Radio security potential in WLAN application

Group No. 07gr1122

Josselin Berthod

Laurent My

June 2007

AALBORG UNIVERSITY

Aalborg University

E-Studyboard

Mobile Communications 10th semester

TITLE:

Radio security potential in WLAN application

THEME:

Mobile Radio Communications

PROJECT PERIOD:

4th February 2007

7th June 2007

PROJECT GROUP:

07gr1122

GROUP MEMBERS:

Josselin Berthod

Laurent My

SUPERVISORS:

Xin Zhou

Patrick Eggers

COPIES: -

Number Of Pages: -

Main Report: -

Appendixes: -

Abstract:

In the wireless communications, the signal is susceptible to be intercepted by eavesdroppers. As the security concerns the link reliability, the purpose of this project is to secure the data information in the physical layer. The idea is to apply a singular value decomposition (SVD) scheme in a multiple-input multiple-output (MIMO) system between the access point and the target user.

The interest of our project is how the eavesdropper will catch the signal. The system has to be robust built-in and should be totally transparent and inherent for the user. This project mainly includes three aspects.

- Evaluate the performance of the SVD scheme in a MIMO narrowband system. In this part we try to enhance the target user capacity by changing the power allocation schemes (Uniform, Water filling).
- Investigate the security robustness of our system regarding the eavesdropper interceptions. In this section, we evaluate the performance of the eavesdropper by applying different processing such as SVD, combining techniques (Equal Gain Combing (EGC), Maximun Ration Combining (MRC)).
- Propose a trade-off between the capacity of the target user and the signal deterioration to prevent the eavesdropper to capture and understand the data information.

Contents

List of Figures

Abbreviations

AOA Angle Of Arrival

AOD Angle Of Departure

CSI Channel State Information

EGC Equal Gain Combining

IPsec Internet Protocol Security

LAN Local Area Network

LOS Line Of Sight

MIMO Multiple Input Multiple Output

MISO Multiple Input Single Output

MRC Maximum Ratio Combining

NLOS Non Line Of Sight

OFDM Orthogonal Frequency Division Multiplexing

OSI Open Systems Interconnection

Rx Receiver

SC Selective Combining

SCF Space Coherence Function

SIR Signal to Interference Ratio

SNIR Signal to Noise plus Interference Ratio

SIMO Single Input Multiple Output

SISO Single Input Single Output

SNR Signal to Noise Radio

OFDM Orthogonal Frequency Division Multiplexing

STC Space Time Coding

SVD Singular Value Decomposition

TLS Transport Layer Security

Tx Transmitter

UPA Uniform Power Allocation

WEP Wired Equivalent Privacy

WPA Wi-Fi Protected Access

WLAN Wireless Local Area Network

WWiSE World-Wide Spectrum Efficiency

Symbol List

a	amplitude
c	light speed
d	distance between Tx and Rx
p	probability function
τ	time variable
G	Diversity Gain
FFT	Fourier Transform Operator
x_e	Eavesdropper space position
x_t	Transmitter space position
x_u	User space position
f_d	Doppler shift
λ	Wavelength
λ	Wavelength
Tx	Transmitter
Rx	Receiver
c	speed of light
υ	Velocity
Δf	Maximum doppler shift
H	Channel Matrix
He	Channel Matrix between transmitter and eavesdropper
V,Ve	matrix which contains the right singular vectors of H,He respectively
$\underline{x}$	input vector
$\underline{y}_{user}$	Output vector of the target user
$\underline{y}_e$	Output vector of the eavesdropper
$\underline{r}$	Received signal vector
$\underline{s}$	Transmitted signal vector

U, Ue	matrix which contains the left singular vectors of H,He respectively
D	**diagonal matrix** which contains the singular values of H
λ_k	k^{th} Singular Value of H
C	Capacity
Nt	Number of transmitter antenna
Nr	Number of receiver antenna
P_k	Power assigned to the kth sub-channel
K	Number of pair of transmitter and receiver antenna
P_N	represents the Noise Power
γ_k	represents the Signal to noise ratio
C_1	capacity for a SISO link
$SNIR_{e1}$	Signal to Noise plus Interference Ratio for the first data stream of the Eavesd
$SNIR_{e2}$	Signal to Noise plus Interference Ratio for the second data stream of the Eav

Preface

This report is the result of the 10th semester project which has been worked from the 1st February to the 7th of june 2007 by the students of Mobile communications group 07gr1122 at the APNet department of Electronic Systems, Aalborg University, Denmark. This report is an investigation on the way to secure wireless communications by acting on the physical layer using a SVD scheme. The project has been achieved on the "space space" domain in narrowband, and is based on the SVD transmission method. This report includes the problem delimitation, and the understanding of the different techniques that we are using in the project.

Once the technical review has been introduced, we defined different scenarios to work on, and we presented the simulation model that we used "Double scattering model". Finally, using a software simulator called "MATLAB", we simulated the defined scenarios in the "double scattering model" to know more about the security robustness of the SVD transmission method. Then we tried a way to optimize this method.

MOBcom group 07gr1122

June 2007

Aalborg University

Acknowledgement

We would like to express our gratitude to our supervisors Xin Zhou and Patrick Eggers for their valuable guidance throughout this project and all those people who directly or indirectly helped us to finish this project.

Josselin Berthod

Laurent My

Chapter 1

Introduction

Nowadays wireless communications is one of the most active areas of technology development. This development is being driven primarily by the demand for new wireless capacity such as voice telephony, video transmission, images, text and data.

However a very important feature of wireless transmissions is the security aspect. Indeed, counter to wired communications which are very secured in each layer of the OSI model, the security is a major weakness for wireless technologies. In wireless communications, the physical layer has an active role in the frailness of the security.

Thus, the goal of our project is to secure the data information in the physical layer by implementing it in a Wireless Local Area Network (WLAN) system.

1.1 Motivation

1.1.1 Security overview

Definition

Wireless network is widely used and popular communication tool, used to exchange messages and documents (including private and personal information, on line commercial transaction, etc). It is also the most exposed network to be attacked. That's why the security issue of a wireless network is very important. Transmission security covers the confidentiality, integrity and authentication of a transmitted information [1]. A confidential transmission can only be received by the person it is addressed to. Its integrity is assured if no unauthorized person can modify its content without being discovered. Authentication allows verifying the identity of the transmitter.

If we take the example of an electronic message, the first step is to enable users of this very open and therefore potentially vulnerable service to perform transactional operations with the following characteristics:

1. Authentication

   The goal of authentication is to reliably learn the name of the originator of a message.

2. Integrity

   The goal of integrity is to be sure that the received digital contents will not be modified while the information is sent.

3. Confidentiality

   The goal of confidentiality is that only the addressee can "open" the electronic message.

In a wireless network, the transmission between two nodes must be highly secure to prevent any kind of interception made by the eavesdroppers.

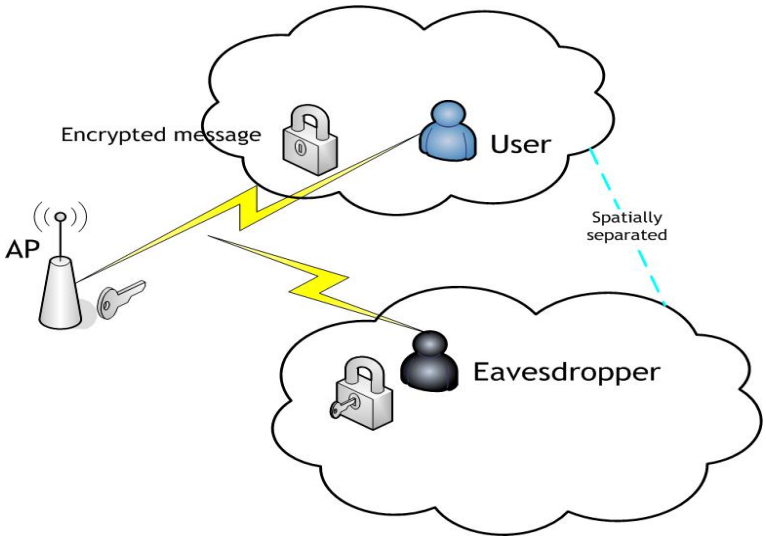

Figure 1.1: Eavesdropper scheme

To prevent any kind of interception, we choose to use the confidentiality characteristic to fight against eavesdroppers. Thus, our project will be based on the way to code the information in order to protect the confidentiality characteristic of the transmitted message. Code phase information, code time information or code frequency information are different codes that we can use to protect information. In the next chapter, we are going to present all of these codes to finally use one of them.

OSI model [2]

Regarding the OSI model, the security issue has been commonly investigated in high layers, such as Internet Protocol Security (IPsec) in the network layer and Transport Layer Security (TLS) in the transport layer. A few protocols have been developed to achieve security in wireless communications in the datalink layer, such as Wired Equivalent Privacy (WEP) which finally seems to be too weak. WEP provides the same encryption key for every user on a network, and this key is only 40 bits. The worst drawback of the WEP, is a mathematical program called "Airsnort", available from many websites, which allows a hacker to eliminate most possible keys in the key management system built into WEP [3]. Wi-Fi Protected Access (WPA)1 and WPA2 are more secured than the WEP, however it can be complicated to setup which makes it unsuitable for domestic users. In order to enhance security in the OSI model, most of the layers have to be secured [2]. That is the reason why, investigating the security aspect of the physical layer is an important complement to the security features obtained in higher layers.

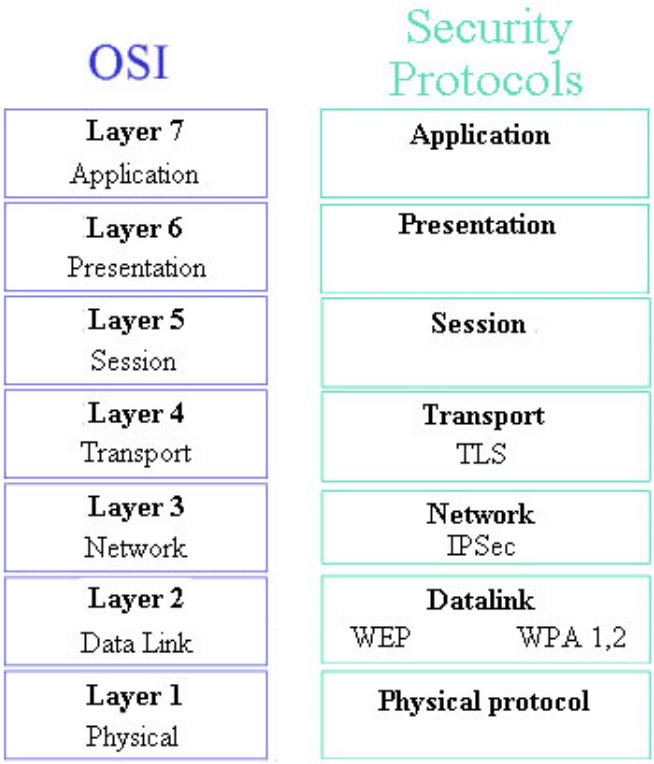

Figure 1.2: Security protocols in OSI model

One of the solution to enhance the security problems in wireless communications by

ensuring a certain confidentiality, is to secure the information in the physical layer. The physical layer is the lowest and the most basic network layer in the OSI model (Open System Interconnect), sending a bit stream of raw bits. This bit stream may be grouped into symbols or words before being converted into a physical signal, and it is transmitted over a physical transmission medium. To protect the transmission, the medium would be enough to keep confidentiality against eavesdroppers. However the question of robustness of such a system would appear at the same time. A good example to illustrate the benefits of securing data in the physical layer, is the transparency and the inherency for the user. For a domestic user with basic level in computer science, security has to be transparent and inherent to him. Security protocols such as WEP, or WPA2, need to be set up, updated, and are not so easy to be manipulated. To secure the physical layer, we will provide a certain level of security and keep the security process invisible to the user.

1.2 Background technology

1.2.1 Transmission Medium

Introduction to the medium

According to [3], a medium is a link between several entities which want to exchange information. This medium can be represented by anything, if it follows the previous definition, such as a man who repeats a sentence from another man to somebody else.

In our project, we are dealing with security in wireless communications. That's why we are considering "the air" as a medium, and radio waves will go through it from the different devices to other equipments supporting wireless communications.

Let us study a very simple case with a SISO link : Figure 1.3

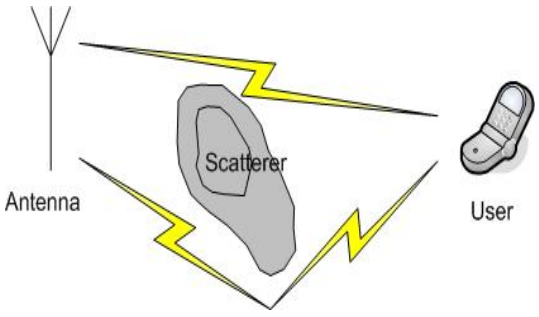

Figure 1.3: SISO Link

A SISO link is referred as a link with only one absolute level compare to the relative

link, which is described later in this part of the report. In a SISO link, the information goes from the transmitter (Single Input) to the receiver (Single Output, one sensor). At the receiver side, we can get only one absolute level of the signal. Regarding the relative link, MIMO can be a good example. The information goes from the transmitter (Multiple Inputs) along different paths to the receiver (Multiple Outputs, multi-sensors), and this give us the option to compare several absolute levels.
Many variables can be exploited to analyse the behavior of the signal over the transmission in order to keep it confidential. These variables are part of the temporal or the space domain described below.

1. Temporal domain analysis:
   In the time domain, which is a waveform analysis, one interesting propagation time-variable is the propagation delay τ, between the transmitter and the receiver.

2. Frequency domain analysis:
   Concerning the frequency domain which is a spectrum analysis, a few parameters such as amplitude or phase can be changed by the motion of the scatterers.

3. Space domain analysis:

   - The locations(x,y,z) of the transmitter and the receiver are reliable parameters to distinguish two different nodes. Such parameters are specific to the user.
   - Another interesting point to explore is the Angle Of Arrival (AOA) and the Angle Of Departure (AOD) at the receiver and the transmitter side respectively.

4. Doppler domain analysis
   It is possible to introduce the doppler shift due to the motion of the terminals.

$$\Delta f = \frac{f\upsilon}{c} = \frac{\upsilon}{\Lambda} \tag{1.1}$$

   - Δf represents the maximum doppler shift
   - f represents the transmitted frequency
   - c represents the speed of light
   - υ is the velocity of the transmitter relative to the receiver in meters/second: positive when moving towards one another, negative when moving away
   - λ is the wavelength of the transmitted signal

As can be seen in Figure 1.3, there are different paths, due to the scatterer in this case. That gives us a Line Of Sight (LOS) path and a Non Line Of Sight (NLOS) path.

A multi-path channel containing several paths can be presented in form of its LOS and NLOS impulse responses or transfer functions depending on the domain that we have chosen (respectively time or frequency).

Figure 1.4 below shows the relation between the four different representations of two dimension links characterization [4] which depend on different variables, using the Fourier transform.

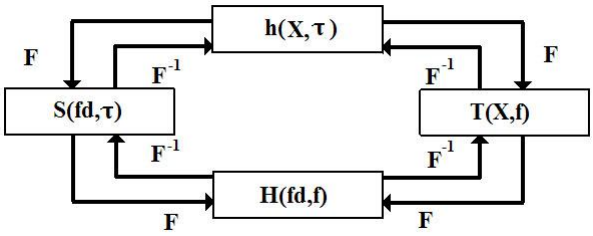

Figure 1.4: Linear Space-variant system: System Functions

- $h(x_t, \tau)$

  It represents the impulse response which depends on the time and space (Space location of the transmitter).

- $T(x_t, f)$

  It represents the Time variant transfer function depending on the frequency (f) and the space location of the transmitter.

- $H(f_d, f)$

  It represents the Doppler variant spreading function depending on the frequency and the Doppler frequency.

- $S(f_d, \tau)$

  It represents the Spreading function depending on the doppler frequency and the delay.

A very important point regarding security aspects of this project is to be able to differentiate these impulse responses or transfer functions using their parameters (frequency, doppler shift, time and space locations). Concerning time domain, the delay can be interesting to distinguish two paths. However, this variable is not enough to specify a user.

Consequently it may become a security problem to use this parameter alone. Another variable is the location (X,Y,Z) of the Transmitter (Tx) and the Receiver (Rx). This would provide us the ability to distinguish with a very precise manner, one node among the others.

Our impulse response and transfer function will take the following form:

$$h(\tau, \underline{x}_t, \underline{x}_r) \rightarrow H(f, \underline{x}_t, \underline{x}_r) \tag{1.2}$$

where x_t and x_r are the space locations of the transmitter and the receiver in the SISO case. The "–>" represents the Fourier transform. The underlined symbols denote vectors.

As can be seen in the following figure, we added an eavesdropper to the SISO link. The aim is to underline the difference between the user and the eavesdropper regarding the impulse response and the transfer function. x_r is the space location of the user and x_e is the space location of the eavesdropper. We can see that adding this space location variable gives a specific impulse response and a transfer function to the user.

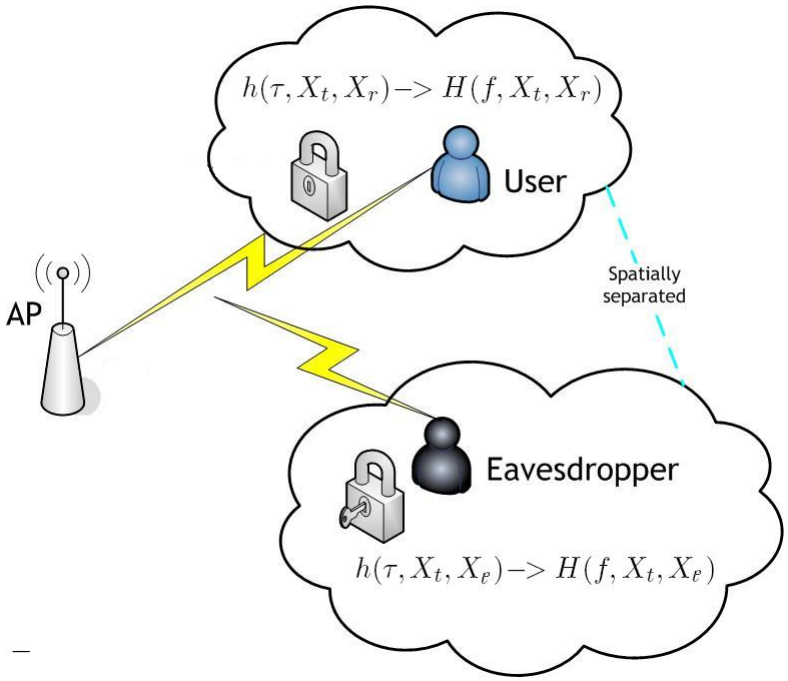

Figure 1.5: SISO link : Difference between user and eavesdropper

Inducing a change in the medium

This general description of a SISO link, reveals that this type of link is not the most efficient to use (due to its single sensor) to get a secured transmission.

Indeed a simple link set up with only one variable (1 antenna, 1 time delay or 1 sub carrier) is easier to be hacked by an eavesdropper than a link with several variables.

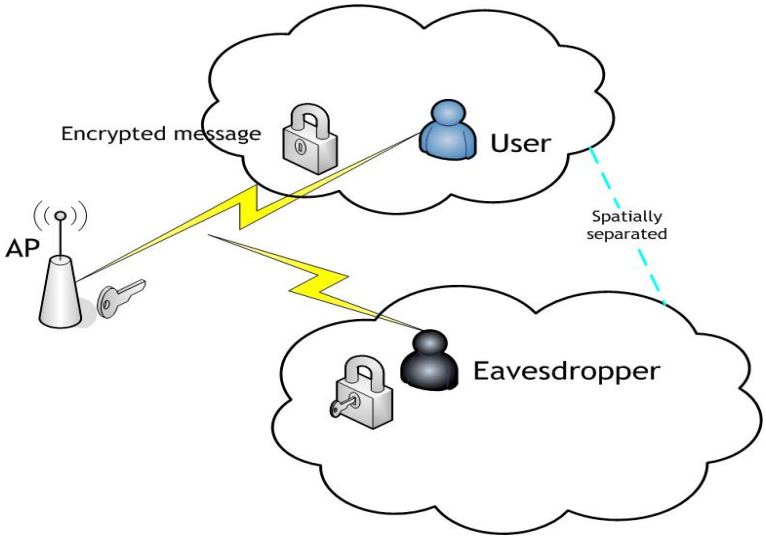

Figure 1.6: General view of our system

In this work, our goal is to enhance the security part in order to fight against eavesdroppers. Thus, the idea of how to secure the medium between AP and user is to introduce a change in the medium.

We want to use differential information from the medium. In order to do this, we need to compare variables with themselves using at least 2 sensors and 2 activators. Figures 1.7, 1.8, and 1.9 below illustrate what we mean by compare variables with themselves.

This kind of link is named "Relative link" and is more robust than a simple "SISO link".

By manipulating 2 variables in the same time (2 antennas, 2 time delays or 2 sub-carriers), it now becomes more difficult for the eavesdropper to get the key to several channels.

1.2.2 Existing principles

There are many existing methods on which it is possible to improve the security aspect. Few of them are already more secure than the others, but can be enhanced regarding the tradeoff between security and efficiency.

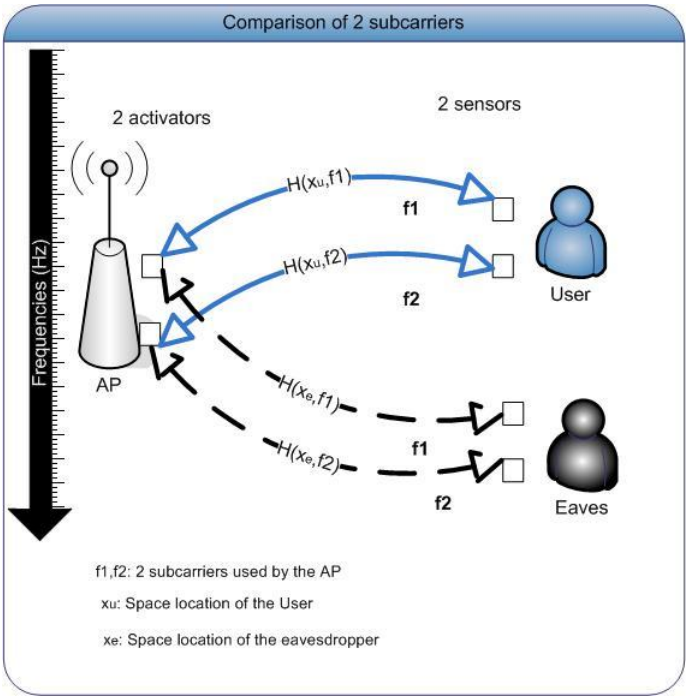

Figure 1.7: Space Frequency

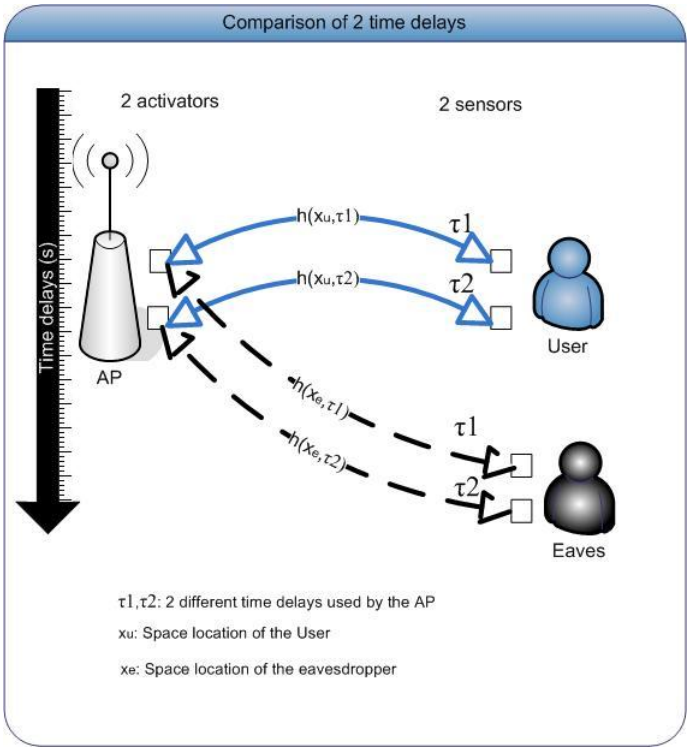

Figure 1.8: Space Time

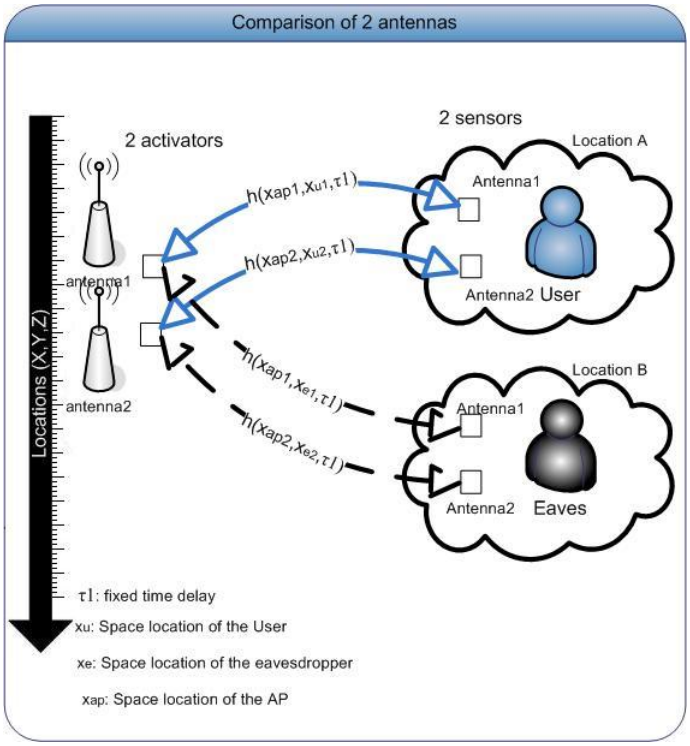

Figure 1.9: Space Space

1. Space Space techniques

   One technique which can be considered as space space technique is **spatial multiplexing** [5]. It multiplexes the information and transmits it via independent channels (different bits from different antennas). Receivers need to know about the Channel State Information (CSI). MIMO technology is the most popular technology using the spatial multiplexing concept.

2. Space-time techniques:

   Space-time coding arises from the diversity concept [5]. It relies on the transmission of multiple and redundant copies of one data stream to the receiver over the time and multiple antennas at the transmitter side. The objective is to sure that, in case of tough environment, the information reaches the destination in a good quality. If the receiver knows about the CSI, it becomes easier. However it is not mandatory to have this condition.

   There are two main Space Time Coding (STC) techniques:

   - Space-Time trellis Coding technique

     This STC scheme is using trellis codes. M-bit information symbols are encoded

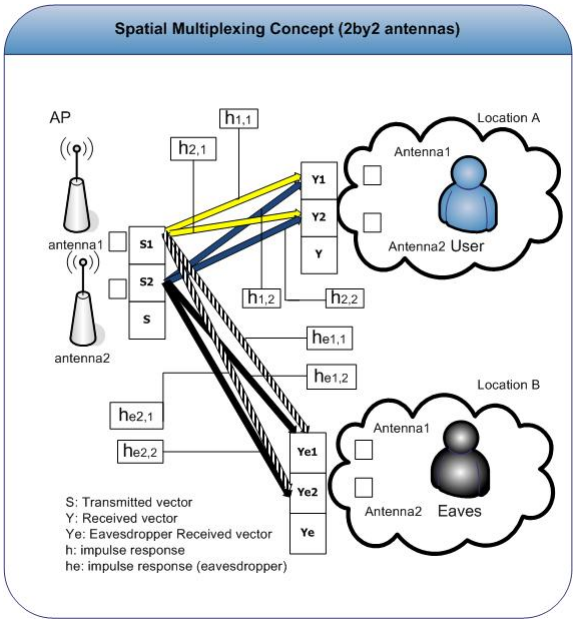

Figure 1.10: Spatial Multiplexing Concept

into N-bit symbols, with N > M and a constraint k (length of the code).

N_1=M_1+M_0+M_{-1}

N_2=M_0+M_{-1}

N_3=M_1+M_{-1}

This technique is providing diversity gain and coding gain, but is more complex than the following STC technique, Space Time Block Coding. [6]

- Space-Time Block Coding technique
  This scheme provides only diversity gain and no coding gain and is less difficult to implement than the trellis one.

3. Space frequency techniques:
   One space frequency technique is Space-Orthogonal Frequency Division Multiplexing (OFDM). Space comes from the spatial separation between the multiple antennas.The OFDM modulation scheme provides efficient results in hostile environments with multi-paths channels, using multiple closely spaced orthogonal sub-carriers. However improvements can be obtained using more than one antenna at the receiver side or at the transmitter and receiver sides, which refers to Space-OFDM.

1.3 Problem definition

This section is a detailed summary of the problem we tackle in this project and delimitations that we applied. The goal of this project is to enhance security in the physical layer in a WLAN system

1.3.1 Project motivation

The broadcasting aspect of the wireless communications compare to the difficulty of physical access in a Local Area Network (LAN), yield us to take into account the security during a transmission [3]. In our case, we want to prevent the eavesdropper to read the transmission between the access point and the target user. That's why in our project we are going to focus on the **confidentiality** aspect which is supposed to protect the transmitted data to be read by a stranger.

Regarding the OSI model, many protocols have already been designed to enhance security in several layers, such as WEP and WPA in Data link layer, or IPSec in the Network layer. Adding security in most of the OSI layers would appears to be an efficient method to secure communications, especially in the physical layer. Physical layer defines the modulation, signal processing, hence it can be useful to act on it. Indeed the broadcasting aspect of the wireless communications is one of the main source of interception hacking. Moreover, dealing with the physical layer, for a domestic user, security will be transparent and inherent to him comparing to set up WPA protocols, that can be very complex for such a user.

1.3.2 Differentiating the user from the eavesdropper

A very important point in order to keep the confidentiality during a transmission, is to differentiate the user from the eavesdropper. We chose one main aspect that we can investigate between the target user and the eavesdropper.

- locations

  The first difference is the localization of the user. In impulse responses, we need to include the space locations of the transmitter and the receiver. The temporal variables with only the space locations of the transmitter are not enough specific , to be used without spatial location variables of the receiver (target user).

- link conditions

  The link conditions,is related to the locations. The link condition deal with the path between the target user and the transmitter. The motion of the target user, may change the link conditions between him and the transmitter. The variation of this link can be interesting to differentiate the target user and the eavesdropper.

1.3.3 Principle choice

As we mentioned previously in the "existing principles" part, there are several methods related to different domains, on which we can improve security or the trade off between efficiency and security. We are going to focus on one of these techniques regarding the security aspect without omitting the efficiency point of view.

Spatial multiplexing

1. benefit of the spatial multiplexing technique

   MIMO, stands to be the future of WLAN. We chose to focus on multiple antennas techniques, because they provide higher throughput (using spatial multiplexing technique) and improve reliability (using diversity technique). That's why spatial multiplexing would appear to be the suitable principle to deal with in our project.

2. Security in spatial multiplexing

   Compared to the diversity concept, which transmits the same signal in each datastream, spatial multiplexing provides several different signals, which will be combined at the receiver side to recover the original signal. This behavior can be considerer as a kind of security.

   Moreover, regarding the rise of MIMO technology which relies on the spatial multiplexing concept, it appears to be closer to the market than the other existing methods that we mentioned previously. The security in spatial multiplexing technique becomes a very important point. Thus, the aim in this project focuses on the trade-off between efficiency and security. We are going to minimize the SNIR for the eavesdroppers, and maximizing the capacity for the target user.

   The security will be investigated following these two questions:

- How is the SNIR of eavesdropper and the capacity of the target user in a normal case? The normal case is when no parameters are modified in the system.
- How is the capacity of the target user with a SNIR of eavesdropper close to 0dB? This case is when we try to deteriorate the signal that the eavesdropper may catch.

Chapter 2

Spatial multiplexing MIMO system

As MIMO technology becomes more and more employed in the wireless industry, it is important to understand the fundamentals of different techniques and their associated benefits. The first sections of this chapter are investigating on the benefits of the MIMO technology and especially the concept of spatial multiplexing. Other sections are dedicated to the different scenarios that we defined. In these scenarios, we clarify different parameters and we are going to act on them in order to appreciate the results.

2.1 Wireless fundamentals

A conventional scheme of a wireless system is a SISO system.

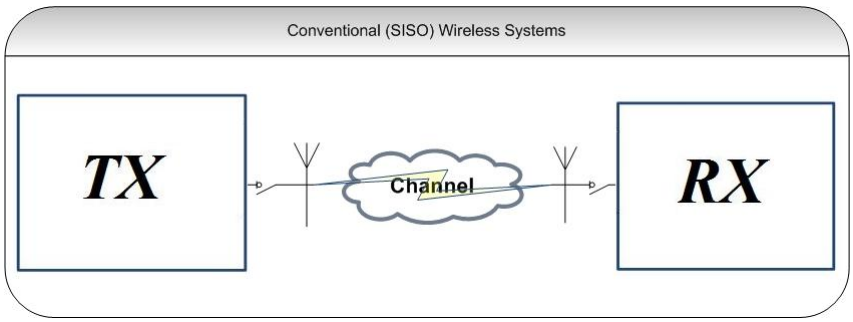

Figure 2.1: Conventional (SISO) Wireless Systems

This type of wireless system is very simple and the installation of this kind of network is very cheap but it exists some shortcomings.

- The system is based on only one antenna in the transmit side and one antenna in the receive side. Thus, if one of the antennas is out of service, the all system will surely

be out of service too. One solution to this problem could be to use several antennas and switch among them in case of one antenna would collapse.

- The only receive antenna should be able to catch the signal sent by the transmitter. So energy is wasted by sending in all directions and it can cause additional interferences to others.
- The system becomes quite sensitive to the interferences from all the directions.
- A single power amplifier limits the output power.

Another aspect to consider in a wireless system is the capability of the received signal to decode the data.

Indeed to decode successfully the data transmitted, the signal strength needs to be greater than the power of the noise plus interference by a certain amount:

- Higher data rates require higher SNIR
- Signal strength decreases with an increased range in a wireless environment.

By increasing the data rate, the first idea is to enhance the conventional single Tx and Rx radio systems by changing different aspects of the transmission. But each aspect that we want to change (transmit power, high gain directional antennas, more frequency spectrum) have some shortcomings.

Benefits of the SISO link

Conventional SISO systems were favored for simplicity and low-cost. Moreover, since the system is set up with 1 transmitter and 1 receiver, we have only one link.

According to [7], use multiple antennas provide several benefits; for example, array gain, diversity gain and multiplexing gain.

2.1.1 MISO(Multiple Inputs Single Output) and SIMO (Single Input Mulitple Outputs) Systems

In these two configuration systems, two gains are available:

1. Array gain

   By using beamformers at either Tx or Rxside, we can have an average increase in the SNR at the receiver, compared to SISO case.

2. Diversity gain

   Diversity appears when the same signal is transmitted by several antennas. Thus, by combining signals from multiple antennas, the diversity gain appears.

2.1.2 The different MIMO systems

There are several way to use multiple antennas in wireless communications and in this section we will explore these different techniques, in MIMO channel.

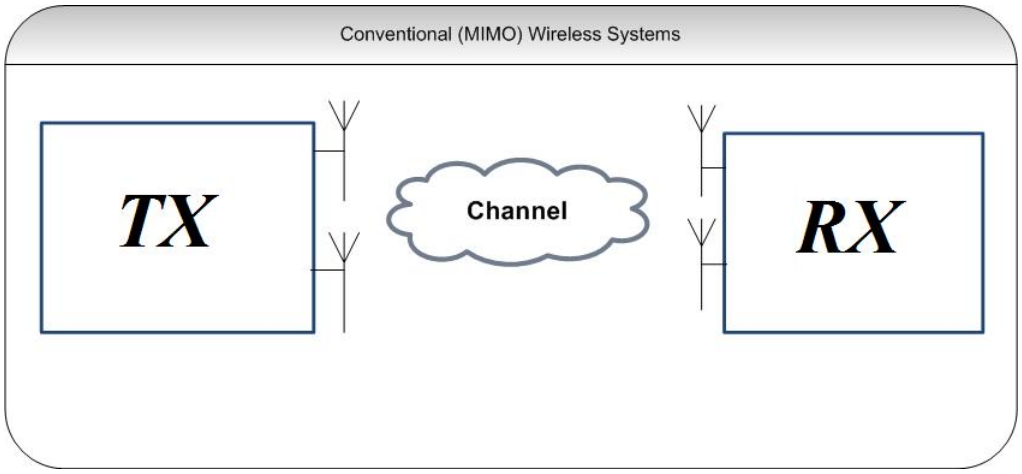

Figure 2.2: Conventional(MIMO)Wireless Systems

Nowadays, MIMO scheme is becoming a key part in almost every new wireless standards and is providing an additional spatial dimension for communications.

There are three basic types of MIMO technologies:

- Beamforming technique

  This technique provides two different gains already considered in the previous section.

  1. Array gain
  2. Diversity gain

- Spatial Diversity

  In a MIMO system, if we decided to transmit the same signal from each antenna, we

have a diversity gain. This is used to improve the quality of the signal, the bit error rate is reduced. Antennas are separated in the way to obtain independent fading of the transmitted signal.

- Spatial Multiplexing
  Compared to the other technologies, the spatial multiplexing gain offers a huge improvement of the capacity by transmitting different signals from the different antennas.

In this project, we decided to study the additional spatial dimension provided by a MIMO system. In order to achieve this choice, we chose to exploit the spatial multiplexing technique.

2.1.3 Spatial Multiplexing

Spatial Multiplexing concept

Spatial multiplexing occurs when several streams are transmitted simultaneously from the Tx to the Rx independently, in a MIMO system. It is important to notice that the multiple streams are transmitted simultaneously (i.e. at the same time and frequency). [8]

Let's see more deeply, in Figure 2.3 what happens in the channel during a spatial multiplexing communication

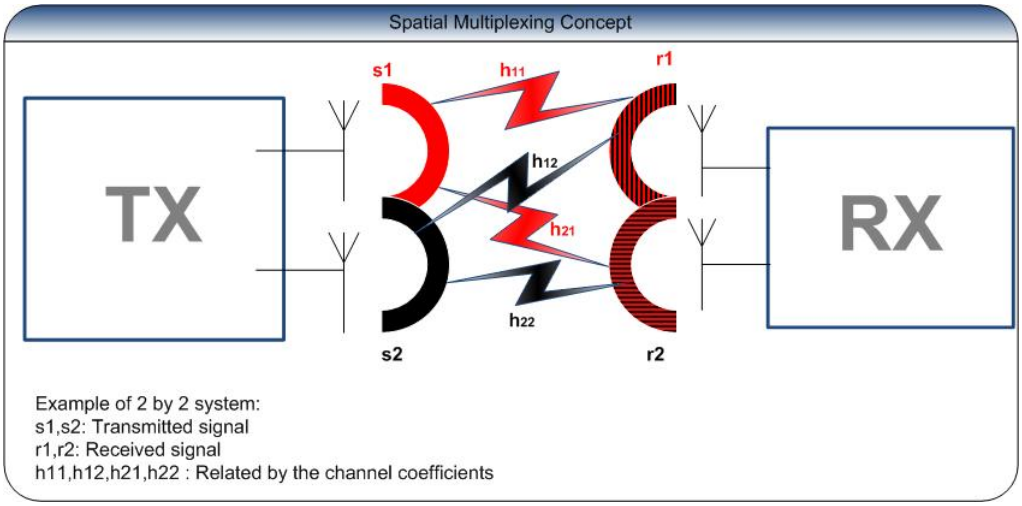

Figure 2.3: Spatial Multiplexing concept

The system is built to communicate with a higher total data rate due to the multiple independent links (on the same channel) between Tx and Rx and also because of the cross-

paths between antennas 2.3. Please notice that the different coefficients are explained in Figure 2.3, where h_{ij} represents the channel coefficient between the j^{th} Tx and the i^{th} Rx. The received signal at Rx1 (r1) and Rx2 (r2) are

$$r_1 = h_{11} \cdot x_1 + h_{12} \cdot x_2 \tag{2.1}$$

$$r_2 = h_{21} \cdot x_1 + h_{22} \cdot x_2 \tag{2.2}$$

At the TX and RX side, signals are processed with the SVD. [9]

$$\mathbf{H} = \mathbf{U} \cdot \mathbf{D} \cdot \mathbf{V}^H \tag{2.3}$$

H: Channel transfer matrix with $[.]^H$ represents the hermitian (transpose(conj)) matrix
U: columns are the eigenvectors of HH^H and form an orthonormal basis.
D: diagonal, λ_1 and λ_2 singular values are the square roots of the eigenvalues of both $H^H H$ and HH^H
V: columns are the eigenvectors of $H^H H$ and form an orthonormal basis.

2.2 First Scenario: The access point knows only the target user

The first scenario is the simplest situation we can have since the Tx (access point) sends a message to the Rx (targer user) without paying attention to any existing eavesdroppers.

In this section we are going to investigate the ability of the target user to receive the signal. We evaluate his performance by 2 parameters (SNR and capacity) taking into account that the transmitter will focus on its transmission to maximize the capacity of the target user. In the next section, we are going to see how the received signal is decode by the target user.

2.2.1 Situation with the target user only

SVD for the target user

In the following part, we want to find the signal received by the target user using SVD technique.

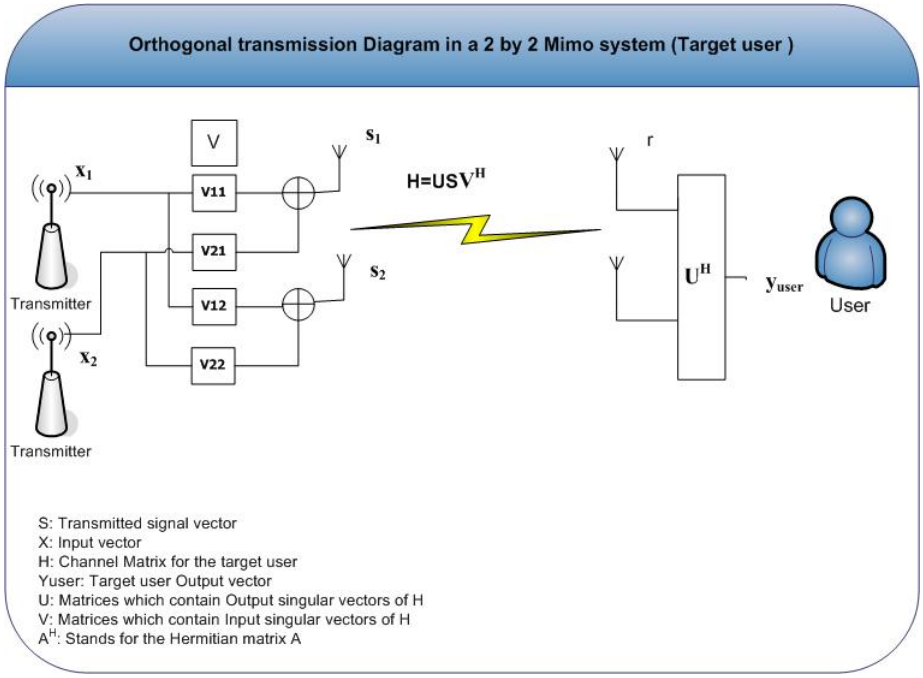

Figure 2.4: Orthogonal transmission diagram in a 2×2 system

As can be seen on the figure (2.4) , $\underline{s}$ is the transmitted signal vector [10] and is composed by s1 and s2.

$$\underline{s} = \mathbf{V} \cdot \underline{x} \tag{2.4}$$

V is the matrix which contains the right singular vectors of **H**, and $\underline{x}$ is the input vector.

$\underline{r}$ is the received signal vector and is equal to

$$\underline{r} = \mathbf{H} \cdot \underline{s} + \underline{n} \tag{2.5}$$

Where **H** is the channel matrix for the user and "$\underline{n}$" stands for the additive noise.

Using Equation (2.4)

$$\underline{r} = \mathbf{H} \cdot \mathbf{V} \cdot \underline{x} + \underline{n} \tag{2.6}$$

We know the channel matrix for the target user is equal to

$$\mathbf{H} = \mathbf{U} \cdot \mathbf{D} \cdot \mathbf{V}^H \tag{2.7}$$

Where **U** is the matrix which contains the left singular vectors of **H**, **D** is a diagonal matrix which contains the singular values of **H** and $\mathbf{V}^H$ means the Hermitian of the matrix **V**.

Then, using Equation (2.7) in equation Equation (2.6) we get

$$\underline{r} = \mathbf{U}\mathbf{D}\mathbf{V}^H \cdot \mathbf{V} \cdot \underline{x} + \underline{n} \tag{2.8}$$

V is a unitary matrix,so

$$\mathbf{V} \cdot \mathbf{V}^H = \mathbf{I} \tag{2.9}$$

this gives us

$$\underline{r} = \mathbf{U} \cdot \mathbf{D} \cdot \underline{x} + \underline{n} \tag{2.10}$$

To continue after the processing, we do:

$\underline{y}_{user}$ is the output vector for the target user, which contains the received signals.

$$\underline{y}_{user} = \mathbf{U}^H \cdot \underline{r} + \mathbf{U}^H \cdot \underline{n} \tag{2.11}$$

Using Equation (2.10) that we calculated just before:

$$y_{user} = \mathbf{U}^H \cdot \mathbf{U} \cdot \mathbf{D} \cdot \underline{x} + \mathbf{U}^H \cdot \underline{n} \tag{2.12}$$

U is an unitary matrix, so

$$\mathbf{U} \cdot \mathbf{U}^H = \mathbf{I} \tag{2.13}$$

then

$$\underline{y}_{user} = \mathbf{D} \cdot \underline{x} + \underline{n} \tag{2.14}$$

For a two by two MIMO system we have the output vector of the target user:

$$y_{user} = \begin{pmatrix} y_{u1} \\ y_{u2} \end{pmatrix} = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \tag{2.15}$$

where λ_1 and λ_2 are the singular values of H which come from the matrix **D**.

As a result, we have two equation

$$y_{u1} = x_1 \cdot \lambda_1 + \underline{n}_1 \tag{2.16}$$

$$y_{u2} = x_2 \cdot \lambda_2 + \underline{n}_2 \tag{2.17}$$

After this part concerning the processing which is going to be used between the access point and the target user, we are focusing the next part on the power allocation. Actually, the way the power is shared among the antennas, is managed at the transmitter side in order to enhance the capacity of the target user.

Power allocation schemes

There are many different ways to share the total power among the transmit antennas. The real goal of the power allocation is to optimize the capacity of the target user. In this section we introduce 2 different techniques to manage the power from the access point.

- Waterfilling power allocation scheme

  In the case of spatial multiplexing, the Tx knows about the channel. Hence, a water-filling power allocation scheme is a suitable strategy to optimize the capacity of the system.

  The following theorem, which is a waterfilling technique, is called "Gallager's water filling theorem", which is [11]:

$$\frac{1}{\lambda_1} + P_1 = \cdots = \frac{1}{\lambda_K} + P_K = Dl \tag{2.18}$$

  Where $D\ell$ is the common level to fill up by the sub-channels.

  As you can see in Figure 2.5, the value of the power is related to the eigenvalues of the subchannels.

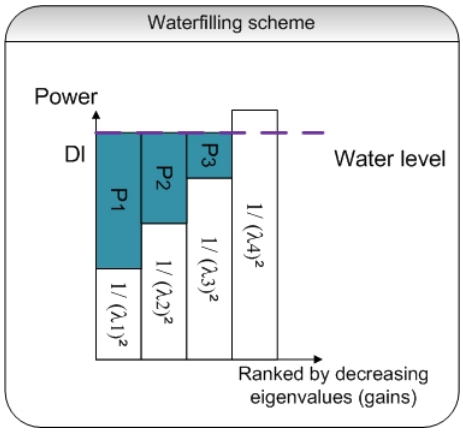

Figure 2.5: Waterfilling scheme

  In figure 2.6, shows how the power is used in a 4x4 case.

  The waterfilling technique is giving more power to a specified data stream (which is a good benefit), however this leads us to have higher order modulations. One other technique which avoids this kind of disadvantage is the Uniform Power allocation scheme.

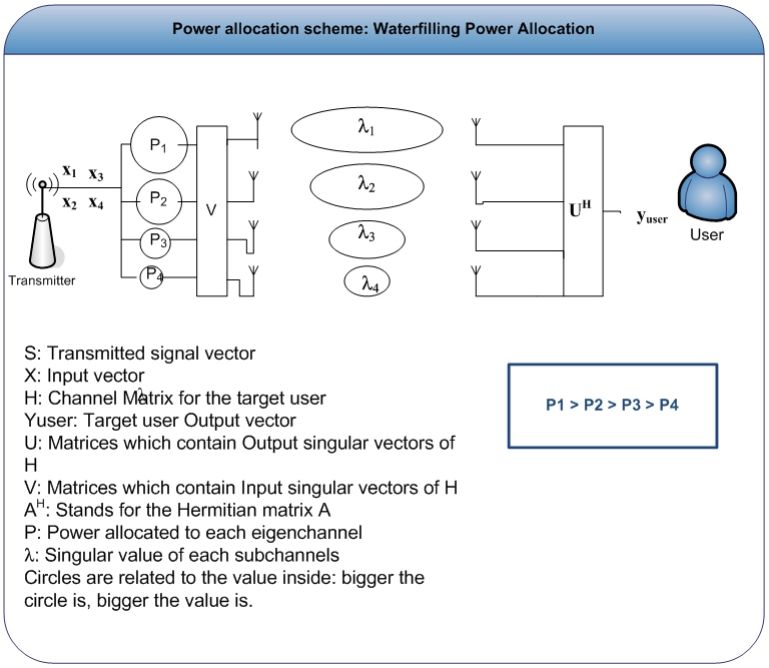

Figure 2.6: Waterfilling power allocation

- Uniform or equal power allocation scheme

  In the Uniform Power Allocation (UPA) scheme, the objective is to distribute the power as uniform manner to get a quite acceptable result. If we choose to use a waterfilling power allocation, we would transmit with higher power through certain data streams that are worst than the others, so it may lead to a huge waste of power.

  As you can see in Figure 2.7, the value of the power is the same for each subchannel and is not related to the eigenvalue of the subchannels.

  As an example, if we choose to work with the equal power allocation:

$$P_1 \doteq \ldots = P_{N_{TX}} = \frac{P_t}{N_{TX}} \tag{2.19}$$

  In our case (2x2 system) with $P_t = 1W$, $P_1 = P_2 = \frac{1}{2}$

SNR of the target user

The Signal to Noise Ratio is defined as the ratio of a signal power to the noise power corrupting the signal [12]. The formula to find the SNR (γ_k) for the target user is:

$$\gamma_k = |\lambda_k|^2 . \frac{P_k}{P_n} \tag{2.20}$$

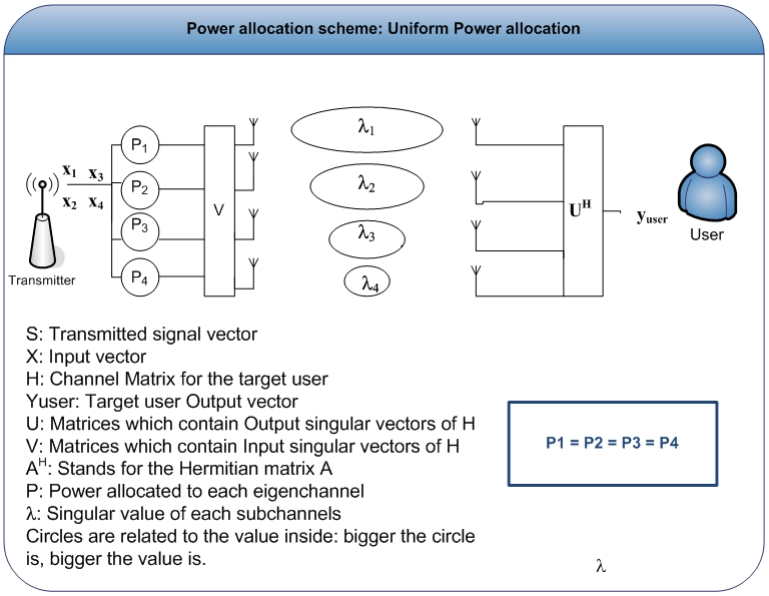

Figure 2.7: Uniform power allocation

where P_k is the power assigned to the kth data stream, $\mid \lambda_k^2 \mid$ is the eigenvalue of the kth data stream and σ_N^2 is the noise power.

To calculate the noise power, we are using the pre-detection of the SNR. [10]

$$SNR^{pre} = \frac{Pt \cdot < |H|^2 >}{P_n} \tag{2.21}$$

Where Pt represents the total transmitted power, that we set to 1 and <.> is the expectation operator [10]. By setting this value with different values, we can choose to work with a very noisy system (SNR^{pre} = 6 or 10dB) or with almost no noise (SNR^{pre} = 30dB). From the equation (2.22), we get the noise power, as an average power

$$P_n = \frac{Pt \cdot < |H|^2 >}{SNR^{pre}} \tag{2.22}$$

Capacity for a spatial multiplexing MIMO system

One of the main benefits offered by the spatial multiplexing , is the improvement of the transmission rate (the capacity) using the spatial multiplexing gain.

In a multiple antenna system, we have several data streams according to the different pairs of antennas. Spatial multiplexing technique provides a min(Nt,Nr) increase concerning the capacity, without additional power expenditure [5], and exactly the same bandwidth, where Nt represents the number of transmitter and Nr represents the number of receiver.

The capacity is given by [11]:

$$C = \sum_{k=1}^{K} log_2(1 + \gamma_k) \tag{2.23}$$

C is in b/s/Hz and K stands for the total number of sub-channel, which is also the rank of H.

If we refer to the previous part where γ_k is defined, the formula can be developed as:

$$C = \sum_{k=1}^{K} log_2(1 + |\lambda_k|^2 . \frac{P_k}{\sigma_N^2}) \tag{2.24}$$

As we mentioned previously, the capacity is enhanced without additional power expenditure. Then the different power depending on the kth sub-channels are [11] :

$$P_T = \sum_{k=1}^{K} P_k \tag{2.25}$$

In a MIMO system with K pairs of antennas. The capacity for K sub-channels will be K times bigger than for a SISO link, when the data on the data streams are different from each other. This capacity can be optimized using the suitable power allocation scheme.

2.2.2 Eavesdropper included

In this section, we still have the transmitter and the target user, however an eavesdropper is trying to catch the signal. It is important to notice, that the Tx (or Access Point) does not know about the eavesdropper. First of all, we defined a way to make the communication the most unlistenable regarding the Signal to Interference Ratio (SIR). Secondly, we want to find the received signal of the eavesdropper using SVD technique.

Singular Value Decomposition for the eavesdropper

Figure 2.8 shows the SVD case with both target user and an added eavesdropper.

Concerning the eavesdropper which is located at a different place from the target user, the channel matrix is different:

$$\mathbf{H}_e = \mathbf{U}_e \cdot \mathbf{D}_e \cdot \mathbf{V}_e^H \tag{2.26}$$

Where $\mathbf{V}_e$ is the matrix which contains the right singular vectors of $\mathbf{H}_e$,

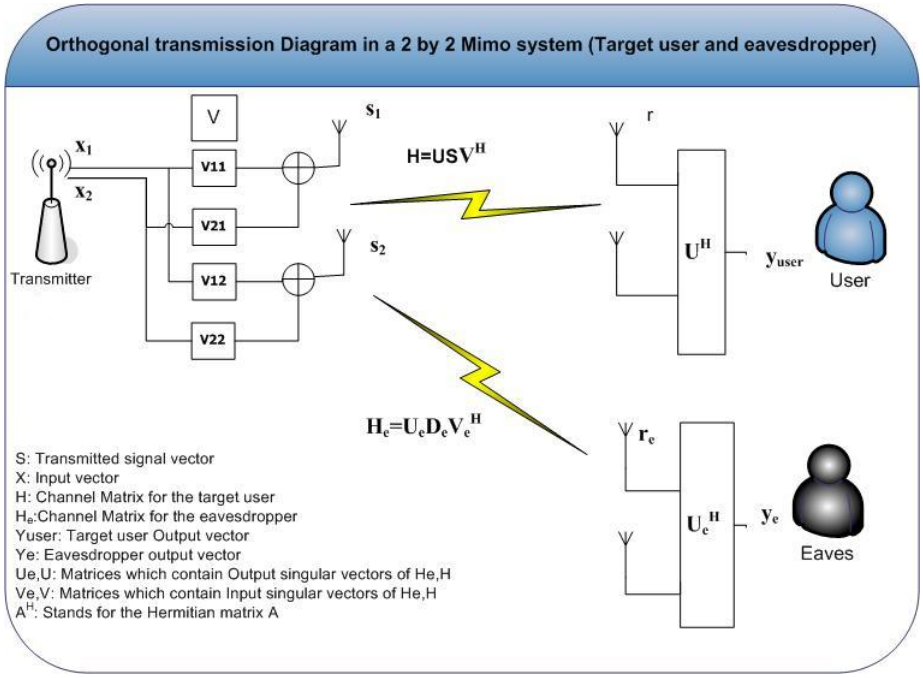

Figure 2.8: Orthogonal transmission diagram with both target user and the eavesdropper in a 2x2 system

then using Equation (2.26), Equation (2.4) and the following equation,

$$\underline{r_e} = \mathbf{H}_e \cdot \underline{s} + \underline{n} \tag{2.27}$$

We obtain

$$\underline{r_e} = \mathbf{U}_e \cdot \mathbf{D}_e \cdot \mathbf{V}_e^H \cdot \mathbf{V} \cdot \underline{x} + \underline{n} \tag{2.28}$$

From this equation (2.28) we can choose to work before the processing $\mathbf{U}_e^H$ of the eavesdropper in order to get the output signal just after the received eavesdropper antennas. In the appendix are detailed the step to get the received signal before processing equation.

$\underline{y_e}$ is the output for the eavesdropper which contains the received signals.

$$\underline{y_e} = \mathbf{U}_e^H \cdot \underline{r_e} + \mathbf{U}_e^H \cdot \underline{n} \tag{2.29}$$

Using the equations Equation 2.28,

$$\underline{y_e} = \mathbf{U}_e^H \cdot \mathbf{U}_e \cdot \mathbf{D}_e \cdot \mathbf{V}_e^H \cdot \mathbf{V} \cdot \underline{x} + \mathbf{U}_e^H \cdot \underline{n} \tag{2.30}$$

We simplify the previous equation using Equation 2.13 , to get

$$y_e = \mathbf{D}_e \cdot \mathbf{V}_e^H \cdot \mathbf{V} \cdot \underline{x} + \underline{n} \tag{2.31}$$

that is to say,

$$y_e = \begin{pmatrix} y_{e1} \\ y_{e2} \end{pmatrix} = \begin{pmatrix} \lambda_{e1} & 0 \\ 0 & \lambda_{e2} \end{pmatrix} \cdot \begin{pmatrix} V_{e11}^* & V_{e12}^* \\ V_{e21}^* & V_{e22}^* \end{pmatrix} \cdot \begin{pmatrix} V_{11} & V_{21} \\ V_{12} & V_{22} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \tag{2.32}$$

respectively for the eavesdropper and the target user.

As a result, we have two received signals at the eavesdropper side.

$$y_{e1} = \lambda_{e1} \cdot (x_1 \cdot ((V_{e11}^* \cdot V_{11}) + (V_{e12}^* \cdot V_{12})) + x_2 \cdot ((V_{e11}^* \cdot V_{21}) + (V_{e12}^* \cdot V_{22}))) + n_1 \tag{2.33}$$

$$y_{e2} = \lambda_{e2} \cdot (x_1 \cdot ((V_{e21}^* \cdot V_{11}) + (V_{e22}^* \cdot V_{12})) + x_2 \cdot ((V_{e21}^* \cdot V_{21}) + (V_{e22}^* \cdot V_{22}))) + n_2 \tag{2.34}$$

Since we know the 2 received signal at the eavesdropper side, it will be easy to determine the quality of the transmission captured by the eavesdropper.

SNIR regarding the eavesdropper

We need to calculate $SNIR_{e1}$**!** ($SNIR_{e1}$**!**) and $SNIR_{e2}$.

They are equal to

$$SNIR = \frac{P_S}{P_I + P_N} \tag{2.35}$$

where P_S the Signal Power, P_I the Interference Power and P_N the Noise Power.
Notice that in a 2x2 case

- $SNIR_{1,1}$ is the SNIR for the first datastream and with x_1 as the intended signal and x_2 as the interference.
- $SNIR_{1,2}$ is the SNIR for the first datastream and with x_2 as the intended signal and x_1 as the interference.
- $SNIR_{2,1}$ is the SNIR for the second datastream and with x_1 as the intended signal and x_2 as the interference.
- $SNIR_{2,2}$ is the SNIR for the second datastream and with x_2 as the intended signal and x_1 as the interference.

In this project, we used $SNIR_{1,1}$ as $SNIR_1$ and $SNIR_{2,2}$ as $SNIR_2$.

Regarding the equation (2.33), we obtain:

$$SNIR_{e1} = \frac{P_{e1} \cdot (\lambda_{e1} \cdot |(V_{e11}^* \cdot V_{11}) + (V_{e12}^* \cdot V_{12}))|^2}{P_{e2} \cdot (\lambda_{e1} \cdot |((V_{e11}^* \cdot V_{21}) + (V_{e12}^* \cdot V_{22}))|^2 + P_N} \tag{2.36}$$

Regarding the equation (2.34), we have:

$$SNIR_{e2} = \frac{P_{e2} \cdot (\lambda_{e2} \cdot |((V_{e21}^* \cdot V_{21}) + (V_{e22}^* \cdot V_{22}))|^2}{P_{e1} \cdot |(\lambda_{e2} \cdot ((V_{e21}^* \cdot V_{11}) + (V_{e22}^* \cdot V_{12}))|^2 + P_N} \tag{2.37}$$

Capacity regarding the eavesdropper

Another parameter that we can also determine is the capacity of the eavesdropper to capture the signal. In order to find the capacity regarding the eavesdropper, we will use the same capacity formula as the target user, with one difference. At the eavesdropper side, it appears a lot of interferences comparing to the target user side where interferences are cancelled by using SVD. So to determine the capacity of the eavesdropper we need SNIR instead of SNR.

The formula of the capacity is [11]:

$$C(b/s/Hz) = \sum_{k=1}^{K} log_2(1 + SNIR_k) \tag{2.38}$$

With all these parameters lay down, we are going to study the processing part of the eavesdropper. Actually, the eavesdropper uses the SVD to decode the capture signal. We wonder how the eavesdropper can enhance its ability to decode the captured signal. That will be our study in the next section.

Combining techniques for eavesdroppers

In this part, we are going to study different combining techniques that the eavesdropper can use to decode the signal instead of using the processing U_e^H (see Figure 2.4)

Diversity combining is the technique applied to combine multiple received signals of a diversity reception device into a single improved signal. Also another aspect of the diversity combining technique is to get the maximum benefit of a combined signal. The criteria employed to measure the benefit are expressed in terms of SNR [13].

If you consider f_1 and f_2 as two received signals, they are respectively constituted by a desired message component s_1, s_2 and an undesired additive noise component n_1, n_2. Then the composite signal is:

$$f(t) = f_1 + f_2 = (s_1 + s_2) + (n_1 + n_2) \tag{2.39}$$

i.e., in the form of a resultant message component $(s_1 + s_2)$ plus a resultant noise component $(n_1 + n_2)$. The summed signal (2.39) may then be a better signal than either f_1 or

f_2 alone; in particular, $f(t)$ may have a higher local SNR with $\frac{|s_1+s_2|^2}{|n_1+n_2|^2}$ than either f_1 or f_2 separated. [13]

More generally [13],

$$f(t) = \sum_{j=1}^{N} a_j \cdot f_j(t) \tag{2.40}$$

in which each f_j is weighted by a combining coefficient a_j, which is proportional to the channel gain.

It exists various diversity combining techniques which can be used. All these techniques can replace the initial SVD applied by the eavesdropper. The goal of this study is to observe the influence of a combining technique at the eavesdropper side.

Below are the various diversity combining techniques which can be distinguished [13]:

- Selection Combining (SC)
- Maximal Ratio Combining (MRC)
- Equal Gain Combining (EGC)
- Optimum Combining OC

a) Selective Combining (SC)

This SC technique is one of the simplest technique. None of the CSI is required. Here the Rx simply looks at the outputs and selects the one with the highest SNR. Thus, the strongest signal is favored, so signals that have undergone deep fades are unlikely to be picked by the Rx.

The design criterion here is that, at any given time, the system simply picks up the best of all the noisy signals f_1,f_2,...,f_N, and uses that one alone; the others do not then contribute to f(t). More precisely, let k denotes the index of a channel for which $SNR_k \geq SNR_j$, j=1,2,...,N; then this type of system is characterized by the design criterion

$$a_j = \begin{cases} 1, & forj = k \\ 0 & forj \neq k \end{cases} \tag{2.41}$$

This is essentially the classical form of diversity communication. SC has the lowest performance and the least complexity [13]

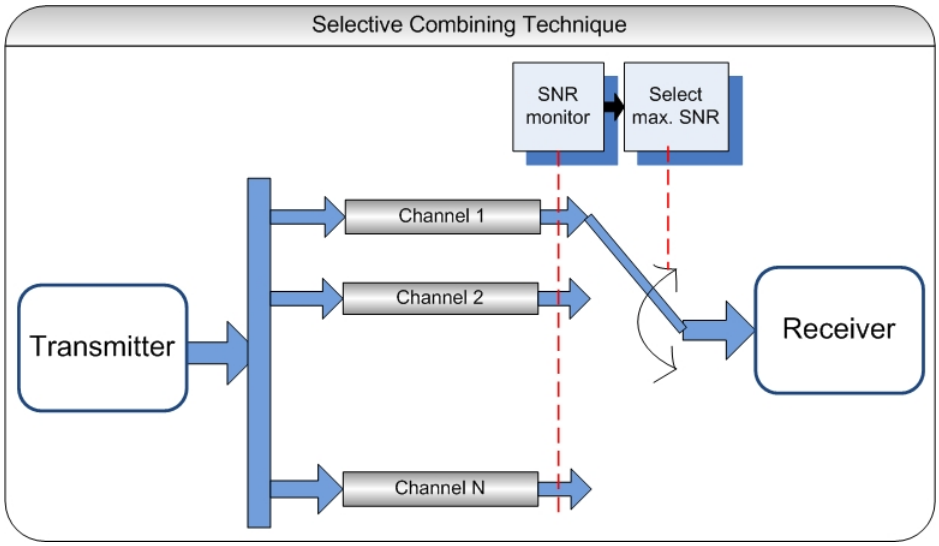

Figure 2.9: Selective Combining

b) Maximal Ratio Combining MRC [14]

In this technique, all the received signals are weighted proportionately to their individual SNIRs and then summed. The individual signals must be co-phased before combining if it takes place before demodulation. Branches with strong signal are further amplified, while weak signals are attenuated.

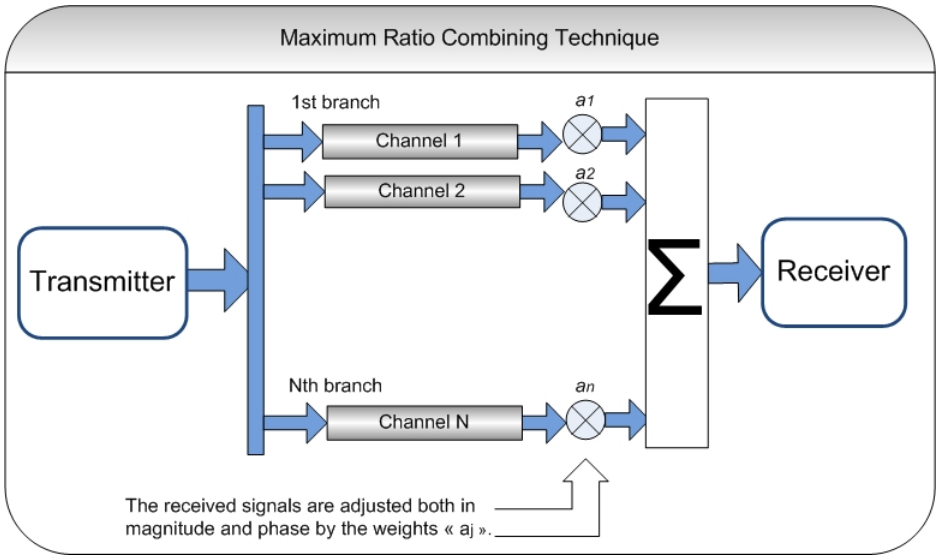

Figure 2.10: Maximum Ratio combining

In this technique, the received signals are adjusted both in magnitude and phase by the weights in the combining filter to maximise the SNR at the output of the combiner. The weighting applied to each diversity branch is adjusted independently from other

branches according to the SNR at that branch. The received signal at the k^{th} branch, y_k, and the output of the MRC combiner, f(t), are given by

$$f(t) = \sum_{j=1}^{N} a_j \cdot f_j(t) \tag{2.42}$$

$$f_j(t) = h_j \cdot x(t) + n \tag{2.43}$$

$$a_j = \frac{h_j^*}{\sigma_N^2} \tag{2.44}$$

Where $(.)^*$ represents the conjugate. The transmitted signal, x is corrupted by the channel effects characterised by h_j ,while a_j is the associated weight of the k^{th} antenna element [14].

c) Equal Gain Combining EGC

This linear diversity technique is characterized by the property that all channels have exactly the same gain [13].

$$a_j = 1, j = 1, \ldots, N \tag{2.45}$$

i.e. the noisy signals are simply added together.

$$f(t) = \sum_{j=1}^{N} f_j(t) \tag{2.46}$$

d) Optimum combining

This technique is the same that the MRC combining technique but in this case, the processing can see the difference between 2 signals in "x". Thus, for example, if we received $y_{e1} = a \cdot x_1 + b \cdot x_2 + n$ then the optimum combining will sense "a" as the desired message, "b" as the self interference and "n" the noise.

2.3 Second scenario: The transmitter knows about the eavesdroppers channel

In this section, the scenario is based on the same background than in the previous one but here the access point is aware of the eavesdropper. So the objective for the Tx is to prevent

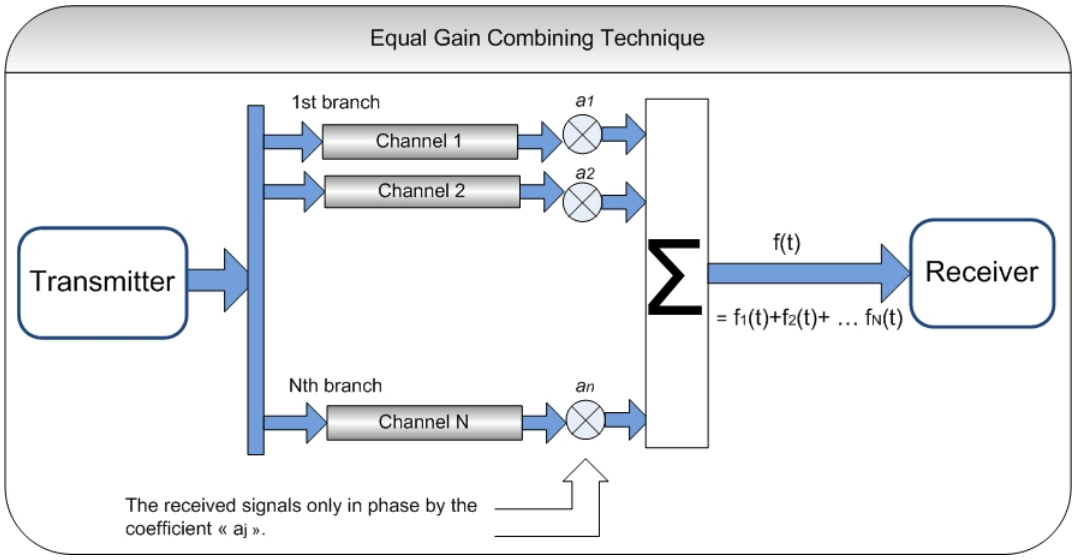

Figure 2.11: Equal Gain combining

the eavesdropper to capture the signal. To achieve that, the Tx can modify some parameters to make the transmission more difficult to catch for the eavesdropper.

2.3.1 Combatting eavesdroppers using singular vectors of the transmitter

The first idea to prevent an eavesdropper to capture your message is to change your transmission parameters. Then, if we change dynamically what is inside the matrix V (see Figure 2.4 the eavesdropper will have a lot of difficulties to catch the signal. On the other hand, the target user will have a lot of difficulties since the orthogonality between the target user and the access point won't be satisfied and a lot of interferences could not be erased in the target user processing. Consequently, we can not modify the matrix **V** which contains the right singular vectors of **H**. Otherwise, we have another alternative against the eavesdropper: we can try to deteriorate its signal by playing on the power allocation.

2.3.2 Combatting eavesdroppers using the inter datastreams SNIR

In order to keep confidentiality against eavesdroppers, we define a strategy to follow in a question form. Our objective is to secure our multiple antenna system on the confidentiality aspect, but also to keep it efficient enough regarding the capacity of the target user. Our strategy is as follow:

- If the SNIR at the eavesdropper side is minimize to 0dB, what is then the maximum

value that the capacity can reach at the target user side?

To clarify this, we focus at the eavesdropper side, to analyze each data stream power comparing to the others.
The figure below is an example with two subchannels.

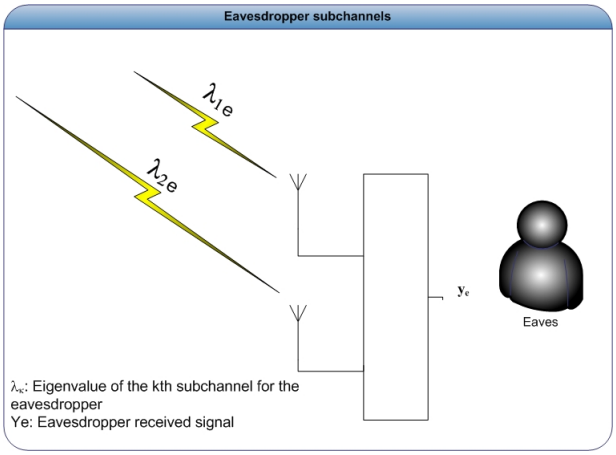

Figure 2.12: Eavesdropper SIR (2 data streams example)

As can be seen in the Figure 2.12, we have two data streams. The SIR (explained just before this figure) among these two subchannels is used to prevent the eavesdropper to intercept the signal at a good quality level.

Investigating The Signal to Interference Ratio(SNIR)

Having the capacity concerning the eavesdropper, it is interesting to see what is happening regarding the capacity when we force the SIR to 0dB, that is to say when

$$SNIR = \frac{P_S}{P_I + P_N} = 1 \tag{2.47}$$

New Power allocation: French Power Allocation

To get a SNIR equal to 0dB, the only possibility is to use a suitable new power allocation. Indeed, the weighting vectors (**V** and **U**) cannot be modified because the orthogonality of the system (SVD) must not be changed. In the following picture is described how we are going to deteriorate the eavesdropper's SNIR.

For this scenario we fix P_2, we apply the strategy in Figure 2.13 and we compare the capacity of the target user versus the SNIR of the eavesdropper with the same methodology than for the first scenario.

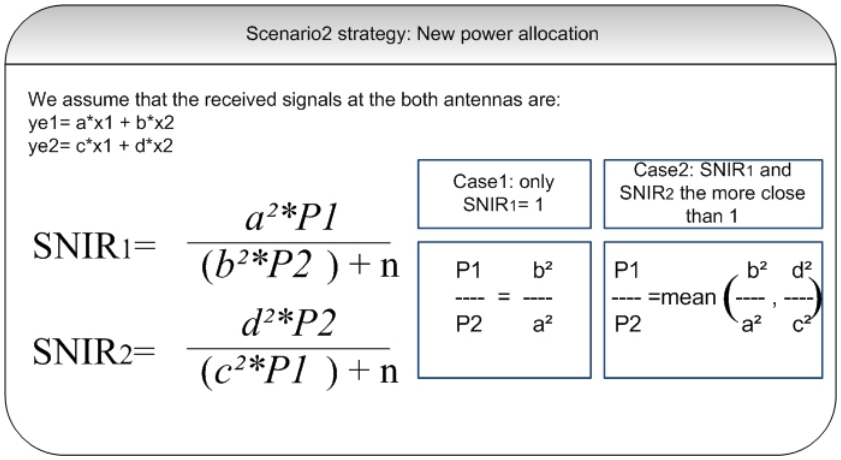

Figure 2.13: Scenario2 strategy: New power allocation

2.4 Chapter 2 Summary

In this chapter, we defined two different scenarios. First case where the tTx (Access Point) doesn't know about the eavesdropper, and the second case, where the Access Point detected the eavesdropper.

2.4.1 The transmitter and the target user

In this scenario, we are going to observe the capacity of the MIMO system based on the spatial multiplexing concept. We will change the value of some parameters to compare the results obtained.

1. We start with a 2x2 MIMO system
2. Power allocation scheme (Waterfilling or Uniform)

2.4.2 The transmitter, the target user and several eavesdroppers

Here, we added some eavesdroppers who want to catch the transmitted signal. Now, our interests are still the capacity for the target but also the SIR among the data streams of the eavesdroppers.
We will change the same parameters than for the first scenario.

1. We start with a 2x2 MIMO system
2. Power allocation scheme (Waterfilling or Uniform)

However we will need also to appreciate the behavior of the SIR and the Capacity when:

1. We change the distance between the eavesdropper and the target user

Moreover, we would like to get a comparative figure between the capacity and the SNIR, to appreciate both of their behavior.

2.4.3 Processing

We decided to change the processing at the eavesdropper side to find out the importance of the processing on the eavesdropper and also to figure out on the ability of our system to be robust and secure against any type of eavesdropper.

2.4.4 Deteriorate the signal received by the eavesdropper

In this second scenario, we want to deteriorate the signal that the eavesdropper is going to catch. So to do that we are going to change some parameters which can be:

- **New distribution of the power** from the access point

Chapter 3

Implementation

With the theoretical background of this project laid down in the previous chapter, we will now present the simulated system models. The primary focus of this work is to determine the ability of an eavesdropper to capture the transmitted signal. In this Chapter we will first describe the different system model we used for our simulation, followed by detailing out the different scenarios under investigation.

3.1 System model: The 802.11n Channel Model

The first channel model that has been investigated is the 802.11n channel model, also called World-Wide Spectrum Efficiency (WWiSE) or TGn Sync. This model is very related to this project, due to the fact that this standard is also specialized in MIMO system. This standard is a very recent one, and the publication is currently expected in September 2008.

We started to go through the 802.11n channel model simulated in matlab "MATLAB implementation of the Indoor MIMO WLAN channel model proposed by the IEEE 802.11 TGn Channel Model Special Committe". We went through the documents related to the matlab simulation, explaining the different environments, the functions, and how to use it.

In the appendix section we describe more deeply the 802.11n Channel model in Matlab, and what we learned from this model. Unfortunately, after studying deeply this system we realized that the 802.11n channel model could not be used for our project.

3.1.1 Why not the 802.11n channel model

We gathered here the reasons why we did not use it for our simulations.

- The numerous functions

  The 802.11n channel model Matlab program is a very complicated channel model and is containing several different environments(A to F). This channel model is taking into account many details using many functions, which all may not be interesting for our case. We tried to minimize this program in order to get only the functions that we wanted to use. However this model is a very complicated program and all the functions are not so easy to remove without affecting the others. Finally we oriented our choice by an easier and more suitable channel model "The double scattering model".

3.2 System model: Double Scattering Environment

After the first system model, we decided to use a second one which has been used for the paper "The Medium is The Message Secure Communication via Waveform Coding in MIMO Systems" [10]. We get this system model thanks to Xin Zhou who was involved in this paper. The idea was to recode some function by ourselves to appropriate the code. Thus, we redone the function dedicated to position the different eavesdroppers from the target user and the function dedicated to generate the channel matrix.

In this part we are going to describe the system model that we used for our simulation. The simulation model includes a narrowband system with one target user and several eavesdroppers. At the starting point, a 2x2 system is assumed in a narrowband environment with double scatter rings of 20m of radius around the transmitter and the target user(receiver). The radio channel is simulated using a double bounce flat-fading Rayleigh model, with 100 scatterers on each scatter ring. The separation between Tx and Rx is 30m. The center frequency(f_c) is 5GHz so the wavelength is $\lambda = 6cm$. (See Figure 3.1)

The Tx and the Rx are assumed Uniform Linear Arrays with Antenna element spacing $d_{Tx} = d_{Rx} = \lambda/2$. 4 Tx elements are static and the 4 Rx elements move along X tracks perpendicular to the antenna array, with a movement step of $\lambda/2$. The spacing between different tracks is 0.4λ. (See Figure 3.2)

As can be seen in Figure (3.2), in the right part of the target user, several eavesdroppers, set up with 2 receiver elements, are placed in order to catch the signal received by the target user. We consider all users to the right of the target user as eavesdroppers following the same track rule than the target user. On the other hand, the distance between

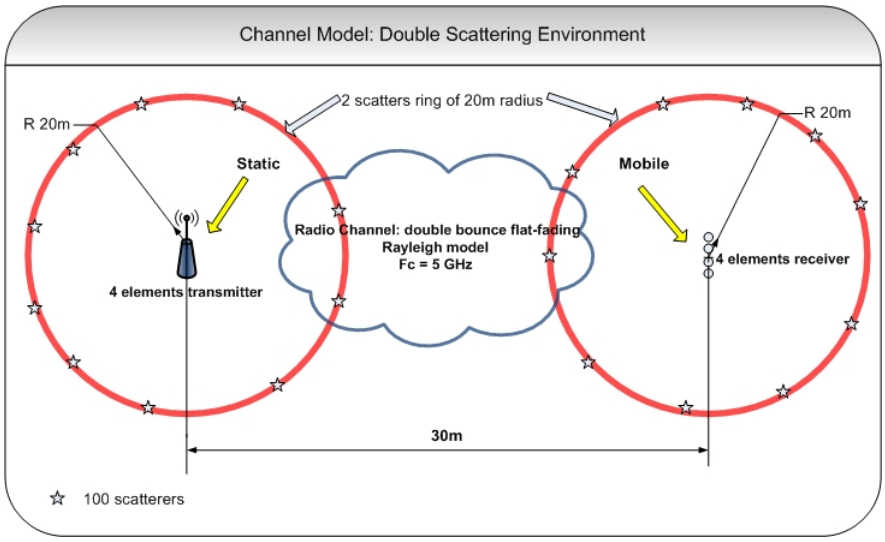

Figure 3.1: Channel Model Double Scattering

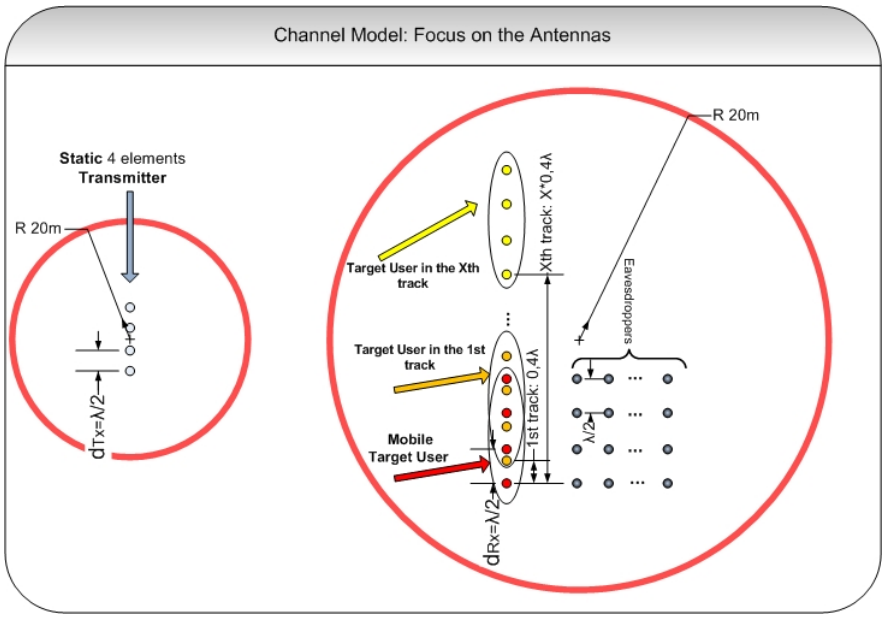

Figure 3.2: Channel Model Focus on the antennas in a 4x4 system

eavesdroppers and the target user is set according to the following distance:

$$D = \frac{\lambda}{100}, \frac{\lambda}{10}, \frac{\lambda}{2} \tag{3.1}$$

All of these distances start from the target user and are more or less near the target user in order to compare the efficiency of the eavesdropper to catch a good signal.(see Figure (3.3))

The system model takes into account that the scatters are located in the far-field, which guarantees the angular field distribution being essentially independent of distance from

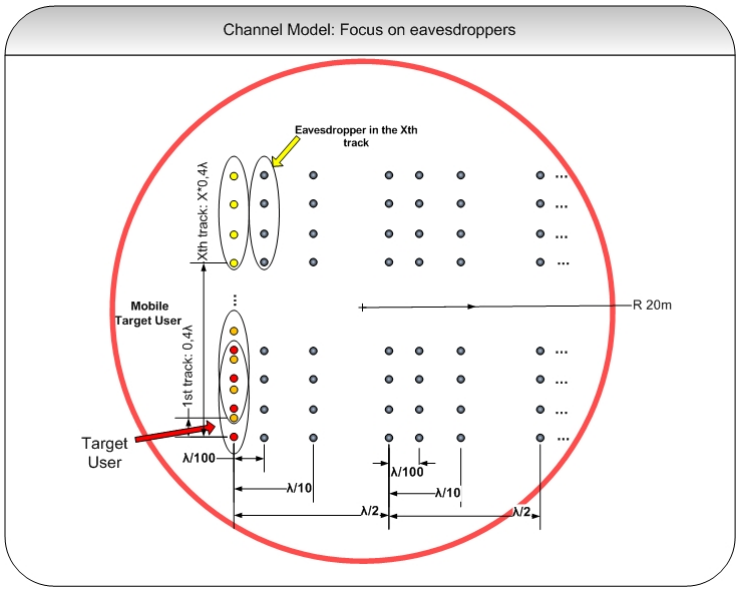

Figure 3.3: Channel Model Double focus on eavesdroppers

the antennas. [15].The far-field region can be calculated by $\frac{2(D_A)^2}{\lambda}$, where D_A is the antenna dimension and λ is the wavelength. [16]

In this model, 100 scatterers are randomly distributed on each scatter ring (see figure 3.4). The propagation path is a two-bounce transmission mode, where LOS does not exist in this preliminary assumption.Figure (3.4) is showing the environment assumption with 4 paths as an instance.

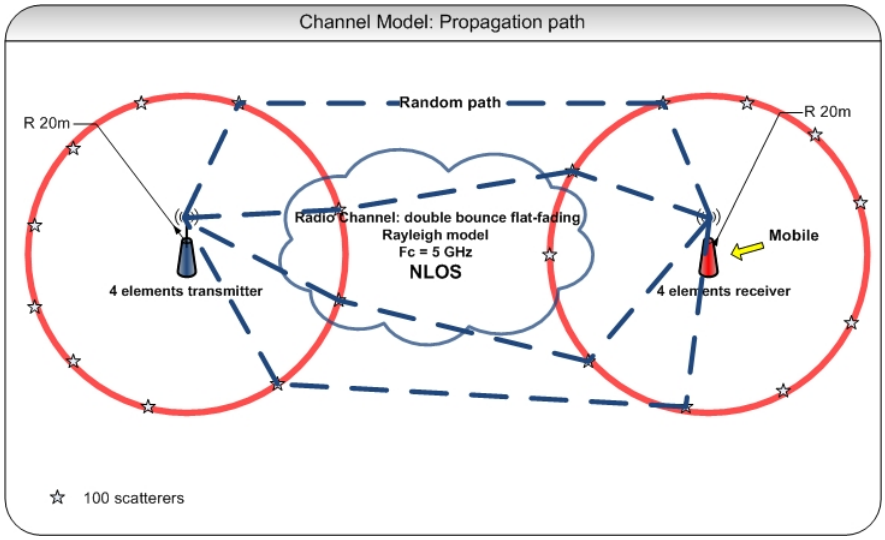

Figure 3.4: Channel Model Propagation path

3.2.1 Parameter Configuration

In the simulation experiment, the carrier frequency f_c is set to 5GHz. Therefore, the wavelength λ is equal to

$$\frac{c}{f_c} = \frac{(3.10)^8}{(5.10)^9} = 0.06m \tag{3.2}$$

Where *c* denotes the light speed. The other parameters are listed in Table below

Simulations Parameters	
Carrier Frequency (f_c)	5GHz
Wavelength (λ)	0.06m
Number of Tx antenna (N_{TX})	2
Number of RX antenna (N_{RX})	2
Number of Scatterers on Each Scatter Ring (Ns)	100
Number of paths	800
Distance between transmitter antennas(d_{Tx})	$\frac{\lambda}{2}$
Distance between receiver antennas (d_{Rx})	$\frac{\lambda}{2}$
Number of Rx movements in the row	10
Number of Rx tracks in the column	500
SNR_{pre}	6,10,30 dB
Transmitted Power (P_t)	1 dB
Number of Eavesdroppers	59
Number of target user	1

The matlab plot below figure3.5 shows the representation of the double scattering model.

3.2.2 Summary of the assumptions of the simulation model

1. Only NLOS paths are considered
2. Respect the Rayleigh rule of thumb
3. Transmitter is static
4. Receivers (Target user and eavesdroppers) are moving
5. Receivers do not cross the circle of scatterers

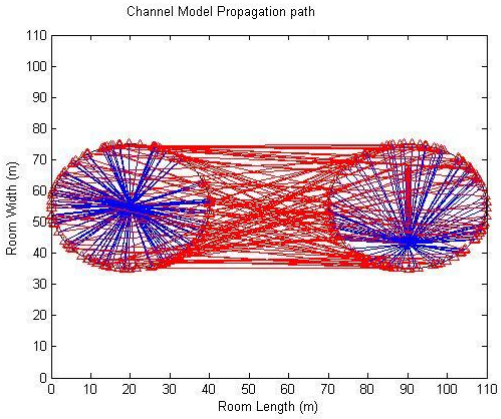

Figure 3.5: Plot of the Channel Model Propagation path

6. 100 scatterers on the circles

7. Noise is set using SNR pre-detection 6,10,30 dB

8. The channel matrix obtained by the channel model has been normalized

3.2.3 Verification of the model

Our simulation model considers only NLOS paths, hence we are going to check whether this model is rayleigh or not. We need to show that there is no correlation among the paths, due to the fact that we are in spatial multiplexing. To conclude this verification of the model, we will show the space coherence function.

Rayleigh Model

In this part, we are investigating the different links (h_{11}, h_{12}, h_{21}, h_{22}). We are trying to find out if the channel link respects the Rayleigh distribution in a two by two case. As can be seen on each plot, it follows the Rayleigh rule of thumb, that is at 1% signal level, the power is -20dB. You can find these plots in the appendix section.

Correlation coefficients

As long as we are in spatial multiplexing, we need uncorrelated links, that is the reason why we verified the complex correlation coefficients between all the links.

Correlation coefficients				
	h_{11}	h_{12}	h_{21}	h_{22}
h_{11}	1	0.0392	0.067	0.0037
h_{12}	0.0392	1	0.0922	0.2277
h_{21}	0.067	0.0922	1	0.0938
h_{22}	0.0037	0.2277	0.0938	1

Spatial coherence function of the model

The Space Coherence Function (SCF) is used to manifest the normalized distance autocorrelation function. It expresses the distance along which the channel holds the similarity [17].

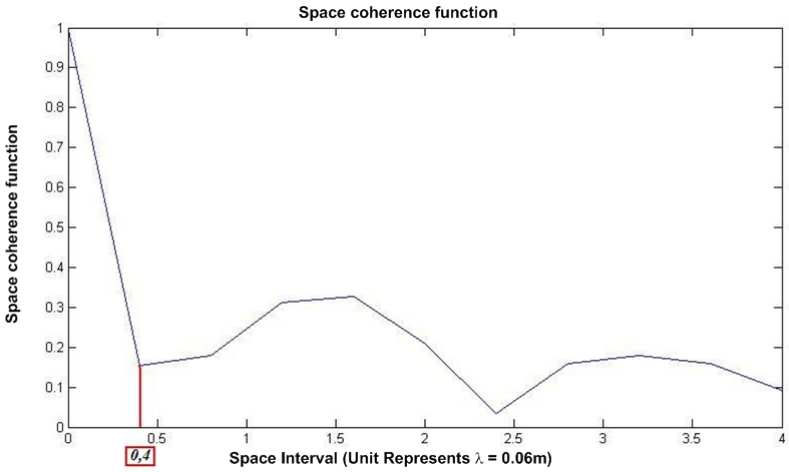

Figure 3.6: Space coherence function

Eigenvalue distribution

In this part, we are going to deal with the eigenvalue distribution. This figure will help us to be sure that our system is well set up.

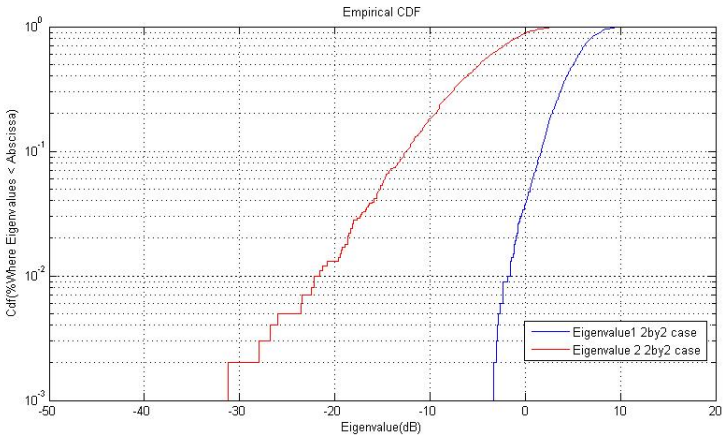

Figure 3.7: Eigenvalues distribution $2 \times 2 case$

In the Figure 3.7 just above, the 50% level indicates a difference of 10dB between these 2 eigenvalues.To make sure that our distribution gives a good response, we compare our difference to the Jakes' model [17], which gather all standard distributions we need. Thus, by checking in this book, we have the confirmation that our figure are what we expected with respect to [17].

The next figure is the eigenvalue distribution for a 4x4 case.

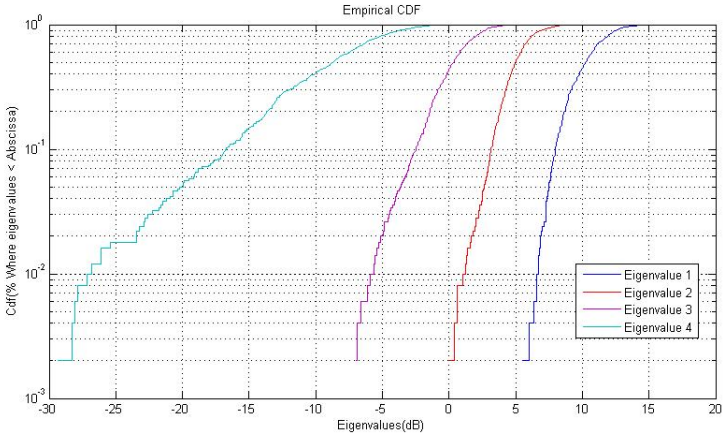

Figure 3.8: Eigenvalues distribution $4 \times 4 case$

We can notice in the Figure 3.8 that the two first eigenvalue are close from each other comparing to the 2x2 case. It is what we should expected for with respect to [17]

3.3 The different scenarios

We defined two main scenarios. The first one is dedicated to observe the behavior of the eavesdropper SNIR. We actually study the performance of the system when the eavesdropper is trying to catch the message. Thus, we compare the capacity of the target user versus the SNIR of the eavesdropper before the processing in the first time and we try, in the second time, different processing to observe the response of the system model.
For the second scenario, we are going to do the same procedure than for the first one except that we will try to force the signal caught by the eavesdropper to be very bad.

3.3.1 Scenario1: Observation Scenario / Blind transmission

In this observation scenario, the Tx (access point) is not able to detect the presence of any eavesdroppers around him. Thus the term "Blind transmission" means that the transmitter is able to see the target user only. It is totaly blind with all the elements around him, hence the access point is not able to have any influence on the eavesdroppers transmission.

Post processing part

In this sub-scenario, what me mean by "post processing" is that we are taking into account the $\mathbf{U}^H$ in the received signal equation.

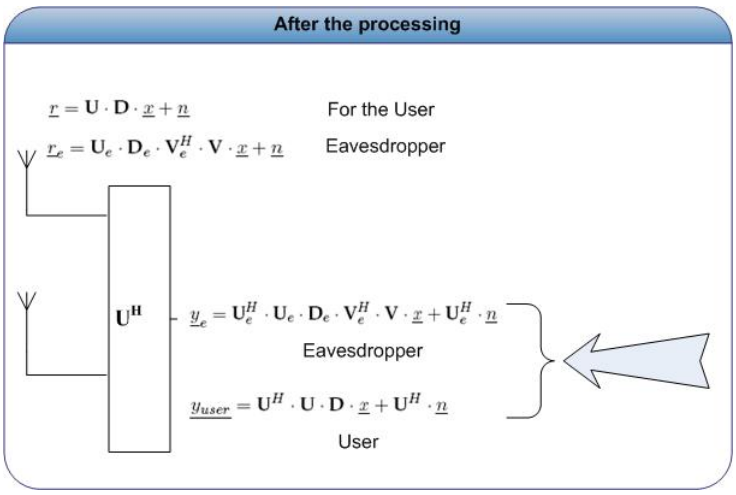

Figure 3.9: Equations to use after the processing

For this sub-scenario, we want to examine different behaviors of our system in changing different parameters.

- Study of the **capacity** of the *target user* using different **power allocation schemes**

  The first behavior to observe is the capacity of the target user regarding the two different power allocations (Uniform power allocation scheme and the Waterfilling power allocation scheme). Figure 3.10 shows the detailed steps to calculate. The goal of this study is to illuminate how important is the influence of the power allocation in our system.

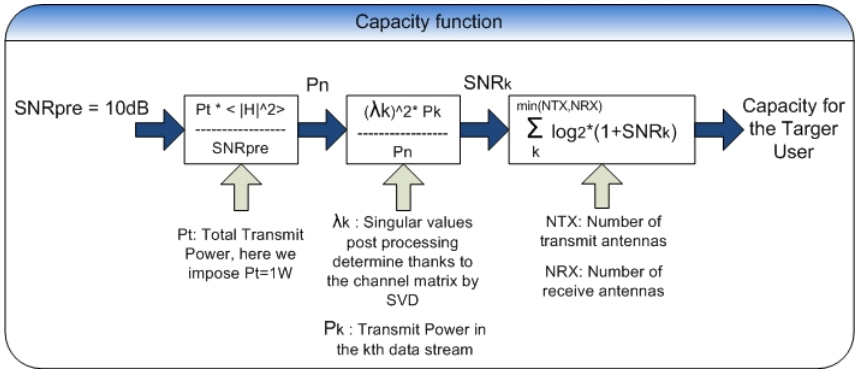

Figure 3.10: Capacity function

- Study of the **SNR** of the *target user* regarding the **SNIR** of the *eavesdroppers*
  The two different SNR (one for each received antennas in the 2x2 system)of the target user is another interesting behavior to study, regarding the different SNIR of most of the eavesdroppers (the closest and the farthest from the target user).
  Moreover for a deeper study, we will apply the two different power allocation schemes.

Pre processing part

Actually we want to explore which kind of signal we can get and above all what kind of SNIR it will give for the eavesdropper.

Here, we want to examine different behaviors of our system in changing different parameters at the eavesdropper side.

- Study of the SNIR of the eavesdroppers without any processing
  Looking at the SNIR of the eavesdropper before any processing, comparing the SNR of the target user may be interesting. The goal of this study is to find out the influence of the processing for the eavesdroppers to catch the signal between the access point and the target user.

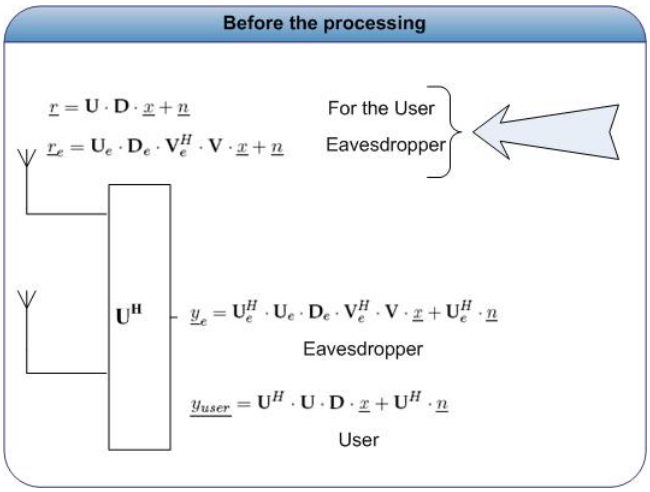

Figure 3.11: Equations to use before the processing

We will appreciate our results using the two different power allocations (Uniform and the Waterfilling scheme).

Processing part

The processing scenario is interesting from the eavesdropper but also for the system model. We want to explore which techniques would appear to be the most suitable to get the best SNIR for the eavesdropper. In order to do that, we just remove the processing (U_e^H) and we try to replace that processing by different combining techniques at the eavesdroppers side.

- SVD eavesdropper side
  No change is apply in the processing comparing to the first scenario.
- Combining techniques
  Instead of getting into the U_e^H processing, we will apply the three different combining techniques.
  1. EGC (see Figure 3.12)
  2. MRC (see Figure 3.13)

3.3.2 Scenario 2: The transmitter knows about the eavesdropper

In this scenario, the Tx (access point) is able to detect the presence of any eavesdropper around it. Thus the access point can have an influence on the eavesdropper transmission

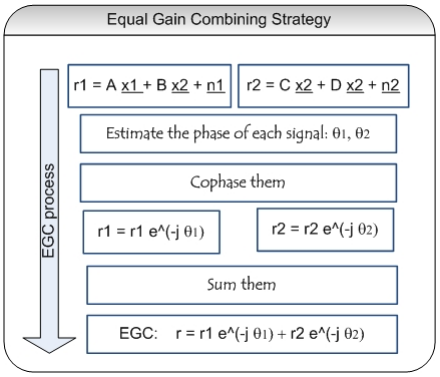

Figure 3.12: Equal Gain Combining Strategy

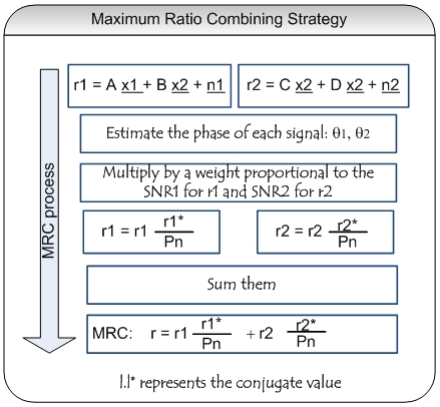

Figure 3.13: Maximum Ratio Combining Strategy

by changing the power allocation. By the equation (2.35), we can see the power transmitted to the eavesdropper plays an important role in the SNIR calculation.
The interesting point here is that if SNIR is approximatively equal to 1(=0 dB), it means that the power of the received signal is almost equal to the power of the interference received by the eavesdropper. In this manner, it would be very difficult for the eavesdropper to capture the transmitted message.
Regarding to this point, we plan to apply the strategy displayed in Figure 2.13 to deteriorate to the maximum of the SNIR at the eavesdropper

- The objective here is to get a trade off between the capacity of the target user and the SNIR of the eavesdropper.

Therefore, for the scenario 2 we are going to apply the same procedure than the first one (Capacity versus SNIR) but taking into account that the power allocation will be set up in order to deteriorate the signal received by the eavesdropper.

3.4 Chapter 3 Summary

In this chapter, we explained why we stopped to use the system model 802.11n.
We introduce another system model: the double scattering environment [10].
We finally described how we intended to implement the two scenarios saw in the previous chapter.

In the next chapter are presented all the results and analysis we got from our simulation.

Chapter 4

Results

This chapter is dedicated to the results of our Matlab simulation. We are going to present all the results of the different scenarios. The results will be presented for each scenario regarding the SNIR of the eavesdropper and the capacity or the SNR of the target User at the same time. Before the practical results, an theoretical analysis will presented in order to inform the reader about the expected practical results.

The table below, is a brief reminder of the different parameters that we changed during the simulations of all the scenarios.

Simulation parameters		
	Scenario 1	Scenario 2
Power allocation	Waterfilling / Uniform	New power allocation
$SNR_{predetection}$	$30dB/6dB$	$30dB/6dB$

Figure 4.1: Simulations parameters table

It is important to know, before going through the analysis of the results, that the level of the SNR_{pre} tells about the noise power level. In case of high SNR_{pre}(30dB), we almost have any noise power. However in case of low SNR_{pre}(6dB), we need to take into account the noise power.

The table **??** gathers all the informations concerning the eavesdroppers that we are using during the simulations.

Below is a brief summary of the different processing used by the eavesdroppers:

Eavesdroppers locations	
	Distance from the target user (λ)
Eavesdropper 1	$\frac{\lambda}{100}$
Eavesdropper 2	$\frac{\lambda}{10}$
Eavesdropper 12	$2 \cdot \lambda$

Figure 4.2: Eavesdroppers locations table

1. **Preprocessing**

   The eavesdroppers will not apply any processing to the received signals. It is the case for the eavesdroppers with only the antennas.

2. **SVD**

   This is the processing used by the target user to remove the interferences. However the eavesdroppers will have interferences using this processing.

3. **EGC**

   First combining technique, which cophases the signals, and adds them together, without being able to distinguish x_1 from x_2.

4. **MRC**

   Second combining technique, is to cophase, to multiply signals by a gain which has to be proportional to their SNIR, and sum the signals at the eavesdropper side. In this algorithm, the eavesdropper using MRC is not able to distinguish the two information signals (x1 and x2).

5. **OC! (OC!)**

   Third and last combining technique, is following the same algorithm than the MRC technique. The difference relies on the ability of the eavesdropper to distinguish the two information signals (x1 and x2).

4.1 Theoretical analysis

4.1.1 Preprocessing theoretical analysis

This analysis has been achieved using this different parameters, gathered in the table below:

Theoretical analyze parameters	
	Parameters
Power allocation	Uniform
SNR_{pre}	$30dB$

From this question (2.10) we can choose to work before the processing $\mathbf{U}^H$ of the target user in order to get the received signal just after the receiver antennas.

$$\underline{r} = \mathbf{U} \cdot \mathbf{D} \cdot \underline{x} + \underline{n} \tag{4.1}$$

$$\begin{aligned} \underline{r} = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} &= \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix} \cdot \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \\ &= \begin{pmatrix} U_{11} \cdot \lambda_1 & U_{12} \cdot \lambda_2 \\ U_{21} \cdot \lambda_1 & U_{22} \cdot \lambda_2 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \end{aligned} \tag{4.2}$$

$$r_1 = \lambda_1 \cdot U_{11} \cdot x_1 + \lambda_2 \cdot U_{12} \cdot x_2 + n_1 \tag{4.3}$$

$$r_2 = \lambda_1 \cdot U_{21} \cdot x_1 + \lambda_2 \cdot U_{22} \cdot x_2 + n_2 \tag{4.4}$$

SNIR1.1 (x1 is the intended signal , and x2 is taking as interference) is calculated using the term related to x1 ($\lambda_1 \cdot U_{21}$) over the term related to x2($\lambda_2 \cdot U_{12}$).

$$SNIR1.1 = \frac{|\lambda_1 \cdot U_{11}|^2 \cdot P_1}{|\lambda_2 \cdot U_{12}|^2 \cdot P_2 + Pn} \tag{4.5}$$

- High SNR_{pre}

  In high SNR_{pre} ($= 30dB$), we have almost no noise (then we assume $P_N = 0$).

- Equal power allocation

  In equal power allocation, $P_1 = P_2 = \frac{Pt}{2}$

then we have,

$$SNIR1.1 = \frac{|\lambda_1 \cdot U_{11}|^2}{|\lambda_2 \cdot U_{12}|^2} \tag{4.6}$$

We looked at the values of the ratio $\frac{|U_{11}|^2}{|U_{12}|^2}$ and it gives at median level (50%), a value equal to 1.(Please see Figure 4.3)

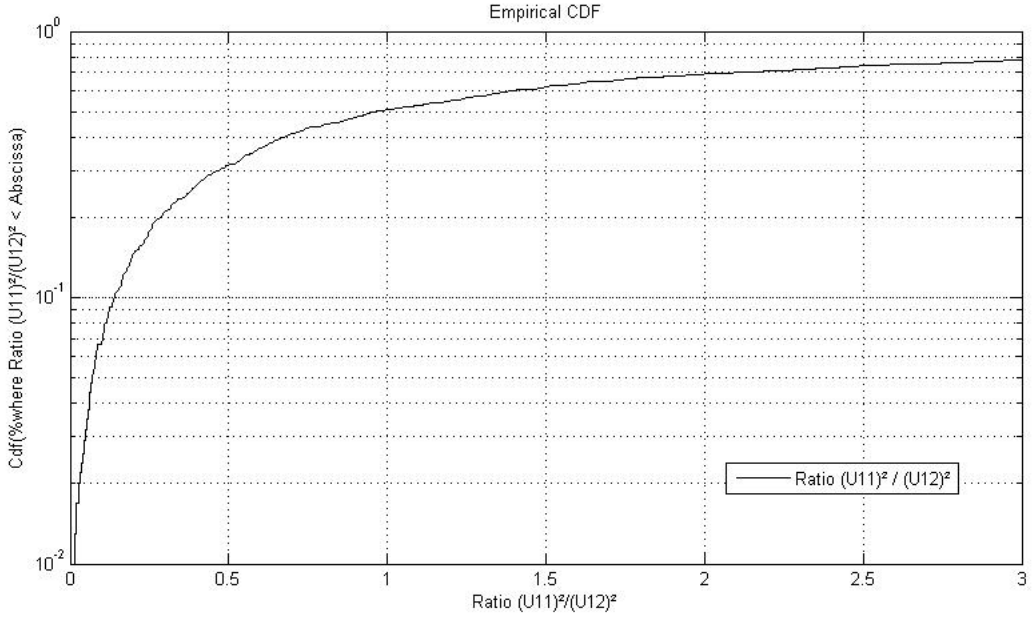

Figure 4.3: Cdf of the Ratio $\frac{|U_{11}|^2}{|U_{12}|^2}$ 2by2

then we have

$$SNIR1.1 = \frac{|\lambda_1|^2}{|\lambda_2|^2} \tag{4.7}$$

Using the same steps, SNIR2 is equal to,

$$SNIR2.2 = \frac{|\lambda_2|^2}{|\lambda_1|^2} \tag{4.8}$$

We looked at the values of the ratio $\frac{|\lambda_1|^2}{|\lambda_2|^2}$ and it gives at median level (50%), a value equal to 12,5 Which represents $(10,96dB)$.

We looked at the values of the ratio $\frac{|\lambda_2|^2}{|\lambda_1|^2}$ and it gives at median level (50%), a value equal to 0.08 Which represents $(-10,95dB)$.

When we look at the difference between the Eigenvalues from Jakes book, we have 10dB difference.

$$(|\lambda_1|^2)_{dB} - (|\lambda_2|^2)_{dB} = (10)_{dB} \tag{4.9}$$

which is equal to this equation,

$$10 \cdot \log_{10} \frac{|\lambda_1|^2}{|\lambda_2|^2} = 10 \cdot \log_{10} 10 \tag{4.10}$$

Then we need

$$\frac{|\lambda_1|^2}{|\lambda_2|^2} = 10 \tag{4.11}$$

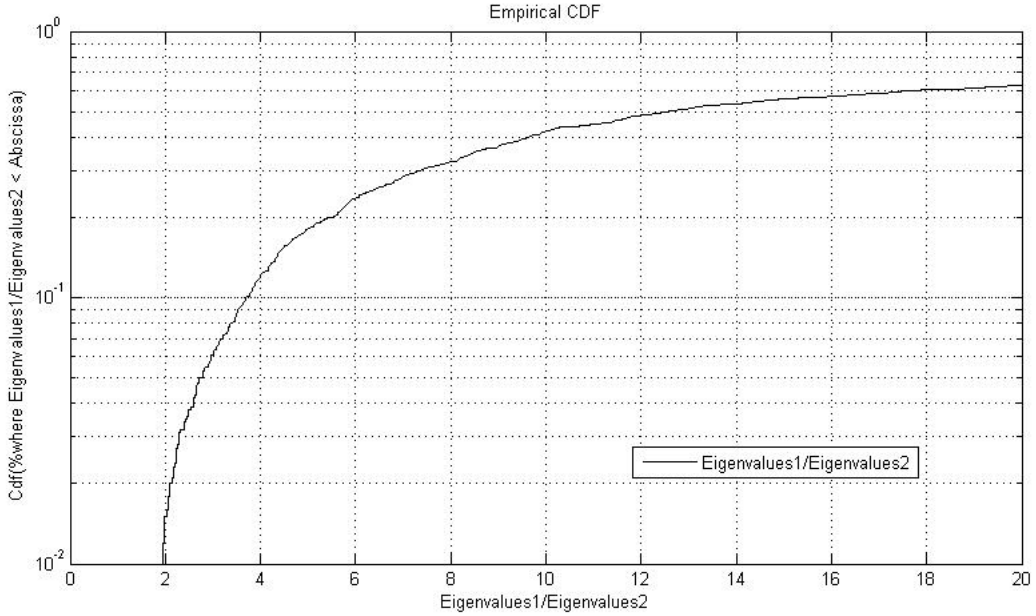

Figure 4.4: Cdf of the Ratio $\frac{|\lambda_1|^2}{|\lambda_2|^2}$ 2by2

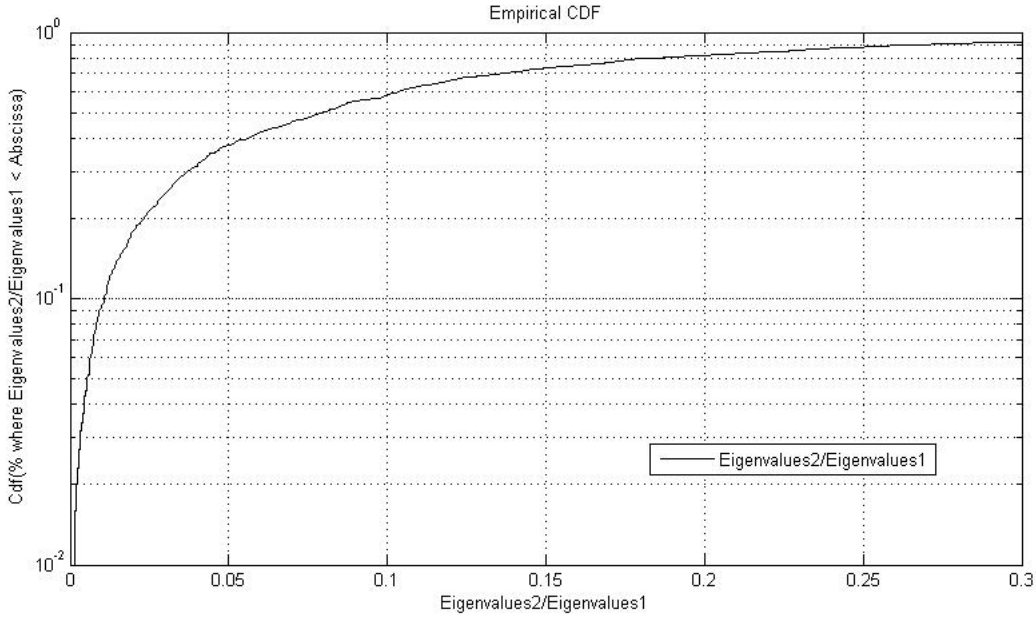

Figure 4.5: Cdf of the Ratio $\frac{|\lambda_2|^2}{|\lambda_1|^2}$ 2by2

This ratio gives 10 in dB from this equation, and we got 10,7 dB for this ratio in our simulation result.

Now we look at the contrary

$$(|\lambda_2|^2)_{dB} - (|\lambda_1|^2)_{dB} = -(10)_{dB} \tag{4.12}$$

which is equal to this equation,

$$10 \cdot \log_{10} \frac{|\lambda_2|^2}{|\lambda_1|^2} = 10 \cdot \log_{10} 0.1 \tag{4.13}$$

Then we need

$$\frac{|\lambda_2|^2}{|\lambda_1|^2} = 0.1 \tag{4.14}$$

This ratio gives -10 in dB from this equation, and we got -10,9 dB for this ratio in our SNIR simulation result.

Then from Jakes book, we have (10dB - (-10dB))20dB difference between the two SNIR in a 2by2 system. In our simulation results , we have (10,9dB- (-10,9))then 21dB of difference between the two SNIR.

As a conclusion, we verified our practical results regarding the theoretical result of SNIR preprocessing for the target user. We will be able to verify the rest of the results concerning the SNIR preprocessing, based on the target user SNIR preprocessing theoretical result.

4.1.2 Post Processing (SVD) theoretical analysis

We are going to study the value of the SNR of the target user at $SNR_{predetection} = 30dB$ with uniform power allocation. The value of the SNIR of the eavesdropper1 ($\frac{\lambda}{100}$, the closest from the target user) should be almost the same than the SNR of the target user. These are the two received signals by the target user (y_1 and y_2):

$$y_1 = \lambda_1 \cdot x_1 + n_1 \tag{4.15}$$

$$y_2 = \lambda_2 \cdot x_2 + n_2 \tag{4.16}$$

Then we calculate the SNR:

$$SNR_{1.1} = \frac{|\lambda_1|^2 \cdot P_1}{P_n} \tag{4.17}$$

with $P_n = 0.001W$, $P_1 = 0.5w$ and $|\lambda_1|^2$=3.1623 (At 50% level, which means 5dB, see Figure 3.7) then the value of $SNR_{1.1}$ should be 32dB at 50% level.

$$SNR_{2.2} = \frac{|\lambda_2|^2 \cdot P_2}{P_n} \tag{4.18}$$

with $P_n = 0.001W$, $P_2 = 0.5w$ and $|\lambda_2|^2$=0.3467 (At 50% level, which means -4.6 dB, see Figure 3.7) then the value of $SNR_{2.2}$ should be 22.38dB at 50% level.

If we look at the Figure 4.6, below, the values of the SNR that we obtained during the simulation are the same than the expected theoretical results.

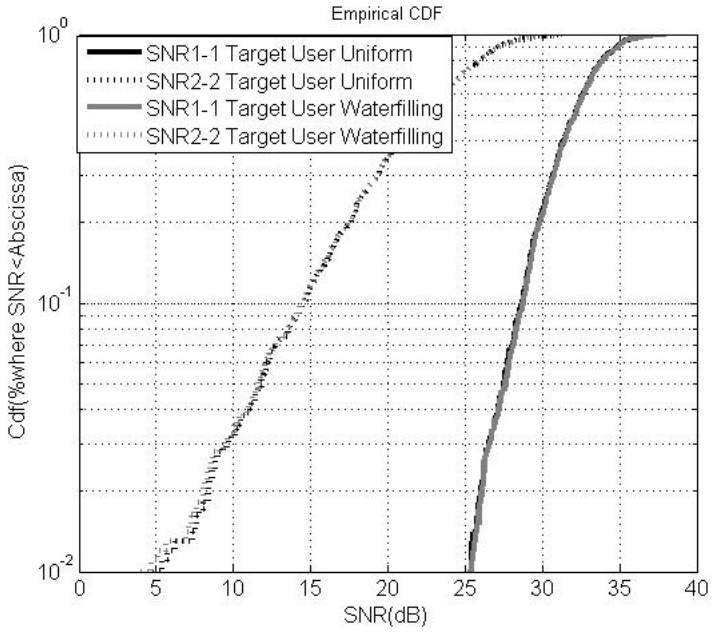

Figure 4.6: SNR postprocessing Target user SNRpre30dB 2by2

The theoretical analysis showed that our simulation results concerning the SNR target user are correct. Now, we are expecting the SNIR of the eavesdroppers almost similar than the SNR value of the target user, to verify our post processing SVD simulation results.

4.1.3 Post Processing (MRC) theoretical analysis

To get the following equations r_1 and r_2, please refer to the calculation which have been achieved in the appendix A.

$$r_1 = \lambda_1 \cdot U_{11} \cdot x_1 + \lambda_2 \cdot U_{12} \cdot x_2 + n_1 \tag{4.19}$$

$$r_2 = \lambda_1 \cdot U_{21} \cdot x_1 + \lambda_2 \cdot U_{22} \cdot x_2 + n_2 \tag{4.20}$$

After MRC processing, the new equations will be as follows:

$$y_1 = \frac{r_1 \cdot g_1}{P_N} \tag{4.21}$$

$$y_2 = \frac{r_2 \cdot g_2}{P_N} \tag{4.22}$$

with,

$$g_1 = (\lambda_1 \cdot U_{11} + \lambda_2 \cdot U_{12})^* = \lambda_1 \cdot U_{11}^* + \lambda_2 \cdot U_{12}^* \tag{4.23}$$

$$g_2 = (\lambda_1 \cdot U_{21} + \lambda_2 \cdot U_{22})^* = \lambda_1 \cdot U_{21}^* + \lambda_2 \cdot U_{22}^* \tag{4.24}$$

We developed y_1 and y_2,

$$y_1 = \frac{(\lambda_1 \cdot U_{11} \cdot x_1 + \lambda_2 \cdot U_{12} \cdot x_2 + n_1) \cdot (\lambda_1 \cdot U_{11}^* + \lambda_2 \cdot U_{12}^*)}{P_N} \tag{4.25}$$

$$y_1 = \frac{[|\lambda_1|^2 \cdot |U_{11}|^2 + \lambda_1 \cdot U_{11} \cdot \lambda_2 \cdot U_{12}^*] \cdot x_1 + [|\lambda_2|^2 \cdot |U_{12}|^2 + \lambda_1 \cdot U_{11}^* \cdot \lambda_2 \cdot U_{12}] \cdot x_2 + (\lambda_1 \cdot U_{11}^* + \lambda_2 \cdot U_{12}^*) \cdot n_1}{P_N} \tag{4.26}$$

$$y_2 = \frac{(\lambda_1 \cdot U_{21} \cdot x_1 + \lambda_2 \cdot U_{22} \cdot x_2 + n_2) \cdot (\lambda_1 \cdot U_{21}^* + \lambda_2 \cdot U_{22}^*)}{P_N} \tag{4.27}$$

$$y_2 = \frac{[|\lambda_1|^2 \cdot |U_{21}|^2 + \lambda_1 \cdot U_{21} \cdot \lambda_2 \cdot U_{22}^*] \cdot x_1 + [|\lambda_2|^2 \cdot |U_{22}|^2 + \lambda_1 \cdot U_{21}^* \cdot \lambda_2 \cdot U_{22}] \cdot x_2 + (\lambda_1 \cdot U_{21}^* + \lambda_2 \cdot U_{22}^*) \cdot n_2}{P_N} \tag{4.28}$$

U is a unitary matrix. So, $U_{11} \cdot U_{12}^* = U_{11}^* \cdot U_{12} = 0$

$$y_1 = \frac{|\lambda_1|^2 \cdot |U_{11}|^2 \cdot x_1 + |\lambda_2|^2 \cdot |U_{12}|^2 \cdot x_2 + (\lambda_1 \cdot U_{11}^* + \lambda_2 \cdot U_{12}^*) \cdot n_1}{P_N} \tag{4.29}$$

$$y_2 = \frac{|\lambda_1|^2 \cdot |U_{21}|^2 \cdot x_1 + |\lambda_2|^2 \cdot |U_{22}|^2 \cdot x_2 + (\lambda_1 \cdot U_{21}^* + \lambda_2 \cdot U_{22}^*) \cdot n_2}{P_N} \tag{4.30}$$

Now, we sum the two signals y_1 and y_2,

$$y_1 + y_2 = \frac{(|U_{11}|^2 + |U_{21}|^2) \cdot |\lambda_1|^2 \cdot x_1 + (|U_{12}|^2 + |U_{22}|^2) \cdot |\lambda_2|^2 \cdot x_2 + (\lambda_1 \cdot U_{11}^* + \lambda_2 \cdot U_{12}^*) \cdot n_1 + (\lambda_1 \cdot U_{21}^* + \lambda_2 \cdot U_{22}^*) \cdot n_2}{P_N} \tag{4.31}$$

U is a unitary matrix. So, $|U_{11}^2| + |U_{21}^2| = |U_{12}^2| + |U_{22}^2| = 1$

Finally,

$$y_1 + y_2 = \frac{|\lambda_1|^2 \cdot x_1 + |\lambda_2|^2 \cdot x_2 + (\lambda_1 \cdot U_{11}^* + \lambda_2 \cdot U_{12}^*) \cdot n_1 + (\lambda_1 \cdot U_{21}^* + \lambda_2 \cdot U_{22}^*) \cdot n_2}{P_N} \tag{4.32}$$

This is useful to calculate the SNIR1.1 (where x1 is the intended signal and x2 the interference)

However, since we are in uniform power allocation, the powers (P_1 and P_2 are equal) will cancel each other. Moreover, the $SNR_{pre} = 30dB$ tells us that the noise will be very small (quasi null), then we can remove the term "P_N".

Back to SNIR calculation

The SNIR equation is:

$$SNIR_{1.1} = \frac{(|\lambda_1|^2)^2}{(|\lambda_2|^2)^2} = \frac{|\lambda_1|^4}{|\lambda_2|^4} \tag{4.33}$$

We know that at mean value, the term $\frac{(|\lambda_1|^2)}{(|\lambda_2|^2)}$ is equal to 12,5 from our simulation results. Then the SNIR is equal to $(12.5)^2 = 150.25$

$$SNIR_{dB}1.1 = 10 * \log_{10} 150.25 = 21.7dB \tag{4.34}$$

Then using the MRC technique, we should expect a value of around 20dB at 50% level.

As can be seen on the figure below which concerns the target user and also the closest eavesdropper ($\frac{\lambda}{100}$)(They should have the same SNIR, due to their positions close from each other), we have a value of about 19dB at 50% level.

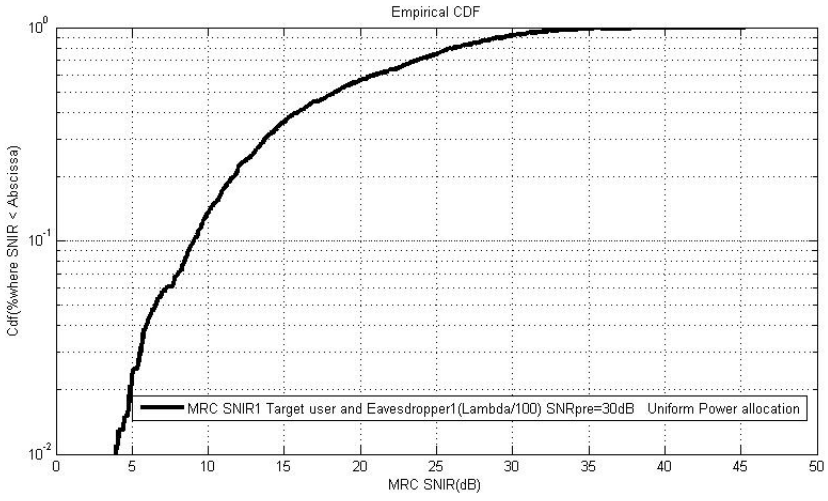

Figure 4.7: MRC SNIR1 SNRpre=30dB Uniform Power allocation

Finally, we can conclude that we got the expected theoretical result in our simulation concerning the MRC technique relative to the SNIR.

Let's move to the practical results and analysis of our simulations.

4.2 MATLAB simulation : First scenario

First of all, the capacities of the target user at $SNR_{pre} = 30dB$ and $6dB$ are presented. Then we focused on the different processing, showing the SNIR of the eavesdroppers(at different positions: Lambda/100,Lambda/10 and 2Lambda), (where any kind of processing are applied to the received signals,SVD, EGC,MRC).

4.2.1 Capacity of the target User

Below are the two Matlab plots of the capacity of the target user in Waterfilling and Uniform power allocation. They have been achieved at $SNR_{pre} = 6dB$ and $SNR_{pre} = 30dB$, which means respectively high and low noise power level.

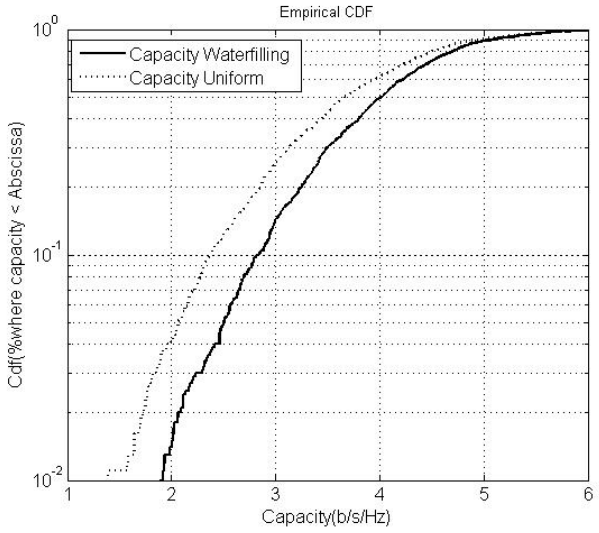

Figure 4.8: Capacity Target user SNR=6dB

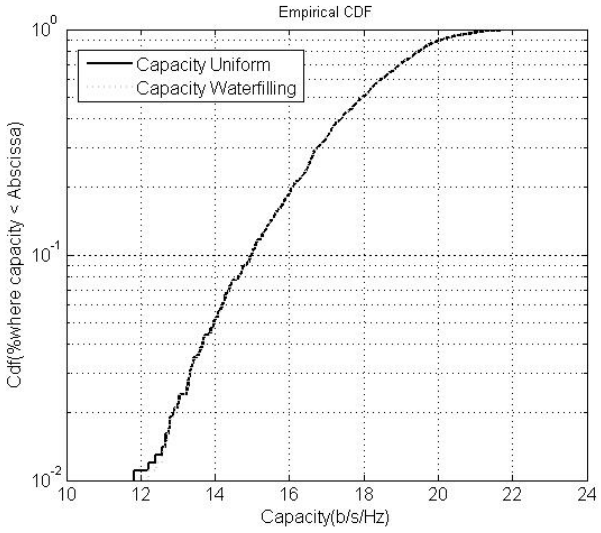

Figure 4.9: Capacity Target user SNR=30dB

- Power allocation

  On the left picture 4.8,as can be seen on this two capacities. Waterfilling gives a better result than Uniform power allocation. This is due to the fact that in case of high noise power level, waterfilling is acting like a switch among the two data streams and is able to give more power to the most interesting data-stream. On the contrary, on the right picture 4.9,Waterfilling and uniform power allocation approach the same result. In case of low noise, waterfilling strategy will be similar to the uniform strategy and will distribute the total transmitted power equally among the data streams.

- High noise power

  As can be seen in Figure 4.8, the capacity reach a value of 4 b/s/Hz in waterfilling power allocation. This value is quite small, and it is due to the noise power level. On the contrary, in low noise power level (right picture **??**), the capacity is much better than for the case $SNR_{pre} = 6dB$ and can reach the value of 18 b/s/Hz both in waterfilling and uniform power allocation.

4.2.2 The different kind of processing for the eavesdropper

Let us focus on the following cases where the eavesdropper is doing any kind of processing with the received signal. Then the eavesdropper may apply an SVD processing. It could also have a kind of combining technique processing (such as EGC,MRC). We will start this analysis with $SNR_{pre} = 6dB$ and then $SNR_{pre} = 30dB$ (where we are going to compare the different processing in uniform and then waterfilling).

Different processing: Uniform at SNR=6dB

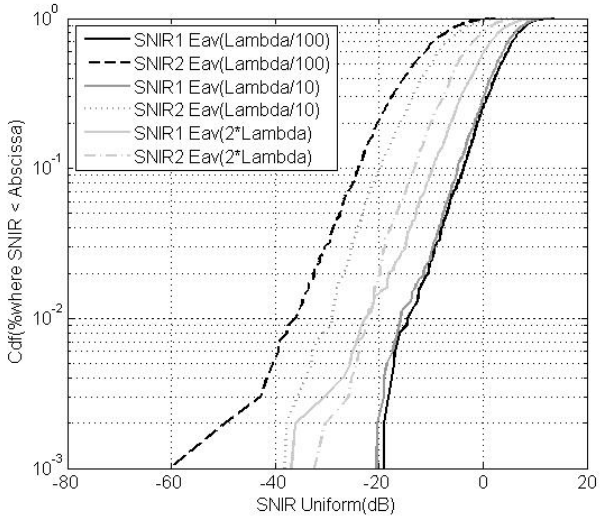

Figure 4.10: SNIR Preprocessing

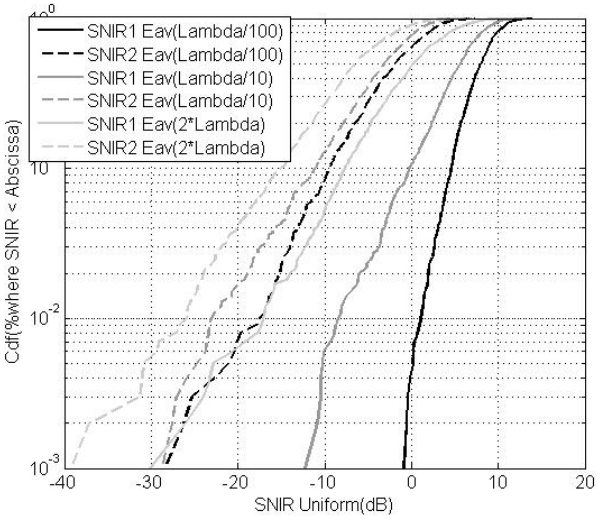

Figure 4.11: SNIR Postprocessing SVD

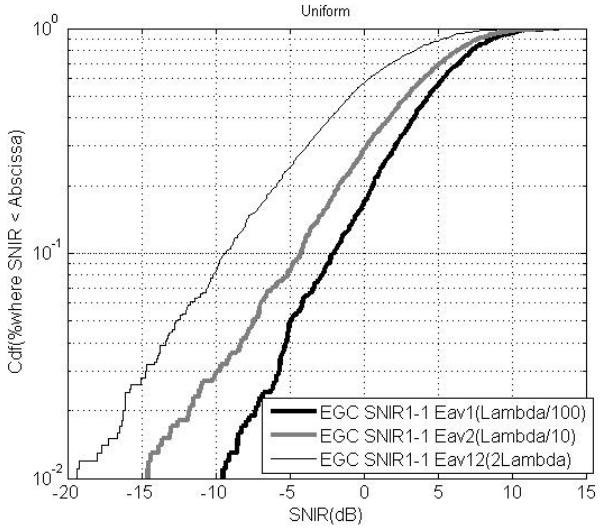

Figure 4.12: SNIR Postprocessing EGC

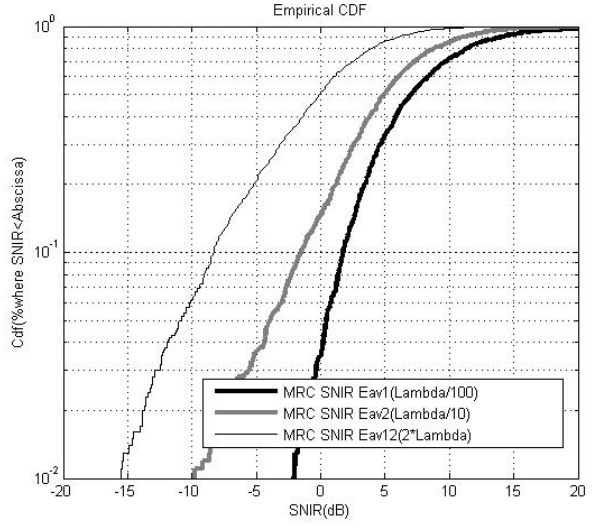

Figure 4.13: SNIR Postprocessing MRC

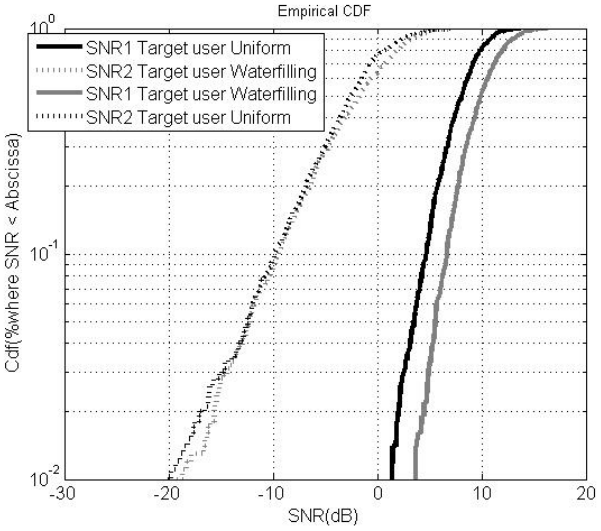

Figure 4.14: SNR Postprocessing SVD

Different processing: Results analysis

- Power allocation

  We used in the group of pictures above, the uniform power allocation.

- Noise power level

  In the above group of figures, we are at high noise power (i.e: SNR_{pre}), that is the reason why the results of the SNIR are not at high values.

- Best processing

  As can be seen, comparing the whole group, the best processing for the eavesdroppers to achieve their best SNIR is the SVD processing 4.11, which is the only one to approach the result of the SNR result of the target user 4.19. However this is true only if the eavesdropper is very close from the target user ($\lambda/100$,$\lambda/10$).

- When the eavesdropper goes away from the target user

  When the eavesdropper is at farther locations from the target user. It can be easily seen, that the SNIR of the eavesdropper is very poor for the SVD 4.11 processing. The best processing in that case would appear to be the MRC 4.13 technique, which provide a not so big difference between SNIR of the different eavesdroppers.

- Slopes of the curves

  It is also interesting to see in the SVD picture 4.11, that the slope of the first eaves-

dropper is quite small, which means a quite good stability. However we can see that once the eavesdropper goes away from the target user, this slope starts to increase very quickly. From this point, the combining technique provides small slope for the curves then more stability for the SNIR of the eavesdropper, except for the closest eavesdroppers from the target user.

Different processing: Waterfilling at SNR=6dB

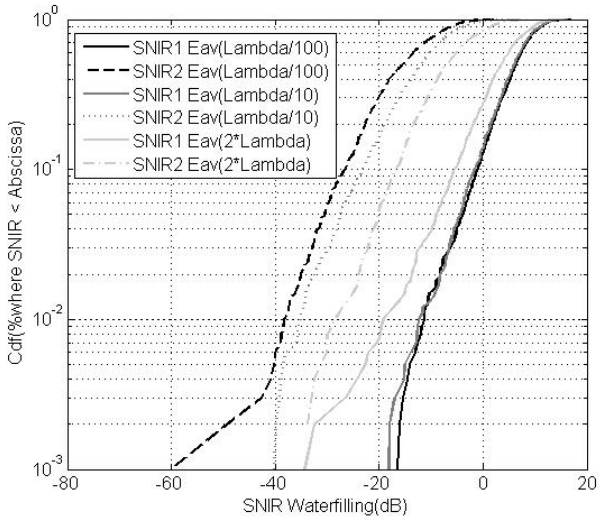

Figure 4.15: SNIR Preprocessing

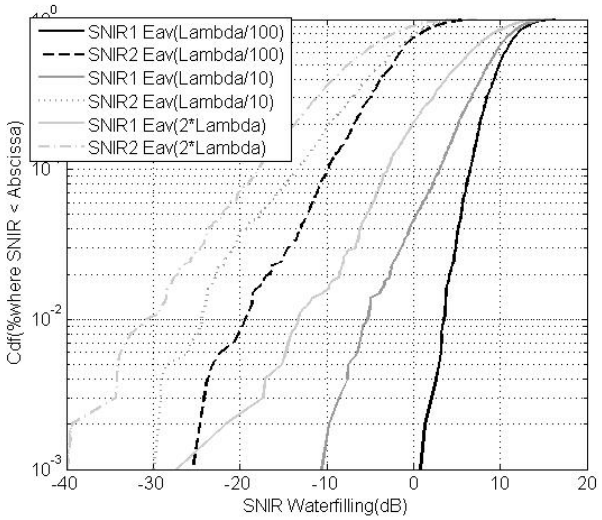

Figure 4.16: SNIR Postprocessing SVD

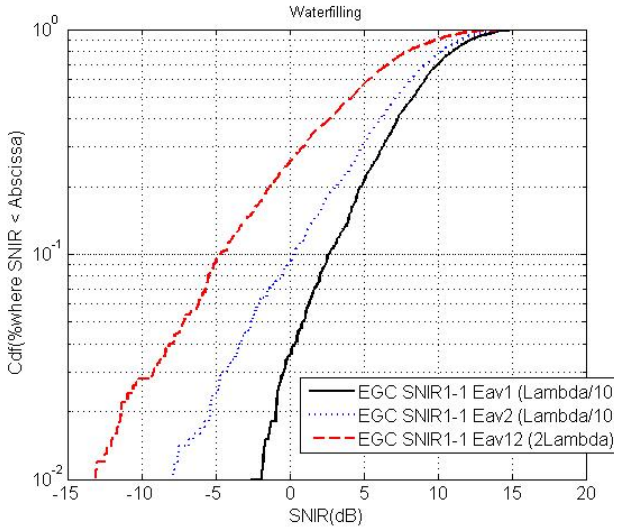

Figure 4.17: SNIR Postprocessing EGC

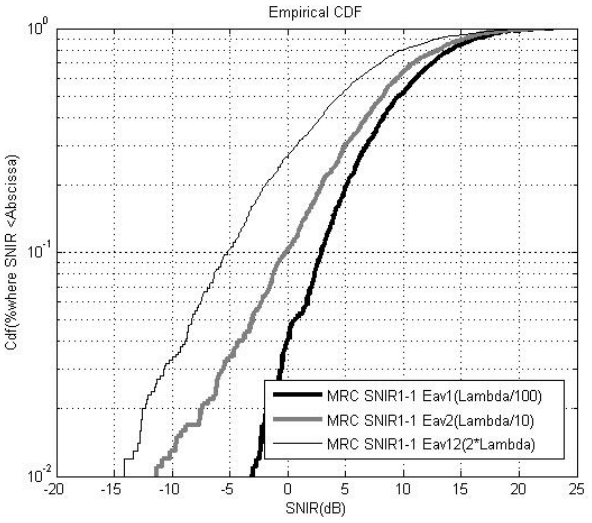

Figure 4.18: SNIR Postprocessing MRC

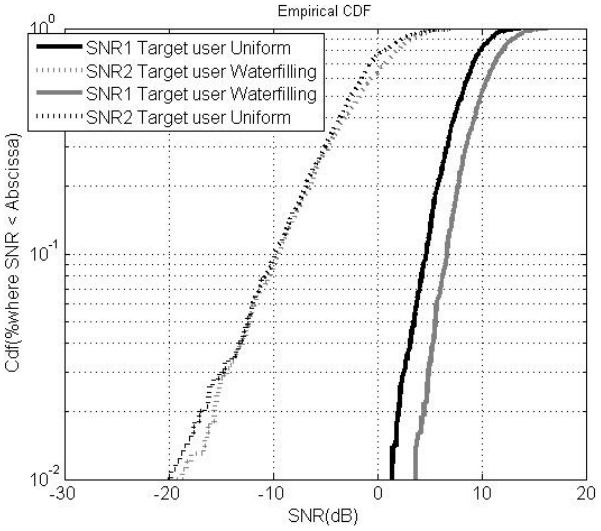

Figure 4.19: SNR Postprocessing SVD

Different processing: Results analysis

- Power allocation

  We used in the group of pictures above, the waterfilling power allocation. It can be seen on the above group of pictures, that in all the cases, waterfilling power allocation provides slightly better results in SNIR for all the processing. It is still because in case of high noise power level, waterfilling is acting like a switch among the two data streams and is able to give more power to the most interesting data-stream.

- Noise power level

  In the above group of figures, we are at high noise power (i.e: $SNR_{predetection}$), that is the reason why the results of the SNIR are not at high values.

- Best processing

  As can be seen, comparing the whole group, the best processing for the eavesdroppers to achieve their best SNIR is the SVD processing 4.11, which is the only one to approach the result of the SNR result of the target user 4.19. However this is true only if the eavesdropper is very close from the target user ($\lambda/100$,$\lambda/10$).

- When the eavesdropper goes away from the target user

  When the eavesdropper is at farther locations from the target user, we can observe the same behavior than in uniform case, however it is interesting to see that the gap

between the eavesdropper1 and 12 is less than before, which means that even farther eavesdroppers start to get a better SNIR than in uniform case.

- Slopes of the curves

  We can observe the same behavior than for the Uniform case, however it is interesting to see, that we have a bit more stability in SVD processing for the eavesdropper12 comparing to the uniform case. Nevertheless, to get more stability for all the eavesdropper in average, it is still better to use combining techniques (such as MRC, or EGC).

Different processing: Waterfilling/Uniform at SNR=30dB

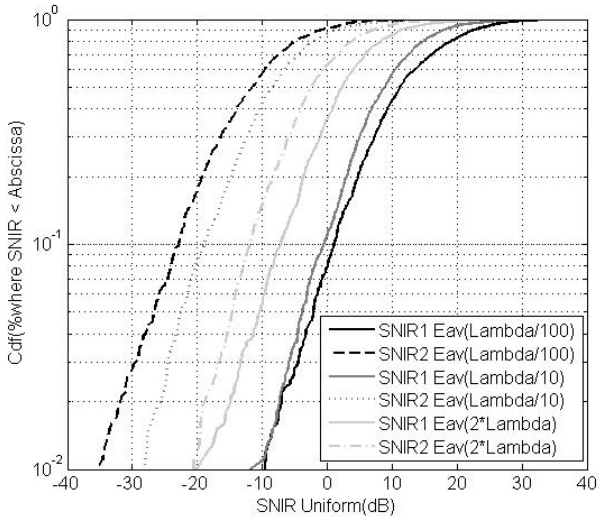

Figure 4.20: SNIR Preprocessing

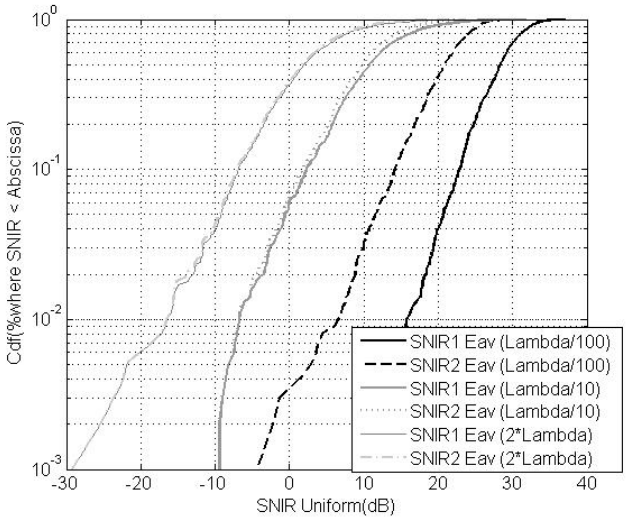

Figure 4.21: SNIR Postprocessing SVD

Different processing: Results analysis

- Power allocation

  We used in the group of pictures above, the uniform power allocation. At high $SNR_{predetection}$ (about 30dB), waterfilling will approach the strategy of the uniform, and then, we will almost have the same results. That is the reason why, we only showed the uniform power allocation at $SNR_{pre} = 30dB$.

- Noise power level

  In the above group of figures, we are at low noise power (i.e: $SNR_{pre} = 30dB$), that

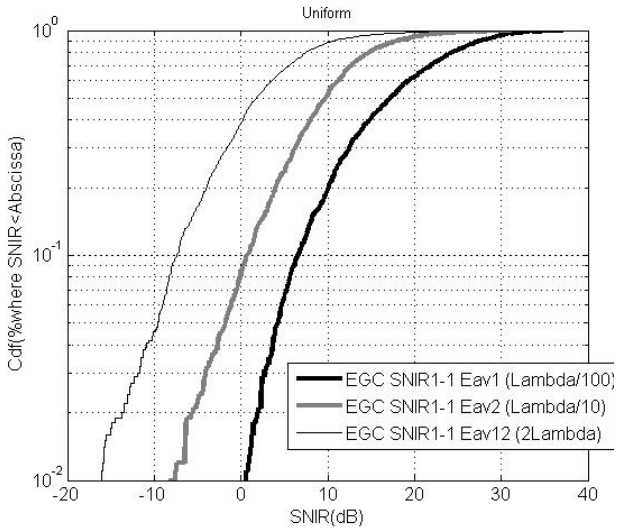

Figure 4.22: SNIR Postprocessing EGC

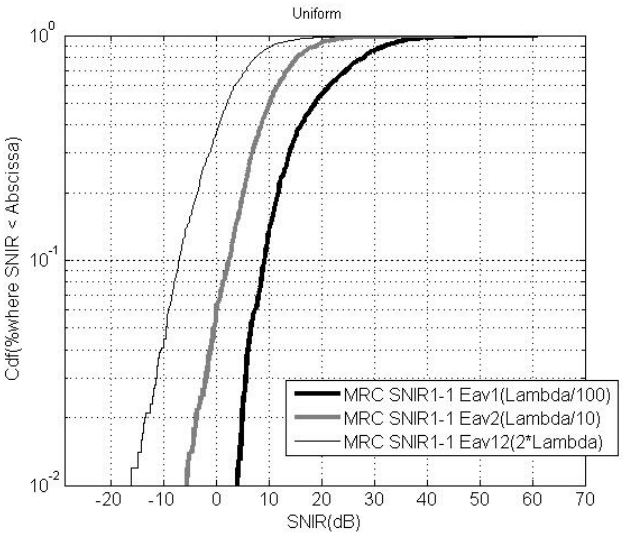

Figure 4.23: SNIR Postprocessing MRC

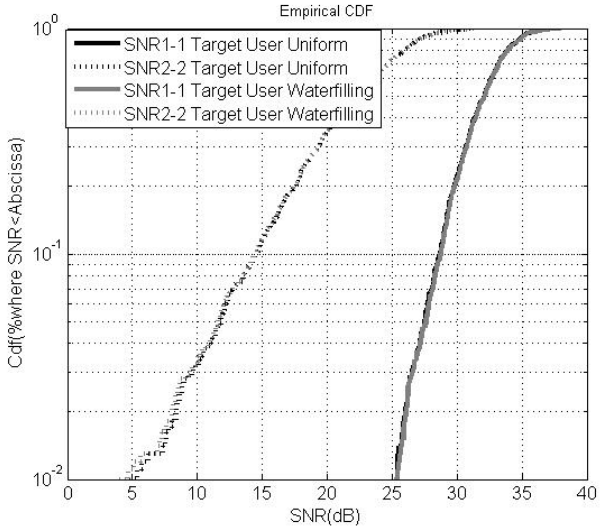

Figure 4.24: SNR Postprocessing SVD

is the reason why the results of the SNIR are really better than at 6dB.

- Best processing

  As can be seen, comparing the whole group, the best processing for the eavesdroppers to achieve their best SNIR is still the SVD processing, almost the same than the target user for the eavesdropper 1. However, using SVD at $SNR_{pre} = 30dB$, the eavesdroppers 2 and 12 have very bad SNIR comparing to the eavesdropper1.

- When the eavesdropper goes away from the target user

When the eavesdropper is at farther locations from the target user, the SVD processing gives very poor results (Eavesdropper2 and 12). On the contrary, combining techniques (EGC and MRC) are giving pretty good results for all the eavesdroppers, even the farthest (1,2 and 12).

- Slopes of the curves
  We can observe the same behavior than the other cases, more stability for the eavesdroppers using MRC or EGC in general. And quite good stability for SVD processing for the eavesdropper 1 only (Closest from target user).

4.2.3 Conclusion of scenario1

As a conclusion of the first scenario, we gathered the observations made during the analysis of the results:

1. What is the best processing for the eavesdropper
   SVD is the best processing for the eavesdroppers to catch the best SNIR.

2. One condition to get a good SNIR once the eavesdropper starts to go away from the target user, its SNIR will get a quite poor level, even in SVD processing.

To conclude on this first scenario, we could say that the SVD processing is already enough robust to keep the confidentiality (even if it is the best processing for the eavesdropper to get a good SNIR).
However, we may be able to optimize this confidentiality and reduce the SNIR of the eavesdropper, even for the closest eavesdroppers. While reducing the SNIR, we will pay attention to the capacity of the target user.

4.3 Second scenario

This scenario considers that the access point knows the target user, but also the eavesdroppers. That is the reason why, the access point is going to reduce as much as it can the SNIR of the eavesdroppers.
We only investigated an MRC and preprocessing for the eavesdroppers. EGC is not so interesting for this scenario, because its results should have the same tendency than MRC with lower values. We are going to compare the SNIR of the eavesdroppers (using MRC processing and preprocessing for each step) with the SNR of the target user (which is using

SVD processing for each step), and also the capacity of the eavesdroppers (still using MRC processing and preprocessing) and the capacity of the target user (Still in SVD processing). Below are the two main points of the scenario 2:

1. Reducing the SNIR of the eavesdroppers acting on the allocation of power.
2. Looking at the capacity and SNR of the target user regarding the new power allocation.

We gathered the results regarding their SNR_{pre} (6dB and 30dB)

4.3.1 SNIR With $SNR_{pre} = 6dB$

Here are presented the results of the SNIR of the eavesdroppers using two different processing:

- Without any processing
- MRC processing

We compare the eavesdroppers SNIR to the SNR of the target user (using SVD processing). We only showed the SNIR1.1 and not the SNIR2.2. The reason is that the SNIR2.2 is really lower than the SNIR1.1.

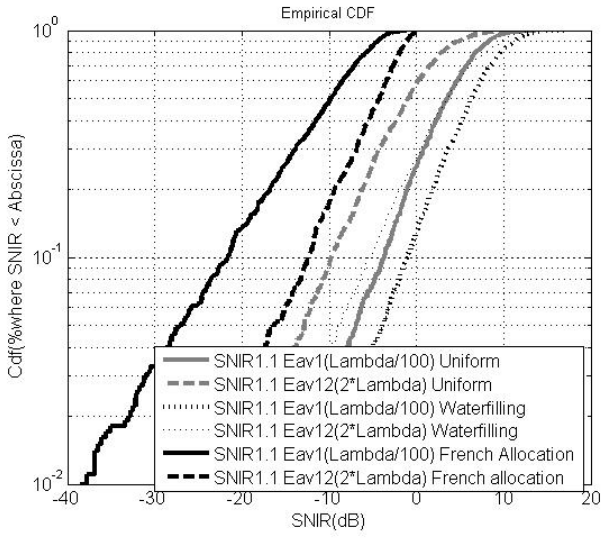

Figure 4.25: SNIR Preprocessing

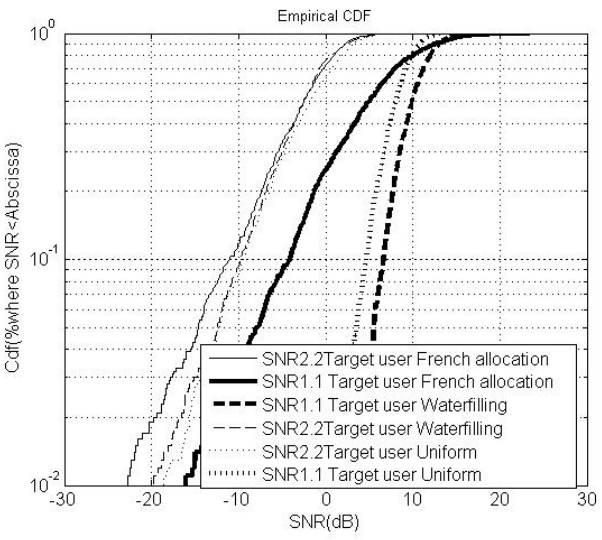

Figure 4.26: SNR Target User SVD

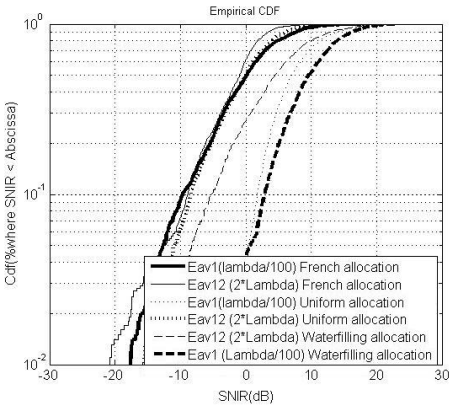

Figure 4.27: SNIR MRC processing

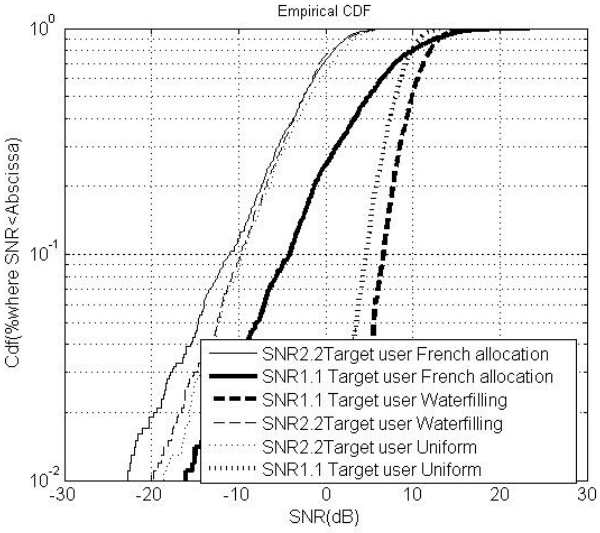

Figure 4.28: SNR Target User SVD

- **Deteriorating the SNIR**

  As can be seen on the above figure related to the preprocessing case 4.25, the two eavesdroppers SNIR go to the negative values using the "French power allocation". Concerning the MRC case using the French power allocation, the two SNIR go to 0dB at 50% level 4.27.

- **Power allocation results** In all the case, the waterfilling power allocation provides the best result, slightly better than uniform power allocation. As it has been said in the first scenario, it is because in case of high noise power, waterfilling power allocation is acting as a switch among the different data-streams. It optimizes the values of the SNIR and capacity, for both target user and eavesdroppers.

- **SNR of the target user**

  Comparing to the SNR of the target user in Uniform and Waterfilling power allocation, the SNR using the French power allocation is at a quite poor value at $SNR_{pre} = 6dB$. This is due to the French power allocation which deteriorates the SNIR of the eavesdroppers but also bring changes at the target user side. We also can have a look at the slopes of the curves on the figures related to the SNR of the target user 4.28, which are bigger in the case of French power allocation. A bigger slope means less stability, because a wider range of values becomes available.

4.3.2 Capacity With $SNR_{pre} = 6dB$

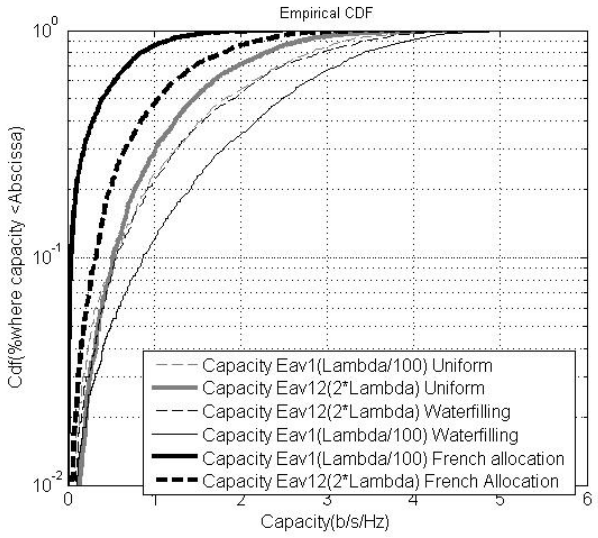

Figure 4.29: Capacity Preprocessing

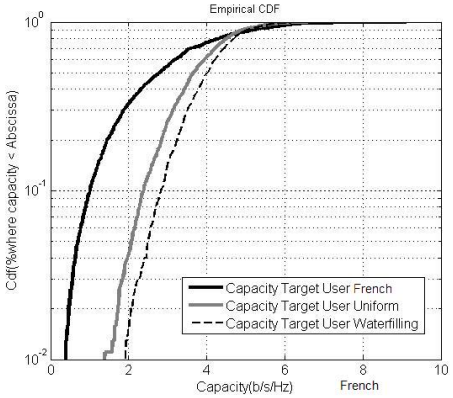

Figure 4.30: Capacity Target User SVD

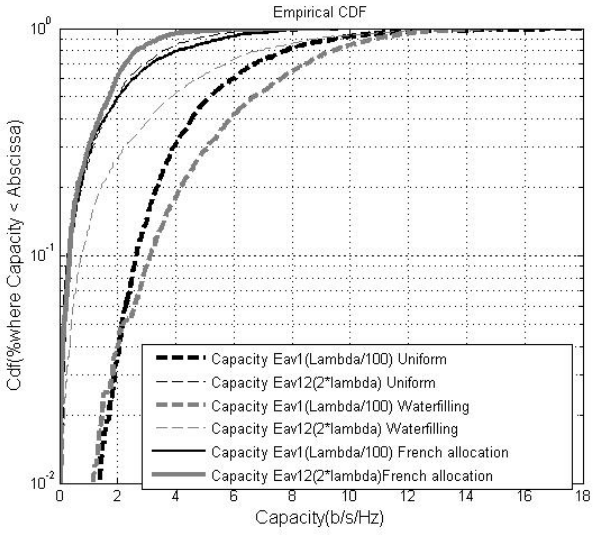

Figure 4.31: Capacity MRC

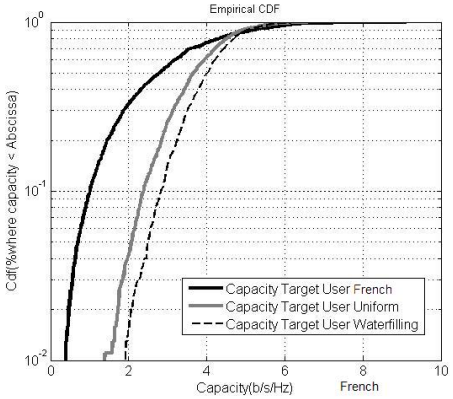

Figure 4.32: Capacity Target User SVD

- **Deteriorating the SNIR**

  As can be seen on the above figure related to the preprocessing case 4.29, the two eavesdroppers SNIR have very poor capacities using the "French power allocation"(about 0.5b/s/Hz at 50% level). Concerning the MRC case using the French power allocation, the two eavesdroppers can get better capacities(C=2b/s/Hz at 50%level) than in preprocessing(C=0.5 b/s/Hz at 50%level), it comes from the processing of MRC

which improves the SNIR as we showed during the first scenario. However their values have been really reduced comparing to the waterfilling and uniform cases (about C=6b/s/Hz at 50% level).

- **Power allocation results**

  Still, In all the cases, the waterfilling power allocation provides the best result, slightly better than uniform power allocation.

- **Capacity of the target user**

  Comparing to the capacity of the target user in Uniform and Waterfilling power allocation, the capacity obtained using the French power allocation is at a quite poor value at $SNR_{pre} = 6dB$ 4.32. This comes from the SNR of the target user which have been reduced by the French power allocation. We also can observe the same tendency regarding the slopes of the curves on the figures related to the capacity of the target user 4.32. These slopes are very good stability indexes.

Let's move to the high SNR_{pre} (30dB, which means low noise power), with the same steps followed at $SNR_{pre} = 6dB$.

4.3.3 SNIR With $SNR_{pre} = 30dB$

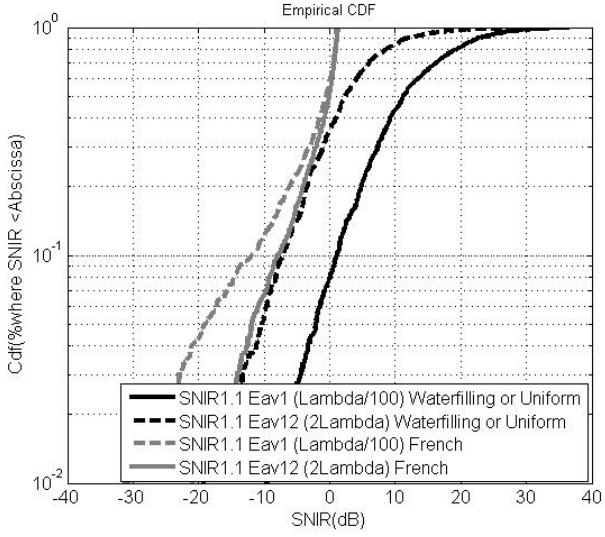

Figure 4.33: SNIR Preprocessing

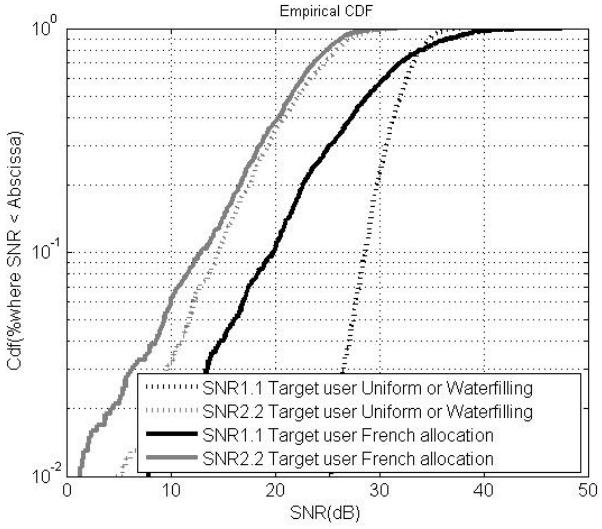

Figure 4.34: SNR Target User SVD

- **Deteriorating the SNIR**

  As we did before, our French power allocation has reduced the SNIR of the eaves-

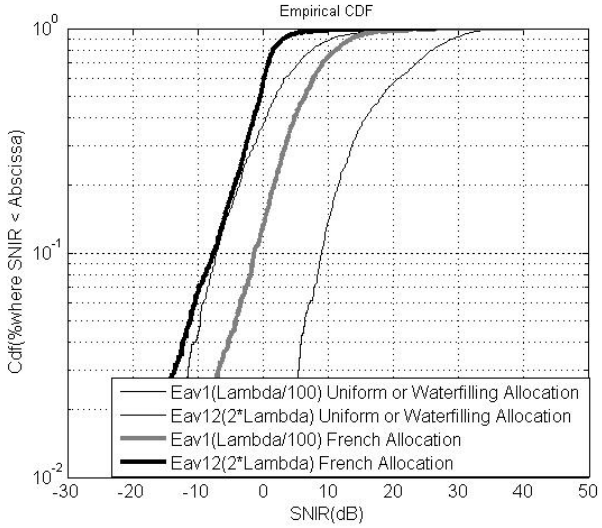

Figure 4.35: SNIR Eavesdropper MRC

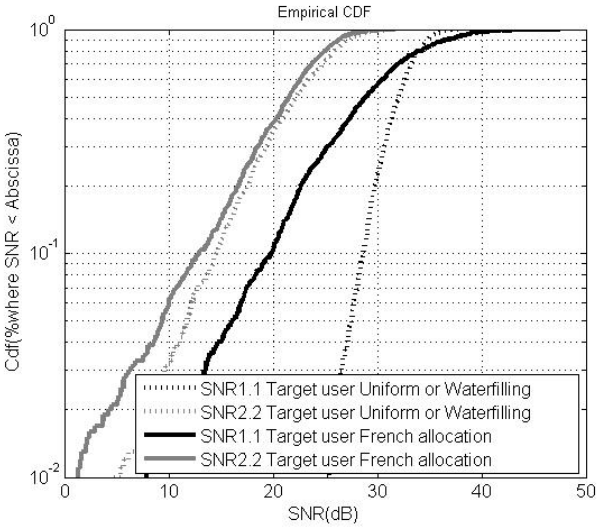

Figure 4.36: SNR Target User SVD

droppers 1 and 12 in preprocessing and MRC cases. As can be seen on the figure 4.35, the SNIR affected by the french power allocation are better than in the preprocessing case. This is still due to the MRC combining technique which provides a better SNIR than the processing

- **Power allocation results**

  It is interesting to see that in this case of low noise power, waterfilling and uniform power allocation give the same result(that is the reason why we gathered them on the figures). This observation has already been made during the first scenario, the waterfilling can not work as a switch since there is almost any noise power.

- **SNR of the target user**

  Comparing to the SNR of the target user in Uniform and Waterfilling power allocation 4.36, the SNR using the French power allocation is at a quite poor value at $SNR_{pre} = 30dB$. We also can consider the slopes of the curves on the figures related to the SNR of the target user 4.36, which are bigger in the case of French power allocation, then we have less stability.

After analyzing the results of the SNIR of eavesdroppers and the SNR of the target user, let's look at these results in term of capacity.

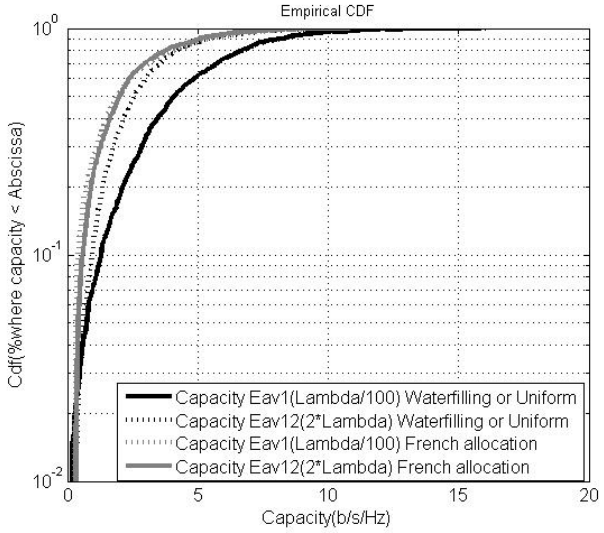

Figure 4.37: Capacity Preprocessing

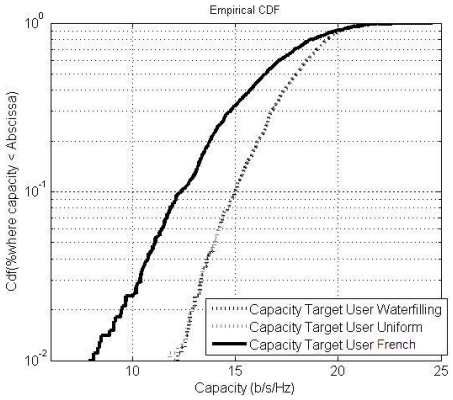

Figure 4.38: Capacity Target User SVD

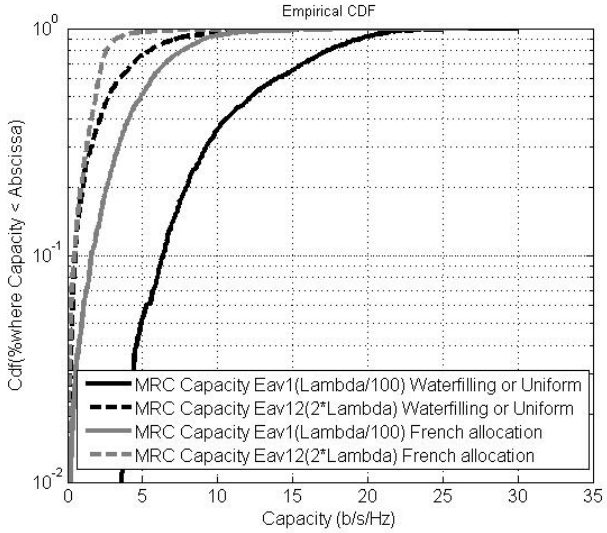

Figure 4.39: Capacity Preprocessing

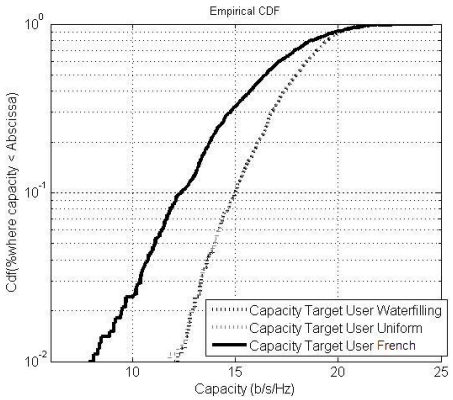

Figure 4.40: Capacity Target User SVD

4.3.4 Capacity With $SNR_{pre} = 30dB$

- **Deteriorating the SNIR**

  It is not surprising to see the capacity of the eavesdroppers being reduced by the French power allocation in Figure 4.37 and in Figure **??**, since the SNIR have been deteriorated.

- **Power allocation results**

  Still, in all the cases, the waterfilling power allocation and the uniform power alloca-

tion provide the same results, as explained in the previous part.

- **Capacity of the target user**

  Comparing to the capacity of the target user in Uniform and Waterfilling power allocation, the capacity obtained using the French power allocation is at a quite poor value at $SNR_{pre} = 30dB$ 4.40. This comes from the SNR of the target user which have been reduced by the French power allocation. We also can observe the same tendency regarding the slopes of the curves on the figures related to the capacity of the target user 4.40.

4.3.5 Conclusion of scenario2

As a conclusion of the second scenario, we gathered the observations made during the analysis of the results:

1. Losses in eavesdropper SNIR and capacity

   It is interesting to see that the French power allocation is able to reduce the eavesdropper SNIR at very low values and especially in the preprocessing case. It is a bit harder for the French power allocation to reduce the eavesdropper SNIR in case of MRC processing.

2. Losses in target user capacity At $SNR_{pre} = 6dB$, having small capacities, a loss of 1dB is quite important. On the contrary, a loss of 1dB, over 17dB is not so big, and especially if this loss of 1dB capacity is useful to reduce the SNIR of the eavesdroppers and to keep the confidentiality.

3. More receiver antennas case If we increase the number of antennas for all the system, that is to say (for the Transmitter, Target user and eavesdroppers), this new power allocation will be less efficient to reduce the SNIR.

In case of high noise level (small SNR_{pre}), it is not very useful to try to optimize the SVD technique. It will be more a loss of capacity than a gain in confidentiality. Nevertheless at low noise level (high SNR_{pre}), the French power allocation can be a a not too bad tradeoff between capacity and confidentiality. However, from a general point of view, the losses in target user capacity are more important than the losses in eavesdropper capacities.

4.4 Conclusion of the whole simulation

This simulation offered a span of different techniques that the eavesdropper would apply to catch the signal. The first part showed that the SVD processing technique is the most interesting for the eavesdroppers to get the best SNIR. This first part of the simulation also underlined the huge losses in SNIR for the eavesdropper once it goes a bit far from the target user position (even in SVD processing). This last observation, shows that SVD technique is already quite robust to keep confidentiality. We may have more antennas, that is to say a 4×4 systems or more, and SVD processing would be even stronger, because eavesdroppers will have more interferences. These added interferences, would deteriorate the SNIR of the eavesdroppers.

The second part has been lead to optimize the SVD processing by adding the French power allocation scheme to reduce the SNIR of the eavesdroppers. It showed that this optimization may be a quite good tradeoff, but only at high noise level, between capacity and the confidentiality. However from a general point of view, the losses in target user capacity are bigger than the losses in eavesdropperSNIR.

To conclude on this simulation, it is obvious to say that SVD technique is already quite robust against eavesdroppers, and even more if we increase the number of antennas(4×4,8×8). The optimization of the SVD technique using the French power allocation does not give very interesting results when eavesdropper are using SVD processing, and even when eavesdropper are using combining techniques(EGC,MRC) as processing. One interesting combining technique which would have been interesting to test is the optimum combining which can reduce the interferences and enhance the SNIR.

Chapter 5

Conclusion and future work

5.1 Conclusion

This project presents one aspect of the security, the confidentiality, in a transmission between an access point and a target user. The main problem in wireless communications is the broadcast aspect of the transmission from the transmitter, when we want to provide a certain confidentiality. We investigated this problem in order to see if we can optimize this confidentiality on the physical layer, based on a SVD transmission between the transmitter and the target user. In spite of the different processing (SVD or combining techniques (EGC,MRC)) that the eavesdroppers may apply to get a good SNIR, our goal has been to achieve a certain tradeoff between the capacity of the target user and reducing the SNIR of the eavesdroppers.

1. First Chapter

   First step has been to achieve the delimitation of the problem, and especially the domain to work in (Space-space domain).

2. Second chapter

   We focused on the technical review in order to gather and explain all the different processing that we would like to use in our simulations at the eavesdroppers side. A theoretical analysis is also provided to show what are the signals that the target user and the eavesdroppers would get using SVD processing.

3. Third chapter

   This step is dedicated to present the simulation model that we used. The different scenarios have also been described in this chapter.

4. Forth and last chapter

   This last step starts with a theoretical analysis of the results that we are expecting (in SNIR) in the different processing (SVD, EGC, MRC). This part is mainly dedicated to providing the results and the analysis of the simulation.

The simulation has been divided in two main parts. First part has been dedicated to observe the behavior of the SNIR of the eavesdroppers using different processing. Then, we used a new power allocation to reduce the SNIR of the eavesdroppers and we looked at the capacity at the target user side, to see if a kind of tradeoff between them can be found.

5.1.1 Conclusion of the first part

- Best processing for the eavesdropper close to the target user

  SVD processing is the best technique to get a SNIR at a very good value (almost the same than SNR of the target user) with a huge stability if the eavesdroppers are very close from the target user ($\lambda/100$, $\lambda/10$, λ).

- SVD processing already quite secured

  It is important to notice that once the eavesdropper goes away from the target user, it will get a poor SNIR. Then we can conclude that the SVD processing is already quite secured.

- Global best processing for the eavesdropper MRC technique appears to be the best processing for eavesdroppers which are not so close from the target user, and offers more stability than the other processing.

- Increase the number of antennas for the eavesdropper

  If we increase the number of antennas of the whole system. The eavesdropper would have more interferences in the received signals, and then the SVD would be even more robust concerning the confidentiality.

5.1.2 conclusion of the second part

- Optimizing the SVD processing

  In case of low noise, we saw that using the new power allocation which reduce the SNIR close to 0dB, doesn't deteriorate so much the capacity of the target user. In that case, the SVD is a bit optimized.

- The other processing
  Combining techniques(EGC,MRC) are easier for the access point to reduce the SNIR.

- More antennas for the whole system
  The new power allocation would be less efficient to reduce all the SNIR if we increase the number of antennas of the eavesdropper, since it will be harder to reduce all the SNIR at the same time.

To conclude on this project, we showed that the SVD processing is already quite robust by itself. However in case of low noise and few number of antennas, an optimization using a intelligent power allocation to reduce the SNIR may be interesting to develop.

5.2 Future work

Even if the SVD has been shown to be already secured by itself in this project, it may be interesting to add a special cases to the scenarios we defined:

1. More antennas for the eavesdroppers only
   Special case where the eavesdropper has more antennas than the target user and the access point.

2. Different motions and positions of the eavesdropper
   It may be interesting to see the results of the defined scenarios with different motions for the eavesdroppers and different positions of the eavesdroppers from the target user (for instance, in front of the target user).

3. Multi users case
   Our scenarios have been achieved using only one target user. Adding other target users would increase the interferences for the eavesdroppers.

4. Other wireless techniques
   It can be interesting to lead the defined scenarios using other wireless techniques, such as OFDM, or space-time coding.

Bibliography

[1] N. T. O Nouali, "Secured electronic mail," *Revue dInformation Scientifique et Technique Vol11(2) 2001 21-34*.

[2] G. Surman, "Understanding security using the osi model," *SANS Institute*, pp. 1–4, Mar 2002.

[3] A. Dornan, *The essential guide to Wireless Communications Applications*. Prentice Hall, 2002.

[4] P. Kyritsi, "Mm7: Short term fading (wideband) physicaldescription," Aalborg University, Tech. Rep., 2007.

[5] J. Mohinder, *Space-Time codes and MIMO Systems*. Artech House, 2004.

[6] free encyclopedia, "Space-time code."

[7] D. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge University Press, 2004.

[8] A. Bourdoux and K. Snoeckx, "Exploiting mimo technology for optimal performance," March 2005.

[9] D. Wolf, "Svd lectures," april 2007.

[10] X. Zhou, P. Kyritsi, P. C. F. Eggers, and F. H. P. Fitzek, "The medium is the message secure communication via waveform coding in mimo systems," *Aalborg University*.

[11] J. Kermoal, L. Schumacher, K. I. Pederson, P. E. Mogensen, and F. Frederiksen, "A stochastic mimo radio channel model with experiment validation," *IEEE journal on selected area in communications*, vol. 20, no. 6, pp. 1211–1226, August 2002.

[12] free encyclopedia, "Signal to noise ratio," april 2007.

[13] D. G. BRENNAN, "Linear diversity combining techniques," *Massachusetts Institute of Technology*.

[14] J. S. T. Su K. Yong and S. McLaughlin, "Performance of diversity combining techniques for antenna arrays," *Signals and Systems Group, Department of Electronics and Electrical Engineering, The University of Edinburgh*.

[15] A. C. T1A1, "Far-field region," 2001.

[16] Balanis., *Antenna Theory, Analysis and Design*, 1997.

[17] J. W.C.Jakes, *Microwave Mobile Communications*, 1974.

Appendix A

Post-Processing: Received signal for the target user

From this question 2.10 we can choose to work before the processing $\mathbf{U}^H$ of the target user **??** in order to get the receive signal just after the received antennas.

$$\underline{r} = \mathbf{U} \cdot \mathbf{D} \cdot \underline{x} + \underline{n} \tag{A.1}$$

$$\begin{aligned} \underline{r} = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} &= \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix} \cdot \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \\ &= \begin{pmatrix} U_{11} \cdot \lambda_1 & U_{12} \cdot \lambda_2 \\ U_{21} \cdot \lambda_1 & U_{22} \cdot \lambda_2 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \end{aligned} \tag{A.2}$$

$$r_1 = \lambda_1 \cdot \mathbf{U}_{11} \cdot x_1 + \lambda_2 \cdot \mathbf{U}_{12} \cdot x_2 + n_1 \tag{A.3}$$

$$r_2 = \lambda_1 \cdot \mathbf{U}_{21} \cdot x_1 + \lambda_2 \cdot \mathbf{U}_{22} \cdot x_2 + n_2 \tag{A.4}$$

A.0.1 SNIR pre-processing for target user

Finally we get these two equations A.3 A.4. From here we can determine SNIR of the target user with the formula 2.22

$$SNIR_1 = \frac{P_1 \cdot (\lambda_1 \cdot \mathbf{U}_{11})^2}{P_2 \cdot (\lambda_2 \cdot \mathbf{U}_{12})^2 + P_n} \tag{A.5}$$

$$SNIR_2 = \frac{P_2 \cdot (\lambda_2 \cdot \mathbf{U}_{22})^2}{P_1 \cdot (\lambda_1 \cdot \mathbf{U}_{21})^2 + P_n} \tag{A.6}$$

P_1 and P_2 are respectively the power transmitted along the 1^{st} and $the2^{nd}$ data stream.

Appendix B

Pre-Processing: Received signal for the eavesdropper

$$\underline{r} = \mathbf{U}_e \cdot \mathbf{D}_e \cdot \mathbf{V}_e^H \cdot \mathbf{V} \cdot \underline{x} + \underline{n} \tag{B.1}$$

$$\underline{r} = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} U_{e11} & U_{e12} \\ U_{e21} & U_{e22} \end{pmatrix} \cdot \begin{pmatrix} \lambda_{e1} & 0 \\ 0 & \lambda_{e2} \end{pmatrix} \cdot \begin{pmatrix} V_{e11}^* & V_{e21}^* \\ V_{e12}^* & V_{e22}^* \end{pmatrix} \cdot \begin{pmatrix} V_{11} & V_{12} \\ V_{21} & U_{22} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \tag{B.2}$$

$$\underline{r} = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} \lambda_{e1} \cdot U_{e11} & \lambda_{e2} \cdot U_{e12} \\ \lambda_{e1} \cdot U_{e21} & \lambda_{e2} \cdot U_{e22} \end{pmatrix} \cdot \begin{pmatrix} V_{e11}^* & V_{e21}^* \\ V_{e12}^* & V_{e22}^* \end{pmatrix} \cdot \begin{pmatrix} V_{11} & V_{12} \\ V_{21} & U_{22} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \tag{B.3}$$

We multiply the two first matrix, and we obtain:

$$\begin{pmatrix} \lambda_{e1} \cdot U_{e11} & \lambda_{e2} \cdot U_{e12} \\ \lambda_{e1} \cdot U_{e21} & \lambda_{e2} \cdot U_{e22} \end{pmatrix} \cdot \begin{pmatrix} V_{e11}^* & V_{e21}^* \\ V_{e12}^* & V_{e22}^* \end{pmatrix} = \begin{pmatrix} \lambda_{e1} \cdot U_{e11} \cdot V_{e11}^* + \lambda_{e2} \cdot U_{e12} \cdot V_{e12}^* & \lambda_{e1} \cdot U_{e11} \cdot V_{e21}^* + \lambda_{e2} \cdot U_{e12} \cdot V_{e22}^* \\ \lambda_{e1} \cdot U_{e21} \cdot V_{e11}^* + \lambda_{e2} \cdot U_{e22} \cdot V_{e12}^* & \lambda_{e1} \cdot U_{e21} \cdot V_{e21}^* + \lambda_{e2} \cdot U_{e22} \cdot V_{e22}^* \end{pmatrix} \tag{B.4}$$

Now we take the result of B.4 and we multiply by $\mathbf{V}$.

$$\begin{pmatrix} \lambda_{e1} \cdot U_{e11} \cdot V_{e11}^* + \lambda_{e2} \cdot U_{e12} \cdot V_{e12}^* & \lambda_{e1} \cdot U_{e11} \cdot V_{e21}^* + \lambda_{e2} \cdot U_{e12} \cdot V_{e22}^* \\ \lambda_{e1} \cdot U_{e21} \cdot V_{e11}^* + \lambda_{e2} \cdot U_{e22} \cdot V_{e12}^* & \lambda_{e1} \cdot U_{e21} \cdot V_{e21}^* + \lambda_{e2} \cdot U_{e22} \cdot V_{e22}^* \end{pmatrix} \cdot \begin{pmatrix} V_{11} & V_{12} \\ V_{21} & V_{22} \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \quad \text{(B.5)}$$

With

$$A = \lambda_{e1} \cdot U_{e11} \cdot V_{e11}^* \cdot V_{11} + \lambda_{e1} \cdot U_{e11} \cdot V_{e21}^* \cdot V_{21} + \lambda_{e2} \cdot U_{e12} \cdot V_{e12}^* \cdot V_{11} + \lambda_{e2} \cdot U_{e12} \cdot V_{e22}^* \cdot V_{21} \quad \text{(B.6)}$$

$$B = \lambda_{e1} \cdot U_{e11} \cdot V_{e11}^* \cdot V_{12} + \lambda_{e1} \cdot U_{e11} \cdot V_{e21}^* \cdot V_{22} + \lambda_{e2} \cdot U_{e12} \cdot V_{e12}^* \cdot V_{12} + \lambda_{e2} \cdot U_{e12} \cdot V_{e22}^* \cdot V_{22} \quad \text{(B.7)}$$

$$C = \lambda_{e1} \cdot U_{e21} \cdot V_{e11}^* \cdot V_{11} + \lambda_{e1} \cdot U_{e21} \cdot V_{e21}^* \cdot V_{21} + \lambda_{e2} \cdot U_{e22} \cdot V_{e12}^* \cdot V_{11} + \lambda_{e2} \cdot U_{e22} \cdot V_{e22}^* \cdot V_{21} \quad \text{(B.8)}$$

$$D = \lambda_{e1} \cdot U_{e21} \cdot V_{e11}^* \cdot V_{12} + \lambda_{e1} \cdot U_{e21} \cdot V_{e21}^* \cdot V_{22} + \lambda_{e2} \cdot U_{e22} \cdot V_{e12}^* \cdot V_{12} + \lambda_{e2} \cdot U_{e22} \cdot V_{e22}^* \cdot V_{22} \quad \text{(B.9)}$$

Finally we get:

$$r_1 = A \cdot x_1 + B \cdot x_2 + n_1 \quad \text{(B.10)}$$

$$r_2 = C \cdot x_1 + D \cdot x_2 + n2 \quad \text{(B.11)}$$

Appendix C

Testing the envelope distribution: Rayleigh distribution

As can be seen on these plots (representing the different links (h_{11}, h_{12}, h_{21}, h_{22})) in a 2x2 case, the envelope distribution is a Rayleigh distribution. We can prove it graphically by the Rayleigh rule of thumb (at 1% signal level, the power is -20dB).

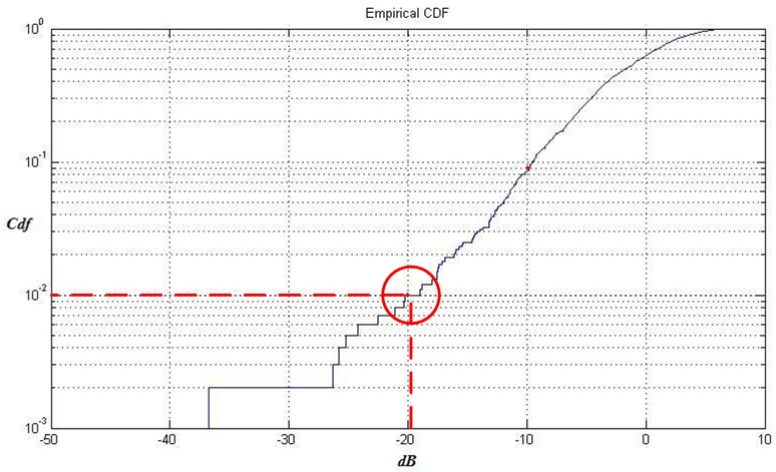

Figure C.1: Rayleigh criterium h11

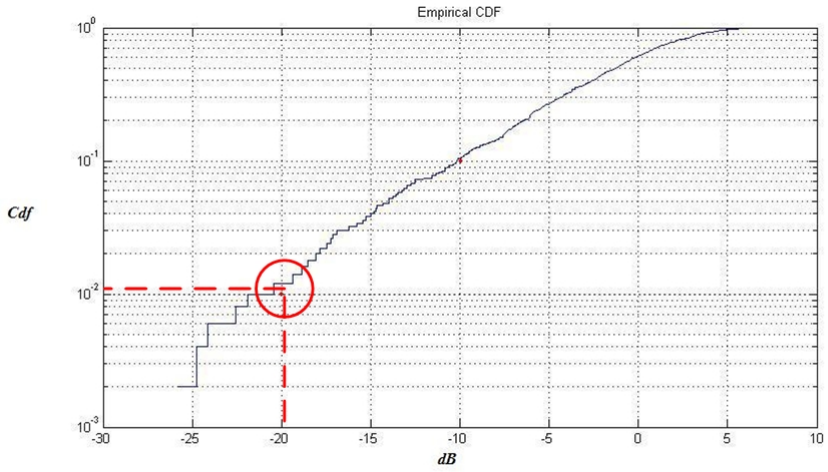

Figure C.2: Rayleigh criterium h12

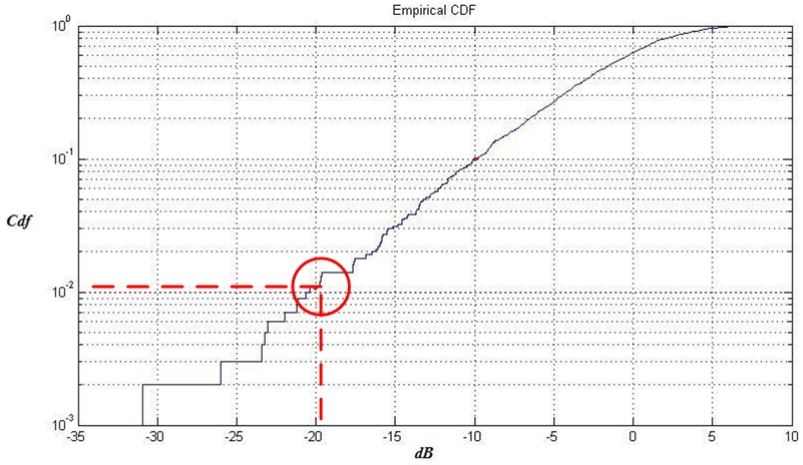

Figure C.3: Rayleigh criterium h21

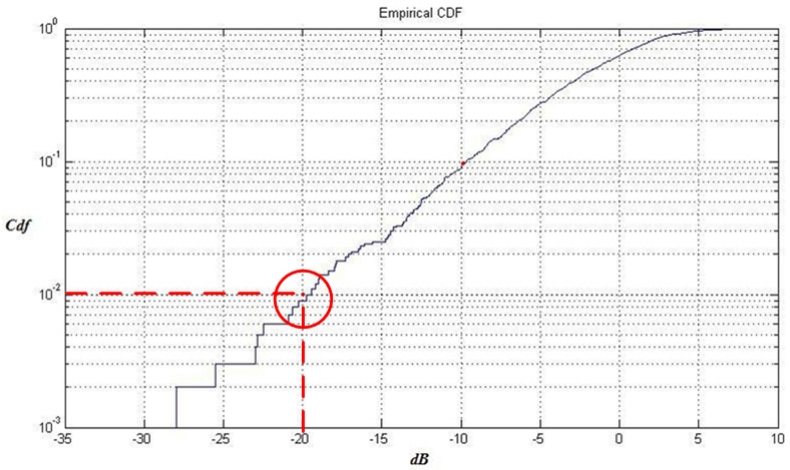

Figure C.4: Rayleigh criterium h22

Appendix D

802.11n channel model

D.1 System model: The 802.11n Channel Model

The first channel model that has been investigated is the 802.11n channel model, also called WWiSE (World-Wide Spectrum Efficiency) or TGn Sync. This model is very related to this project, due to the fact that this standard is also specialized in MIMO system. This standard is a very recent one, and the Publication is currently expected in September 2008.

We started to go through the 802.11n channel model simulated in matlab "MATLABő implementation of the Indoor MIMO WLAN channel model proposed by the IEEE 802.11 TGn Channel Model Special Committe". We went through the documents related to the matlab simulation, explaining the different environments, the functions, and how to use it. We are going to describe briefly the 802.11n Channel model in Matlab, and what we learned from this model. We will finish by a subsection explaining why we didn't use this model.

In this Matlab program, we used the program called "example-MIMO.m". This program is using all the functions contained by the 802.11n Matlab program.

D.1.1 802.11n Matlab description

In this Matlab program, we used the program called "example-MIMO.m". This program is using all the functions contained by the 802.11n Matlab program.

D.1.2 Parameters and results of the program

Below is a summary of the parameters useful in our project that we wanted to modify:

Parameters

- Different environments(A to F) to simulate (they are described later in the report).
- MIMO systems with different number of transmitter antennas and receiver antennas.
- Distance between the transmitter and the target user.

Below is a summary of the parameters useful in our project that we may modify:

Parameters

- Spacing between the antenna elements for the transmitter and the receiver.
- Simulation Length In Coherence Times (Length of simulation in Coherence Times)
- SamplingRate Hz (Sampling rate of the simulation, in Hz)

These are the Results that we can obtain, running the Matlab program "example-MIMO.m":

Results

- The channel matrix of the simulation
- The spatial correlation coefficients
- the Power delay profile
- CDF's of the taps
- Doppler spectra of the taps

D.1.3 The different environments

Here is a summary of the MIMO WLAN channel model environments provided by the matlab program. In this description model, K refers to the "Ricean Factor". The K factor is the relation between the power of the LOS component and the power of the Rayleigh component.

1. $K = 0$

   When the K factor is equal to zero, it means that there are only NLOS components, and the envelop $r = |h|$ is following a rayleigh distribution.

2. $K > 0$

   Then when $K > 0$, it means that in addition to the many NLOS paths, there is a LOS path, and the envelop $r = |h|$ is following a ricean distribution.

- Model A(Flat fading model "optional")
  Environment : Narrowband
  Delay Spread : 0 ns
  Scattering situation: LOS/NLOS

- Model B
  Environment : Residential
  Delay Spread : 15ns
  Scattering situation: LOS(K=0)/NLOS

- Model C
  Environment : Residential/Small Office
  Delay Spread : 30ns
  Scattering situation: LOS(K=0)/NLOS

- Model D
  Environment : Office
  Delay Spread : 50ns
  Scattering situation: LOS(K=3)/NLOS

- Model E
  Environment : Large Open Space/Office
  Delay Spread : 100ns
  Scattering situation: LOS(K=6)/NLOS

- Model F
  Environment : Large Open Space
  Delay Spread : 150ns

Scattering situation: LOS(K=6)/NLOS

D.2 Utilization of the program

D.2.1 Parameters that we used

Many variables have been modified to simulate our results. This is a summary of the value that we have set.

- We used a "Downlink" connection
- Environment A which is narrowband
- MIMO system : 2by2 / 4by4
- Spacing between antenna elements
- Distance between the Tx and target user (meters)
- Distance between the Tx and Eavesdropper (meters)

D.2.2 Assumptions

1. The receiver knows the channel
2. Antennas are omnidirectional antennas

D.2.3 Interests of the program

We used this program in order to obtain:

- The channel matrix **H**
  This Channel matrix will be used to calculate the received signals of the users using SVD method.