATH_LOSS_TYPES:
        ber_heatmap_reflection_simulation(
            width=20,
            height=20,
            buildings=buildings_single,
            transmitter=transmitter_single,
            ris_points=ris_points_single,
            receivers=receivers_single,
            N=25,
            K=4,
            path_loss_calculation_type=path_loss_calculation_type,
            num_symbols=num_symbols
        )

    # Multiple reflection simulation
    buildings_multiple = [
        (0, 10, 10, 10),
        (2, 4, 7, 1)
    ]
    transmitter_multiple = (1, 1)
    ris_points_multiple = [(0, 9), (10, 9)]
    receivers_multiple = [(16, 14), (12, 18)]

    for path_loss_calculation_type in PATH_LOSS_TYPES:
        ber_heatmap_reflection_simulation(
            width=20,
            height=20,
            buildings=buildings_multiple,
            transmitter=transmitter_multiple,
            ris_points=ris_points_multiple,
            receivers=receivers_multiple,
            N=16,
            K=2,
            path_loss_calculation_type=path_loss_calculation_type,
            num_symbols=num_symbols
        )
```

Code A.17: Main Simulation Scenarios

This function sets up and runs simulations for two distinct scenarios: 1. A single RIS reflection setup with two buildings, a transmitter, and two receivers 2. A multiple RIS reflection setup with two RIS surfaces in series

Each scenario is simulated with all three path loss models: sum, product, and active RIS. These simulations generate the heatmaps presented in Section 5.2, allowing us to visualize how BER varies across space under different conditions.

The simulations for the BER plots shown in section 5.1 are implemented in the ‘plot_ber_curves()‘ function:

```
def plot_ber_curves():
    N = 16    # Number of reflecting elements
    K = 2     # Number of antennas
    eta = 0.9 # Reflection efficiency

    for J in range(1, 3):  # Number of receivers
        for M in range(1, 3):  # Number of RIS surfaces
            print(f"Processing J={J}, M={M}")
            snr_range_db = np.arange(-10, 31, 2)
            ber_simulated_receiver = []
            ber_simulated_eavesdropper = []
            ber_simulated_direct = []
            ber_simulated_receiver_double = []
            ber_simulated_eavesdropper_double = []

            for snr_db in snr_range_db:
                result_receiver, result_eavesdropper, result_direct,
    result_receiver_double, result_eavesdropper_double = calculate_ber_simulation(
    snr_db, K, N, J, M, eta)
                ber_simulated_receiver.append(result_receiver)
                ber_simulated_eavesdropper.append(result_eavesdropper)
                ber_simulated_direct.append(result_direct)
                ber_simulated_receiver_double.append(result_receiver_double)
                ber_simulated_eavesdropper_double.append(result_eavesdropper_double
    )
                print(f"Processed SNR = {snr_db} dB:\t{result_receiver:.2f}\t{
    result_eavesdropper:.2f}\t{result_direct:.2f}")

            plt_name = f'SSK BER Performance with RIS (K={K}, N={N}, J={J}, M={M})'
            plt.figure(figsize=(10, 6))
            plt.semilogy(snr_range_db, ber_simulated_direct, label=f'Simulation
    Direct')
            plt.semilogy(snr_range_db, ber_simulated_receiver, label='Simulation
    Receiver')
            plt.semilogy(snr_range_db, ber_simulated_receiver_double, label='
    Simulation Receiver Double RIS Source')
            plt.semilogy(snr_range_db, ber_simulated_eavesdropper, label=f'
    Simulation Eavesdropper')
            plt.semilogy(snr_range_db, ber_simulated_eavesdropper_double, label=f'
    Simulation Eavesdropper Double RIS Source')
            plt.grid(True)
            plt.xlabel('SNR (dB)')
            plt.ylabel('Bit Error Rate (BER)')
            plt.title(plt_name)
            plt.legend()
            plt.savefig(f"./simulations/results/{plt_name}.png", dpi=300, format='
    png')
            print(f"Saved {plt_name}.png\n\n")
```

Code A.18: BER Curve Plotting Function

This function systematically evaluates BER performance across different signal-to-noise ratios (SNR), generating plots for each combination of receiver count (J) and RIS surface count (M). These plots allow us to compare the performance of legitimate receivers versus eavesdroppers under different conditions.

A.5 Utils Module

Although not shown in the provided code snippets, we also implemented a util module that handles noise generation and SNR calculations:

```python
def snr_db_to_sigma_sq(snr_db: float, power: float = 1.0) -> float:
    """
    Convert SNR in dB to noise variance

    Parameters:
    -----------
    snr_db : SNR in dB
    power : Signal power (default 1.0)

    Returns:
    --------
    Noise variance sigma_sq
    """
    snr_linear = 10**(snr_db/10)
    return power / snr_linear

def create_random_noise_vector(size: int, sigma_sq: float) -> np.ndarray:
    """
    Create a random noise vector with specified variance

    Parameters:
    -----------
    size : Size of the noise vector
    sigma_sq : Noise variance

    Returns:
    --------
    Random noise vector
    """
    return np.random.normal(0, np.sqrt(sigma_sq/2), (size,)) + 1j * np.random.
    normal(0, np.sqrt(sigma_sq/2), (size,))
```

Code A.19: Util Module Functions