Radio Security/Privacy and complexity Trade-offs for 4G

Group No. 08gr1120

Mathieu Gobeaut
Richard Tchissambou

June 2008
Aalborg University

Aalborg University
E-Studyboard
Mobile Communications 10th semester

TITLE:

Radio Security/Privacy and complexity Trade-offs for 4G

THEME:
Mobile Radio Communications

PROJECT PERIOD:
4$^{\text{th}}$ February 2008
5$^{\text{th}}$ June 2008

PROJECT GROUP:
08gr1120

GROUP MEMBERS:
Mathieu Gobeaut
Richard tchissambou

SUPERVISORS:
Xin Zhou
Patrick Eggers

COPIES: 3

PAGES: 73

Abstract:

In wireless communications, transmissions are susceptible to be intercepted by eavesdroppers. As security implies links reliability, the purpose of this project is to secure communications at the physical layer to prevent the home user from configuring his wireless connection security application by himself. The idea is to apply a beam-hopping pattern at an access point, which will allow to choose the direction in which to send a signal and combine it with a power control to guarantee the target user with receiving the same amount of power during a whole communication.

This project mainly includes two aspects.

- Evaluate the performance of the beam hopping pattern. In this part, we try to deteriorate the signal received by the eavesdropper by orienting the beam towards the target user.
- Investigate the efficiency of a power control processing called Automatic Gain Control (AGC) and combine it with the previous technique to perturbate the eavesdropper signal even more and make it very difficult for him to decode a signal sent by the access point to the target user.

Contents

Table of Contents ii
List of Figures iv
List of Tables v
Abbreviations vi
Preface ix
Acknowledgement x

1 Introduction 1
1.1 Security overview 1
1.1.1 Security terms 1
1.1.2 OSI model 3
1.2 Target user and eavesdropper: differentiation 6
1.3 Single Input Single Output (SISO), Single Input Multiple Output (SIMO), Multiple Input Single Output (MISO) and Multiple Input Multiple Output (MIMO) system 8
1.4 Problem Definition 9
1.4.1 Motivation 9
1.4.2 Previous works on security at the physical layer level . 10
1.4.3 What can be further investigated in the physical layer security? 11
1.4.4 Our problem choice 12

2 System description and Environment 14
2.1 System layout 14
2.1.1 System 14
2.1.2 Antenna system 15
2.1.3 Channel 16
2.1.4 Power consideration 17
2.2 Algorithm 19

3 Implementation 23
3.1 Simulation conditions 23
3.2 Parameters definition and scenarios 24
3.3 Procedure 25

3.3.1 Acquisition phase 25
3.3.2 Sending of the information 26

4 Results 27
4.1 Influence of the number of clusters 30
4.1.1 First scenario : Fixed beam 30
4.1.2 Second scenario : Beam-Hopping 33
4.1.3 Third scenario : Beam-Hopping + Automatic Gain Control (AGC) 42
4.1.4 Comparison 49
4.2 Influence of the radius of clusters 49
4.3 Influence of the beamwidth 50
4.4 Conclusion 52

5 Conclusion and future work 55
5.1 Conclusion 55
5.1.1 Conclusion for the first part 56
5.1.2 Conclusion for the second part 57
5.1.3 Conclusion for the third part 57
5.2 Future work 58

Bibliography 61

List of Figures

1.1 Open System Interconnection (OSI) Model 3
1.2 Difference between user and eavesdropper [1] 7
1.3 SISO, MISO, SIMO andMIMO systems 9
1.4 Conventional SISO system 9
1.5 Beam Hopping applied by AP 13

2.1 System layout 15
2.2 How scattering affects the average channel impulse response . 18
2.3 Aquisition phase 20
2.4 Directional power profile 21
2.5 Operation phase 21

4.1 Environment response 29
4.2 Fixed beam oriented in the 90° direction 31
4.3 Average power received by the target user and the eavesdropper after 10 simulations (0°) 32
4.4 Average power received by the target user and the eavesdropper after 10 simulations (90°) 32
4.5 Power received by the target user and the eavesdropper after 1 simulation (0°) 33
4.6 Power received by the target user and the eavesdropper after 1 simulation (90°) 34
4.7 Cumulative Distribution Function (CDF) of the Signal to Eavesdropper Ratio (SER) (0°)[dB] 35
4.8 CDF of the SER (90°)[dB] 36
4.9 CDF of the Signal to Noise Ratio (SNR) (0°)[dB] 37
4.10 CDF of the SNR (90°)[dB] 38
4.11 Power received by both TU and Eavesdropper over 1 simulation (5cl vs 3cl) 38
4.12 CDF of the SER [dB] (5cl vs 3cl) 39
4.13 CDF of the SNR [dB] (5cl vs 3cl) 39
4.14 Power received by both TU and Eavesdropper over 1 simulation (4cl vs 4cl) 40
4.15 CDF of the SER [dB] (4cl vs 4cl) 40

4.16 CDF of the SNR [dB] (4cl vs 4cl) 41
4.17 Power received by both TU and Eavesdropper over 1 simulation (3cl vs 5cl) 41
4.18 CDF of the SER [dB] (3cl vs 5cl) 42
4.19 CDF of the SNR [dB] (3cl vs 5cl) 42
4.20 Power received by both TU and Eavesdropper over 1 simulation (5cl vs 3cl) 43
4.21 CDF of the SER [dB] (5cl vs 3cl) 44
4.22 CDF of the SNR [dB] (5cl vs 3cl) 45
4.23 Power received by both TU and Eavesdropper over 1 simulation (4cl vs 4cl) 45
4.24 CDF of the SER [dB] (4cl vs 4cl) 46
4.25 CDF of the SNR [dB] (4cl vs 4cl) 46
4.26 Power received by both TU and Eavesdropper over 1 simulation (3cl vs 5cl) 47
4.27 CDF of the SER [dB] (3cl vs 5cl) 48
4.28 CDF of the SNR [dB] (3cl vs 5cl) 48
4.29 SER comparison between the reference fixed beam (left) and the hopping antenna system without AGC (right) (4cl vs 4cl) [dB] 49
4.30 SER comparison between the reference fixed beam (left), the hopping antenna system without AGC (right) and the hopping antenna system with AGC (down) (4cl vs 4cl)[dB] 50
4.31 CDF of the SER [dB]: Influence of radius (4cl vs 4cl) 51
4.32 CDF of the SNR [dB] comparison between the radius in scenario 2 (4cl vs 4cl) 51
4.33 CDF of the SNR [dB] comparison between the radius in scenario 3 (4cl vs 4cl) 51
4.34 3 different patterns [dB] 52
4.35 CDF of the SER with a Half-Power Beamwidth (HPBW) of 10° (top left), 25° (top right) and 60° (down) [dB] 53
4.36 CDF of the SNR with a HPBW of 10° (top left), 25° (top right) and 60° (down)(scenario 3) 53

List of Tables

1.1 Security protocols used in the different layers 4

4.1 Simulations parameters table 27
4.2 Clusters parameters table 28
4.3 Radius parameters table 29
4.4 Beamwidth parameters table 29

Abbreviations

AGC Automatic Gain Control

AOA Angle Of Arrival

AOD Angle Of Departure

AP Access Point

BLAST Bell Labs Ayered Space Time

BPSK Binary Phase Shift Key

CDF Cumulative Distribution Function

CDMA Code Division Multiple Access

CIA Communication Integrity Availability

CSI Channel State Information

DSSS Direct Sequence Spread Spectrum

FDD Frequency Division Duplex

FDMA Frequency Division Multiple Access

FHSS Frequency Hopping Spread Spectrum

HPBW Half-Power Beamwidth

IEEE Institute of Electrical and Electronics Engineers

IP Internet Protocol

IPsec Internet Protocol Security

ISI InterSymbol Interference

ISO International Organization for Standardization

IT Information Technology

LAN Local Area Network

C

LLC Logical Link Control

MAC Media Access Control

MIMO Multiple Input Multiple Output

MISO Multiple Input Single Output

OFDM Orthogonal Frequency Division Multiplex

OSI Open System Interconnection

PAN Personal Area Network

PDU Protocol Data Unit

PIN Personal Identification Number

P

PPP Point-to-Point Protocol

PSK Phase Shift Key

QAM Quadrature Amplitude Modulation

QoS Quality of Service

QPSK Quadrature Phase Shift Key

Rx Receiver

SCSI Small Computer Systems Interface

SCTP Stream Control Transmission Protocol

SDU Session Data Unit

SER Signal to Eavesdropper Ratio

SIMO Single Input Multiple Output

SISO Single Input Single Output

SIR Signal to Interference Ratio

SINR Signal to Interference plus Noise Ratio

SNR Signal to Noise Ratio

STC Space Time Code

SVD Singular Value Decomposition

TCP Transmission Control Protocol

TDMA Time Division Multiple Access

TLS Transport Layer Security

Tx Transmitter

UDP User Datagram Protocol

WAN Wide Area Network

WPA Wi-Fi Protected Access

WEP Wired Equivalent Privacy

Preface

This report is the result of the 10th semester project which has been worked from the 4th February to the 4th of june 2008 by the students of Mobile communications group 08gr1120 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 Beam-Hopping technique. The project has been achieved on the space domain in narrowband, and is based on the mechanical Beam-Hopping technique applied to the Access Point antenna system. This report includes the problem delimitation, and the understanding of the different parameters used in the project.
Once the technical review has been introduced, several scenarios are defined to be investigated, and the simulation model used, "the single scattering model", is detailed. Finally, using the "MATLAB" software simulator, the defined scenarios are simulated in the "single scattering model" to explore the security robustness of the Beam-Hopping method. Then this method is optimized.

MOBcom group 08gr1120

June 2008
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.

Mathieu Gobeaut Richard Tchissambou

Chapter 1

Introduction

1.1 Security overview

1.1.1 Security terms

Security is "the precautions taken to ensure against theft, espionage, or other danger, or the state of being free from danger, damage, or worry condition" [2]. In the general sense, security is a concept similar to safety. The nuance between the two is an added emphasis on being protected from dangers that originate from outside. Individuals or actions that encroach upon the condition of protection are responsible for the breach of security. In our domain, we could define security as the condition that results from establishement and maintenance of protective measures that ensure a state of inviolability from hostile acts of influences [3].
As far as communications security is concerned, [4] defines this term by the measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. Communications security includes several steps:

- cryptosecurity to ensure message confidentiality and authenticity.
- emission security to deny unauthorized persons from intercepting and analysing information.
- physical security to safeguard classified equipments, materials and documents from access or observation by unauthorized persons.
- traffic-flow security to conceal the presence and properties of valid messages on a network.
- transmission security to protect transmissions from interception and exploitation by means such as frequency hopping or spectrum analysis.

Because protecting confidential information is a business requirement and also an ethical and legal requirement, in this report we aim at protecting information from interception by eavesdroppers. First of all we need to define several terms which are parts of security in order to choose which one to investigate. Basically, the information security can be divided into three main goals known as the Communication Integrity Availability (CIA) triad:

- **Confidentiality** of information which means that this information must only be accessed, used, copied or disclosed by persons who have been authorized to do so and only when there is a genuine need to do so. It is required for maintaining the privacy of the people information held by an organization.
- **Integrity** of information which implies that data cannot be created, modified or deleted without authorization. For example when a virus is set up on a computer, there is a loss of integrity because this virus might erase data or files on this computer.
- **Availability** of information which requires that when information is needed, it is available and that the computing systems and the security controls of it function correctly.

To respect those three basics, we could investigate the access control part of a transmission. Of course, only people who are authorized should be able to access protected information. To do so, it is mandatory to explore the foundation on which access control mechanisms are built, which means identification and authentication.

- **Identification** is "the act of determining the properties of something, usually by research or calculation" [5].
- **Authentication** is "the act of validating, finding or testing the truth of something" [6].
- Once a person, a program or a device has been identified and authenticated, it is necessary to determine which resources they are allowed to access and which actions they are allowed to perform. This process is known as **authorization**.

As an important point in protection, security controls should be improveable and upheld. Besides, a log journal should be held as to keep track of failed and granted attempts of authentication. The most effective way to protect information is to transform it into a form unusable by anyone other than an authorized user. **Encryption** allows it. The concept of encryption is to allow only an authorized user to decrypt information thanks to a cryptographic key he is the only one to possess. Cryptography protects information while this is in transit and in storage. For instance, wireless communications can be encrypted using Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA) protocols.

1.1.2 OSI model

Working on security aspects requires some knowledge about communications and computer network protocol design. This network protocol design is often represented by a layered, abstract description and referred to as the OSI model. OSI is an International Organization for Standardization (ISO) standard for worldwide communications. This standard influences the design of computer networking protocols in several layers for the Information Technology (IT) Industry [7]. The OSI model is illustrated in Figure 1.1 where the nature of the data controlled at a level is shown. In Table 1.1.2, we can see a sum up of the layers with their functions and some common security protocols used at each level of the stack. The aim of the OSI model is to divide networks into several components so that it becomes easier to secure them, level by level, and reduces their vulnerabilities.

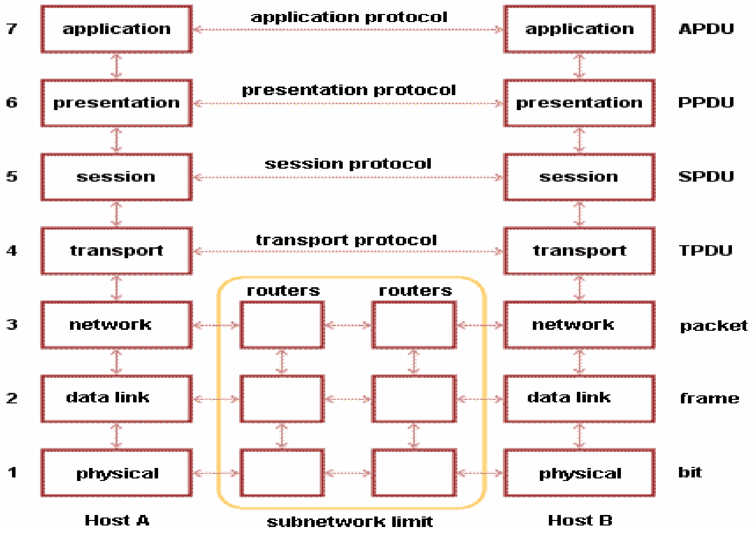


Figure 1.1: OSI Model

Data Unit	Layer	Function	Security Protocols
Data	7.Application	Network process to application	
	6.Presentation	Data representation and encryption	
	5.Session	Interhost communication	SSH, SCP, CHAP [8] [9] [10]
Segment	4.Transport	End-to-end connections and reliability	TLS, SSL [11]
Packet, Datagram	3.Network	Path determination and logical addressing(IP)	IPSec [12]
Frame	2.Data link	Physical addressing (MAC, LLC)	WEP, WPA, WPA2 [13]
Bit	1.Physical	Media, signal and binary transmission	

Table 1.1: Security protocols used in the different layers

Application layer

This layer provides application services for the application processes. It does not perform services to the end user but to user-defined application processes. To maintain security in this layer, anti-virus softwares and firewall systems have been developed to respectively prevent the user from external attacks and to control the access of applications to the network. Finally, applications can also implement their own security controls (assuming that communications will be subject to attack) by requiring the use of strong authentication and encryption to validate and protect data as it travels across the network.

Presentation layer

The presentation layer is susceptible to use different syntaxes and semantics. In fact, the presentation layer allow the data to pass from the application layer into the network. To maintain the security, input should be checked very carefully before being passed into functions that use the input to control operations.

Session layer

Dialogues and connections between computers are controlled by the session layer, which means established, managed and terminated. In the OSI model, this session is responsible for graceful close of sessions, and also for session checkpointing and recovery [14]. Accounts have specific expirations for credentials and authorization. Finally, a limited failed session attempts can be implemented to avoid brute-force attacks on access credentials.

Transport layer

The transfer of data between end users is made transparent and reliable to the upper layers through the transport layer. The reliability of a link is kept thanks to different processes such as flow control, segmentation and de-segmentation, and error control [15]. To maintain security, a protocol named Transport Layer Security (TLS) has been developed to prevent eavesdropping, tampering and message forgery. TLS involves three basic phases:

1. Peer negotiation for algorithm support
2. Key exchange and authentication
3. Symmetric cipher encryption and message authentication

Network layer

The Network layer provides functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks while maintaining the Quality of Service (QoS) requested by the Transport layer. The most famous protocol of this layer is the Internet Protocol (IP) one which manages the connectionless transfer of data one hop at a time, from end system to destination end system through several routers. Internet Protocol Security (IPsec) is a suite of protocols for securing IP communications by authenticating and/or encrypting each IP packet in a data stream. IPsec also includes protocols for cryptographic key establishment.

Data link layer

The data link layer is responsible for the procedures of data transfer between network entities and for detection and correction of errors occuring in the physical layer. Some protocols have been developed on this layer to maintain security, such as WEP or WPA protocols. But these protocols seem not to be strong enough and also difficult to manage for the domestic user. That's why we need to investigate a way to secure the physical layer in a transparent and inherent way for the user as a complement security to the security features obtained in higher layers.

Physical layer

This layer sets all the physical and electrical specifications for devices and particularly the relationship between a device and a physical medium, e.g. layouts of pins, voltages, cable specifications, hubs, repeaters, network adapters, and more. The physical layer guarantees the establishment and termination of a connection to a communication medium, and also its participation in the process whereby the communications resources are effectively shared among multiple users. This layer is in charge of the modulation or the conversion between the digital representation of data in users equipment and the corresponding signals transmitted over a communication channel. These signals operate over the physical cabling, e.g. copper, optical fiber, or over a radio link.

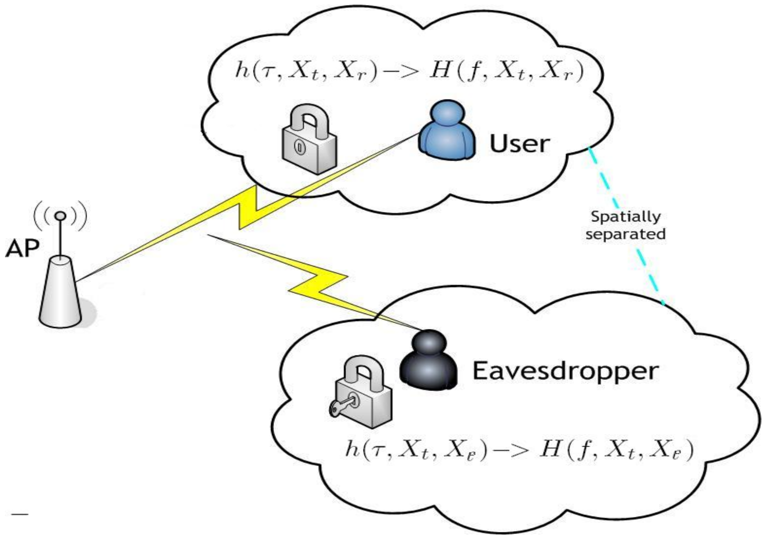
Each layer of the OSI model owns weaknesses and vulnerabilities, but as this thesis refers only to physical layer security, we will only mention about this layer known vulnerabilities and several means to control them. The physical layer can present weaknesses, as listed in [16], such as loss of power, loss of environment control, physical theft of data and hardware, physical damage or destruction of data and hardware, unauthorized changes to the functional environment (data connections, removable media, adding/removing resources), disconnection of physical data links, undetectable interception of data. To control those aforementioned vulnerabilities, it is possible to use some solutions like locked perimeters and enclosures, electronic lock mechanisms for logging and detailed authorization, video and audio surveillance, Personal Identification Number (PIN) and password secured locks, biometric authentication systems, data storage cryptography, or even electromagnetic shielding.

1.2 Target user and eavesdropper: differentiation

The goal of our project is to prevent an eventual eavesdropper from intercepting the information intended to the target user and we focus on the physical layer security aspect. There are several ways to distinguish the target user from the eavesdropper using:

- space
- time

- or frequency domain.



$h(\tau, X_t, X_r) -> H(f, X_t, X_r)$
User
AP
Spatially separated
Eavesdropper
$h(\tau, X_t, X_e) -> H(f, X_t, X_e)$

Figure 1.2: Difference between user and eavesdropper [1]

Figure 1.2 from [1] represents the positions of the access point, the target user and the eavesdropper. This figure differenciates the user from the eavesdropper using two dimensions, i.e. time τ, or frequency f, and space X . The target user and the eavesdropper are spatially separated, so we will be able to differenciate them spatially due to their different spatial locations by nature. Typically, the Access Point (AP) needs to know the users' locations to differenciate them and this is possible by applying in an open loop system. The channel impulse response can be:

- either instantaneous Channel State Information (CSI).
- or averaged CSI.

Given this assumption, the AP is now able to know unique frequency and time profiles for each of the users.
We will use a function called impulse response as the response of our system. The Fourier transform of the impulse response is known as the transfer function. It is usually easier to analyze systems using transfer functions (in frequency domain) as opposed to impulse responses (in time domain), because the calculation are much more easier. Actually we do not have to use a convolution but only a product to calculate the received signal. The Fourier transform of a system's output may be determined by the multiplication of the transfer function with the input function in the complex plane, also

known as the frequency domain. The Fourier transform can be represented through this form:

$$h(\tau, \underline{X}_t, \underline{x}_e) \xrightarrow{F} H(f, \underline{x}_t, \underline{x}_e) \tag{1.1}$$

where h is the impulse response of the system, H is the transfer function, τ is the propagation delay, $\underline{x}_t$ and $\underline{x}_r$ are the space locations of the transmitter and the receiver. The $\xrightarrow{F}$ represents the Fourier transform. The underlined symbols denote vectors. We can easily distinguish with the transfer function the differences between the eavesdropper and the target user.

Then, we have to distinguish two types of system, the closed loop and the open loop one.

- A closed loop system is a system where the transmitter needs to have a feedback. Let us give an example. The AP will send the information to the mobile phone using a downlink connection and will wait for the feedback of the mobile phone through uplink connection.

- An open loop system is a system where the transmitter does not need a feedback from a receiver to proceed. An open loop system is efficient and has low complexity when coupled with average coding. The assumption is that the Uplink is known by the AP and that the Downlink is considered as the same as the Uplink because the movement of the target users and the eavesdropper is quite small in space domain (small area). So the system is quite stable between uplink and downlink because the average response is the same. Scrambling coding is an option of average technique.

1.3 SISO, SIMO, MISO and MIMO system

SISO systems in control engineering usually refer to a simple control system with one input and one output. In radio, it is the use of only one antenna both at the transmitter and receiver side. It is opposed to MISO, SIMO and MIMO systems, which use multiple antennas either at transmitter side, or receiver side or both. It is obvious that MISO, SIMO andMIMO systems present some advantages. They are more robust against a possible eavesdropper because the information will be sent using several antennas, so they improve the transmission performances in terms of diversity, array, multiplexing and interference reduction gains. They are also more robust regarding to the equipment. Indeed, if one antenna is not working, the information can still be sent using the other antennas. The figure 1.3 shows the four different kinds of system. Figure 1.4 shows us a SISO system. On this figure, h denotes the CSI from the AP to the target user. x is the signal sent by the the AP.

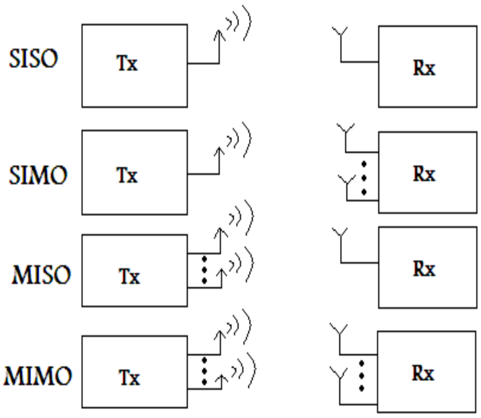


Figure 1.3: SISO, MISO, SIMO andMIMO systems

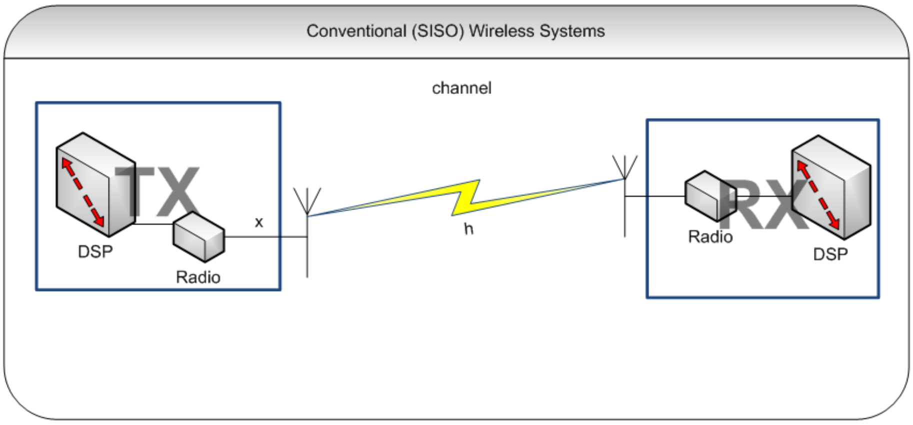


Figure 1.4: Conventional SISO system

1.4 Problem Definition

1.4.1 Motivation

In 2007 a survey [17] sponsored by RSA Security showed that in London Business Center, companies' networks had grown with a 62% factor but that 36% of those networks were vulnerable. This proportion of possibly weak systems becomes bigger if we focus on domestic networks, considering that home users do not spend the same amount of money as companies to secure their network. The home users do not hire specialized technicians to set up their network and be sure that the security level is high enough. Home users usually configure their equipment by themselves and the result is often

not sufficient to guarantee the confidentiality and/or the integrity of their information. Setting up a WEP key to control access to a network is not within the range of everybody and even when it is, this security protocol can be broken using a mere free software that you can find on the web. A WPA encryption protocol has been developed to improve the WEP. However it involves longer sequences of encryption and WEP is nowadays the default protocol of encryption so end users have to activate WPA on their own. Complete beginners in the realm of networks spend a huge amount of time and money on their hotline trying to get through this problem.
To avoid this kind of situations to the common end users who do not have a clue about the security aspects involved during the configuration of their networks, we choose to investigate the security aspect at a lower level so that this process becomes totally transparent to them. In this thesis, we concentrate on smart processes applied in the physical layer to ensure safe and protected data transmissions.

1.4.2 Previous works on security at the physical layer level

In [18], the authors investigate a way to secure communications via waveform coding in MIMO systems. To improve the security of the link, they propose to use multiple antenna systems and to code information. In a student project [1], the main idea is to apply a Singular Value Decomposition (SVD) scheme in a MIMO system between the access-point and the target user, and to avoid the interception and decoding of the signal by eavesdroppers, which means security of the data information in the physical layer in this case. The authors evaluated the performance of the SVD scheme in a MIMO narrowband system, investigated the security of the system regarding the eavesdropper interceptions and finally proposed a trade-off between capacity of the target user and the electronic message. In [19], the authors investigate a way to enhance the security of wireless sensor network, using two randomized array transmission schemes to secure wireless sensor network at the physical layer. They assume that the unauthorized user have a good received quality of the signal and is aware about all the transmission protocols. [20] proposes an interesting method to secure the transmission at the physical layer as well. The idea is to induce a deterministic noise-like interference to the undesired receivers. The results are shown through simulations by measuring the upper bound of the information-theoretical secrecy and error performances.
Many works were already driven on physical layer wireless security, but there is still some interesting point to investigate. [18] , [1], [19], [20], [21], [22]

1.4.3 What can be further investigated in the physical layer security?

While reading several works on the subject, we pointed out three main aspects of the physical layer wireless security which could be interesting to develop.

Fingerprinting

Fingerprinting can be implemented in several ways. It can:

- consist of using the medium to carry overlay information on top of the baseline information. This overlay information can be either a part of the transmitted data in order to increase the rate performance or an encryption key to improve the link security [18]. This can be referred to as "stream fingerprinting".
- consider modulation of bits with several modulations techniques such as two Binary Phase Shift Key (BPSK) modulations instead of one Quadrature Phase Shift Key (QPSK) to decode the transmitted signal. The bit rate is decreased but the security is increased because an eavesdropper does not know which kind of modulation has been used. This can be referred to as "‘modulation fingerprinting".

It would be interesting to investigate this latter part to see if sufficient security level can be achieved and if eavesdropping can be prevented. Basically, we could focus on the bit level to check if data may be corrupted as previous work [18] on the former part showed some satisfying results at block and symbol levels.

Imperfect CSI

The difficulty considering imperfect CSI is to differenciate the eavesdropper from the target user. It is possible that in this case, the eavesdropper has a better signal than the target user and some smart technique should help to solve this problem. It is very interesting to investigate this work because it is very close to the reality. Moreover, all previous works on physical security had always taken into account a perfect CSI.

Beam Hopping

Using average CSI would allow us to spend less time on measuring instantaneous CSI. Basically, the smart point would be to apply a beam hopping pattern to the system so that the AP would 'jump' from a beam to another to reach the target user, trying to avoid interception of his signal by an eavesdropper.

1.4.4 Our problem choice

Previous works on security at physical layer [1], [18]- [22] introduced closed loop systems with multiple input antennas at the transmitter side as to be able to estimate instantaneous channel impulse responses. As a security aspect, we want to investigate a more simple model requiring an open loop system which allows us to use average CSI by assuming that the CSI in dowlink is the same as the uplink ones. To do that, we will test the efficiency of a beam-hopping pattern applied to the AP who would jump from a beam to another to reach a given target user represented by several clusters in the far-field of the AP's indoor service area. It might create a very turbulent state at a possible eavesdropper.

Since the AP has no feedback from any user because of open loop assumption, it can only deal with directional CSI. Thanks to this directional consideration, a SISO system can be applied, which means that both AP and users are equipped with a single port antenna. This ensures low hardware complexity at both sides, assuming that the receiver is a mobile station such as a handportable device. The AP is able to scan the environment thanks to a beam pattern $A(\theta)$ it will sweep along the service area in order to get directional CSI and compute the power response $E(\theta)$ of the environment. Several clusters are randomly located in the service area and each cluster is constituted of 20 scatterers, so the AP could change the direction of the beam with respect to the directional response of the environment. A target user and a possible eavesdropper are distinguished in this open loop SISO system by their clusters' spatial location, but we don't know anything about the eavesdropper as he is only listening and not broadcasting.

Figure 1.5 represents our scenario considering only the AP and the target user represented by his different clusters. One beam $A(\theta)$ is created by the AP and swept along the service area. The average CSI over all the scatterers from each cluster allows the AP to estimate the response of the environment $E(\theta)$ with respect to the directions θ it scanned.

We consider the presence of an eavesdropper in the simulation environment who stays completely transparent to the AP. We will estimate the average power received by the target user and the eavesdropper over several positions of the clusters in the room. Then, we will process a power control to guarantee the target user with receiving the same amount of power during his whole communication. This should make the power received by the eavesdropper more erratic. The results of these cases will be compared with a fixed beam applied to the AP to conclude about the efficiency, confidentiality and integrity of data guaranteed by the beam hopping technique to a target user.

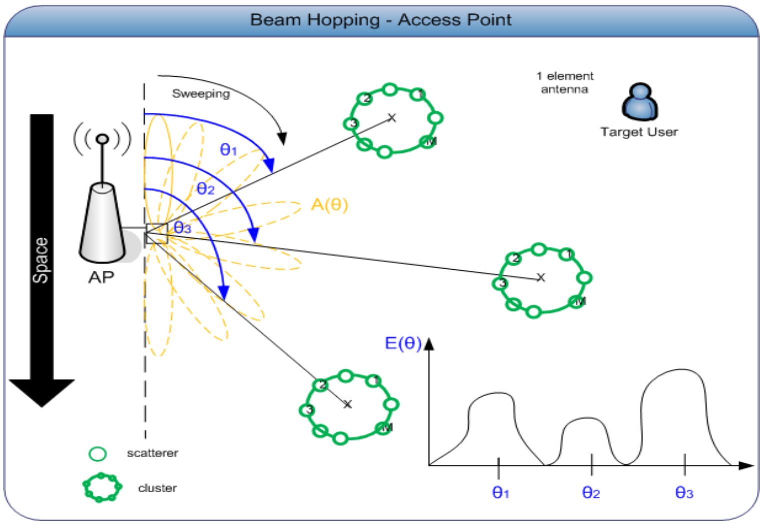


Figure 1.5: Beam Hopping applied by AP

Chapter 2

System description and Environment

2.1 System layout

2.1.1 System

Our system is described in Figure 2.1. The goal of the AP is to maintain a stable link to the target user, as we don't know anything about the eavesdropper. This can be done assuming that the downlink CSI is equal to the uplink CSI, i.e. an open loop system is applied because of very few changes in the space location of the target user and consequently in the channel impulse response which can be averaged. The AP is constituted by a single input antenna. It will be able to generate a beam and sweep it along the service area of dimensions (D_1, D_2). The randomly located target user is composed of only one antenna for low hardware complexity and cost. This target user is associated with several randomly located uniformly distributed clusters in the service area with an angle $\theta_{cluster}$ from the AP, and a radius of $1m$. We assume that this assumption of the radius fits to different things we can find in an indoor environment, as for example a bookcase, a table or a bed. Several scatterers are randomly located on these circular clusters in the service area to establish multipath and are uniformly distributed. All the scatterers have the same amplitude but their phase are different with uniform distribution, assuming uncorrelated scattering which means incoherent voltage summation, i.e. non coherent power summation. Finally the eavesdropper is also randomly located in the service area, composed of a single antenna and associated with its own randomly located uniformly distributed clusters of scatterers. Its goal is to intercept the signal sent by the AP to the target user.

Our system can be considered as a SISO system, because we have a single

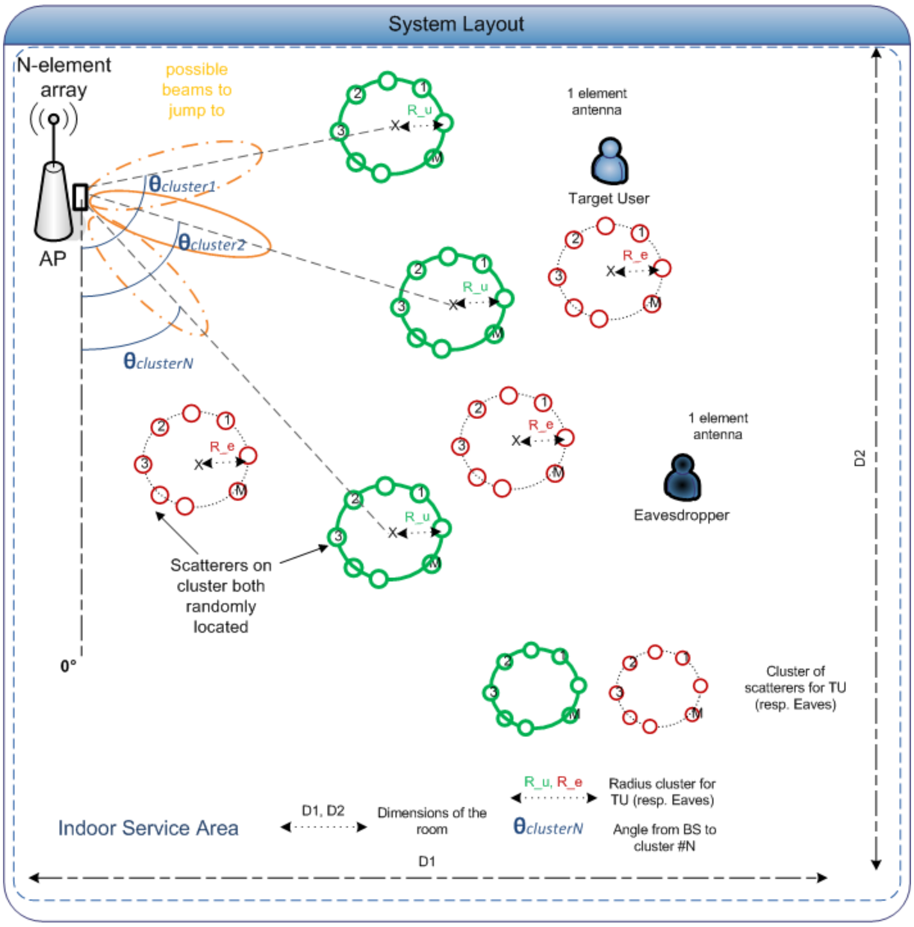


Figure 2.1: System layout

antenna at both transmitter (the AP) and receiver sides (the target user and the eavesdropper).

For a general SISO system, the transmitted signal is:

$$y(t) = \overline{h_k(t)} \otimes x(t) \tag{2.1}$$

where $y(t)$ denotes the output of the AP's antenna, $\overline{h_k(t)}$ is the average channel impulse response relative to the AP's antenna and the cluster k. $x(t)$ is the signal sent by AP.

2.1.2 Antenna system

One important aspect of our project is the characterization of the beam. Therefore, the sort of pattern we will create is not important, we can con-

sider a pattern with only one beam. Indeed, we will consider this kind of pattern for simplicity in our scenarios. What we need to consider here is the HPBW, i.e. the angle covered by the pattern of the AP and associated to the halved power transmitted.In our scenarios, we will vary the width of the beams to see the influence on the power received by both target user and eavesdropper.
As we only need to deal with directional responses, we will use a simple directional antenna with a directional pattern. Moreover, a mechanical system will allow us to steer the pattern in the chosen direction.

2.1.3 Channel

Before going into the channel model, we will explain how the signal can be modified when it is sent from the transmitter to the receiver. Three kinds of mechanism can perturb a signal: reflections from large object, diffractions of electromagnetic waves, and signal scattering:

- We can observe reflections when a wave impinges on a smooth surface with very large dimensions compared to the Radio Frequency signal wavelength.
- We can observe diffraction when the path between transmitter and receiver is obstructed by a dense body with large dimensions compared to the wavelength.
- Finally, we can observe scattering when a wave impinges on either a large rough surface or any surface whose dimension are on the order of the wavelength.

All these perturbations of signal lead to a phenomenon called multipath effect. The receiver will receive the signal from two or more paths. In our project, we have to take into account this multipath phenomenon because for example, we can consider this transmission will be between a base station and a mobile phone, and all these effects (diffraction, reflection, scattering) happen to occur in the far-field of an indoor environment. To respect the far-field consideration, the distance d between the AP and a cluster must respect the following condition:

$$d \geq \frac{2*D^2}{\lambda} \tag{2.2}$$

where D is the size of the AP's antenna and λ is the wavelength. If we set $\lambda = 12.5cm$ (i.e. $f_c = 2.4GHz$) and $D = 20cm$, $d \geq 0.64cm$ which is really small compared to the dimensions of the indoor environment and always respected. This is why the center of the clusters should be located not closer to the AP than $1.64m$ for clusters with 2 meters diameter.

We will consider an indoor service area of dimensions $(D_1 \gg \lambda, D_2 \gg \lambda)$, e.g. an amphitheater, and an average CSI, because of open loop SISO system. The target user's small movements imply fading channel manifestations called "small-scale fading". Indeed, motion causes doppler shift in the received signal components. To build our channel model, we can use the Rayleigh fading channel model. Rayleigh fading is a model used when there are many objects in the environment which scatter the radio signal before it arrives at the receiver. Rayleigh fading is most applicable when there is no dominant propagation along a line of sight between transmitter and receiver. This model assumes that the magnitude of a signal will vary randomly, or fade, according to a Rayleigh distribution. We consider narrowband case for simplicity.

2.1.4 Power consideration

We will use a power modelling to model the quality of signal received by the target user. What the target user receives fully depends on what the cluster gets. As the AP only broadcasts towards what he can see, i.e. the clusters, the power received by a cluster from the AP will represent the power received by the target user with respect to our previous small-scale fading assumption. It means that we do not need to consider the signal from the scatterer to the target user, we just take into account the signal from the AP to the different scatterers.

The instantaneous and average CSI are calculated as following:

$$h_{i,k} = A \times \exp(j\phi_{i,k}) \times \exp(\tfrac{j \times 2\pi \times L1_{i,k}}{\lambda}) \tag{2.3}$$

$$\overline{h_k} = \sqrt{\tfrac{(\sum_{i=1}^{N_{scatt}} |h_{i,k}|^2)}{N_{scatt}}} \tag{2.4}$$

where $h_{i,k}$ is the instantaneous channel impulse response from AP relative to the scatterer i in cluster k, A is the amplitude of the scatterer and $\phi_{i,k}$ represents the phase of the scaterrer i in cluster k. $L1_{i,k}$ is the distance from AP to the the scatterer i in cluster k, λ is the wavelength. N_{scatt} is the number of scatterers in one cluster ($N_{scatt} = 20$ in our case), and $\overline{h_k}$ is the average impulse response from AP to cluster k.

Knowing the average CSI allows us to calculate the average power received by AP from each target user's clusters (uplink communication)

$$Pr_{i,k} = |h_{i,k}|^2 \times Pt_{TU} \tag{2.5}$$

$$\overline{Pr_k} = \tfrac{(\sum_{i=1}^{N_{scatt}} Pr_{i,k})}{N_{scatt}} \tag{2.6}$$

where $Pr_{i,k}$ is the received power at AP's antenna from the scatterer i in cluster k, Pt_{TU} is the normalized power sent by the target user and $h_{i,k}$ is the instantaneous channel impulse response (see equation (2.3)). N_{scatt} is the number of scatterers in one cluster ($N_{scatt} = 20$ in our case) and $\overline{Pr_k}$ is the average power received by AP from cluster k.

To obtain the average power received at a cluster, we compute the Friis transmission equation in far-field which is:

$$\overline{Pr_{cluster}k} = Pt \times G_{AP}(\theta_{cluster}k) \times \left(\frac{\lambda}{4\pi \times L1i,k}\right)^2 \tag{2.7}$$

where Pt is the transmitted power by the AP's antenna set to $20dBm$, $G_{AP}(\theta_{cluster}k)$ is the antenna gain of the AP towards cluster k, λ is the wavelength, $L1i,k$ is the distance between AP and the scatterer i in the target user's cluster k.

As our system is considered as an open loop, we assume that the downlink(from AP to target user) is the same as the uplink because of a small change in the space location of the target user. So if we look at Figure 2.2, we can see what happens during an uplink communication when a scatterer affects the average channel impulse response with its proper amplitude A and phase phi with respect to distances L1 and L2.

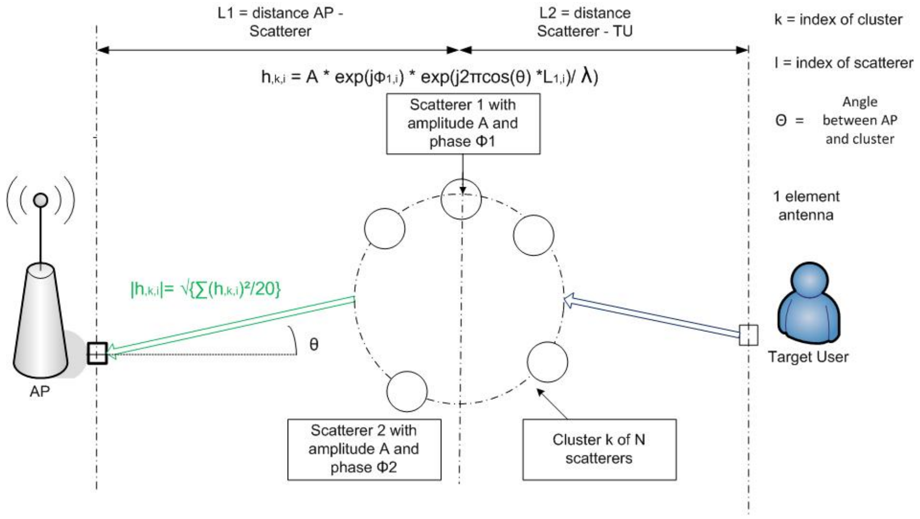

L1 = distance AP - Scatterer
L2 = distance Scatterer - TU
k = index of cluster
I = index of scatterer
h,k,i = A * exp(jΦ1,i) * exp(j2πcos(θ) *L1,i)/ λ)
Scatterer 1 with amplitude A and phase Φ1
Θ = Angle between AP and cluster
1 element antenna
|h,k,i|= √{∑(h,k,i)²/20}
θ
Target User
AP
Scatterer 2 with amplitude A and phase Φ2
Cluster k of N scatterers

Figure 2.2: How scattering affects the average channel impulse response

Our main parameters for our channel model are:

- center frequency: $f_c = 2.4GHz$
- service area dimensions: $D1 = 30m, D2 = 30m$

- number of target user: $nb_{user} = 1$
- number of eavesdropper: $nb_{eaves} = 1$
- radius of cluster: $1m$
- transmitted power by the AP's antenna: $Pt = 20dBm$
- noise floor: $N = -80dBm$
- number of clusters according to ref. [23], [24]
  - Scenario 1
    - number of target user's clusters: $nb_{user}cluster = 5$
    - number of eavesdropper's clusters: $nb_{eaves}cluster = 3$
  - Scenario 2
    - number of target user's clusters: $nb_{user}cluster = 4$
    - number of eavesdropper's clusters: $nb_{eaves}cluster = 4$
  - Scenario 3
    - number of target user's clusters: $nb_{user}cluster = 3$
    - number of eavesdropper's clusters: $nb_{eaves}cluster = 5$
- number of scatterers per cluster: $nb_{scatt} = 20$

2.2 Algorithm

The system performance can be divided in two types as referred in [25].

- *The Acquisition Phase* is the state when the array is sweeping his pattern (or beam) along the environment. At the beginning, the AP creates a beam in a direction and gets the directional channel response from the clusters. Then it sweeps this beam to another direction and gets another directional channel response from the clusters as shown in Figure 2.3. In this Figure, any eavesdropper is represented as we don't have any directional response from him. When all the directions have been explored, the AP obtains the directional power profile (Figure 2.4) of the service area and goes to the Operation Phase. The sweeping measurement response is calculated as following:

  $$M(\theta) = \oint_{\theta} E(\theta).A(\theta - \theta_{cluster})d\theta \tag{2.8}$$

  As we assume uncorrelated scattering, which means incoherent power summation, the equation (2.8) reduces to:

$$M(\theta) = E(\theta) \otimes A(\theta - \theta_{cluster}) \qquad (2.9)$$

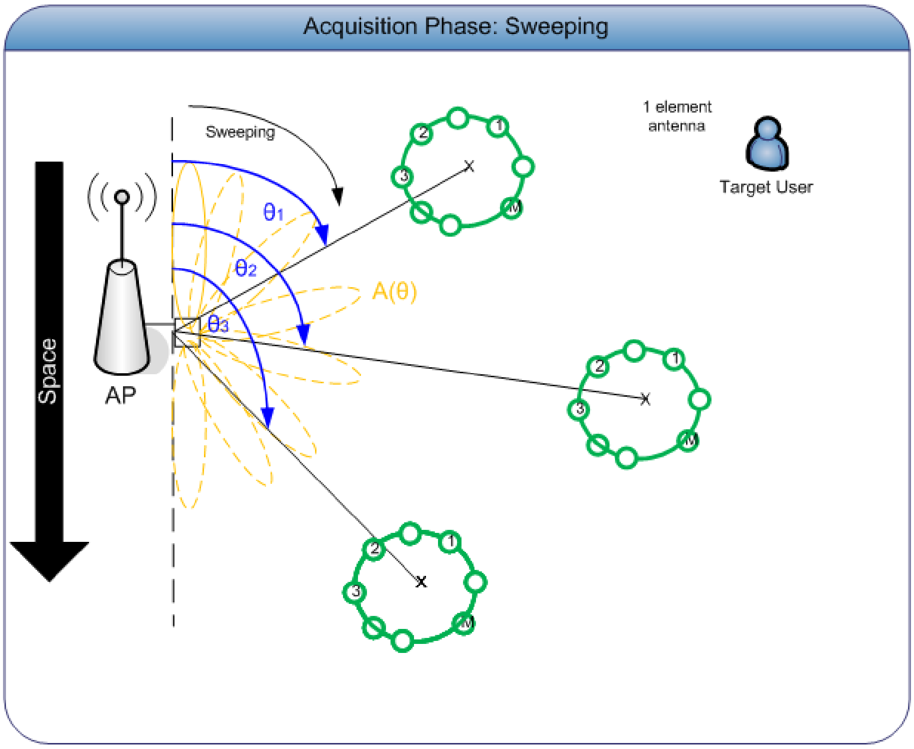


Figure 2.3: Aquisition phase

- *The Operation Phase* (after the Acquisition Phase) is a state where the array chooses the direction corresponding to the best directional channel response (consequently the highest power) to sweep his beam and send his signal (Figure 2.5). Finally, to guarantee the target user a good quality of signal throughout the sweeping process which means a constant power received, we apply to the array a power control algorithm. This power control is making sure that the target user always receives the same amount of power by sending an appropriate amount of power in the direction of a given cluster. This process would avoid the eavesdropper to receive a decent and constant power and so to listen to the target user's communication.

  We can remark in our algorithm that for each position of the clusters, we are sweeping the pattern along the whole environment to get the directional responses which will be used to jump from a cluster to

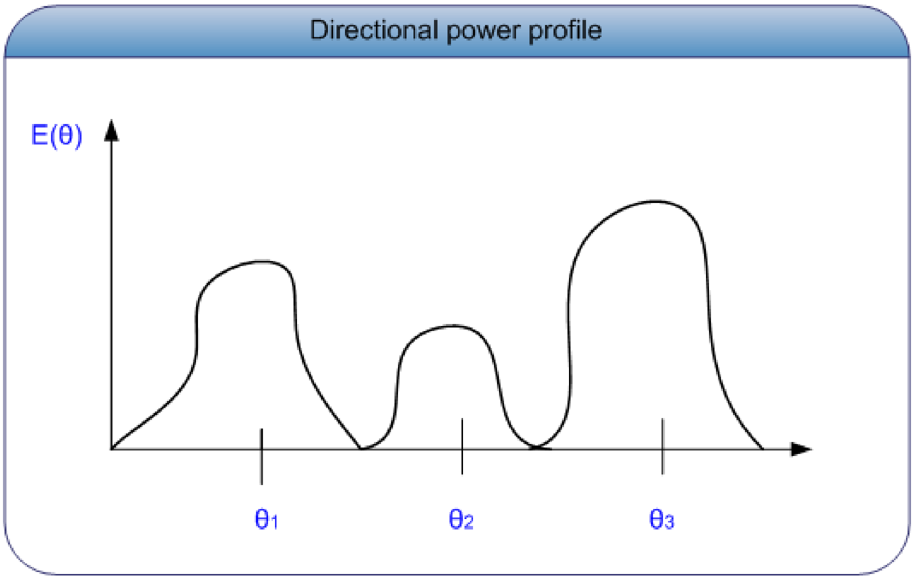


Figure 2.4: Directional power profile

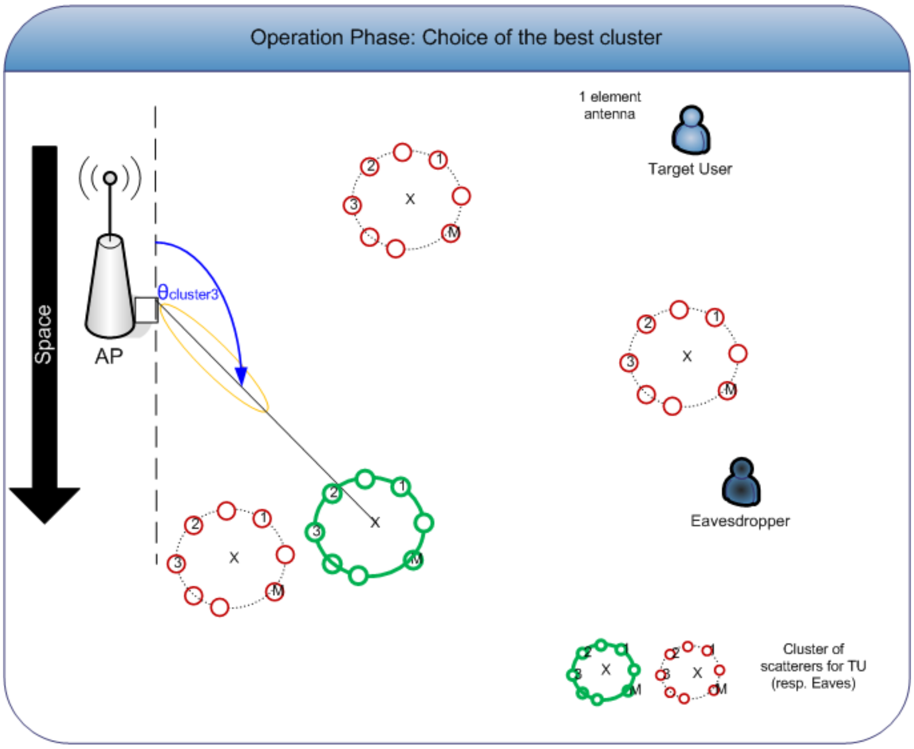

Operation Phase: Choice of the best cluster
1 element antenna
Target User
Space
AP
θcluster3
1
2
3
M
X
Eavesdropper
Cluster of scatterers for TU (resp. Eaves)

Figure 2.5: Operation phase

another to send the desired signal to the target user. It consists of our beam sweeping/hopping algorithm.

The implementation parameters of the Matlab code are given in the next part of this report.

Chapter 3

Implementation

3.1 Simulation conditions

The service area is defined thanks to the AP, which is set up at the origin of the axes as shown in Figure 2.1. The service area will not exceed 30m*30m, as we consider an indoor environement such as an amphitheater. The AP is constituted by a single antenna.

The target user is randomly located in the defined service area, and his circular clusters are constituted by 20 scatterers located on the circle. The radius of the circle is set to $1m$ and changed to $1.5m$ for comparison. The scatterers are randomly uniformly distibuted on the circle. The amplitude of each scatterer is $1dB$ but their phase is randomly chosen.
The eavesdropper is also randomly located in the defined service area, and his circular clusters are constitued by 20 scatterers located on a circle. However, we don't know anything about the eavesdropper, like his position or his power as he is not emmiting any signal. The eavesdropper is only listening and trying to intercept any other signals.
A Rayleigh fading environment is assumed and the angular spread is set to 0°. To represent the Rayleigh distribution we will consider 20 waves (because of the 20 scatteres) arriving at the AP (knowing that a minimum of 8 waves are necessary to represent a Rayleigh distribution) [26]. The amplitude of each of these waves is the same while a random phase is generated for each of them.

As a reminder, the average power received at a cluster is calculated as following:

$$\overline{Pr_{cluster}k} = Pt \times G_{AP}(\theta_{cluster}k) \times \left(\frac{\lambda}{4\pi \times L1i,k}\right)^2 \tag{3.1}$$

where Pt is the transmitted power of the AP set to $20dBm$ in our simulations, $G_{AP}(\theta_{cluster}k)$ is the gain of the AP set to either $5dBi$, $8dBi$, $9dBi$, or $10dBi$ depending on the beamwidth of its beam pattern. $L1i,k$ is the distance between the AP and the cluster concerned. The gain of the cluster is set to 1 or $0dBi$ so this is why it does not appear in the equation.

In our project, we evaluate and compare the power received by the target user and the power received by the eavesdropper when the AP is equipped with a mechanically sweeping antenna. All the results will be shown in the next chapter.

3.2 Parameters definition and scenarios

The noise floor in our simulations is set to $-80dBm$ which seems to be a realistic threshold for an indoor service area as shown in [27] and [28].

The SER is a parameter we will use to check when the amount of power received by the target user is superior to the power received by the eavesdropper. This parameter is given by the relationship:

$$SER = \frac{S}{E} \tag{3.2}$$

where S is the power received by the target user, E is the power received by the eavesdropper. We will plot the CDF of the SER.

The SNR is an absolute parameter we will check to evaluate the efficiency of our results as the SER is just a relative value. This parameter is given by the relationship:

$$SNR = \frac{S}{N} \tag{3.3}$$

where S is the power received by the target user or eavesdropper, N is the noise floor in the service area set to $-80dBm$. We will plot the CDF of the SNR.

The power received by the target user P_{user} (resp. eavesdropper P_{eaves}) is a parameter used to evaluate the amount of power received after one simulation, knowing that we consider 200 different positions of both target user and eavesdropper's clusters in one simulation. We will plot this curve and check how often the power of the eavesdropper is higher thant the target user's one. Then we will make an average of this power over 10 simulations. One point of this curve will represent an average of the power received by the target user P_{user} (resp. eavesdropper P_{eaves}) over 200 positions of clusters. Afterwards, we will make the same simulations using a power control, which will allow us to adjust the power sent by the AP so that each cluster receives the same amount of power. All these results will be compared with a reference, which is a non hopping antenna.

To do that we will consider 3 scenarios:

- Fixed beam: This first scenario will be the reference, what will allow us to see if the solution we propose will perturbate the signal received by the eavesdroper.
- Beam hopping: In this scenario, we will use a beam hopping system to send the signal to the target user. The algorithm described below will allow us to jump between clusters to send this signal to the one receiving the highest power.
- Beam hopping + AGC: We will add to the previous scenario a power control, which makes the power of the signal received by the target user always constant.

3.3 Procedure

Let us describe the procedure we will follow to plot the results of our simulations. This procedure is divided in two steps:

- acquisition phase
- operation phase

  We will repeat these two steps each time we will repeat our algorithm.

3.3.1 Acquisition phase

- for each position of the clusters
  - sweep the service area

  - find the directional responses of the clusters of the target user
  - estimating the average CSI from each cluster of the target user to AP (see equation (2.3))
  - adapt the beam towards the cluster, which presents the best CSI

3.3.2 Sending of the information

- for each position of the clusters
  - computing the power received by the AP from each cluster (see equation (2.6))
  - computing the gain towards the cluster with the best CSI
  - estimating the received power at this chosen cluster of the target user (see equation (3.1))
  - adapting the power so that each cluster receives the same amount of power (Power control)
  - estimating the received power at each cluster of the target user and eavesdropper (see equation (3.1))
  - comparing those received signals to the noise floor.

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 number of clusters for both target user and eavesdropper, the radius of these clusters and the beamwidth of the main beam in the radiation pattern of the AP. Table 4.1 below, is a brief reminder of the different parameters we changed during the simulations of all the scenarios.

Simulation parameters			
	Scenario 1: Reference	Scenario 2	Scenario 3
Power management	Fixed Beam	Beam Hopping	Beam Hopping + AGC
Number of positions of the clusters in 1 simulation	200	200	200
Number of simulations	10	10	10

Table 4.1: Simulations parameters table

The AGC power management consists of guaranteeing the target user with a constant amount of power received, i.e. a dynamic power allocation at AP before transmitting its signal. The number of positions of the clusters per simulation is set to 200 for both target user and eavesdropper's clusters which means that these clusters will be moved 200 times to uniformly distributed random locations in the service area during 1 simulation. The number of simulations represents how many times both target user and eavesdropper are moved to uniformly distributed random locations in the service area. As we consider 10 simulations, this means that the clusters will change positions

$200 * 10 = 2000$ times over all the simulations.

Below is a Table 4.2 summarizing the parameters related to both target user and eavesdropper's clusters .

Clusters parameters			
	Scenario 1	Scenario 2	Scenario 3
Number of scatterers per cluster	20	20	20
Number of target user's clusters	4	5/4/3	5/4/3
Number of eavesdropper's clusters	4	3/4/5	3/4/5
Radius of clusters [m]	1	1	1

Table 4.2: Clusters parameters table

For scenario 2 and scenario 3 the results will be divided in three parts:

- when the target user is associated with more clusters than the eavesdropper
- when the target user and eavesdropper are associated with the same number of clusters
- when the target user is associated with less clusters than the eavesdropper

Inside each of these parts we will focus on three representative figures. The first interesting plot to check is the average power received by both target user and eavesdropper for each movement of the clusters within one simulation. This tells us about the efficiency of the antenna pattern. Then we focus on the average power received by both target user and eavesdropper for every movement of the clusters over all the simulations which allows us to have a more general view of the amount of power received over a huge number of locations considerations. Then we look at the CDF of SER to check how often the target user has a better signal than the eavesdropper. Obviously, the more often the target user has a better signal, the more efficient is the antenna pattern management. Finally, we observe the SNR for both target user and eavesdropper to see if the eavesdropper's clusters are located close to the target user's ones.

Afterwards, we will focus on the effects of the radius and the beamwidth of the antenna pattern on the power received by both target user and eavesdropper's clusters.

Below are two Table 4.3 (resp.Table 4.4) summarizing the parameters related to both target user and eavesdropper's radius (resp. beamwidth).

Radius parameters			
	Scenario 1	Scenario 2	Scenario 3
Number of scatterers per cluster	20	20	20
Number of target user's clusters	4	4	4
Number of eavesdropper's clusters	4	4	4
Radius of clusters [m]	1/1.5	1/1.5	1/1.5

Table 4.3: Radius parameters table

Beamwidth parameters			
	Scenario 1	Scenario 2	Scenario 3
Number of scatterers per cluster	20	20	20
Number of target user's clusters	4	4	4
Number of eavesdropper's clusters	4	4	4
Beamwidth [°]	60°	10°/25°/60°	10°/25°/60°

Table 4.4: Beamwidth parameters table

The last part of this chapter will compare the results obtained with a reference.

Figure 4.1 below represents the response of the environment. We take into account this information in every scenario to be able to choose the direction of the pattern. We observe that the best received power from the environment comes from the direction 100-120° on this figure so the AP will mechanically hop its beam towards this direction. This figure is quite flat because in this case, the target user's clusters are quite close to each other, which leads to a smooth response of the environment.

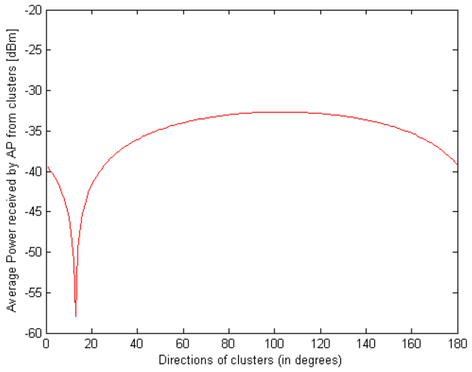


Figure 4.1: Environment response

4.1 Influence of the number of clusters

4.1.1 First scenario : Fixed beam

This first scenario will be used as a reference for the next scenarios. Indeed, we will consider a fixed beam pattern, which will be used to send the information towards the target user and the eavesdropper. In this simulation, we consider 4 clusters for both target user and eavesdropper. The radius of the cluster is set to $1m$. The signal will be sent in a random direction and we will estimate the power received by both target user and eavesdropper, using two different orientations of the beam: 0° and 90°.

Beam pattern

Figure 4.2 represents one of the two fixed patterns used in this scenario, this one being oriented at 90°. We will compare the results obtained using a pattern oriented in the 90° direction and a pattern oriented in the 0° direction. Their half-power beamwidth is of 60° for an antenna gain of $5dBi$. Making a comparison of the results we will obtain with this two fixed beams is interesting because we should theoritically obtain the same SER for the two orientations of the beam as the clusters for both target user and eavesdropper are randomly uniformly located.

Average power received

Figure 4.3 (resp. Figure 4.4) represents the average power received by both target user (full line with stars) and eavesdropper (dotted line with diamonds) considering a beam with an orientation of 0° (resp. 90°). The shape and value obtained are similar on both figures. The orientation of the beam doesn't influence the results, because we are considering the same number of clusters for both target user and eavesdropper and all the clusters are randomnly located. So the closer to the AP one cluster is, the higher power he receives during the simulation. It is relevant that the received power is slightly higher (around 1dB better) with a beam oriented at 90° since the maximum values of the gain can be reached on both sides of the beam whereas it can only happen on the left side of the beam for a 0° oriented beam (the service area is 180° wide from the AP's point of view).
Figure 4.5 and Figure 4.6) showing the power received for each new position of the clusters lead to the same observation with a minimum

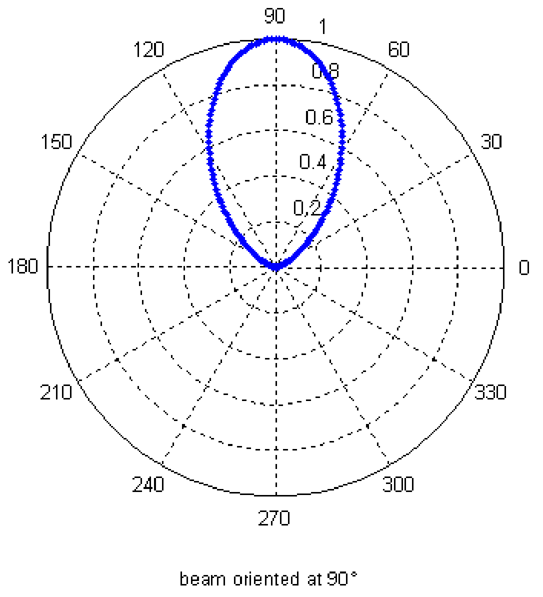


Figure 4.2: Fixed beam oriented in the 90° direction

value of received power by the target user of $-79dBm$ for a 90° oriented beam and $-89dBm$ for a 0° oriented beam which exceeds the noise floor and is not usedul to the target user. The same difference is observable for the minimum power received by the eavesdropper.

SER

Figure 4.7 and Figure 4.8 represent the CDF of the SER with an orientation of the beam of 0° and 90°. The results are in compliance with what we expected. Indeed, the power received by the target user is equal or higher than the power received by the eavesdropper on both curves 50% of the time. This is because all the clusters are randomnly located, so we have equal chances to have a cluster of a target user (resp.eavesdropper) closer than a cluster of an eavesdropper (resp.target user) to the AP. These results will be considered as a reference for the others scenarios.

SNR

In Figure 4.9 and Figure 4.10 are shown the CDF of the SNR for both orientations of the beam. The target user and the eavesdropper present almost the same curves still because of the randomness of their clusters location. Their maximum SNR is of $60dB$ for both of them.

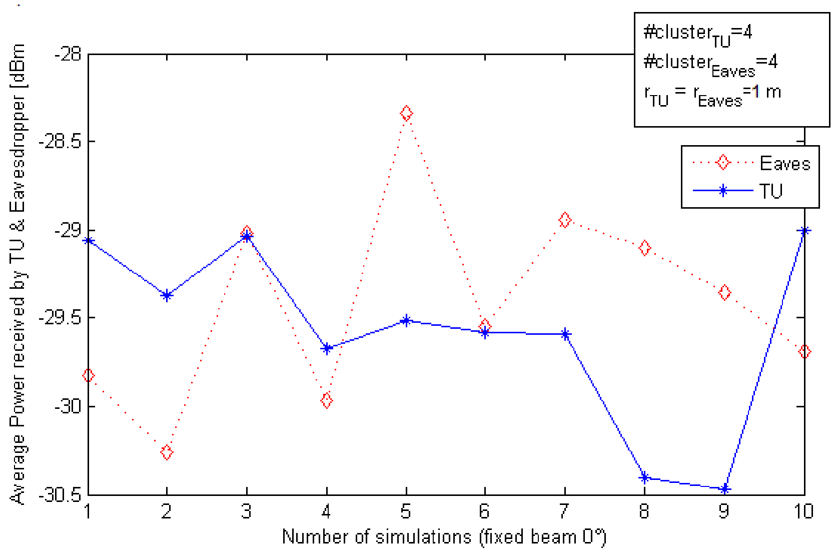


Figure 4.3: Average power received by the target user and the eavesdropper after 10 simulations (0°)

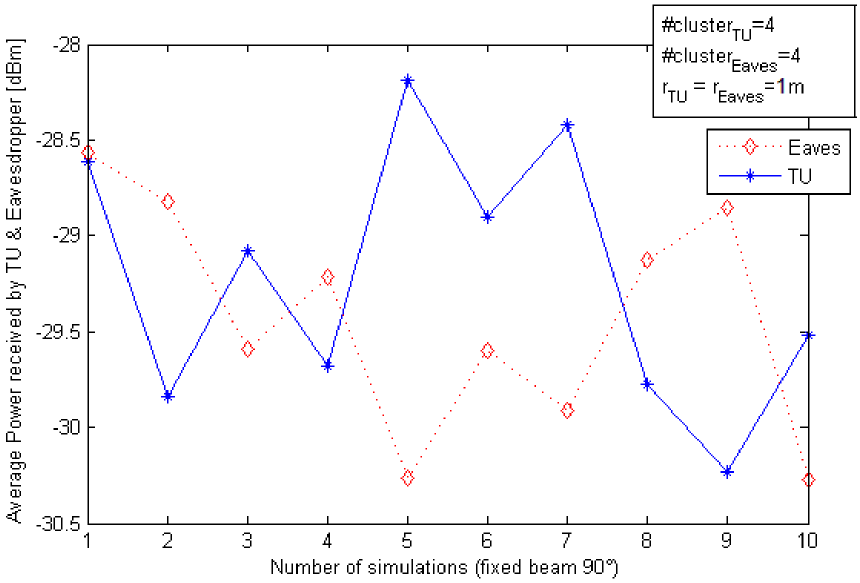


Figure 4.4: Average power received by the target user and the eavesdropper after 10 simulations (90°)

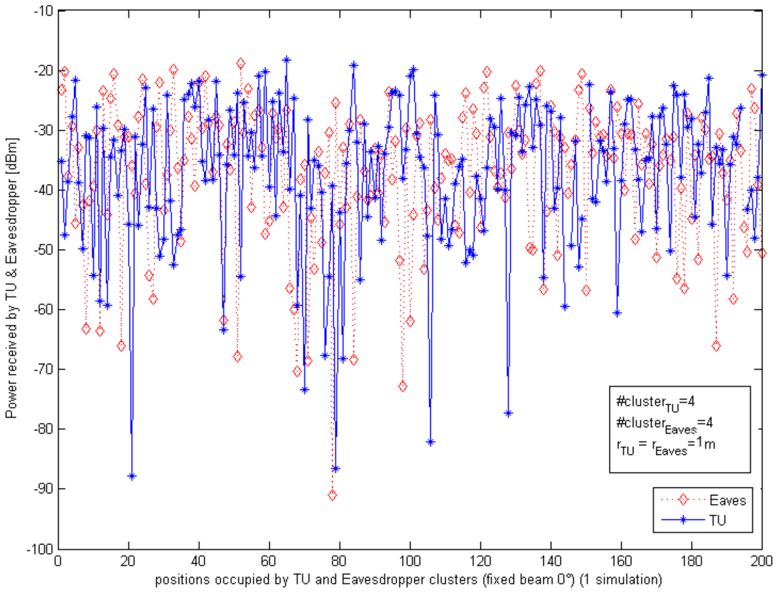


Figure 4.5: Power received by the target user and the eavesdropper after 1 simulation (0°)

They should support the same modulation rate and it would be possible for the eavesdropper to decode the target user's signal.

4.1.2 Second scenario : Beam-Hopping

In this scenario, we apply a beam-hopping technique to the AP's pattern so it can sweep its beam along the environment to get its response and choose one of the target user's cluster to 'jump' its beam towards.

The target user is associated with more clusters than the eavesdropper

In this case, we considered 5 clusters for the target user and 3 clusters for the eavesdropper.

In Figure 4.11, we can see that the power received by the target user (full line with stars) is most of the time better than what the eavesdropper receives (dotted line with diamonds) due to more clusters

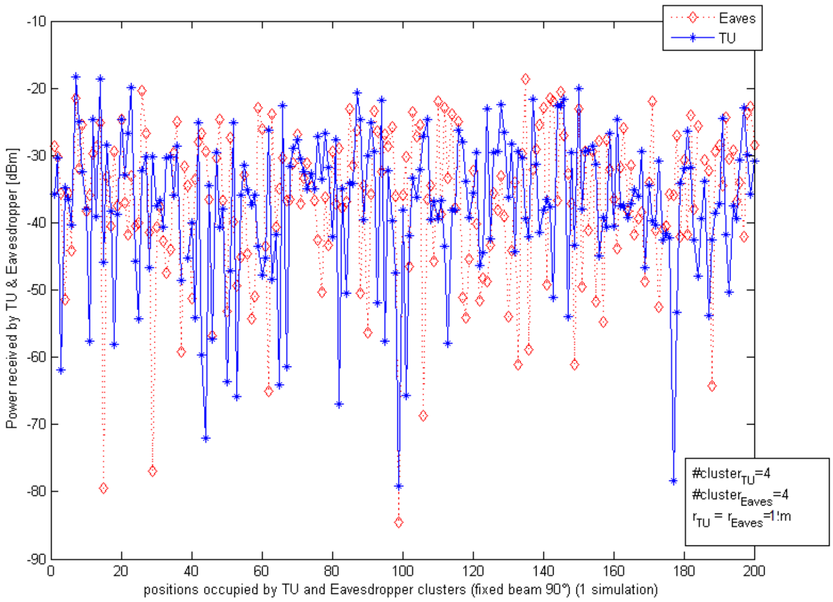


Figure 4.6: Power received by the target user and the eavesdropper after 1 simulation (90°)

located in the service area giving less chances to the eavesdropper to catch the signal sent by the AP towards one of the target user's cluster.

Then, the plotted CDF in Figure 4.12 shows that the eavesdropper receives a higher power from the AP than the target user in less than 18% of the cases. In other terms, the target user has a better quality of signal in 82% of the simulations with a bigger number of clusters associated with him. As another reference, the target user reaches a 30 dB higher power than the eavesdropper in 10% of the simulations.

In Figure 4.13, it is obvious that the SNR (steeper curve on the right) of the target user is very good and steep (i.e. stable signal) compared to the eavesdropper (curve on the left) and always above $40dB$. However for the eavesdropper this ratio happens to be negative in a few cases, i.e. the eavesdropper is unable to catch any exploitable signal and its curve is really flat compared to the target user's one meaning that its signal is erratic. Besides, in 20% of the cases considered, the difference between the 2 ratios is bigger than $18dB$ which is quite interesting if we consider a suitable modulation rate for the target user's signal.

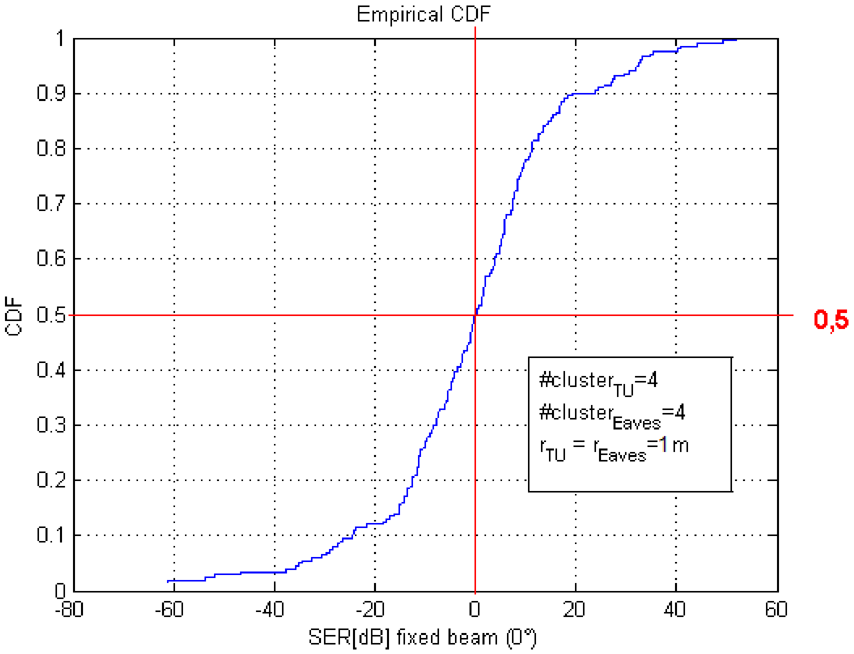


Figure 4.7: CDF of the SER (0°)[dB]

The target user and eavesdropper are associated with the same number of clusters

In this case, we considered 4 clusters for the target user and 4 clusters for the eavesdropper.

In Figure 4.14, we can see that the power received by the target user (full line with stars) is most of the time better than what the eavesdropper receives (dotted line with diamonds) due to to the orientation of the beam in the direction of the target user. However, the curve of the power received by the eavesdropper is more often over the target user one than on the Figure 4.11, because we are considering one cluster less for the target user and one cluster more for the eavesdropper than the previous case (5 clusters for the target user and 3 for the eavesdropper). Meanwhile, the eavesdropper still presents low power levels down to $-85dBm$, i.e. below the noise floor.

The CDF in Figure 4.15 shows that the eavesdropper receives a higher power from the AP than the target user 27% of the time. In other terms, the target user has a better quality of signal in 73% of the simulations with the same number of clusters associated with him. As an other reference, the target user reaches a 20 dB higher power than the eavesdropper in 16% of the simulations.

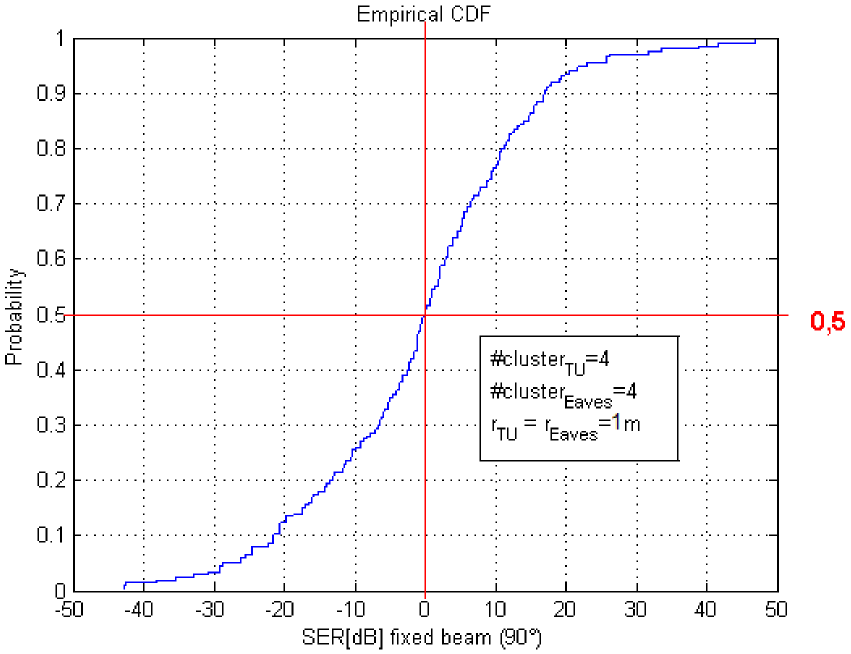


Figure 4.8: CDF of the SER (90°)[dB]

In Figure 4.16 the difference between the two curves in 20% of the simulations is of approximately $14dB$. This variation leads to a quite good SER on Figure 4.15 as the target user's clusters are obviously closer to the AP. Besides the eavesdropper's curve is very flat and makes its signal unstable with poor SNR (lower than 0dB) in almost 5% of the cases. The target user's curve is steep, sign of stability, and always above $40dB$, guaranteeing him with a good and stable signal.

The target user is associated with less clusters than the eavesdropper

In this case, we consider 3 clusters for the target user and 5 clusters for the eavesdropper.

In Figure 4.17, we can see that the power received by the target user (full line with stars) is almost two thirds of the time better than what the eavesdropper receives (dotted line with diamonds) due to directional pattern towards one of his cluster but since the eavesdropper has more clusters associated, it still has good chances to catch the signal sent by the AP towards one of the target user's cluster. Whereas the power levels for the eavesdropper happen to be really low and down

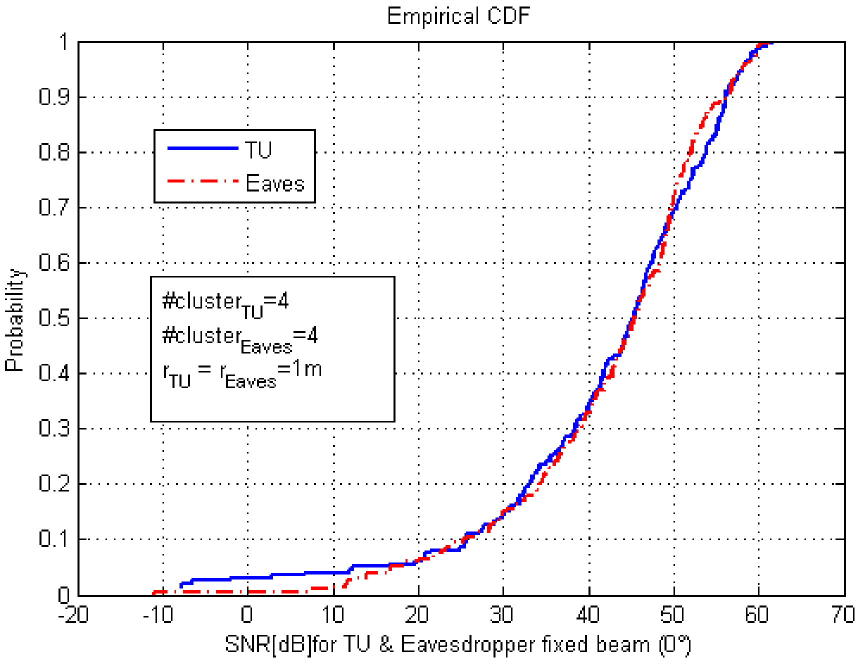


Figure 4.9: CDF of the SNR (0°)[dB]

to the noise floor sometimes.

The CDF in Figure 4.18 shows that the eavesdropper receives a higher power from the AP than the target user in 40% of the cases. In other terms, the target user has a better quality of signal in 60% of the simulations with a smaller number of clusters associated with him. As an other reference, the target user reaches a 20 dB higher power than the eavesdropper in 12% of the simulations.

In Figure 4.19, the target user has a better SNR (steeper curve on the right) than the eavesdropper (curve on the left) but the difference is not that big since in 20% of the simulations the target user's SNR is only $6dB$ higher than the eavesdropper's one. Of course, the target user's curve is always above $40dB$ and the eavesdropper's curve is quite flat but these two curves tend to equalize around 20% of the time also. This is quite bad for the target user who can have is transmission decoded quite often in this case.

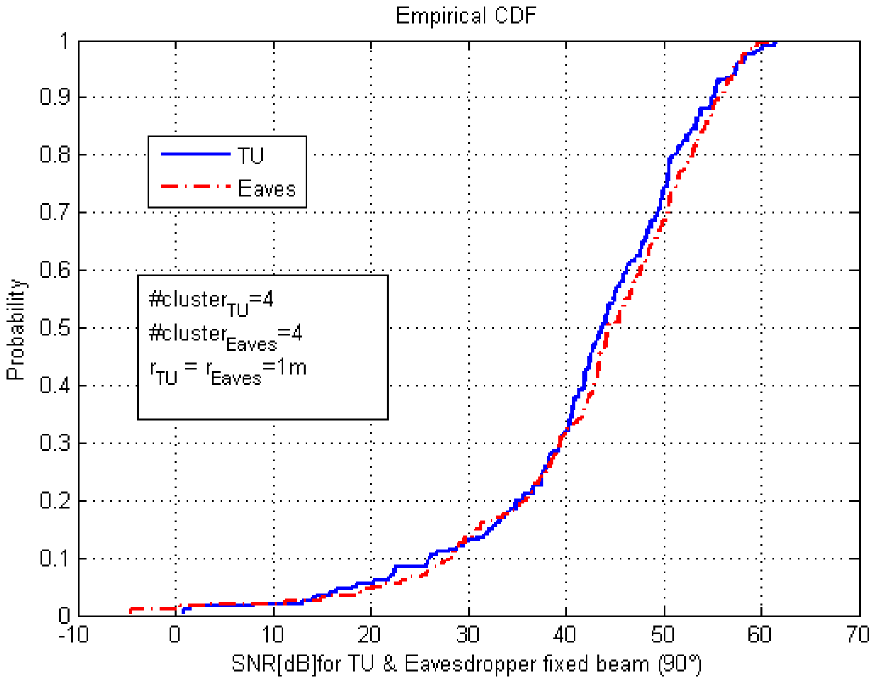


Figure 4.10: CDF of the SNR (90°)[dB]

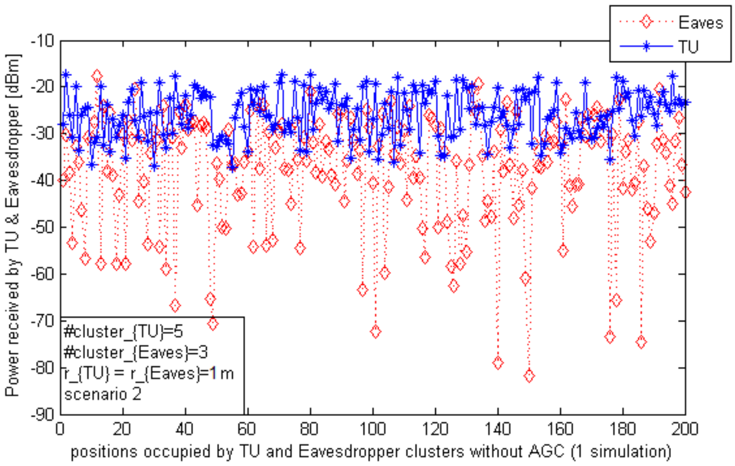


Figure 4.11: Power received by both TU and Eavesdropper over 1 simulation (5cl vs 3cl)

Conclusion for the second scenario

Considering more clusters associated with the target user than with the eavesdropper leads to the best results in terms of power received

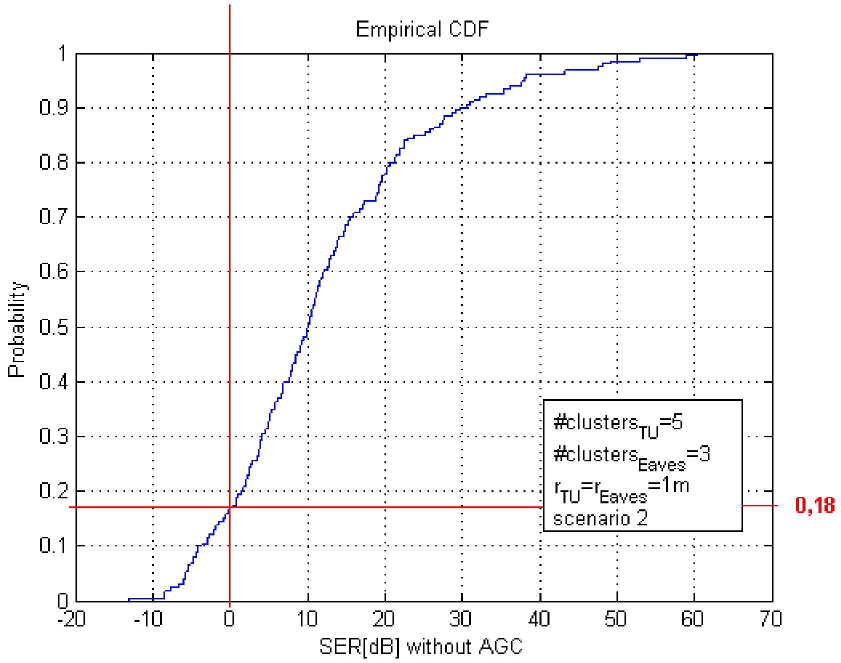


Figure 4.12: CDF of the SER [dB] (5cl vs 3cl)

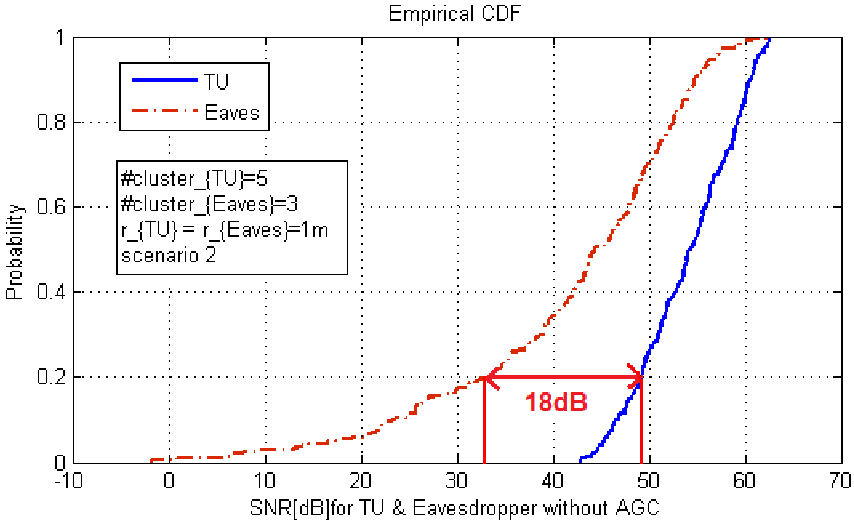


Figure 4.13: CDF of the SNR [dB] (5cl vs 3cl)

over each simulation, in terms of SER and also SNR.
Besides, considering the same number of clusters for both target user and eavesdropper or less clusters for the target user still shows that the latter receives a higher power in both cases. It is clear that adding

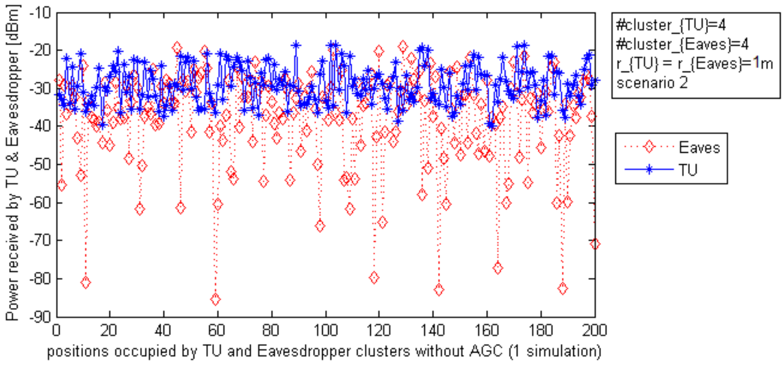


Figure 4.14: Power received by both TU and Eavesdropper over 1 simulation (4cl vs 4cl)

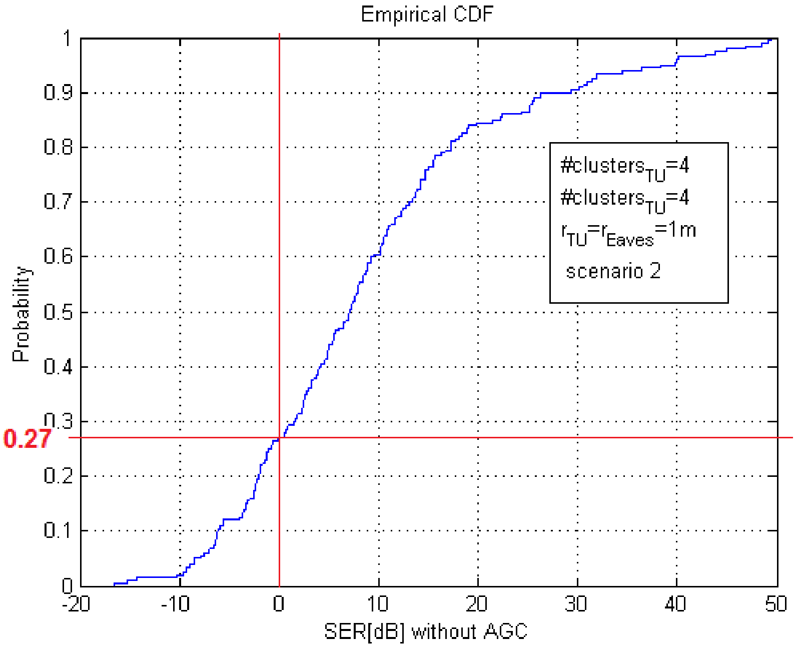


Figure 4.15: CDF of the SER [dB] (4cl vs 4cl)

more and more clusters for the eavesdropper would make the SER tend to 0dB in 50% of the simulations and the SNR of the eavesdropper approaching the target user's one more and more often, but this necessitates a huge number of clusters for the eavesdropper compared to the target user and has not been reached in our simulations yet. Obviously, the Beam-Hopping technique deteriorates the SNR of the

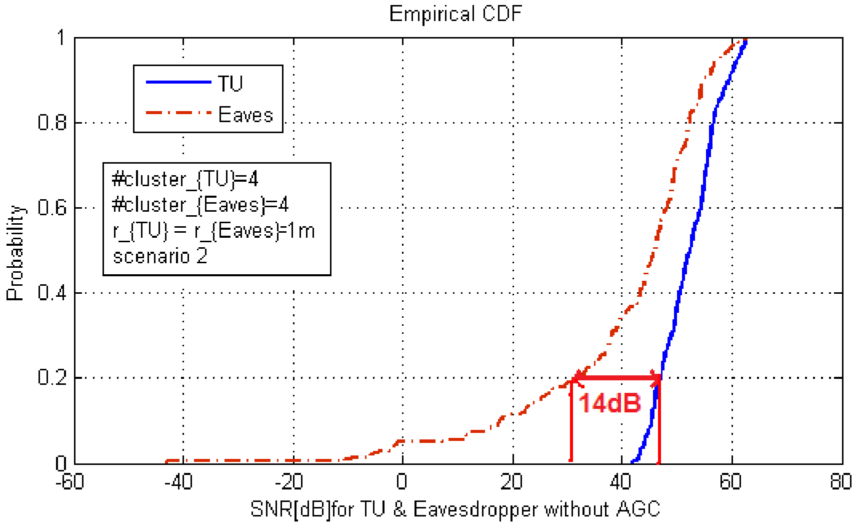


Figure 4.16: CDF of the SNR [dB] (4cl vs 4cl)

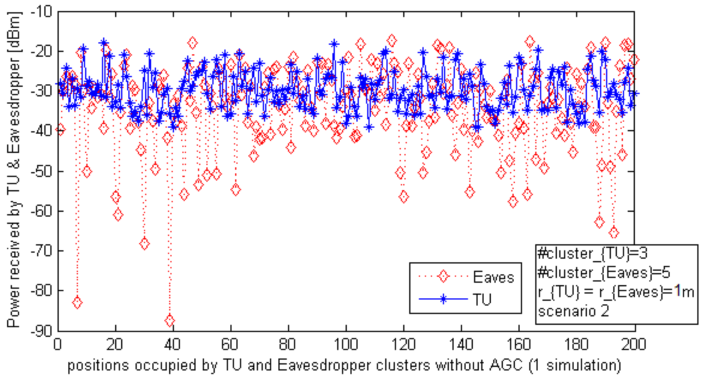


Figure 4.17: Power received by both TU and Eavesdropper over 1 simulation (3cl vs 5cl)

eavesdropper while improving the one of the target user, and at the same time provides better results than when a fixed beam is applied at the AP.

The two main points of the second scenario are:

- Optimizing the pattern in the direction of the target user's clusters
- Checking if the directional pattern makes it more difficult for the eavesdropper to catch a stable signal

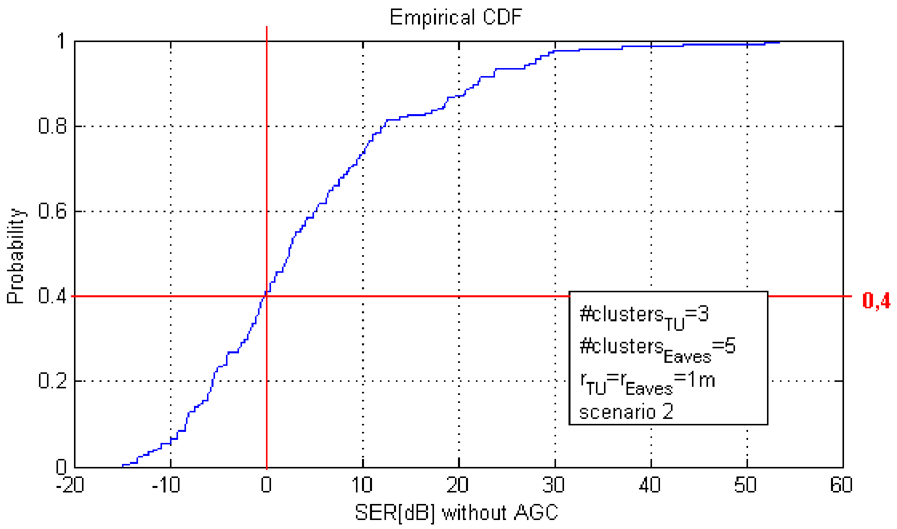


Figure 4.18: CDF of the SER [dB] (3cl vs 5cl)

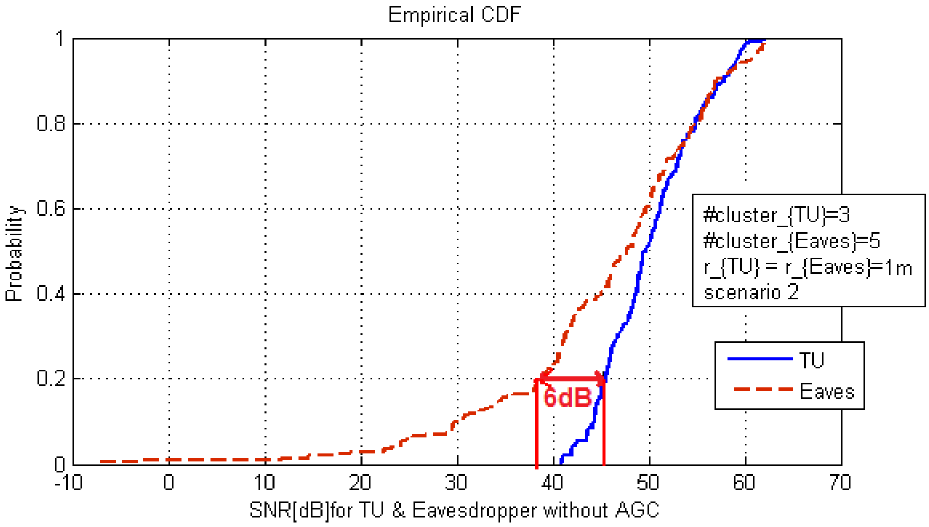


Figure 4.19: CDF of the SNR [dB] (3cl vs 5cl)

4.1.3 Third scenario : Beam-Hopping + AGC

Besides the fact that the AP is still jumping its beam towards one of the target user's cluster, it is also applied a process called AGC that can guarantee the target user with receiving the same amount of power for any position of his clusters. Indeed the AP will adapt his power transmitted so that the target user will always receive a power of $-25dBm$.

The target user is associated with more clusters than the eavesdropper

In this case, the target user is associated with 5 clusters while the eavesdropper is associated with 3.

The average received power level after AGC is set to $-25dBm$ for the target user in Figure 4.20. We can see that variance of the eavesdropper's power is really big with a maximum value of $-12dBm$ and a minimum of $-88dBm$ which is happening due to the fact that his clusters are located at the edge of the service area with great angles between them and the target user's clusters with respect to the AP.
It can happen that the eavesdropper receives more than $-25dBm$ when the target user is very far from the AP and the eavesdropper is very close to it with an angle approaching the direction of the target user. In this case, the AP will send a lot of power so that the target user receive $-25dBm$. As a consequence, the eavesdropper will receive a higher power than $-25dBm$.

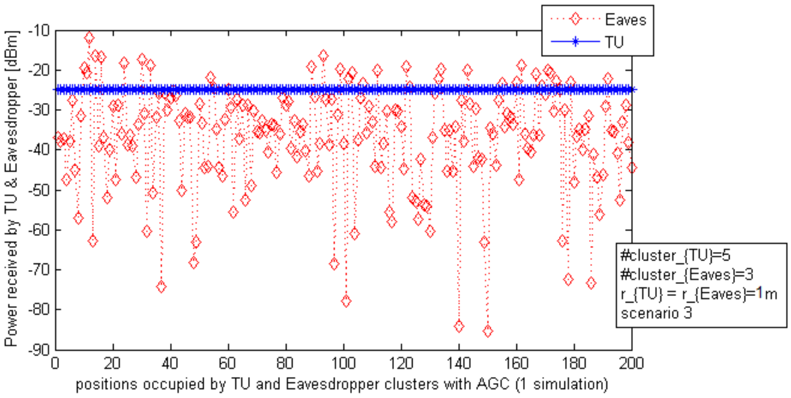


Figure 4.20: Power received by both TU and Eavesdropper over 1 simulation (5cl vs 3cl)

Concerning the CDF of the SER, we can see in Figure 4.21 that the eavesdropper receives a higher power from the AP than the target user in less than 18% of the cases. In other terms, the target user has a better quality of signal in 82% of the simulations with a bigger number of clusters associated with him. As an other reference, the target user reaches a 30 dB higher power than the eavesdropper in 18% of the simulations. This is reflected in Figure 4.22 where the SNR of the target user is always $55dB$ due to the noise floor set at $-80dBm$. In 20% of the cases, the difference between the power received by the target user and the one receive by the eavesdropper is $20dB$. The target user's clusters receive a lot more power than the eavesdropper's thanks to AGC and the orientation of the beam.

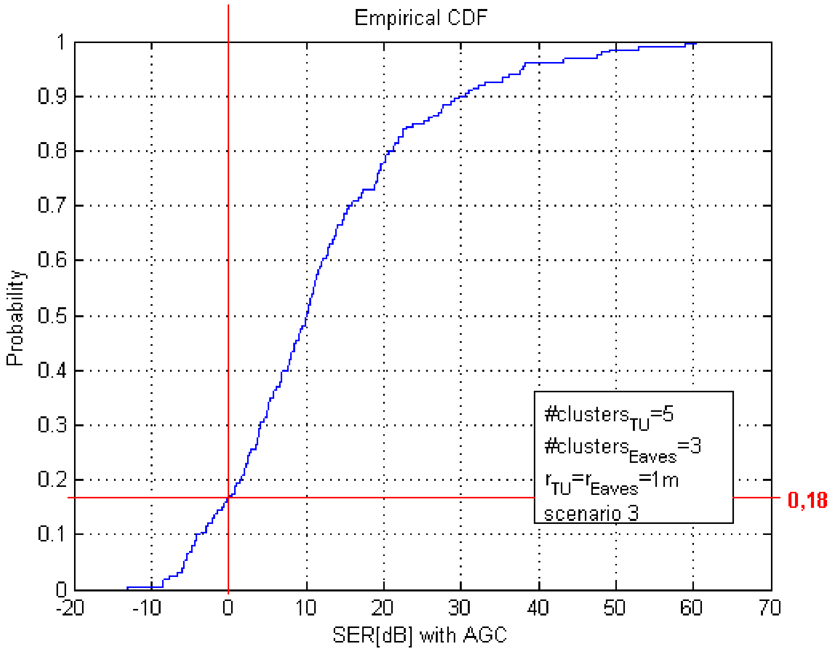


Figure 4.21: CDF of the SER [dB] (5cl vs 3cl)

The target user and eavesdropper are associated with the same number of clusters

In this case, the target user is associated with 4 clusters and the eavesdropper is associated with 4 clusters as well.

The average received power level after AGC is set to $-25dBm$ for the target user in Figure 4.23. We can see that variance of the eavesdropper's power is still big with a maximum value of $-9dBm$ and a minimum of $-77dBm$ which is happening due to the fact that his clusters are located at the edge of the service area with great angles between them and the target user's clusters with respect to the AP as said previously.

Concerning the CDF of the SER, we can see in Figure 4.24 that the eavesdropper receives a higher power from the AP than the target user

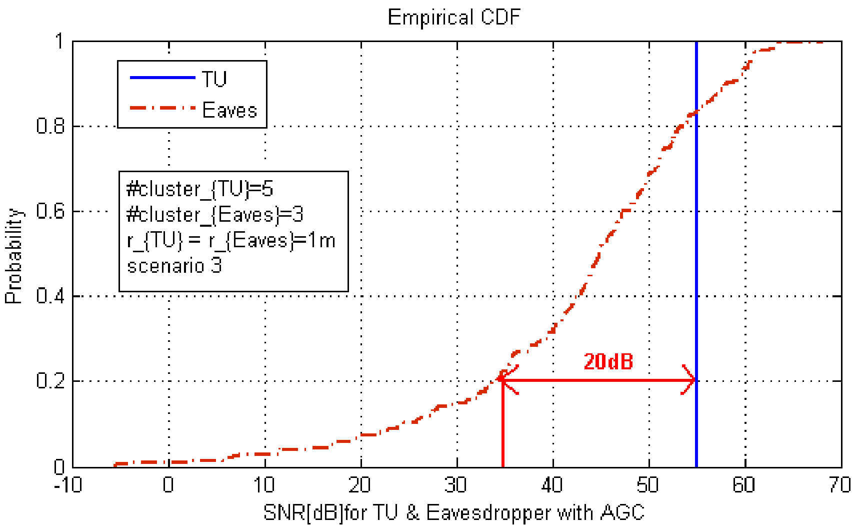


Figure 4.22: CDF of the SNR [dB] (5cl vs 3cl)

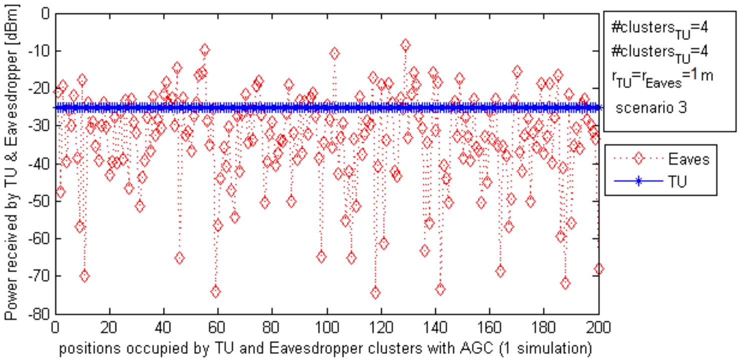


Figure 4.23: Power received by both TU and Eavesdropper over 1 simulation (4cl vs 4cl)

in less than 27% of the cases. In other terms, the target user has a better quality of signal in 73% of the simulations. As an other reference, the target user reaches a 20 dB higher power than the eavesdropper in 15% of the simulations. These quite good results are confirmed by the SNR plot in Figure 4.25 which shows us that the eavesdropper has 30% of the chances to get a SNR smaller than 40dB while the target user has always a 55dB SNR. Finally, the difference between the power received by the target user and the one received by the eavesdropper is 17dB in 20% of the cases.

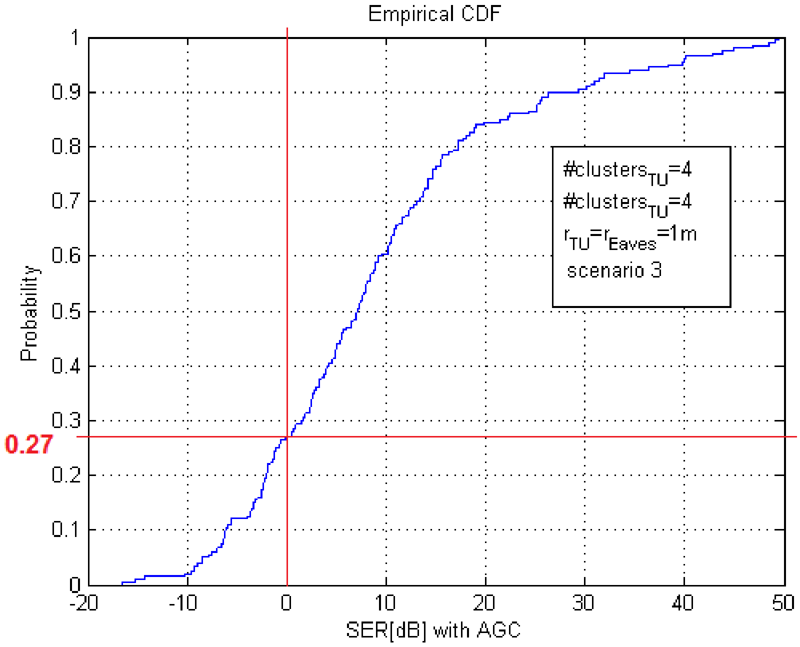


Figure 4.24: CDF of the SER [dB] (4cl vs 4cl)

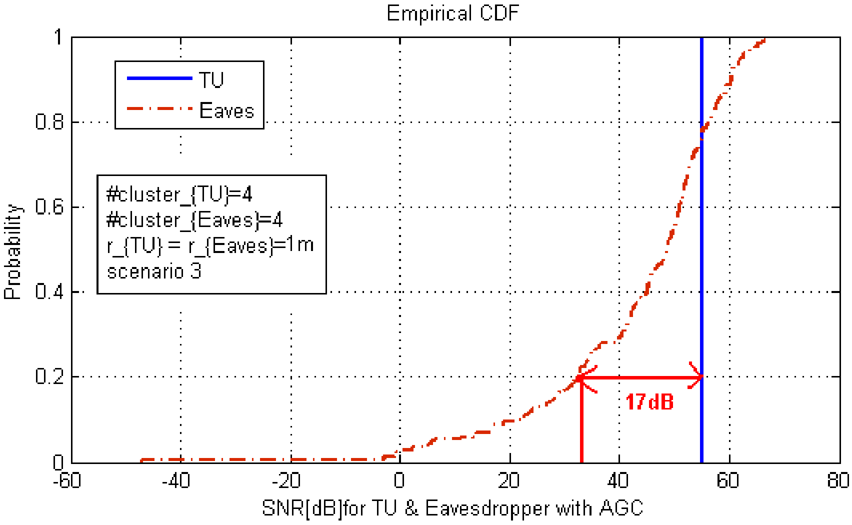


Figure 4.25: CDF of the SNR [dB] (4cl vs 4cl)

The target user is associated with less clusters than the eavesdropper

In this case, the target user is associated with 3 clusters while the eavesdropper is associated with 5.

The average received power level after AGC is set to $-25dBm$ for the target user in Figure 4.26. The eavesdropper receives a better power for much more positions than previously because of his good chances over the target user to catch the signal from the AP with 2 more clusters randomly located in the service area. We can see that the variance of the eavesdropper's power is still big with a maximum value of $-10dBm$ and a minimum of $-89dBm$.

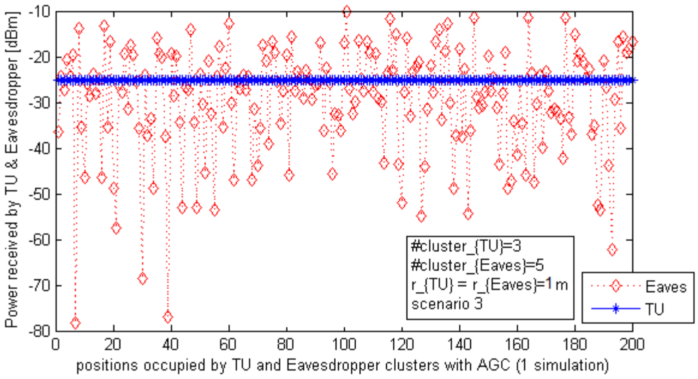


Figure 4.26: Power received by both TU and Eavesdropper over 1 simulation (3cl vs 5cl)

Concerning the CDF of the SER, we can see in Figure 4.27 that that the eavesdropper receives a higher power from the AP than the target user in less than 40% of the cases. In other terms, the target user has a better quality of signal in 60% of the simulations. As an other reference, the target user reaches a 10 dB higher power than the eavesdropper in 23% of the simulations. The results are confirmed in Figure 4.28 where the SNR of the eavesdropper is better than the target user's one in 40% of the cases. Finally, the difference between the power received by the target user and the one received by the eavesdropper is $12dB$ in 20% of the cases.

Conclusion for the third scenario

The Beam Hopping pattern combined with an AGC process lead to a constant power level delivered to the target user while the eavesdropper receives an erratic signal oscillating in a big range of values all the time. Of course these observations are emphasized when the target user benefits from a bigger number of clusters. Besides, the CDF of the SER in both cases are really steep which attests the efficiency of the AGC process making eavesdropping more difficult. The same

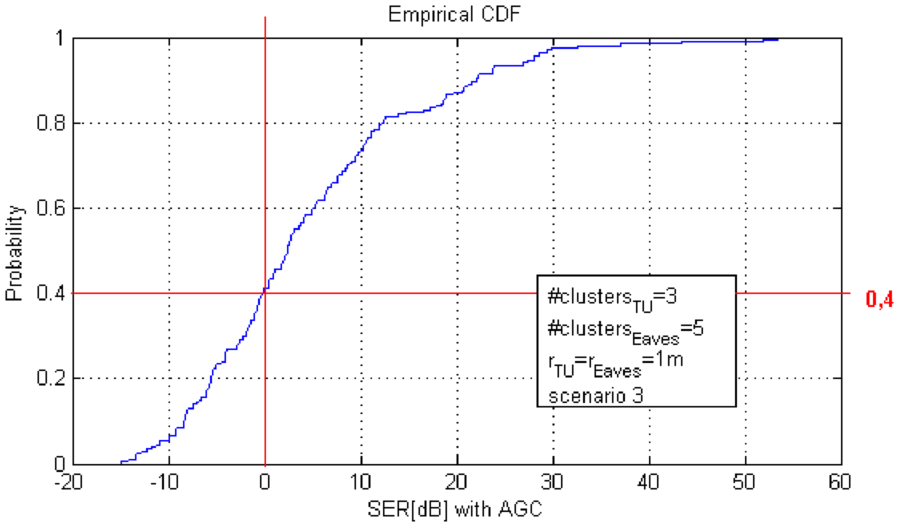


Figure 4.27: CDF of the SER [dB] (3cl vs 5cl)

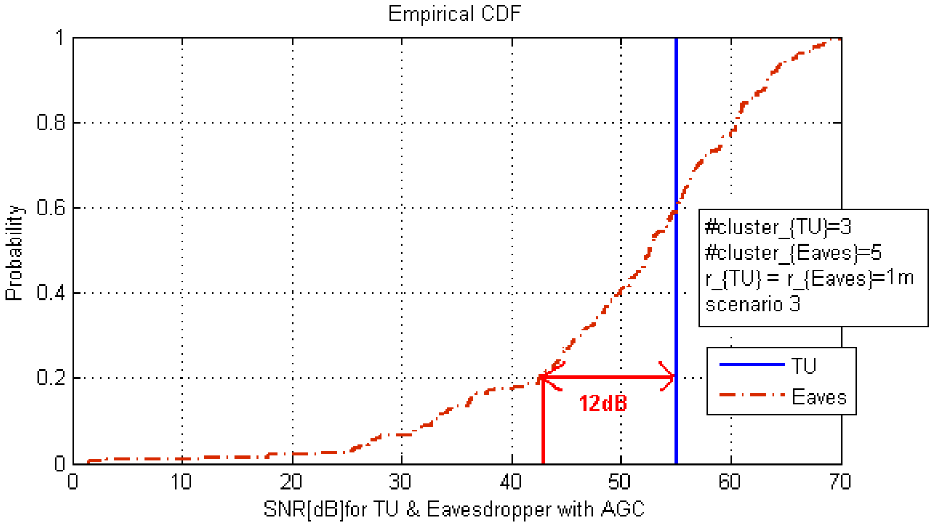


Figure 4.28: CDF of the SNR [dB] (3cl vs 5cl)

observation can be made on the SNR of the target user. The two main points of the third scenario are:

– Applying an AGC process to the optimized directional beam pattern.

– Checking if the AGC combined with the directional pattern makes it more difficult for the eavesdropper to catch a stable signal while always guaranteeing the target user with a constant amount of power.

4.1.4 Comparison

These simulations offered two techniques to perturb the signal received by the eavesdrooper.

The first part showed that the use of a mechanical hopping antenna brings a big improvement in the perturbation of the signal received by the eavesdropper. Indeed, the chances that the average power received by the eavesdropper would be equal or higher that the one received by the target user decrease from 50% to 27% (Figure 4.29) when using Beam-Hopping. It allows us to say that it is more difficult for the eavesdropper to catch the signal sent by the AP.

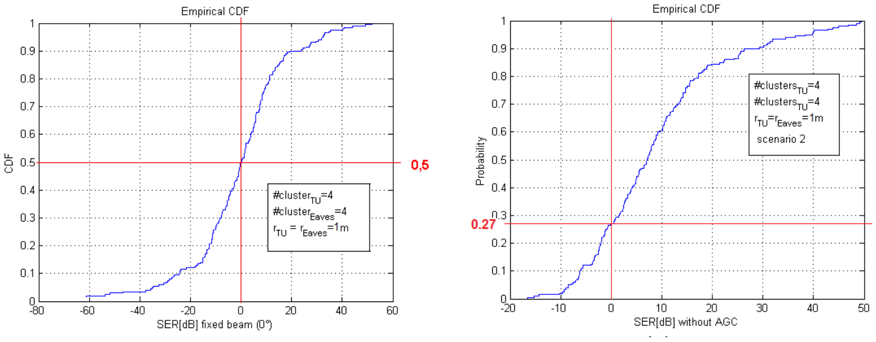


Figure 4.29: SER comparison between the reference fixed beam (left) and the hopping antenna system without AGC (right) (4cl vs 4cl) [dB]

Finally, the Figure 4.30 displays the results of the three scenarios regarding the SNR. Adding the AGC to the beam hopping pattern system makes the life more difficult for the eavesdropper, which means that it will be very hard for him to catch the signal. Moreover, if a target user's cluster is very close to the AP and the eavesdropper's one farther, the power sent by the AP would be very weak. As a consequence, the power received by the eavesdropper's cluster will be even weaker than without AGC.

4.2 Influence of the radius of clusters

This section is dedicated to the influence of the radius of the clusters on the power received by both target user and eavesdropper's clusters.

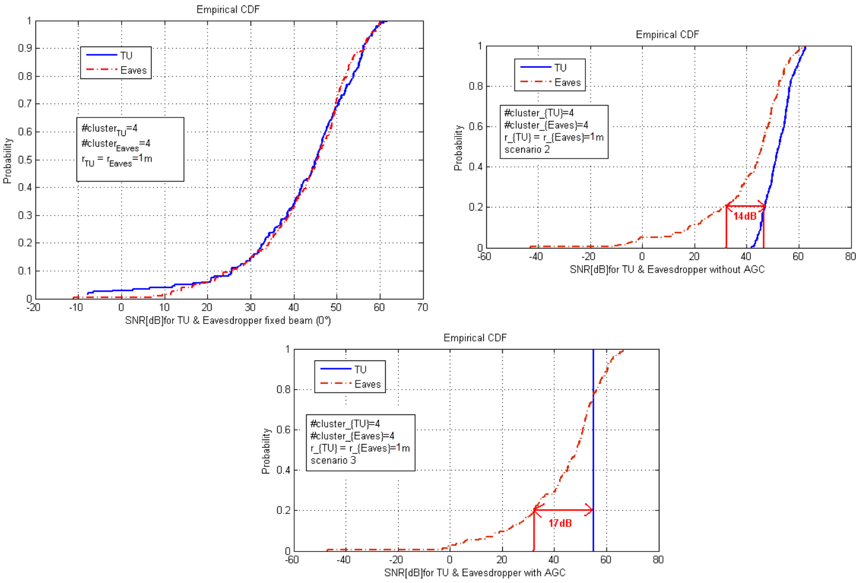


Figure 4.30: SER comparison between the reference fixed beam (left), the hopping antenna system without AGC (right) and the hopping antenna system with AGC (down) (4cl vs 4cl)[dB]

We can easily see in Figure 4.31, Figure 4.32 and Figure 4.33 that the radius of the clusters has a weak influence on the results. Indeed, we can see in Figure 4.31 that the eavesdropper receives a higher power from the AP than the target user does in less than 20% of the cases, because the beam is wide enough to reach all the scatterers on a cluster when the radius is either $1m$ or $1.5m$. This is confirmed on Figure 4.32 and Figure 4.33 where the difference between the power received by the target user and the one received by the eavesdropper is always the same.

4.3 Influence of the beamwidth

Figure 4.34 represents the pattern created with different values of the HPBW. In this part, we use the same number of clusters for both target user and eavesdropper. The radius is also the same and set to $1m$. The wider the beam will be, the lower the maximum gain will be.

Figure 4.35 shows the CDF of the SNR using different values of HPBW. As a reminder, the eavesdropper had less than 50% of chances

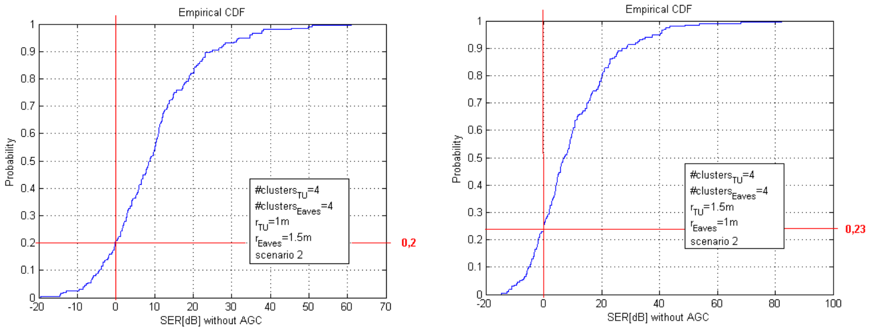


Figure 4.31: CDF of the SER [dB]: Influence of radius (4cl vs 4cl)

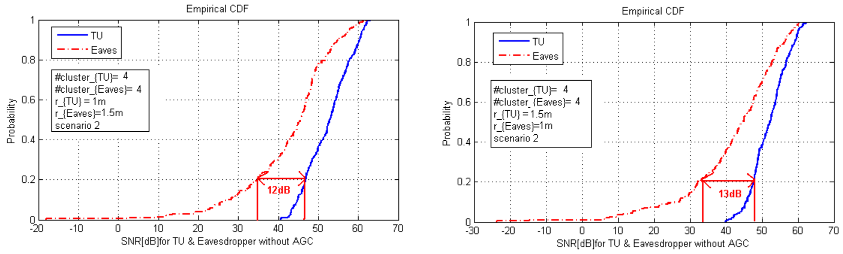


Figure 4.32: CDF of the SNR [dB] comparison between the radius in scenario 2 (4cl vs 4cl)

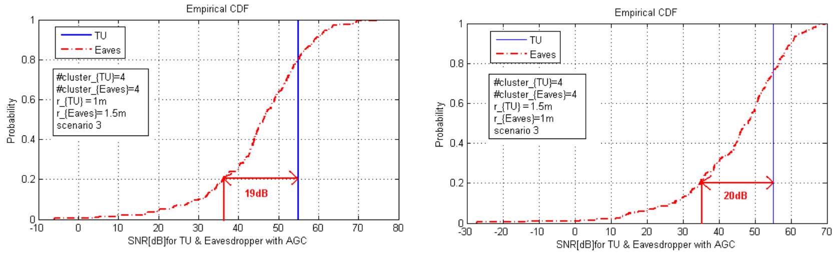


Figure 4.33: CDF of the SNR [dB] comparison between the radius in scenario 3 (4cl vs 4cl)

to have a power received equal or lower than the power received by the target user.

The results using a HPBW=10° (top left) are the best ones, as the eavesdropper receives a higher power from the AP than the target user does in less than 19% of the cases. Using a a HPBW=25° (top left), the eavesdropper receives a higher power from the AP than the target user in less than 24% of the cases.Using a a HPBW=60° (top left),

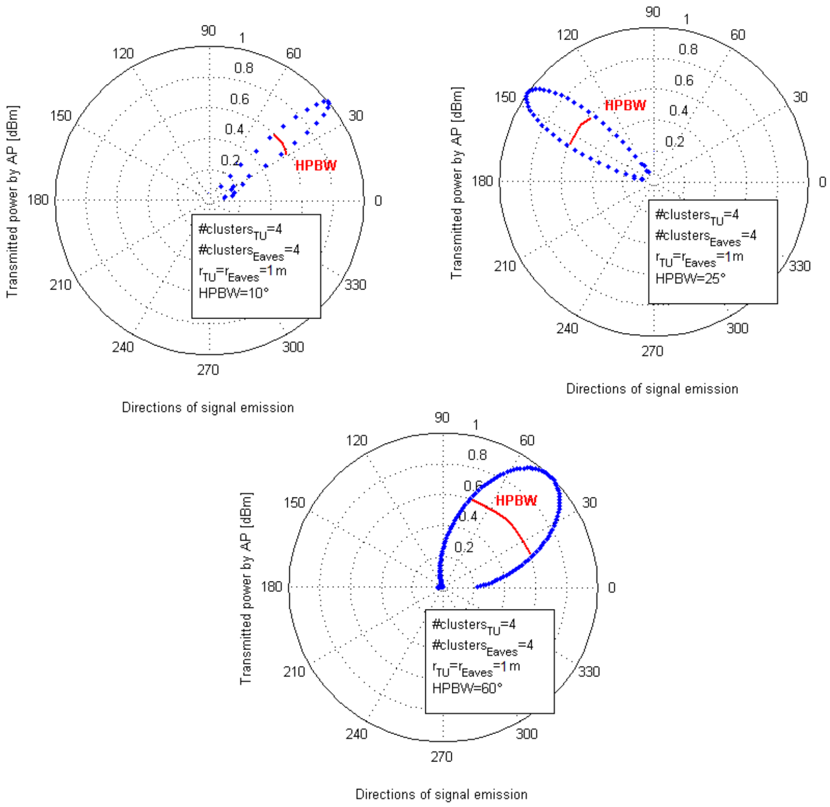


Figure 4.34: 3 different patterns [dB]

the eavesdropper receives a higher power from the AP than the target user in less than 27.% of the cases. Indeed, the narrower the beam is, the higher the gain will be for the target user. As a consequence, the power received by the target user will be higher. Morever, the beam is wide enough to reach all the scattererd on the cluster.

4.4 Conclusion

To conclude on this simulation, it is obvious to say that combining a beam-hopping pattern technique with a AGC is already quite robust against eavesdroppers. Indeed, the results in this case are better than the reference and also than the case when we only use the beam-hopping pattern. Therefore, it can happen that the eavesdropper stays a certain period with receiving a very good average power. This lets us suppose that he would be able to catch some information during this period.

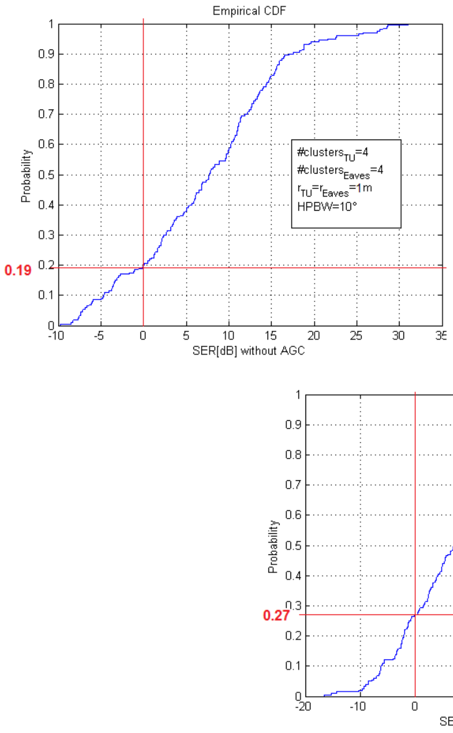


Figure 4.35: CDF of the SER with a HPBW of 10° (top left), 25° (top right) and 60° (down) [dB]

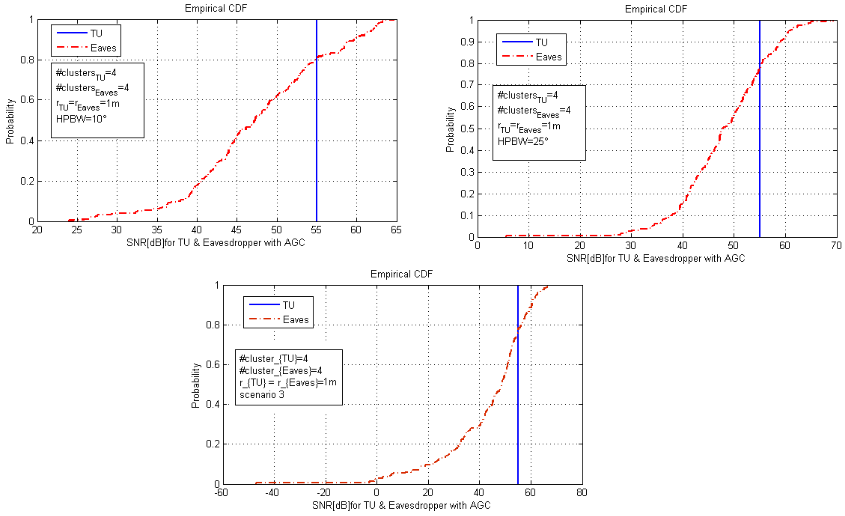


Figure 4.36: CDF of the SNR with a HPBW of 10° (top left), 25° (top right) and 60° (down)(scenario 3)

One interesting technique which would have been interesting to test is the use of a threshold applied to the environmental power profile which would have allowed us to send the signal towards more than one cluster at the same time.

Chapter 5

Conclusion and future work

5.1 Conclusion

This project presents one aspect of the security in a transmission between a target user and an AP. What is the key topic in wireless communications is how to guarantee the target user with confidentiality and integrity of his data. In this purpose, we investigated a way to optimize the security level at the physical layer so that confidentiality is delivered to the target user in a transparent way. To do so, our project is based on Beam-Hopping techniques applied to the AP radiation pattern. These techniques were investigated to check if an eavesdropper would be able to catch a stable signal in a multipath indoor environment, assuming that the AP would broadcast its signal in optimized directions for the target user. The other goal was to achieve a certain trade-off between security/privacy and hardware complexity so that the solution could be realizable and reach the market.

1. First chapter.
   First of all, we had to restrict our problem to a certain domain of work (space domain), a certain type of system (SISO) and to narrow down to a problem that has not been dealt with yet by searching for previous works on the subject.

2. Second chapter.
   In this chapter, we focused on describing the technical processings that we would like to apply to our system and especially to the AP. An entire description of the antenna system (mechanical steering pattern), the channel (average CSI, open-loop, far-field

and Rayleigh fading considerations), the power modelling (power summation because of non-coherent scattered responses) and the beam-hopping algorithm is made.

3. Third chapter.
   This third step is used to describe the simulation environment and the several scenarios we plan to investigate in this environment.

4. Fourth and last chapter.
   This last chapter displays the results obtained from the different Matlab simulations we ran.

Our simulations are divided into thre main parts. The first part analyzes the influence of the number of clusters associated with the target user and the eavesdropper on the SER considering a fixed beam (standard) AP, a beam-hopping AP and another beam-hopping AP with a gain control algorithm applied to it.
The second part observes the same SER parameter and the average power received by both target user and eavesdropper when different radius of clusters are chosen and considering the same three kinds of scenarios as previously. Finally, the last part deals with the influence of the beamwidth for the pattern over the same curves considering the same kind of APs.

5.1.1 Conclusion for the first part

- Best type of antenna system for AP.
  The most efficient type of antenna for the AP is the beam-hopping system combined with an AGC that allows the target user to get a stable signal while the eavesdropper receives an erratic signal with a great variance no matter if the eavesdropper is associated with more clusters than the target user.

- Beam-Hopping technique alone is not sufficient.
  The Beam-Hopping technique provides results favouring the target user but the eavesdropper is still able to catch a good signal in almost 30% of the cases which is not sufficient to trust the technique applied without another algorithm to optimize it. Besides, the SNR of the target user could be stabilized while the SNR of the eavesdropper would be deteriorated.

- Beam-Hopping technique combined with AGC improves significantly the standard AP with a fixed beam pattern.
  Considering uniformly distributed random locations for both target user and eavesdropper leads to equal probabilities of having a good signal for both if the AP has its radiation pattern fixed. However, applying Beam-Hopping techniques and adding gain control processing hugely improves the chances of the target user to catch a stable signal and so make it more secure for his communications by increasing the difference between the target user and the eavesdropper SNR ($0dB$ for the fixed beam to $17dB$ in the best case for beam hopping with AGC) .

5.1.2 Conclusion for the second part

- Best type of antenna system for AP.
  The most efficient type of antenna for the AP is still the beam-hopping system combined with an AGC no matter if the eavesdropper's clusters have a bigger radius than the target user's ones.

- The radius of the clusters is not a significant parameter in the simulations.
  Considering uniformly distributed random locations for both target user and eavesdropper's clusters leads to equal probabilities of having a good signal for both if the AP has its radiation pattern fixed. However, the Beam-Hopping techniques and above all adding gain control processing hugely improves the chances of the target user to catch a good stable signal even though the eavesdropper's clusters are considered bigger.

5.1.3 Conclusion for the third part

- Best type of antenna system for AP.
  The most efficient type of antenna for the AP is still the beam-hopping system combined with an AGC no matter if the beam is wide or narrow.

- The beamwidth of the pattern is an important parameter.
  Considering uniformly distributed random locations for both target user and eavesdropper's clusters leads to equal probabilities

of having a good signal for both if the AP has its radiation pattern fixed. However, the Beam-Hopping techniques and above all adding gain control processing hugely improves the chances of the target user to catch a good stable signal. But in cases of a small beamwidth, the results are better because the power received by the target user will be higher thanks to a bigger gain and the eavesdropper would have to be really close to the target user to catch a decent signal.

5.2 Future work

The Beam-hopping technique (beam steering) combined with the gain control processing have shown some interesting results in terms of stability of target user's signal and security but a few cases could be investigated more deeply to proof the method efficiency such as:

1. More antenna elements at the AP.
   The AP could be equipped with more antenna elements to improve the precision of the beam pattern.

2. Several target users and/or several eavesdroppers.
   It could be interesting to simulate the system with more users involved to get an idea of the efficiency of the techniques in a real mobile network situation with several customers to protect from possible eavesdropping.

3. Apply a threshold to the response of the environment to be able to send the signal toward more than one cluster.

4. Adaptive beamwidth with respect to the response of the environment

Bibliography

[1] J. Berthod and L. My, "Radio security potential in wlan application," *Master thesis Aalborg University*, June 2007.

[2] C. Dictionary, "Security," March 2008.

[3] Wikipedia, "Security," p. access: February 208, June 2007.

[4] U. Government, "Federal standard 1037c, mil-std-188," *National Informations Systems Security Glossary and DoD Dictionary of Military and Associated Terms*, 2001.

[5] C. Dictionary, "Identification," March 2008.

[6] ——, "Authentication," March 2008.

[7] FrameIP, "Osi model," March 2008.

[8] openSSH, "http://www.openssh.org," September 2007.

[9] M. Prikryl, "http://www.winscp.net," March 2007.

[10] B. Lloyd and W. Simpson, "Ppp challenge handshake authentication protocol (chap)," August 1996.

[11] T. Dierks and E. Rescorla, "The transport layer security (tls) protocol version 1.1," April 2006.

[12] K. G. Paterson and A. K. L. Yau, "Cryptography in theory and practice: The case of encryption in ipsec," March 2006.

[13] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications: the insecurity of 802.11," April 2001.

[14] Wikipedia, "Osi model," 2006, access: February 2008.

[15] G. Surnam, "Understanding security using the osi model," *GSEC Practical version 1.3*, March 2002.

[16] D. Reed, "Applying the osi seven layer network model to information security," *SANS Institute, GIAC GSEC Practical Assignement version 1.4b*, November 2003.

[17] R. Security, "Wireless adoption leaps ahead, advanced encryption gains ground in the post-wep era," *http://www.rsa.com/*, June 2007.

[18] X. Zhou, P. Kyritsi, P. Eggers, and F. Fitzek, "The medium is the message: Secure communications via waveform coding in mimo systems."

[19] X. E. Li, M. Chen, and E. P. Ratazzi, "Array-transmission based physical-layer security techniques for wireless sensor networks," *IEEE International Conference on Mechatronics Automation*, pp. 1618–1623, July 2005.

[20] M. L. Jørgensen, B. R. Yanakiev, G. E. Kirkelund, P. Popovski, H. Yomo, and T. Larsen, "Shout to secure: Physical-layer wireless security with known interference," *IEEE GLOBECOM 2007*, pp. 33–38, 2007.

[21] X. Li, M. Chen, and E. Ratazzi, "Array-transmission based physical-layer security techniques for wireless sensor networks," *Mechatronics and Automation, 2005 IEEE International Conference*, 2005.

[22] P. M. N. Islam, "Information assurance in wdm networks: Physical layer security," *Department of Electrical Engineering and Computer Science University of Michigan, Ann Arbor, MI*, 2003.

[23] G. Sanguinetti, J. Laidler, and N. D. Lawrence, "Automatic determinantion of the number of clusters using spectral algortihms."

[24] N. Czink, M. Herdin, H. Özcelik, and E. Bonek, "Number of multipath clusters in indoor mimo propagation environments."

[25] S.Haykin, "Cognitive radio:brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, February 2005.

[26] R. D. Taranto, H. Yomo, P. Popovski, K. Nishimori, and R. Prasad, "Cognitive mesh network under interference from primary user," August 2007.

[27] J. E. Håkegård, "Typical coverage and capacity of multi-cell wireless lans," December 2006.

[28] D.Malone, P. Clifford, D.Reid, and D.J.Leith, "Experimental implementation of optimal wlan channel selection without communication."