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

1 Introduction **2**
- 1.1 Physical Layer Security . . . 2
- 1.2 Reconfigurable Intelligent Surface . . . 3
- 1.3 Using RISs for Physical Layer Security . . . 3
- 1.4 RISs and Physical Layer Security for Vehicular Networks . . . 3
- 1.5 Future Directions . . . 4

2 Hidden comunication by targeted reflections **4**

3 Space Shift Keying Modulation **6**
- 3.1 Direct Detection . . . 7
- 3.2 Diagonalized Reflection Detection . . . 7

4 Cascaded Channel Estimation **8**

5 Expanding to multiple users **8**
- 5.1 Reflecting to multiple users . . . 8
- 5.2 RISs in parallel . . . 9
- 5.3 RISs in series . . . 9
- 5.4 Complex reflections . . . 10

6 Simulation Results **10**
- 6.1 BER stocastic simulation . . . 11
  - 6.1.1 Single RIS reflection (M=1) . . . 12
  - 6.1.2 Double RIS reflection (M=2) . . . 13
- 6.2 BER realistic scenario simulation . . . 14
  - 6.2.1 Channel gain calculation . . . 14
  - 6.2.2 Path loss calculation . . . 14

Bibliography **27**

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 rate 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 relaiability. Our simulations include realistic channel modeling, incorporating Rician fading and different path loss calculations, and presents 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.

Chapter 1

Introduction

1.1 Physical Layer Security

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. However, they also bring new security concerns, especially in wireless communications.

We have two type of threats we need to protect against. Active attacks, like jamming a frequency, distrupt and block the flow of information; while passive attacks, like eavesdropping, are more subtle and we need to make our signals undeciphrable with encryption or noise. There are different methods we can use to mask our communications: we can fingerprint the legitimate users, spread it through multiple frequencies, use directional antennas or artificial noise schemes [21].

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 [25].

In particular to eavesdropping, there is a huge opportunity for improvements. While distruptions have been studied for long, especially in military communications, message encryption is usually delegated to the higher levels [18]. 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 [22], it is important to be protected at all layers.

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 [20], but there are some practical strategies we can implement.

In [13] a statistical model is created to calculate the probability of achieving secrecy from eavesdroppers in unknown locations, while in [9] and [8] it is discussed how we can use the antenna spare power to induce artificial noise to assure the legitimate receiver has better signal.

1.2 Reconfigurable Intelligent Surface

Reconfigurable Intelligent Surfaces (RISs) are a new technology that can help in improving the securitya 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 phenomena to a programmable variable that is possible to (partially) control and optimize [6].

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 [6].

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 easly put in any surface like walls or ceilings [2].

1.3 Using RISs for Physical Layer Security

RISs can be used to greatly increase not only the network performance but also its security [14]. 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 understable from eavesdroppers, while having a decoding for the legitimate user linear [16].

Another paper [30] studied how to use a novel RIS based channel randomization technique to improve the secrecy rate, and another one [3] 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 [24] it is used an aerial RIS to mitigate the effects of the disturbance and increase the transmission power and reliability.

1.4 RISs and Physical Layer Security for Vehicular Networks

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 [5].

The sector is just starting to be studied, but there are already some promising result. Network simulators made specific, like CoopeRIS, allow to study and progress this field [19].

Vehicular networks need low latency and high security. Active attack may jeopardize drivers' and people's safety, while also slowing down 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 [15].

Recent studies shows how RISs can be used to protect the vehicular network against illegitimate users. In [17] the authors study how RISs can improve the average secrecy capacity and secrecy outrage probability.

1.5 Future Directions

Network intensive technologies like IOT and CAV are gaining traction fast, thanks to the many benefits they bring to society and the newest technologies that now allow this incredibly huge traffic load.

The security of these networks is still a big concern, and it is necessary to study and implement new technologies to protect them. RISs are a promising technology that can help in this regard. Being cost effective, fairly passive and easy to deploy, they can assist in overcoming the problems of 6G like signal fading and out of LOS communication [2].

However, while we have some initial literature in both physical layer security using RISs, and using RISs to improve vehicular network performances, not much has been made in studying all three of these aspects [17].

Practical solutions could be studied and simulated starting from the resources presented here. RISs can be used both to mask the network signal or to make it noisier for unwanted listeners located in different places.

For example, starting from [9], it could be studied how cooperating vehicles could calculate together with a RIS how to add noise to other locations while moving in space, and so needing constant modifications in the calculations themselves.

Modern cars have as much computing power as a modern personal computer: for example, Tesla cars have an integrated GPU to utilize the autonomus driving feature [23], which could be used for highly efficient matrix calculations [4].

In conclusion, the future of vehicular networks is bright, but it is necessary to study and implement new technologies to protect them. RISs are a promising technology that can help in this regard, and it is necessary to study how to use them to improve the security of vehicular networks.

Chapter 2

Hidden comunication by targeted reflections

We will start from the paper *Reconfigurable Intelligent Surface: Reflection Design Against Passive Eavesdropping* [16], 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.

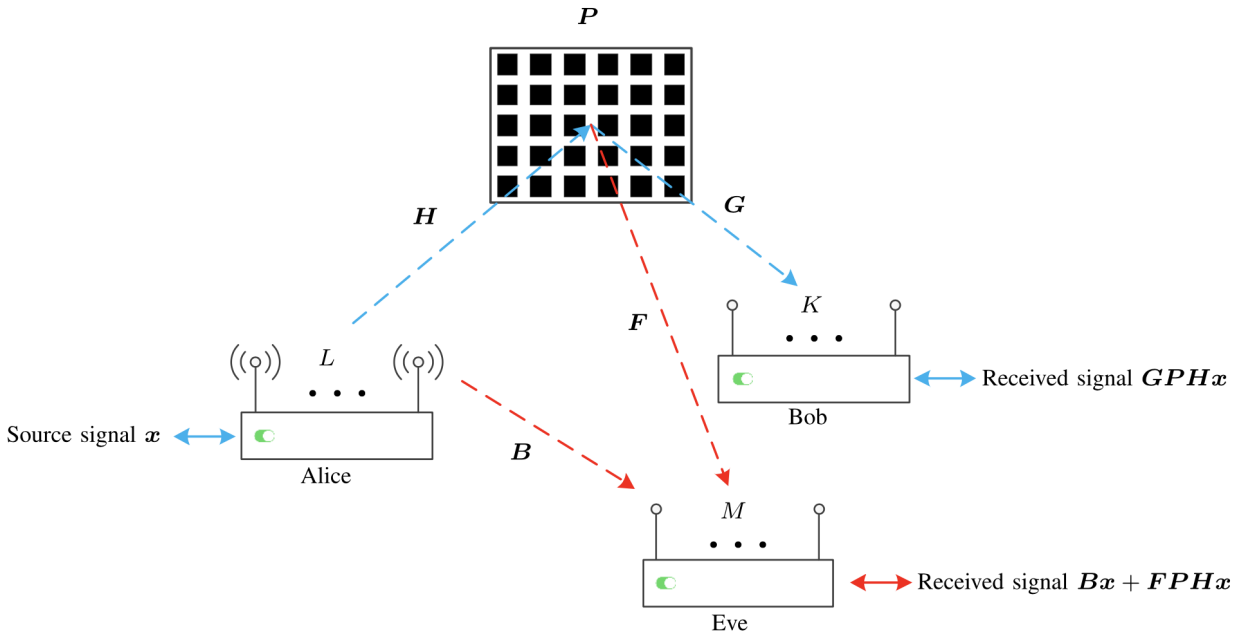

Figure 2.1: Setup

In [16], the authors studied how to use RISs to allow communications between two users without LOS, while making the signal undeciphrable for eavesdroppers. We call L the transmitter's antennas, K the receiver's antennas, M the eavesdropper's antenna, and N the RIS reflecting elements. We assume $L \geq K \geq 2$.

We define $H \in \mathbb{C}^{NxL}$ the channel response [1] from the transmitter to the RIS, $G \in \mathbb{C}^{KxN}$ the channel response from the RIS to the receiver, $P = diag\{p\} \in \mathbb{C}^{NxN}$ 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 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 others, 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* [12], which we will summarize in a later chapter.

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

Formally, the condition we want to satisfy is:

$$||[GPH]_{:,1:K} - [[GPH]_{:,1:K}]_{diag}||^2 = 0 \tag{2.1}$$

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

Given

$$W = \sum_{i,j=1,i\neq j}^{K} (g_{j,:} \odot h_i^T)^H (g_{j,:} \odot h_i^T) \tag{2.2}$$

$$rank(W) = K(K-1) \tag{2.3}$$

$$rank(W) - nullity(W) = N \tag{2.4}$$

$$nullity(W) = N - (K^2 - K) \tag{2.5}$$

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

The formula (2.1) can be rewritten as

$$Wp = 0 \tag{2.6}$$

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

$$W = R\Sigma V^{H2} \tag{2.7}$$

With SVD, we have $\Sigma = diag(\sigma) \in C^{NxN}$ a diagonal matrix. the first $rank(W) = K^2 - K$ elements of σ are non-zero, while the last $nullity(W) = N - (K^2 - K)$ elements are zero [7].

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

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

The last k columns of R' are a span of the null space

$$N(A^H) = [r_{m-k}, ..., r_m] \in \mathbb{C}^{mxk} \tag{2.8}$$

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

$$N(A) = \begin{bmatrix} v'^H_{n-k} \\ ... \\ v'^H_n \end{bmatrix} \in \mathbb{C}^{kxn} \tag{2.9}$$

Being A an Hermitian matrix, the two null spaces are both solutions to $Ax = 0$.

Consider now $W \in C^{NxN}$. The paper in question uses equation (7) to find the solutions, since W is hermitian and square. Taken $U \in \mathbb{C}^{Nx(N-(K^2-K))}$ the last $N - (K^2 - K)$ columns of the left singular matrix R. $U \in N(W)$ for the explanation above. We then have

$$WU = 0 \tag{2.10}$$

$$p = Uq \tag{2.11}$$

$$WUq = 0 \tag{2.12}$$

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

Chapter 3

Space Shift Keying Modulation

But how can the actors communicate, if the result is a diagonal matrix with random value?

We will use a technique called *Space Shift Keying* (SSK) Modulation [12], where *antenna indices are used as the only means to relay information.* Given K the number of antenna of the actors in the system, we can send $log_2(K)$ bits by mapping each combination of bits to a specific antenna. [1]

[2] An hermitian transpose of V (V^H), means we fist transpose the matrix ($V \to V^T$), then take the conjugate of every element (so invert the sign of the immaginary part).

[1] 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 [11], where they discuss a more general approach using multiple

TABLE I
EXAMPLE OF THE SSK MAPPER RULE.

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

Figure 3.1: SSK conversion table

3.1 Direct Detection

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

$$y = Bx + \sigma^2 \tag{3.1}$$

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

$$j = arg\ max_j\ p_y(y|x_j, B) = arg\ min_j\ ||y - b_j||^2 \tag{3.2}$$

3.2 Diagonalized Reflection Detection

Following [16], for a reflected signal we have

$$y = GPHx + \sigma^2 \tag{3.3}$$

Given that GPH is a diagonal matrix and x has only one element equal to 1, the resulting vector $GPHx$ 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.

$$j = arg\ max_j\ y_j \tag{3.4}$$

active antennas at the same time. The general approach will also work with our proposed solution.

Chapter 4

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* [10]. 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 G and H.

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

Chapter 5

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 indipendent reflections of RISs.

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

5.1 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

[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 antenna 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).

$$\forall j \in [1...J] \rightarrow ||G_j PH - [G_j PH]_{diag}||^2 = 0 \tag{5.1}$$

$$\forall j \in [1...J] \rightarrow W_j p = 0 \tag{5.2}$$

$$\begin{bmatrix} W_1 \\ W_2 \\ ... \\ W_j \end{bmatrix} p = 0 \tag{5.3}$$

$$\begin{bmatrix} W_1 \\ W_2 \\ ... \\ W_j \end{bmatrix} = W \in \mathbb{C}^{JNxN}, W = R\Sigma V^H \tag{5.4}$$

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

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

$$N(W) = \begin{bmatrix} v^H_{N-J(K^2-K)} \\ ... \\ v^H_N \end{bmatrix}^H \tag{5.5}$$

Take $U_1 \in \mathbb{C}^{N-J(K^2-K)xN}$ the last $N - (K^2 - K)$ rows of V^H, and

$$U = U_1^H \in \mathbb{C}^{NxN-J(K^2-K)} \tag{5.6}$$

We now can apply the same method as before

$$p = Uq \tag{5.7}$$

$$WU = 0 \tag{5.8}$$

$$WUq = 0 \tag{5.9}$$

5.2 RISs in parallel

Given the previous property, it follows that we can use M indipendent 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

$$\sum_{m=1}^{M} G_j P_m H_m x = (\sum_{m=1}^{M} G_j P_m H_m)x \tag{5.10}$$

The sum of diagonal matrixes 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.

5.3 RISs in series

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

$$\text{Transmitter} \rightarrow \text{RIS 1} \rightarrow ... \rightarrow \text{RIS M} \rightarrow \text{Receiver} \tag{5.11}$$

We call $C_i \in \mathbb{C}^{NxN}$ the channel gain between P_i and P_{i+1}. We need to solve

$$||GP_1C_1...P_MH - [GP_1C_1...P_MH]_{diag}||^2 = 0 \tag{5.12}$$

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.

$$\forall m \in [1, M-1] : p_m[i] = \eta * r_i * e^{j\theta_i} \tag{5.13}$$

Given now

$$G' = GP_1C_1...P_{M-1}C_{M-1} \in \mathbb{C}^{KxN} \tag{5.14}$$

We can consider now the problem of solving

$$||G'P_MH - [G'P_MH]_{diag}||^2 = 0 \tag{5.15}$$

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

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

5.4 Complex reflections

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

For example, let's say it receives the signals GP_1H_1x and $GP_1C_1P_2H_2x$. To solve this system, instead of setting P_1 randomly, we would need first to solve it using G and H_1, then solve P_2 using $G' = GP_1C_1$ and H_2. The sum of the two signals would still be readable for the receiver correctly.

While the calculations of P_1 depends on G and H_1, the signal would still be random and undeciphrable for an eavesdropper receiving it.

Chapter 6

Simulation Results

We can now test more complex setups by doing Bit Error Rate (BER) analysis.

[2] It is also possible to set up randomly the last $M-1$ RIS and calculate the first one using G and $H' = C_1P_2C_2...P_M$. The properties still holds.

[3] Estimate the channel gains G and H, based on [10], could be more difficult, given that we do not have full controll on $P = P_1C_1...P_M$ anymore. We can however estimate directly G' by keeping the same random $P_1, ..., P_{M-1}$ in both the acknowlegdment round and the message trasmission round, and just modify P_M after estimating G' and H to correctly deliver the message.

6.1 BER stocastic simulation

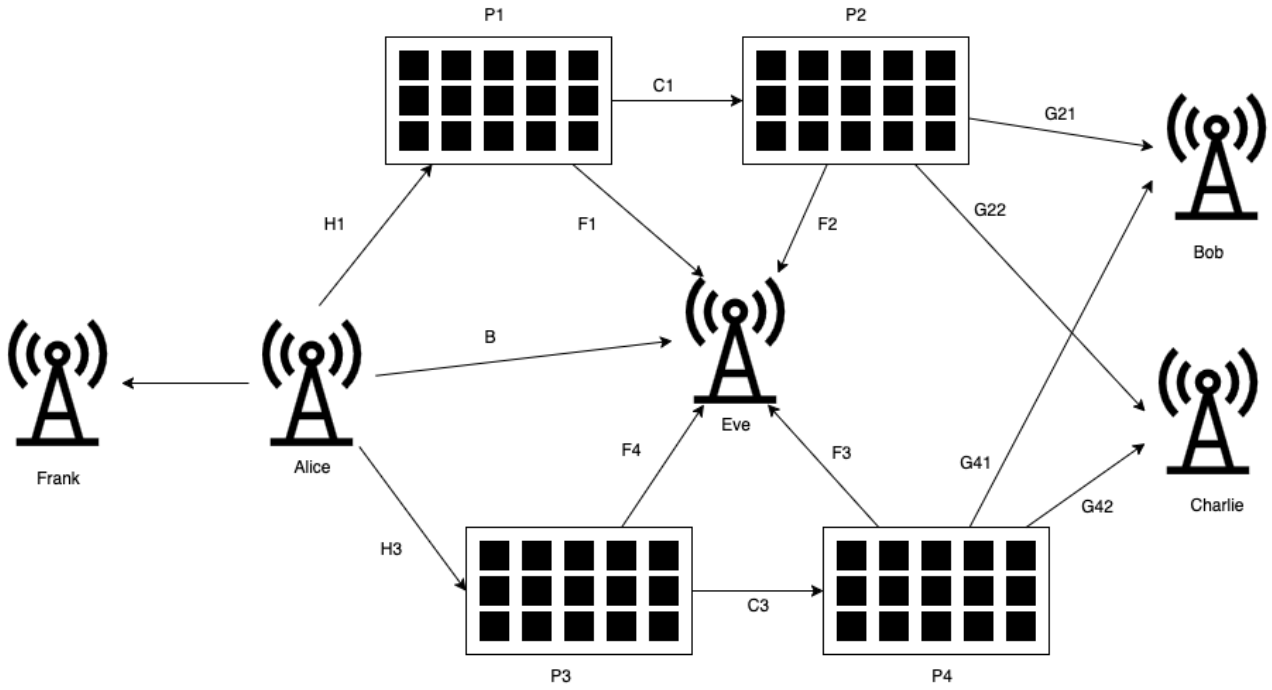

Figure 6.1: Complex Setup

For example, here we have a single transmitter *Alice* and multiple receivers. *Frank* is a direct receiver in line of sight. *Bob* and *Charlie* receive the signal from two double RIS reflection. *Eve* receives both the direct signal and the reflecting signal from all RISs. [1]

More in general, 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]

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 [16].

The direct link and the eavesdropper will try to understand the message by following the equation (3.2), while the receivers will try to understand it by following the equation (3.4).

[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 not line of sight, the message would be completely unreadable from the start, since it would receive random matrixes.

[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.

6.1.1 Single RIS reflection (M=1)

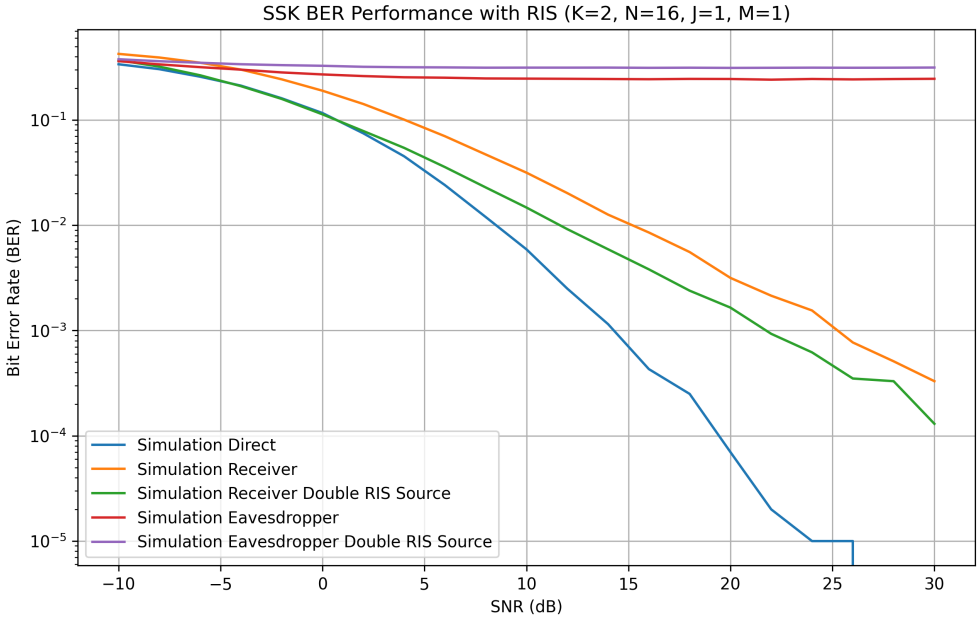

Figure 6.2: SSK BER Performance with RIS (K=2, N=16, J=1, M=1)

We can see in $(M = 1, J = 1)$ the results match with [16], 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.

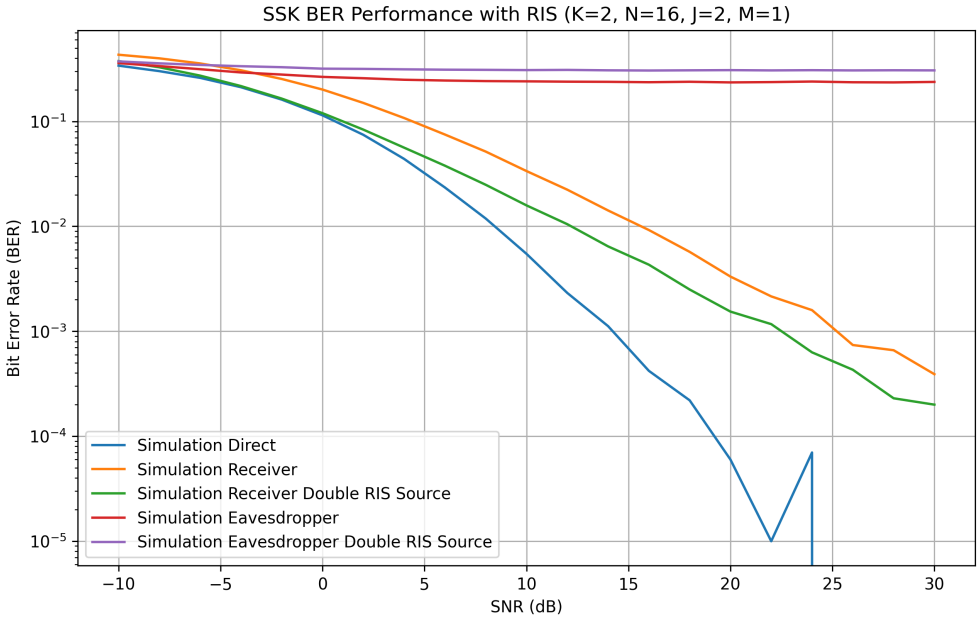

Figure 6.3: SSK BER Performance with RIS (K=2, N=16, J=2, M=1)

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.

6.1.2 Double RIS reflection (M=2)

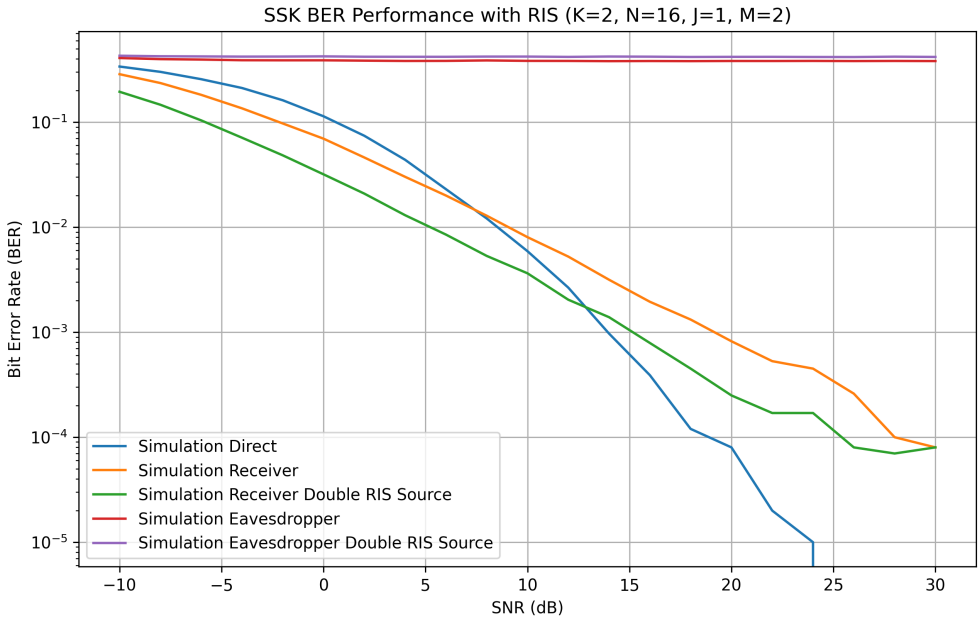

Figure 6.4: SSK BER Performance with RIS (K=2, N=16, J=1, M=2)

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

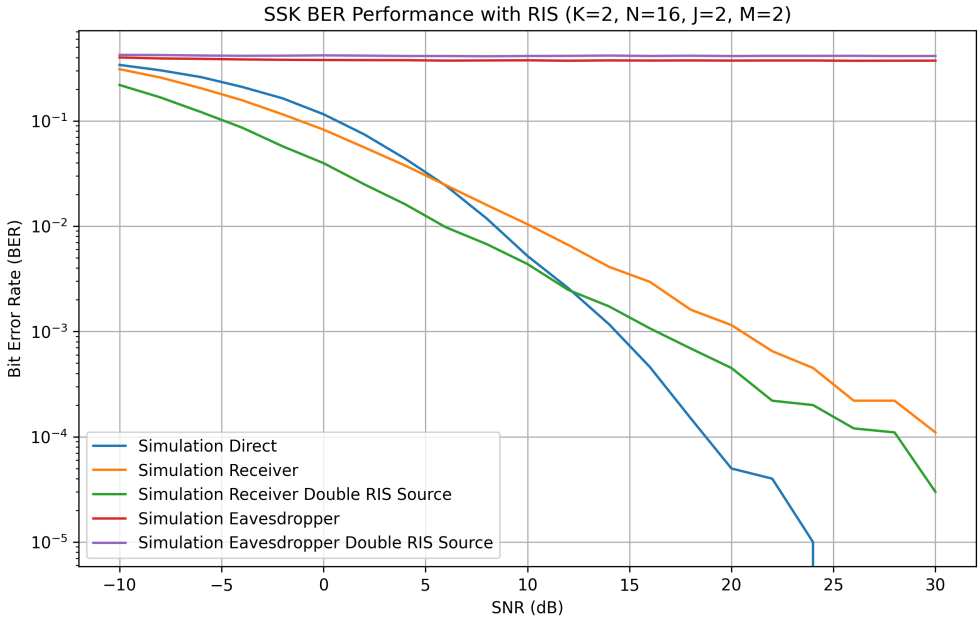

Figure 6.5: SSK BER Performance with RIS (K=2, N=16, J=2, M=2)

Combining all together, our properties still hold strong.

6.2 BER realistic scenario simulation

We can now simulate our framework in a realistic scenario. We first need to model the channel gain H and the path loss, based on the distance between the actors. We will define λ as the wavelenght of the signal, and d as the distance between two actors.

6.2.1 Channel gain calculation

We model the Rician fading [29] matrix Ξ, 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

$$\nu^2 = \frac{\tau\xi}{1+\tau} \tag{6.1}$$

$$\sigma^2 = \frac{\xi}{2(1+\tau)} \tag{6.2}$$

and we can generate Ξ by creating a random complex matrix where the real and the imaginary values are extracted from a gaussian distribution $C(\frac{\nu}{\sqrt{2}}, \sigma)$ [28]

Then, given an actor r with n_r antennas disposed as a *uniform linear array*, we can define the *unit spatial signature in the directonal cosine* $\Omega = cos\phi$ [26] as

$$e_r(\Omega) = \frac{1}{\sqrt{n_r}} \begin{bmatrix} 1 \\ exp(-j2\pi\Delta\Omega) \\ exp(-j2\pi 2\Delta\Omega) \\ \vdots \\ exp(-j2\pi(n_r-1)\Delta\Omega) \end{bmatrix} \tag{6.3}$$

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 [26] as

$$H = \Xi \odot \sqrt{n_t n_r} exp(-j2\pi d/\lambda) e_r(\Omega_r) e_t(\Omega_t)^H \tag{6.4}$$

This equation can be used both for a direct transmission between two actors, or between an actor and a RIS.

6.2.2 Path loss calculation

We begin by modeling the free space path loss [27] between two points as

$$PL = ((4\pi/\lambda)^2 d^k)^{-\frac{1}{2}} \tag{6.5}$$

where k is equal to 2 when the antennas are isontropic

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

$$y = PL_B * Bx \tag{6.6}$$

Given a reflected signal with channel gain GPH, where

- G is the communication transmitter-RIS
- H is the communication RIS-actors
- P is the RIS reflection coefficient diagonal matrix

we have two different LOS communications. We have different way 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 $y = PL_H * GPHx$. 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 $y = PL_G * PL_H * GPHx$. In case of multiple RISs, we multiply the path loss of all connections. We will call this as a *product path loss*
- 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 $y = PL_{G+H} * GPHx$. In case of multiple RISs, we add all the distances. We will call this as a *sum path loss*

We will see how these different considerations vary the results and the efficacy of the proposed framework.

- 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
- 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
- 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.

The graphs below show some example situations, and prove our framework does also work in more realistic situations. Below, we used $\lambda = 0.08m, \tau = 0.6, \xi = 1, \eta = 0.9, SNR = 10db, K = 2, N = 16$. Each square represent an actor receiveing the signal (an eavesdropper, or a legitimate receiver if shown), with its own BER.

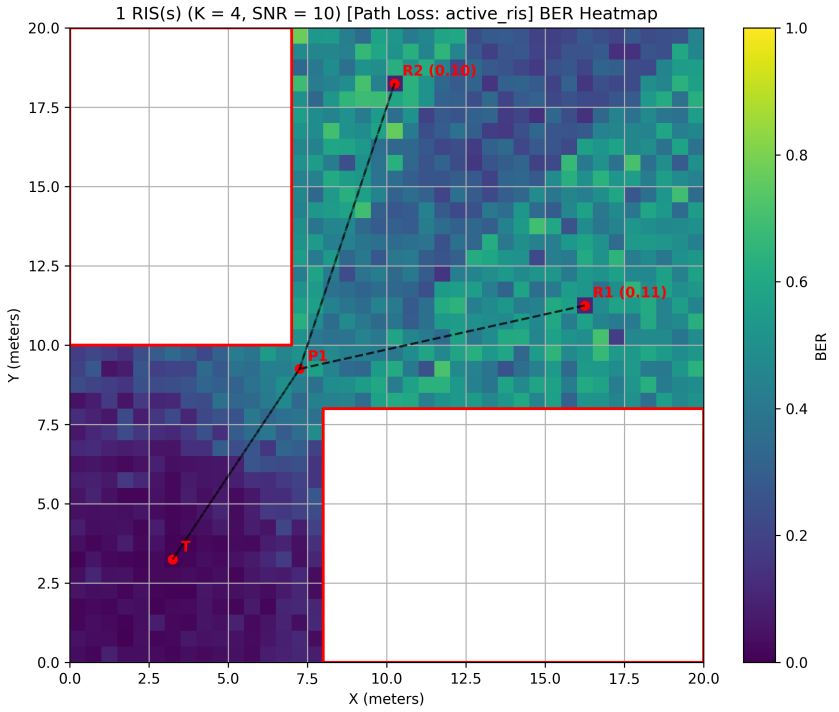

Figure 6.6: 1 RIS(s) (K = 4, SNR = 10) [Path Loss: active ris] BER Heatmap

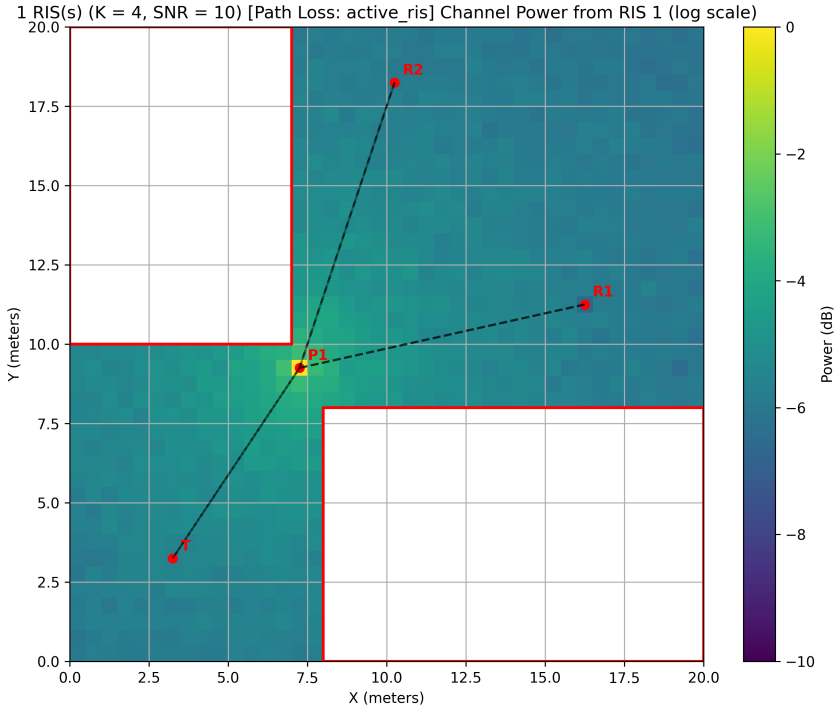

Figure 6.7: 1 RIS(s) (K = 4, SNR = 10) [Path Loss: active ris] Channel Power from RIS 1 (log scale)

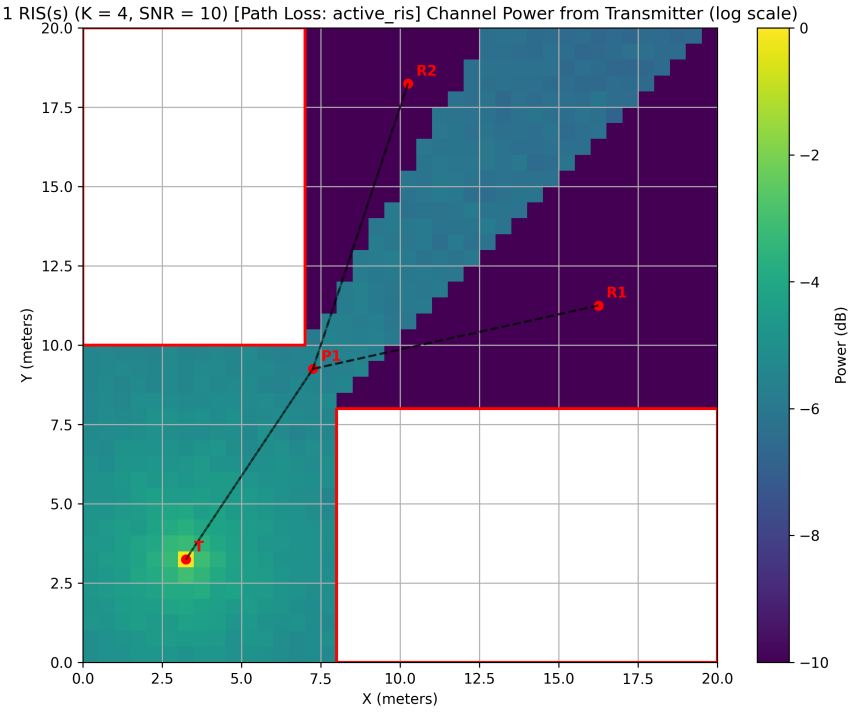

Figure 6.8: 1 RIS(s) (K = 4, SNR = 10) [Path Loss: active ris] Channel Power from Transmitter (log scale)

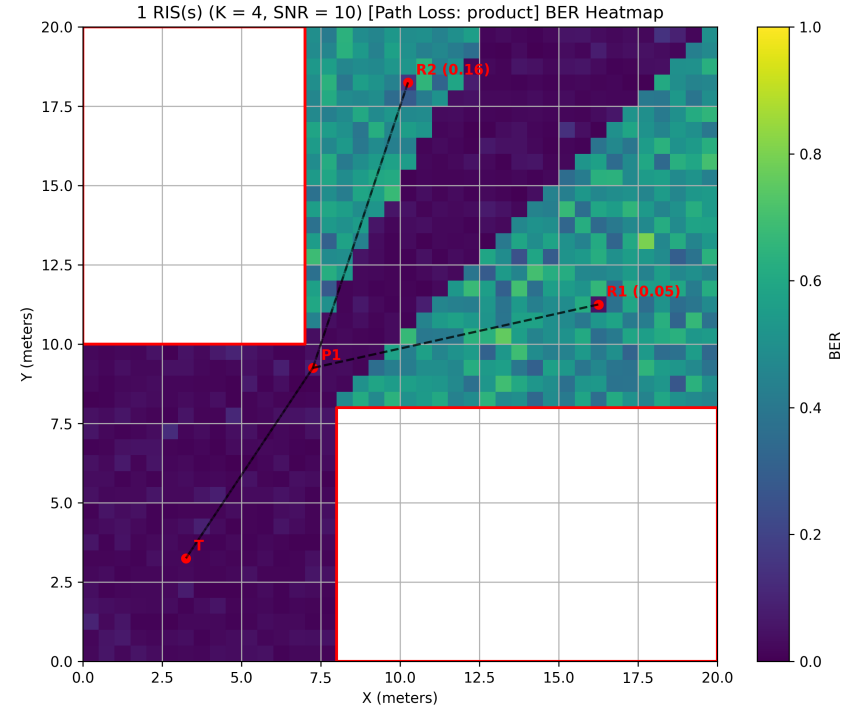

Figure 6.9: 1 RIS(s) (K = 4, SNR = 10) [Path Loss: product] BER Heatmap

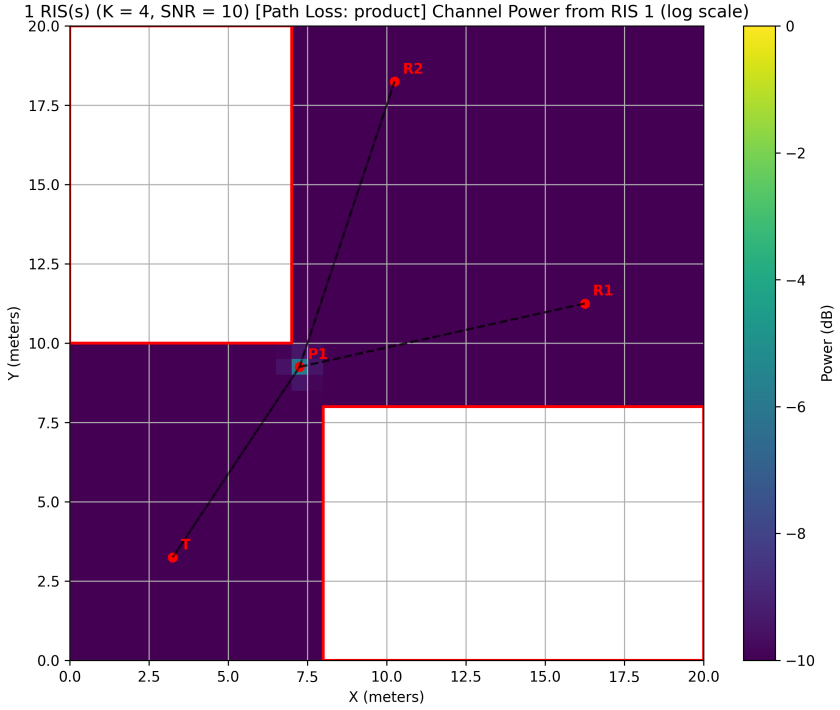

Figure 6.10: 1 RIS(s) (K = 4, SNR = 10) [Path Loss: product] Channel Power from RIS 1 (log scale)

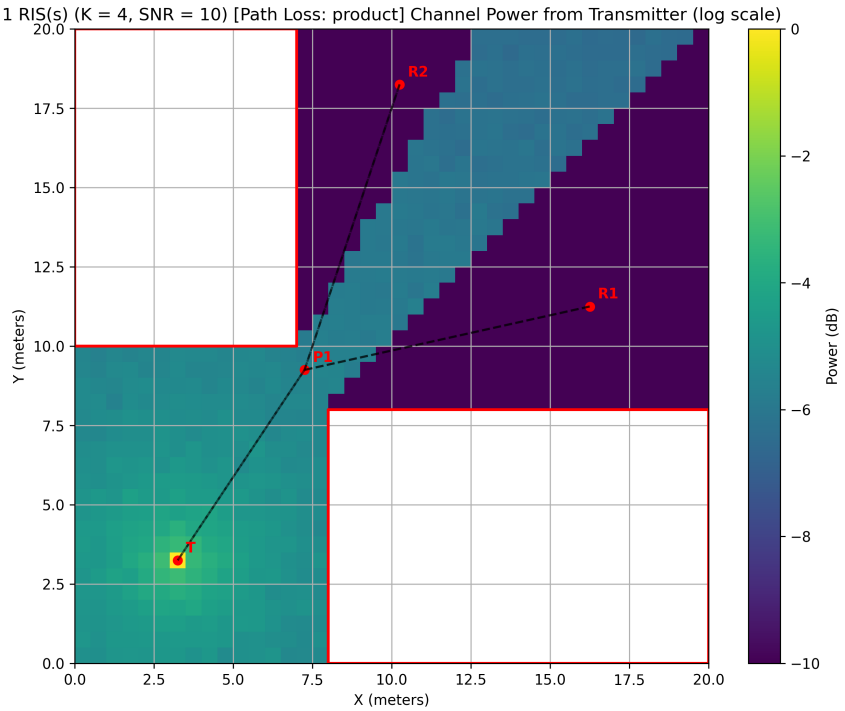

Figure 6.11: 1 RIS(s) (K = 4, SNR = 10) [Path Loss: product] Channel Power from Transmitter (log scale)

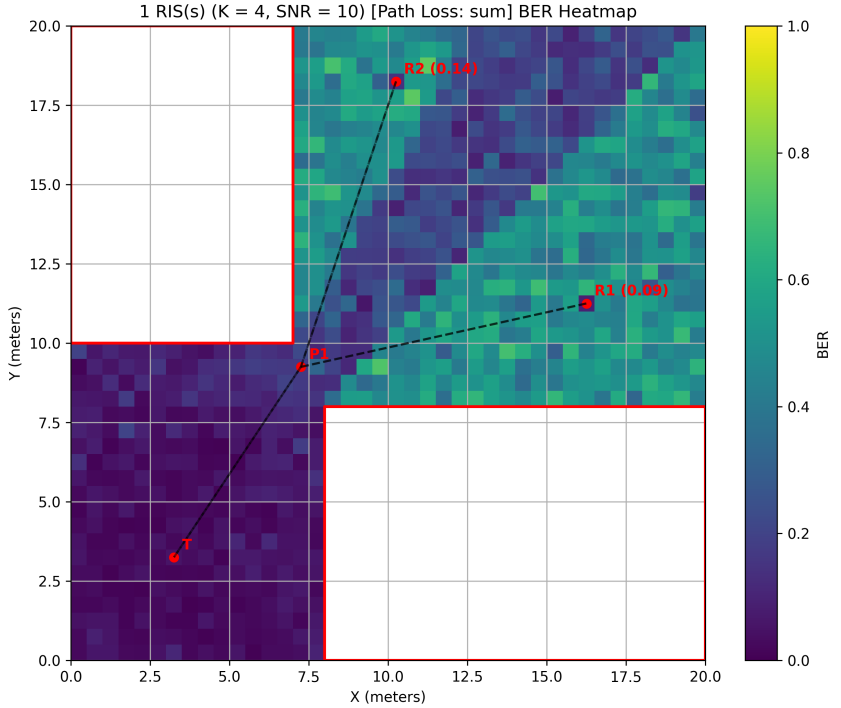

Figure 6.12: 1 RIS(s) (K = 4, SNR = 10) [Path Loss: sum] BER Heatmap

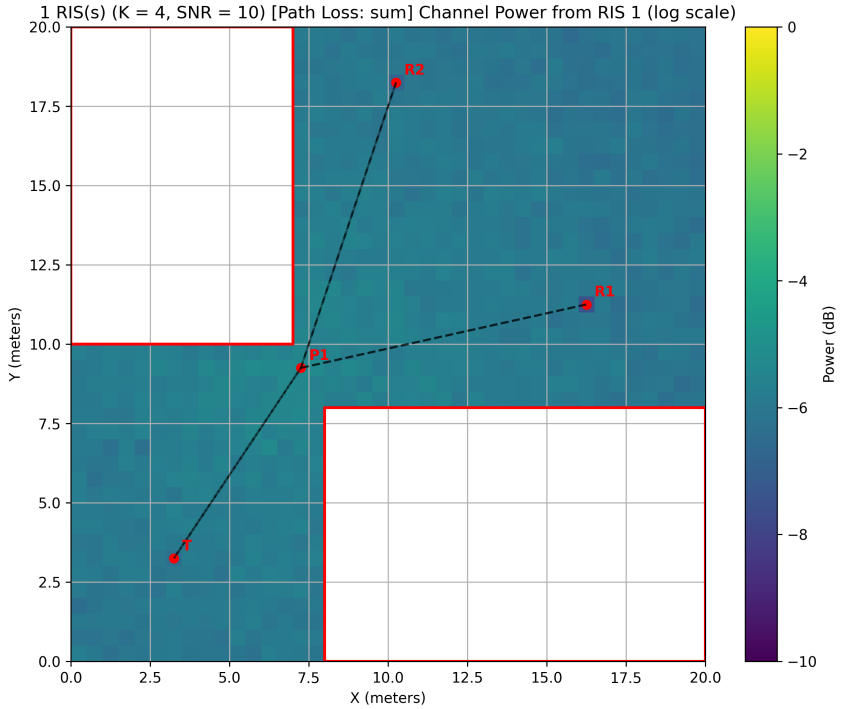

Figure 6.13: 1 RIS(s) (K = 4, SNR = 10) [Path Loss: sum] Channel Power from RIS 1 (log scale)

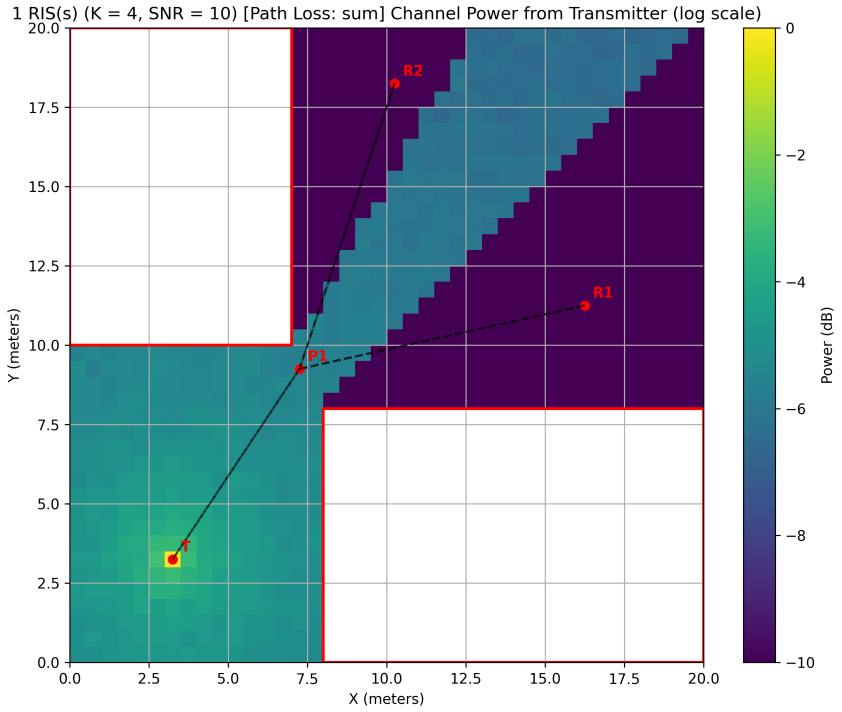

Figure 6.14: 1 RIS(s) (K = 4, SNR = 10) [Path Loss: sum] Channel Power from Transmitter (log scale)

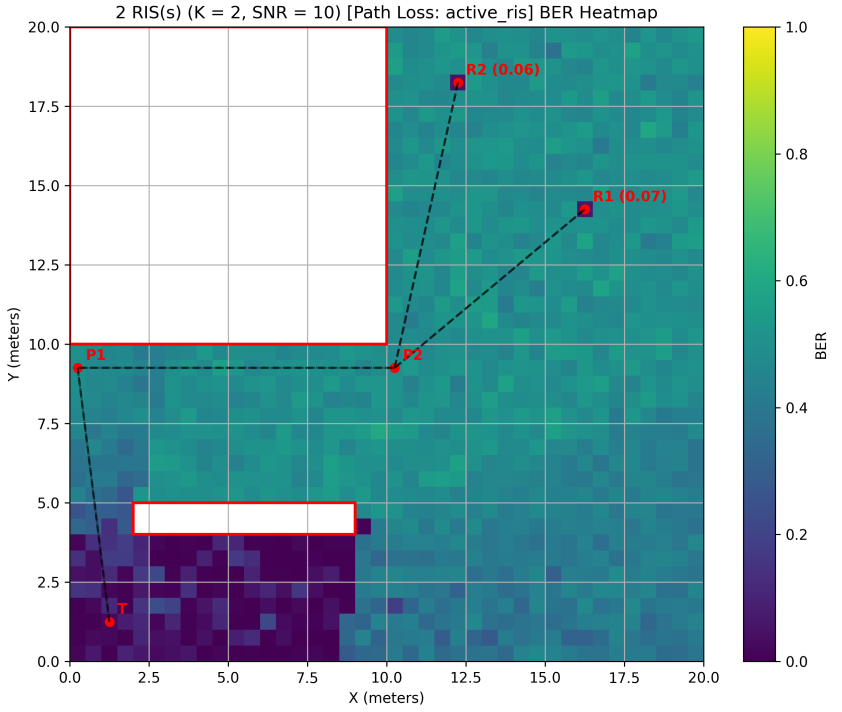

Figure 6.15: 2 RIS(s) (K = 2, SNR = 10) [Path Loss: active ris] BER Heatmap

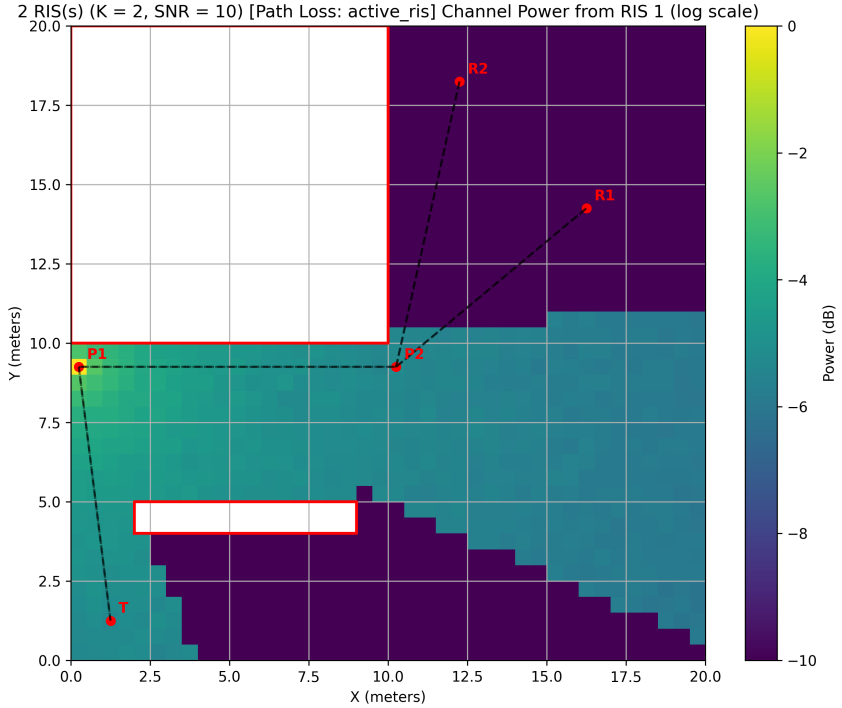

Figure 6.16: 2 RIS(s) (K = 2, SNR = 10) [Path Loss: active ris] Channel Power from RIS 1 (log scale)

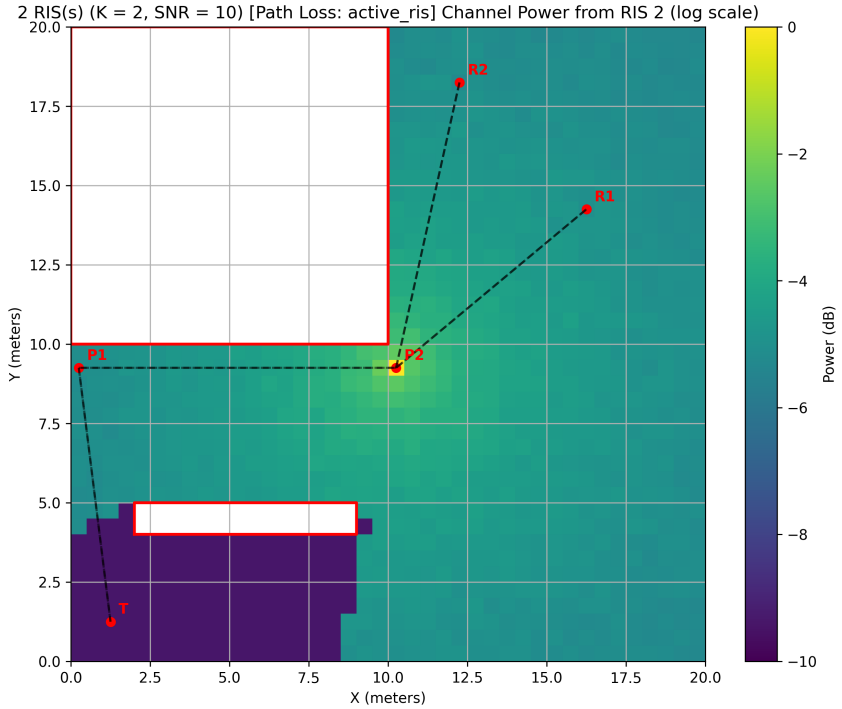

Figure 6.17: 2 RIS(s) (K = 2, SNR = 10) [Path Loss: active ris] Channel Power from RIS 2 (log scale)

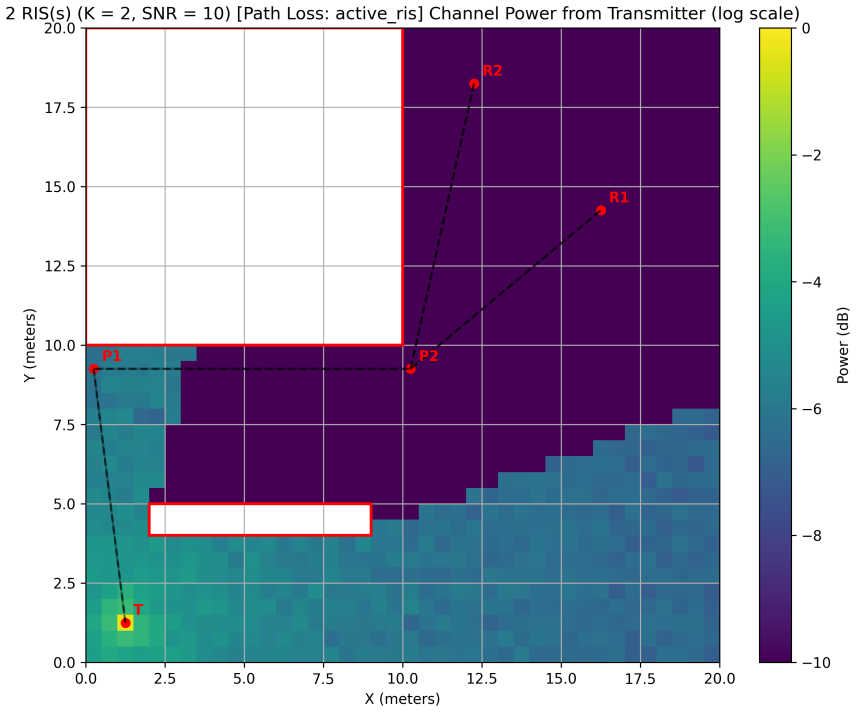

Figure 6.18: 2 RIS(s) (K = 2, SNR = 10) [Path Loss: active ris] Channel Power from Transmitter (log scale)

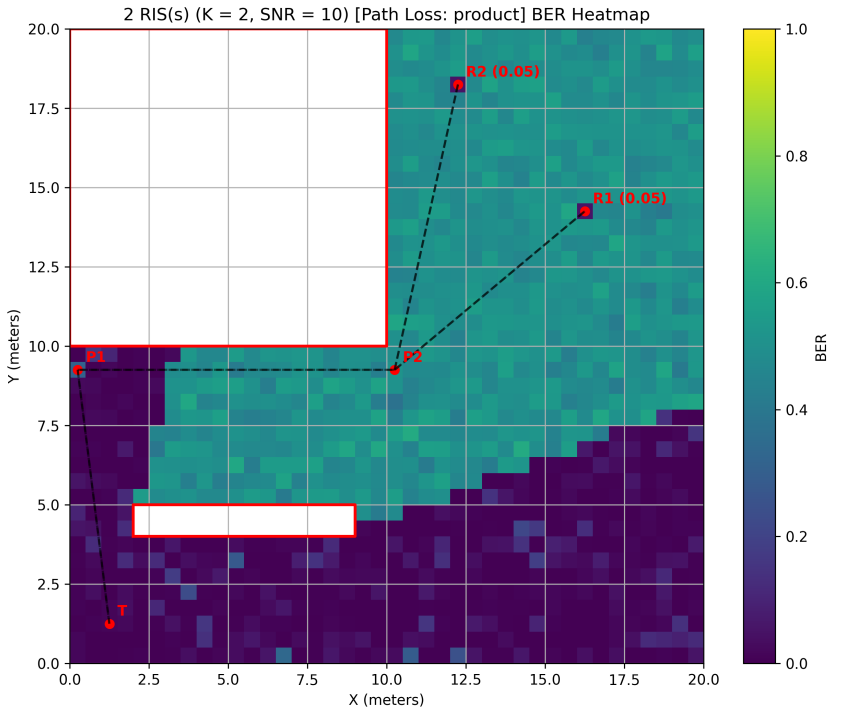

Figure 6.19: 2 RIS(s) (K = 2, SNR = 10) [Path Loss: product] BER Heatmap

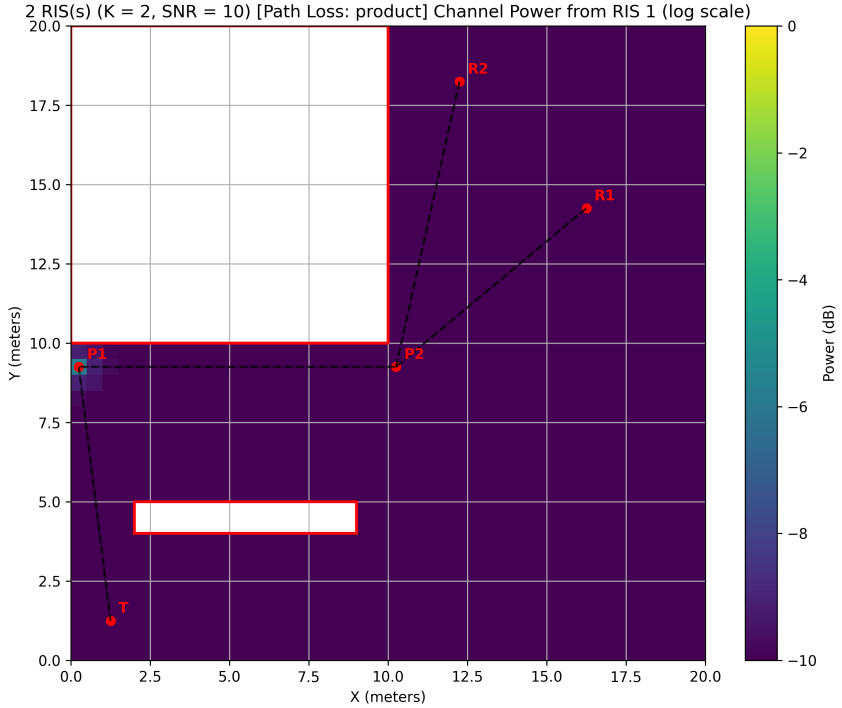

Figure 6.20: 2 RIS(s) (K = 2, SNR = 10) [Path Loss: product] Channel Power from RIS 1 (log scale)

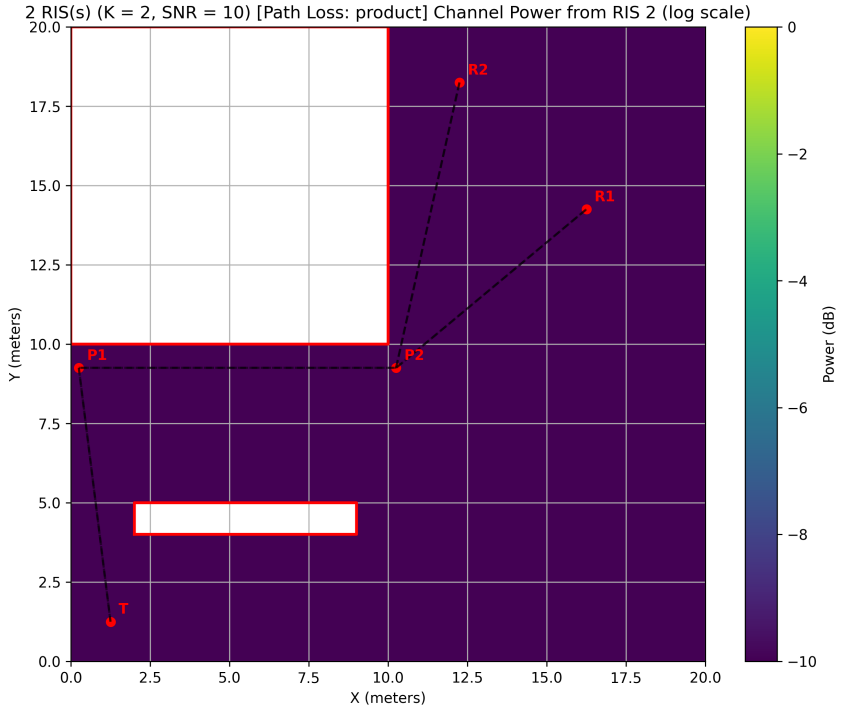

Figure 6.21: 2 RIS(s) (K = 2, SNR = 10) [Path Loss: product] Channel Power from RIS 2 (log scale)

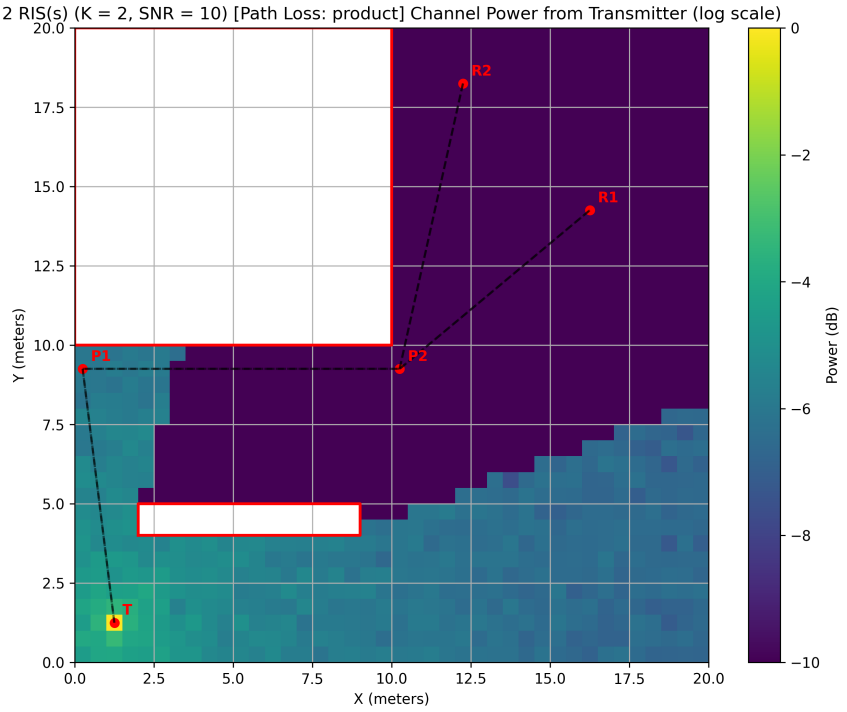

Figure 6.22: 2 RIS(s) (K = 2, SNR = 10) [Path Loss: product] Channel Power from Transmitter (log scale)

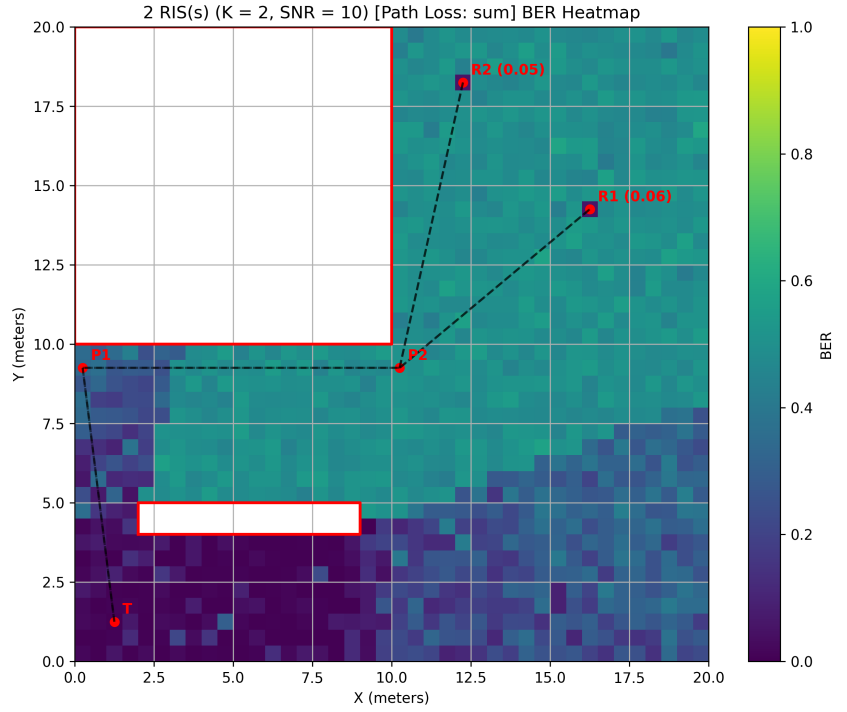

Figure 6.23: 2 RIS(s) (K = 2, SNR = 10) [Path Loss: sum] BER Heatmap

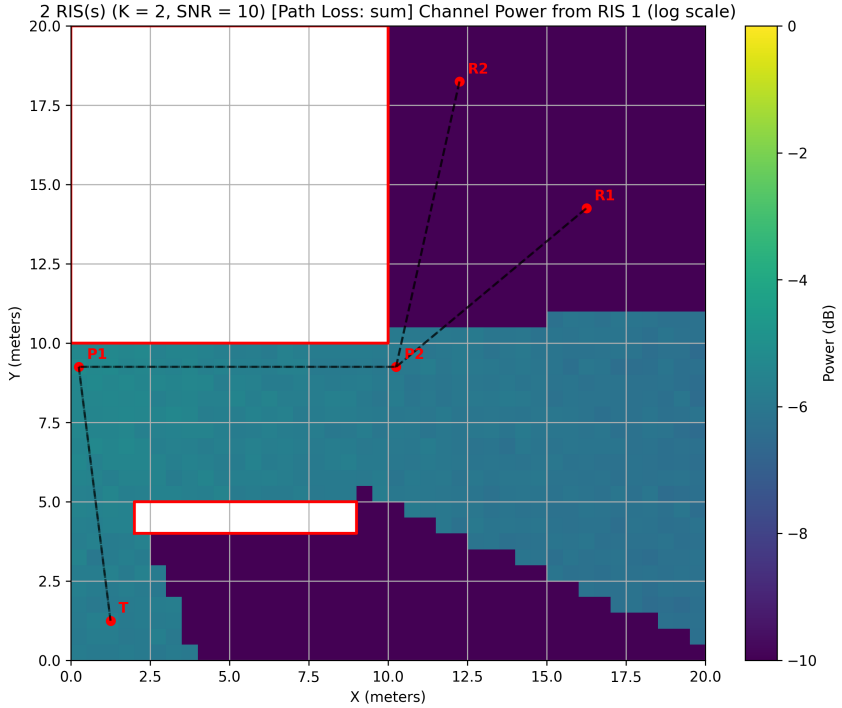

Figure 6.24: 2 RIS(s) (K = 2, SNR = 10) [Path Loss: sum] Channel Power from RIS 1 (log scale)

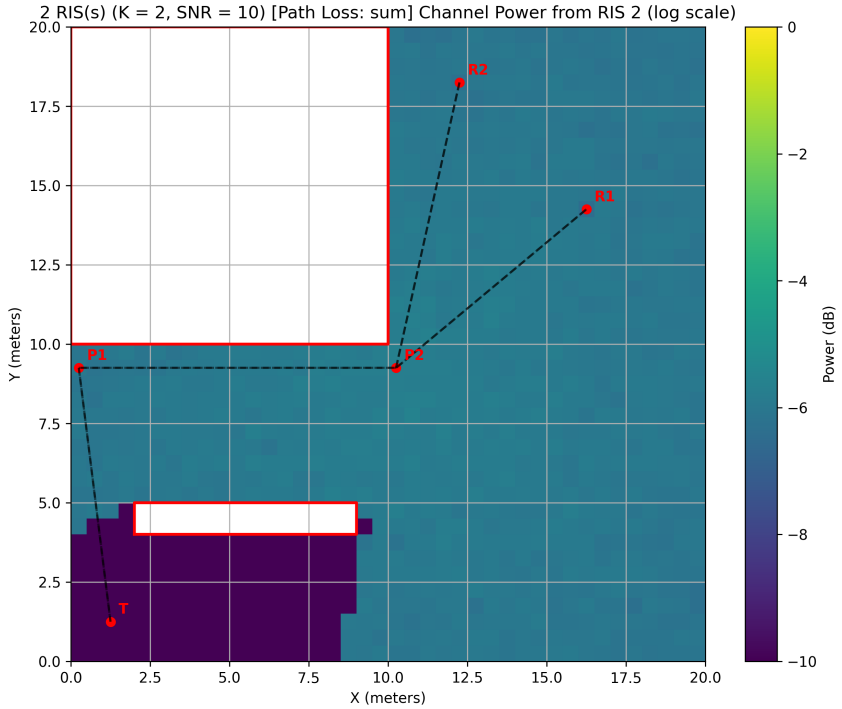

Figure 6.25: 2 RIS(s) (K = 2, SNR = 10) [Path Loss: sum] Channel Power from RIS 2 (log scale)

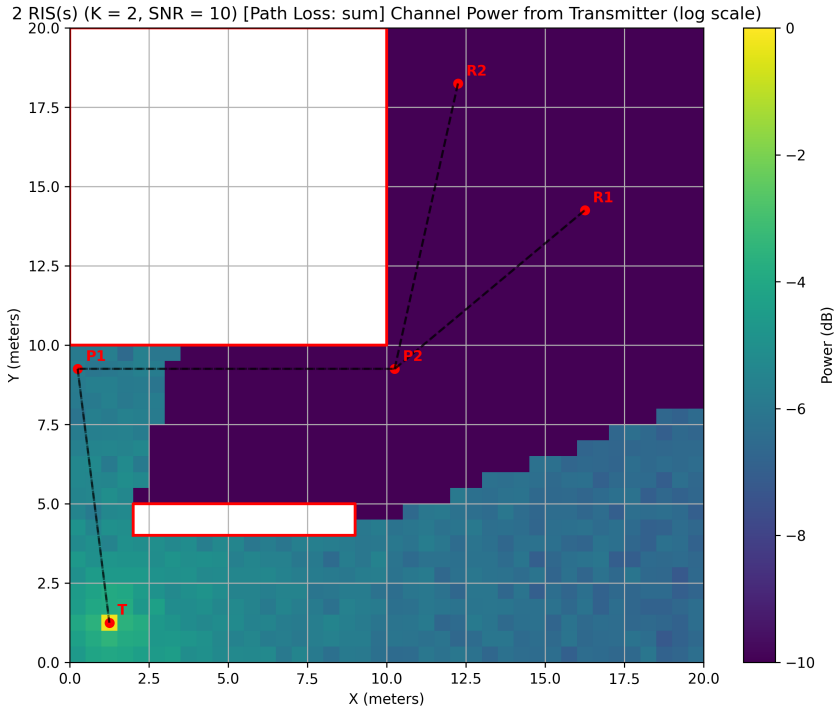

Figure 6.26: 2 RIS(s) (K = 2, SNR = 10) [Path Loss: sum] Channel Power from Transmitter (log scale)

Conclusion

In this paper, we have expanded on the work presented in [16] 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 prooposed 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 accomodate complex situation
- A wide combination of these properties in realistic network conditions

With our Bit Error Rate (BER) simulations, we proved and demostrated how the receivers are able to receive correctly the messages with a low error percenteage, while ensuring no other malicious actor can decypher the signal when not having direct Line of Sight (LOS) from the transmitter. Even when this link is present, our configurations ensure the RIS distrupt 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 strenght using path loss. These added simulation will aid exporting our solution from a mathematical proof to an effectivle 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 reducing the load on higher layers wich could impact negatively the usefulness of communications when latency and frequency of communication is crucial.

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 protocol, like GSSK [11] instead of the proposed SSK [12]
- 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 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] 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.

[3] 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.

[4] Steven Dalton, Luke Olson, and Nathan Bell. Optimizing sparse matrix—matrix multiplication for the gpu. *ACM Trans. Math. Softw.*, 41(4), October 2015.

[5] 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.

[6] 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.

[7] 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`.

[8] 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.

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

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

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

[21] 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.

[22] 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.

[23] Ludwig Streloke and Jörg Franke. Electrifying the road: Disruptive shifts in automotive value creation. In *2024 1st International Conference on Production Technologies and Systems for E-Mobility (EPTS)*, pages 1–8, June 2024.

[24] 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.

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

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

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

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

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

[30] 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.