INTERFERENCE AS AN ISSUE AND A RESOURCE IN WIRELESS NETWORKS

A THESIS SUBMITTED IN FULFILMENT OF REQUIREMENTS FOR

THE DEGREE OF

DOCTOR OF PHILOSOPHY

OF UNIVERSITY COLLEGE LONDON

2017

By

Raoul F. Guiazon

Communications and Information Systems Group

Department of Electronic and Electrical Engineering

Contents

Declaration

I, Raoul Guiazon confirm that the work presented in this thesis is my own. Where information has been derived from other sources, I confirm that this has been indicated in the thesis.

Abstract

This dissertation will be focused on the phenomenon of interference in wireless networks. On one hand, interference will be viewed as a negative factor that one should mitigate in order to improve the performance of a wireless network in terms of achievable rate, and on the other hand as an asset to increase the performance of a network in terms of security. The problems that will be investigated are, first, the characterisation of the performance of a communication network modelled as an interference channel (IC) when interference alignment (IA) is used to mitigate the interference with imperfect knowledge of the channel state, second, the characterisation of the secrecy in the Internet-of-Things (IoT) framework where some devices may use artificial noise to generate interference to potential eavesdroppers.

Different scenarios will be studied in the case where interference is unwanted; the first one is when the channel error is bounded. A lower bound on the capacity achievable in this case is provided and a new performance metric namely the saturating SNR is derived. The derived lower bound is studied with respect to some parameters of the estimation strategy when using Least-Square estimation to estimate the channel matrices. The second scenario deals with unbounded Gaussian estimation errors, here the statistical distribution of the achievable rate is given along with a new performance metric called outage probability that simplifies the study of the IC with IA under imperfect CSI. The results are used to optimise the network parameters and extend the analysis further to the case of cellular networks. In the wanted interference situation, the secrecy of the worst-case communication is studied and the conditions for secrecy are provided. Furthermore the average number of secure links achievable in the network is studied according to a theoretical model that is developed for the IoT case.

List of Figures

List of Mathematical Notations

$\mathbf{a}$	Denotes vectors
$\mathbf{A}$	Denotes matrices
$(\cdot)^T$	Represents the transpose operation
$(\cdot)^*$	Represents the conjugate transpose operation
$\mathtt{span}(\mathbf{A})$	Vector space generated by the columns of the matrix $\mathbf{A}$
$(\cdot)_k$	Returns the k^{th} row of an input matrix
$[\cdot]_k$	Returns the k^{th} column of an input matrix
$\|\cdot\|_2$	Represents the square-norm
$\|\cdot\|_{\mathrm{F}}$	Represents the Frobenius norm of a matrix
$\mathbb{E}\{\cdot\}$	Returns the mean of a random variable
$\mathbb{P}(\cdot)$	gives the probability of an event
$\mathbb{P}_x\{\cdot\}$	Palm probability of x
$\bigotimes$	Represents the convolution operation
$\mathbf{I}_n$	Is the identity matrix of size $n \times n$
$\mathcal{CN}(\mu, \sigma^2)$	Complex Gaussian random variable of mean μ and variance σ^2
$\Gamma(\cdot)$	Gamma function
$E_1(\cdot)$	Exponential integral
$\mathcal{I}_1(\cdot)$	Modified Bessel function of the first kind
$\mathbb{A}(\cdot)$	Area of a random region

A realisation of a random variable X is denoted by a corresponding lower case letter x.

List of Acronyms

5G Fifth Generation.

AN Artificial Noise.

ASC Average Number of Secure Connections.

AWGN Additive White Gaussian Noise.

BS Base Station.

C-Rx Cloud Receiver.

CDMA Code Division Multiple Access.

CSI Channel State Information.

D2D Device to Device.

DoF Degree of Freedom.

DTV Digital Television Network.

FDMA Frequency Division Multiple Access.

IA Interference Alignment.

IBFD Inband Full Duplex.

IC Interference Channel.

ICSI Imperfect Channel State Information.

IoT Internet of Things.

IoT-GW IoT Gateway.

LOS Line Of Sight.

LS Least-Square.

LTE Long Term Evolution.

MAC Multiple Access Channel.

MIMO Multiple Input Multiple Output.

NB-IoT Narrow Band IoT.

PDF Probability Density Function.

PLS Physical Layer Security.

PPP Poisson Point Process.

RSA Rivest-Shamir-Adleman (cryptosystem).

SINR Signal to Noise plus Interference Ratio.

SIR Signal to Interference Ratio.

SNR Signal-to-Noise Ratio.

TDMA Time Division Multiple Access.

UE User Equipment.

Acknowledgement

First and foremost, I would like to thank Prof. Kai-Kit Wong for giving me the opportunity to do this PhD under his supervision. His guidance and wisdom have been key to the success of this journey. It is an honour to have a supervisor like him.
I also want to thank my industrial supervisor Dr. Michael Fitch at BT for his help in steering my research towards interesting directions and for arranging several visits at the BT research centre in Ipswich. These visits have been very inspirational to my work.
I thank the EPSRC and BT for funding my PhD and the Fondation de France through the Georges Besse Foundation for giving me the support I needed to achieve my goals.
Many thanks to my friends for all the happy times we shared together.
A special thanks to Mr and Mrs Djofack, my heart is always with you and your family.
Last but not least, my deepest thanks go to my mother and sister, only you can truly understand the value and meaning of this achievement. I can never thank you enough for all the love and support you have provided me with my whole life. I could not have been blessed with a better family.

With deepest gratitude and warmest affection, I dedicate this thesis to my loving mother

Anne Guiazon

Who has always been a constant source of wisdom and inspiration.

Chapter 1

Introduction

The 21st century is undoubtedly the era of ubiquitous connectivity for people and objects. Technology is evolving at a tremendous speed to meet this objective. The terms "Smart cities", "Smart homes", "Smart grids" are all denominations of this same trend - The increasing interconnectivity of things, people and services [1] - they reveal the emergence of new kinds of networks of interconnected things, called the Internet of Things (IoT) [2]. Thanks to this, many types of applications will be made possible in the near future, such as remote health monitoring, efficient electric power management and distribution, self-driving cars and more [3]. It's needless to say, a tremendous amount of new devices will require access to the communication infrastructure, which will have to be at least, fast [4], reliable [5], secure [6] and of course, able to handle so many new devices at the same time [7]. Leading experts such as the IT company Gartner forecast that by 2020 more than 20 billion IoT devices will be connected to the cloud.
In this dissertation, the focus is on two key aspects that will enable these future networks to come true, namely, security and accessibility.

- The accessibility in this context is the ability of a device to connect to the network. Here and throughout this dissertation, communications are only considered to occur via wireless links. Therefore, the issue at hand for this aspect is interference mitigation, since interference will certainly be a limiting factor in terms of achievable throughput in an overcrowded network of devices.

- Security here means the ability of a device to conceal its transmissions to unintended receivers. This aspect will be studied here from a Physical Layer point of view in the particular case of IoT networks.

Both aspects will be more rigorously developed in the following sections and chapters of this dissertation.

1.1 Motivation and Scope

1.1.1 Accessibility

A key component of multi-user wireless networks is the interference management strategy in use in order to allow multiple users to access the same spectrum. In today's networks, interference mitigation mostly means avoiding interference in the first place [8]. For example, techniques such as TDMA or FDMA are used to orthogonalise the different users of a network across time or frequency. In a TDMA system it means that the devices will transmit their signals in different non-overlapping time slots, whereas in FDMA systems non-overlapping frequency slots are used instead. It is easy to see that with such techniques, the total available resource is shared evenly amongst the users and that, the more users there are the less resources are available per user.
Recently, a new technique has been proposed in [9, 10], called Interference Alignment (IA) this technique promises in some cases that all users can get half of the total available resource regardless of their number.
IA is a linear precoding technique, it requires cooperation amongst the users in order to structure every transmitted signal in the network so that, each receiver receives the interference from the unintended transmitters in a reduced subspace, namely the interference subspace, whereas, the desired signal is received in a vector space orthogonal to the interference subspace called interference-free subspace or desired signal space. The orthogonality of these spaces makes it very simple to remove the interference and keep only the desired signal. Understand that in this case, all the users can transmit over overlapping time and frequency slots, the orthogonal entities in this case are the

desired signal and the interference viewed relatively to each receiver. Cadambe and Jafar in [11] have shown that under some assumptions the sum rate of the network would increase linearly with the number of user when IA is used. This is in sharp contrast with other interference mitigation techniques such as TDMA or FDMA where the sum-rate is inversely proportional to the number of users. IA was also shown to achieve the degree-of-freedom (DoF) capacity of the interference channel [12, 13].
In order to achieve the result mentioned above, the authors assumed infinite time or frequency diversity and perfect channel knowledge, which is not practical in a real setting. A great deal of efforts have been spent on operating IA in more realistic settings [14], some papers are investigating the extreme case where there is almost no channel knowledge, for example in [15], IA was considered without CSI but using only the knowledge of the network topology. Blind IA was also investigated in [16] without any knowledge of the channel coefficients. In the middle, other researchers have considered IA in a MIMO setting with constant and perfectly known channels and no time nor frequency diversity. In this case, IA does not promise a tremendous improvement on the sum rate but still doubles what's possible with techniques relying on orthogonalisation [17]. Then imperfect Channel State Information (CSI) has been considered e.g [18–20]. In an attempt to reduce the overhead for sharing CSI globally, opportunistic IA was studied in [21, 22]. Another issue that has been studied extensively is the feasibility of IA for different number of streams and antennas per user, e.g., [23–25].
In this dissertation, IA is considered in the K-user MIMO interference channel and the impact of channel estimation errors on the performance of interference alignment is investigated in different cases :

1. The impact of a bounded channel estimation error on the rate per user is studied. This type of errors can be linked to quantisation errors when the CSI is measured at the user end then quantised and fed back at the transmitter. Some interesting results will be shown in this case, including the lower bound of the maximum achievable rate with bounded CSI error.

2. The CSI error is then linked to the estimation method, in this case, the Least Square (LS) method is considered. The evolution of the capacity lower bound will be studied according to the parameters of the estimation phase, namely the

training Signal-to-Noise Ratio (SNR) and number of pilot symbols.

3. The case where the estimation error is not bounded but follows a Gaussian distribution is investigated and the PDF of the capacity per user is derived in this case. This PDF is then used to derive a new metric called Outage Probability which simplifies the study of the K-user MIMO interference channel with IA. Using the outage probability, the performance of IA will be investigated in a block fading environment and also in cellular networks for inter-cell interference mitigation.

1.1.2 Security

Security is a very important aspect of communication networks, especially in wireless networks, where the communicating parties have less control over who can listen in to their communications. Numerous applications and services require perfect security, for example, online financial transactions, remote health monitoring, remote surveillance of sensitive sites, self-driving cars and more... Recently, security has become an even greater concern for the broad public following the release of confidential documents by Edward Snowden which revealed the extent to which the US intelligence could eavesdrop on personal communications. Following that, point-to-point encryption has begun a democratisation process on messaging apps. However, security in today's networks are mostly based on cryptographic techniques [26, 27] which rely upon mathematical principles that are yet to be proven, the most popular being the RSA encryption algorithm [28, 29] but there are also other methods based on elliptic curves [30–33]. These techniques often require the sharing of a common key to encrypt or decrypt the messages being sent, which increases the implementation complexity.
Wireless networks are moving towards the integration of more and more devices and sensors, these devices, if not careful can represent weak links in an otherwise secure network. A survey made by the company Hewlett Packard in 2014 has found that there is on average 25 security vulnerabilities on the IoT devices then available on the market. Securing these devices using existing cryptographic techniques is difficult or impossible in some case because of their limited processing power or battery life [34, 35]. This will be even more true in the case of sensor networks where each sensor is designed to

function on a battery for an extended period of time, over 10 years for some devices as in the specification of LTE release 13 [36]. This shows that different techniques are needed to insure the security of tomorrow's networks.
The solution that is considered in this dissertation is coming from the area of Physical Layer Security (PLS), the techniques employed by PLS utilise properties of the communication medium to enhance the security of the transmissions. The advantage of PLS is that less constraints can be put on the communicating devices. This property makes it a perfect fit for IoT networks. There has not been a lot of research so far on the application of PLS in IoT networks. In [37] the authors consider a game theoretic approach in order to mitigate the effects of malicious jamming in IoT networks. In this case the idea is to leverage the capabilities of the IoT controller in order to protect the IoT devices against a physical layer attack. The reference [38] published in 2015 contains a comprehensive survey of the advances and remaining challenges to that date to applying PLS to resource constrained IoT networks.
The problem of security in IoT networks is tackled in this dissertation by considering the capabilities of the different devices populating these networks. The strategy will be to create strong interference at the eavesdroppers while ensuring that the IoT controller can always decode the signal it receives from the IoT devices. The focus here is solely on the uplink transmission, i.e. from the IoT devices to the IoT controller.

1.2 Contributions and organisation

In this dissertation, the performance of IA is analysed in the K-user MIMO interference channel when IA is applied to the network with an imperfect knowledge of the channels between the transmitters and receivers. Different applications of the results developed in that context are considered. Furthermore, the problem of protecting IoT uplink data is considered using physical layer security techniques. The rest of this dissertation will be organised as follows :
Chapter 2 : Background on IA and PLS, In this chapter, communication channel models will be introduced to set the context for further work on interference management and security, then, the mathematical aspects and state of the art of Interference

Alignment and Physical Layer Security will be presented.

Chapter 3 : IA with Bounded CSI Error, In this chapter, the case of imperfect CSI with bounded errors is considered and a lower bound of the channel capacity using IA is derived. It's shown that this lower bound is within 1 bps/Hz of the capacity of the perfect CSI case, up to a certain signal-to-noise ratio (SNR) which is referred to as the saturating SNR. Further, a new metric called modified DoF (mDoF) is introduced in order to characterise the multiplexing performance of IA with imperfect CSI at finite SNR. The results obtained are then applied to the case where the CSI is obtained using LS estimation. Simulation results for the 3-user case are provided.

The contributions in this chapter were published in Wireless Communications Letters :

- **R. Guiazon**, K.-K. Wong, and D. Wisely, Capacity analysis of interference alignment with bounded CSI uncertainty, Wireless Communications Letters, IEEE, vol. 3, no. 5, pp. 505-508, Oct 2014.
- **Guiazon, R.F.**; Kai-Kit Wong; Fitch, M., "Evolution of capacity lower bound of interference alignment with least-square channel estimation," in Signal and Information Processing (ChinaSIP), 2015 IEEE China Summit and International Conference on , vol., no., pp.582-585, 12-15 July 2015

Chapter 4 : Distribution of the Capacity with Gaussian CSI error. In this chapter, achievable performance of the interference channel is studied when perfect IA techniques are used based on imperfect CSI. In particular, the statistical distribution of the maximum achievable rate per stream of the channel is obtained. Utilising this analytical results, new non-asymptotic performance metrics are derived then used to 1) optimise the number of streams per user for maximising the network sum-rate and 2) assess the performance of IA in the time-varying block fading channel. Numerical results are provided to reveal the accuracy of these analytical results.

The contributions of this chapter were published in the journal Transaction on Wireless Communications.

- **Guiazon, R.F.**; Wong, Kai-Kit; Fitch, M., "Capacity Distribution for Interference Alignment with CSI Errors and Its Applications," in Wireless Communica-

tions, IEEE Transactions on , vol.PP, no.99, pp.1-1

Chapter 5 : Coverage probability. In this chapter, the application of IA in cellular networks is considered. The issue here is the reduction of inter-cell interference between neighbouring cells especially for the mobile devices located near the cell edges. An expression of the coverage probability is given and compared with the results given by the simulation model.
The contribution of this chapter were published in the special issue on Next Generation Wireless Communications.

- R. Guiazon, K. K. Wong, and M. Fitch, "Coverage probability of cellular networks using interference alignment under imperfect CSI," Digital Commun., SI on Next Generation Wireless Commun. Tech.

Chapter 6 : PLS in IoT Networks. In this chapter, the problem of securing IoT uplink data is considered. Full-duplex, jamming techniques and helper nodes are used together to help low-power IoT devices secure their communications. The concept of neutralisation region is also utilised in order to characterise the performance of an abstract model where some regions of the network are protected against eavesdroppers by helper nodes.
Chapter 7 : Conclusion and Future work. This chapter will summarise the main achievements of this work and introduce a new system model for future work.

Chapter 2

Background on IA and PLS

The objective of this chapter, is to provide the reader with the tools and information necessary to understand the development that will follow in the subsequent chapters of this dissertation. References will be provided for the interested readers to gain a deeper understanding of the notions introduced throughout.
General information about communication channels will be provided at first then, the focus will shift onto the Interference Channel (IC) it will be the main framework for the study of IA in following chapters. Subsequently, the basics of Interference Alignment will be introduced as well as Physical Layer Security.

2.1 Introduction

In the late 1940s, Claude Shannon invented the first systematic framework to describe and analyse communication channels [39]. Originally his intention was to characterise the amount of information that could be transmitted through telephone lines and correct for distortions. The ideas presented in his paper, "A mathematical theory of communication" were groundbreaking and still form as of today, the foundations of Information Theory.
Shannon's communication channel consists of a transmitter that sends information through a transmission medium -with noise and distortion- and a receiver that wants to decode all information sent by the transmitter free of distortion. This first com-

munication channel is called Point to Point channel, since the information flows from a single transmitter to a single receiver. Shannon's analysis of this channel was quite extensive, defining rigorously the notion of channel capacity that would guide engineers for many years throughout the optimisation of communication networks.
Today's networks are made of multiple transmitters and receivers with various communication scenarios. Ultimately, the Graal of Information Theory would be the characterisation of the capacity region of a general communication channel where, all the nodes are allowed to communicate with whichever other node inside the network. However due to possible interference between the nodes, this characterisation has eluded researchers ever since Shannon formalised his theory. Even in the case of two transmitter-receiver pairs with each transmitter creating interference at the other receiver, the complete characterisation of the capacity region has not been found yet. The characterisation of the capacity region of the 2-user interference channel has been done in very special cases [40–42], where counter-intuitively it is shown that strong interference doesn't harm the capacity. A tight approximation within half a bit of the capacity region was given in [43] in 1981 and for nearly 3 decades not much happened in this area.
The study of the general communication channel mentioned above being too complex, researchers have focused on simplified models that still provide insights into how to optimise modern communication networks. Examples of such models and their applications are listed below.

- The Gaussian point-to-point channel, this channel is one of the simplest that one could imagine, it consists of one transmitter and one receiver transmitting messages through a channel that is corrupted by additive white Gaussian noise. As simple as it seems, finding the capacity of this channel had to wait for Claude Shannon in 1948. Circuit switched networks are typical examples.

- The broadcast channel (BC) is a type of communication channel where one transmitter wishes to send information to several receivers, for example the downlink of cellular networks or the Digital television (DTV) network are broadcast channels. The set of simultaneously achievable rate by all user is the relevant metric in this case [44]. The capacity region of this type of channel is not known in general but

several inner bounds and outer bounds have been derived that coincide in specific cases with the capacity region [44–48].

- The Multiple Access Channel (MAC) consists of many users trying to send information to the same receiver. This corresponds for example to the case where several devices send information to the same base station. This will be the framework of chapter 6 when IoT networks are considered.

- The Interference Channel (IC) is the model that we'll be focusing on in the next chapters, it is formed of K pairs of transmitters and receivers where each transmitter wishes to communicate with a single receiver but at the receiver side the reception is impaired by all the signals coming from the unwanted transmitters. This channel includes all previous channels as special cases. A cellular network can be studied under this model. For example, the transmitters could be adjacent base stations and the receivers would the users belonging to different cells but that are scheduled on the same time/frequency.

2.2 More on the Interference Channel

An example of interference channel can be seen on figure 2.1 for the K=3 user case. The received signal at any receiver (say k) is given by the following expression

$$\mathbf{y}_k = \underbrace{\mathbf{H}_{k,k}\mathbf{x}_k}_{\text{Desired signal}} + \underbrace{\sum_{\substack{i=1,\\ i\neq k}}^{K} \mathbf{H}_{k,i}\mathbf{x}_i}_{\text{Interference}} + \underbrace{\boldsymbol{\eta}_k}_{\text{Noise}} \tag{2.1}$$

Where K is the number of user pair, $\mathbf{H}_{k,i}$ is the channel matrix between the i^{th} transmitter and the k^{th} receiver, $\boldsymbol{\eta}_k$ is the noise, $\mathbf{x}_i$ is the signal from transmitter i and $\mathbf{y}_k$ is the received signal at the k^{th} receiver.

In the interference channel, the performance of the network is limited by the interference received from the other users, that's because the interference signal produced by the unintended transmitters can be of power comparable to that of the desired signal.

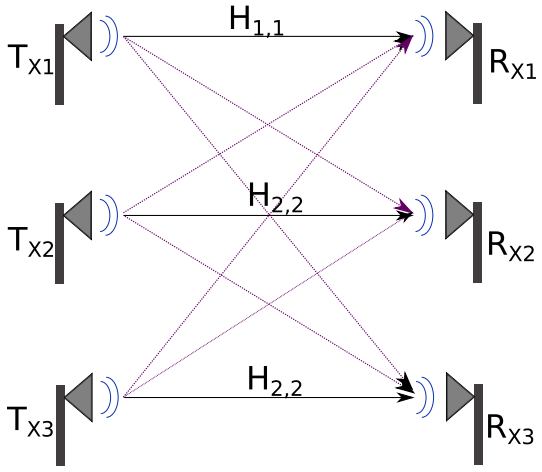


Figure 2.1: Interference Channel with 3 users, transmitters on the left and receivers on the right. Dotted lines represent interference whereas plain lines are the desired links

This is the case for example in the downlink of cellular networks when users are located at the cell edges. Therefore it is very important to find efficient ways to mitigate this interference.
There are several methods used to mitigate interference in the interference channel :

- Consider interference as noise [49–51] : This solution works when the desired signal power is greater than the aggregated interference. In [51] this assumption was used in order to obtain tractable inner bound of the capacity region of the IC.

- Decode the interference first [40] : This can be applied when the interference power is stronger than the signal power. It becomes more and more impractical when the number of user increases.

- Use orthogonalisation across time (TDMA), frequency (FDMA) or code (CDMA) [52] : That's the most commonly used method however the drawback is that the available resource per user decreases when more users join the network.

- Code over the interference (Dirty paper coding) [53] : This technique requires knowledge of the other user data in a non causal way which makes it more suited for use in the broadcast channel model.

Recently IA was added to this list as a new method to mitigate the interference in wireless networks. This happened when Jafar and Shamai in [9] showed that by doing some smart precoding it was possible to achieve the Degree-Of-Freedom (DoF) of the MIMO X channel. The DoF being defined as the pre-log factor in the expression of the sum-Rate of the network which can also be expressed as

$$\text{DoF} = \lim_{\rho \to \infty} \frac{R_\Sigma(\rho)}{\log(\rho)} \tag{2.2}$$

Where ρ represents the Signal-to-Noise Ratio (SNR) and R_Σ is the sum-rate of the network.

2.3 Interference Alignment

Interference Alignment is a linear precoding technique, it is implemented in the K-user interference channel by designing precoding matrices at the transmitters and decoding matrices at the receivers which are able to confine the interference at each receiver in a reduced dimension space and keep the desired signals in a space orthogonal to the interference space. The principles of IA were introduced in [9, 54] and further developed in [10] where the authors considered a K-user frequency selective or time varying interference channel with global channel state information (CSI) - Knowledge of the channel matrices at every node of the network. With this setting they have shown that using interference alignment would enable each user to access half of the total available resource (time or frequency) at high SNR regardless of the number of user in the network. This approach was thus called the *half the cake* approach in analogy to a way of slicing a cake such that everyone could get half of it regardless of the number of people. This is in sharp contrast with the orthogonalisation techniques where the total available resource is divided equally amongst the different users, meaning that they all get $\frac{1}{K}$ of the total resource if K is the total number of user.
The principle of interference alignment is illustrated on the figure 2.2 and 2.3 where it is shown how by aligning the interference on the same time slot, the users manage to

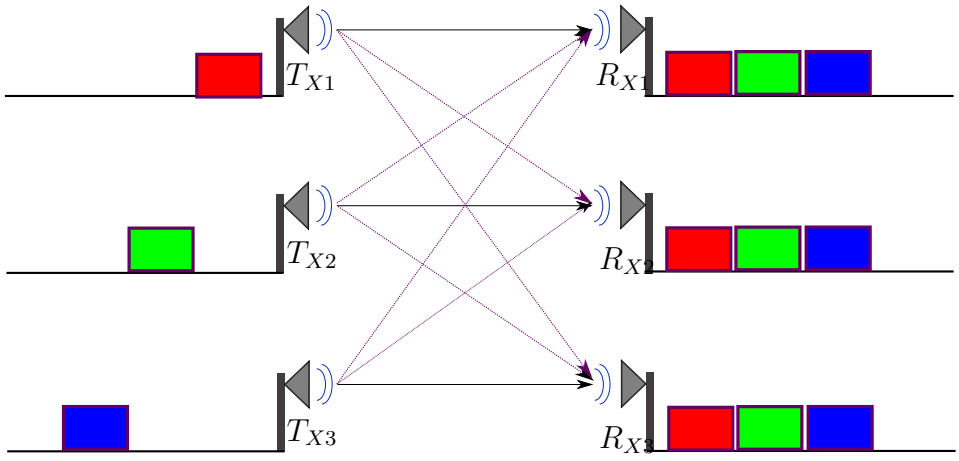


Figure 2.2: Illustration of the TDMA transmission scheme where every user transmits its signal at a given time slot that does not overlap with the other user's time slots.

recover the desired information free from interference using only 2 time slots instead of 3 as is the case in a TDMA system. In this toy example the trick is that the signal travels faster on the direct links by one time slot compared to the cross-links.
Even though interference alignment can be applied using time or frequency diversity, it is limited by the assumption about full channel knowledge especially in the case of time varying channels where it's impractical to know the channel coefficients in advance or instantly at all transmitting and receiving nodes. Because of this, a lot of research has been produced on IA in the K-user MIMO interference channel with constant channel coefficients over time [23, 55, 56]. In this case, IA is implemented using the spatial dimensions offered by MIMO systems.

The aim of interference Alignment when using spatial dimensions is the same - confine the interference in a reduced dimension space and transmit the desired signal into a space orthogonal to the interference space (Figure 2.4).
The drawback is that with only finite spatial dimensions it's been shown [57] that the total DoF achievable by the network is at most $\frac{2}{K}$ which is far from the $\frac{1}{2}$ initially promised by IA.
A mathematical definition of IA will given below. But first, let's take a look at the

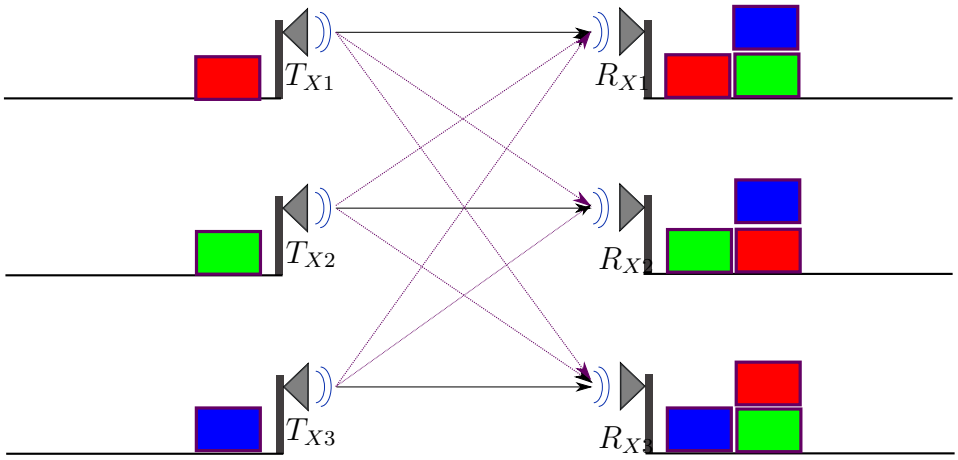


Figure 2.3: Illustration of the Interference Alignment scheme where the interference are aligned at the receivers so that only 2 times slots are needed instead of 3.

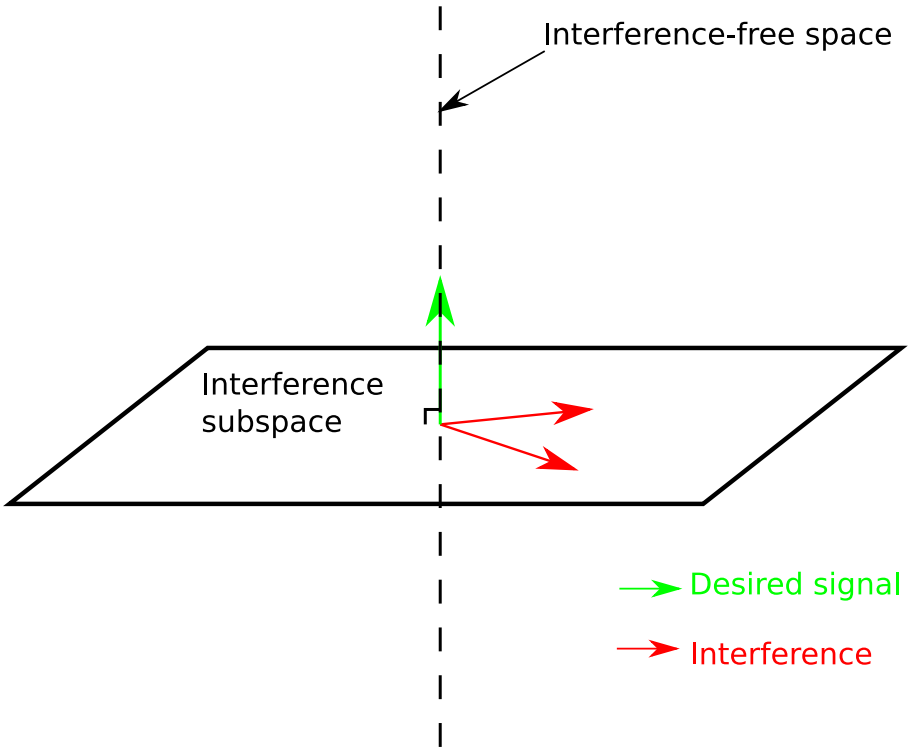


Figure 2.4: Illustration of IA in a 3-dimension space

expression (2.1) of the signal received by the k^{th} user of the network.

$$\mathbf{y}_k = \underbrace{\mathbf{H}_{k,k}\mathbf{x}_k}_{\text{Desired signal}} + \underbrace{\sum_{\substack{i=1,\\ i\neq k}}^{K} \mathbf{H}_{k,i}\mathbf{x}_i}_{\text{Interference}} + \underbrace{\eta_k}_{\text{Noise}}$$

Each receiver wants to get rid of the interference term and keep only the desired signal, therefore with the knowledge of the channel matrices $\mathbf{H}_{i,j}\ \forall(i,j)$ the users will generate precoders $\mathbf{V}_k$ to separate the desired signal and the interference into orthogonal vector spaces at every receiver and will also generate interference cancelling matrices $\mathbf{U}_k$ that will be applied at each receiver to suppress the interference and leave the desired signal interference free.
The matrices $\mathbf{V}_k$ and $\mathbf{U}_k$ are defined after the following conditions :

$$\begin{cases} \text{rank}(\mathbf{U}_k\mathbf{H}_{k,k}\mathbf{V}_k) = d_k \\ \quad \mathbf{U}_k\mathbf{H}_{k,j}\mathbf{V}_j = 0 \qquad \forall(k,j) \end{cases} \tag{2.3}$$

Where d_k is the number of streams that the k^{th} user wants to transmit.
The conditions above are not always achievable, therefore there's been a large body of literature dealing with the feasibility conditions of interference alignment [23–25].

2.4 Interference Alignment with Imperfect CSI

The IA method presented so far involved only perfect channel knowledge at all the nodes of the network, however in a practical scenario the channel state will have to be estimated and therefore will be imperfect. Different kinds of phenomena influence the quality of the CSI, from mobility to rain. Even with high estimation accuracy, the CSI becomes naturally outdated because of slow variations of the channel. Moreover, assuming that the CSI is known globally implies that some information has to be fed back between the nodes of the network and will cause some quatization error and overhead [19]. Motivated by this, some algorithms have been designed in [11, 58] to

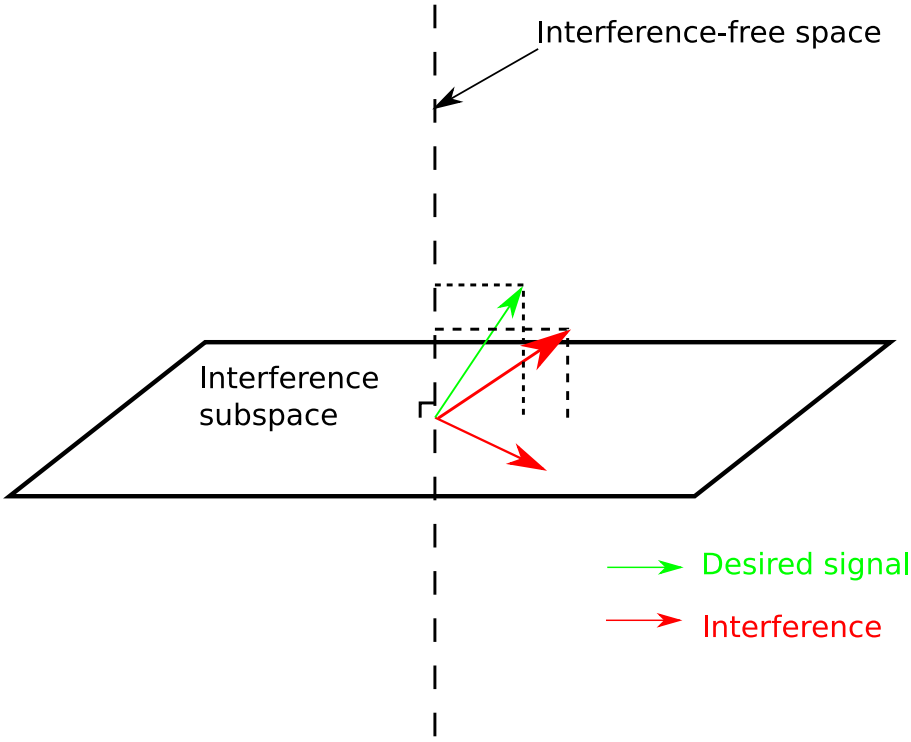


Figure 2.5: Illustration of imperfect IA in a 3-dimension space

perform Interference Alignment with local knowledge only. But these algorithms require channel reciprocity between the transmitters and the receivers which is not always guaranteed in practice.

If imperfect CSI is considered, then the interference created at each receiver will not be perfectly aligned and some of the interference power will end up in the desired signal space and corrupt the desired message, in the same way some of the desired signal power will leak into the interference vector space and will be cancelled out by the interference cancelling matrix (Figure 2.5). It's been shown in [18, 19] how the average sum-rate of the network is affected by the channel estimation error, the performance of IA with imperfect CSI in the Interference Broadcast channel has also been investigated in [20] where an IA algorithm robust to CSI uncertainty is provided.

2.5 Physical Layer Security

At the early age of communication security, secret keys known only to the transmitter and receiver were the only way to ensure confidentiality. For example, the Vernam's one-time pad cipher [59] is an excellent illustration of this, where the message being transmitted is XORed with a random key of the same length.

The mathematical foundations for modern information-theoretical security were laid by Shannon [60] in 1949. In his work, was considered a model where a secret key is used only once to encrypt the message. The notion of perfect secrecy was introduced to say that the cryptogram generated by encrypting the message with the secret key does not provide any information about the original message. This implies that the a posteriori probability of the transmitted message computed at the eavesdropper using the received signal is equal to its a priori probability. Intuitively this means that from an eavesdropper point of view, receiving the cryptogram and trying to recover the original message based on that, is equivalent to guessing it at random from the same distribution as the source. It also implies [61, 62] perfect secrecy is achievable if the secret key has at least as much entropy as the message to be encrypted.

Physical layer security has really taken momentum after the work of Wyner [63] in 1975, where the degraded wire-tap channel model was introduced. In this model shown on figure 2.6, a message S is generated by a random source then encoded into a signal X by the transmitter, that signal is sent through a channel where it's degraded and received by the receiver as Y, then Y is further degraded passing through a wire-tap channel to the eavesdropper and received as Z by the latter. This model has been further developed by Carleial and Hellman in [64, 65]. Wyner's objective was to maximise the transmission rate to the receiver whilst minimising the amount of information leaked to the eavesdropper. However, the definition of security used by Wyner is weaker than the perfect secrecy introduced by Shannon. For a single message S uniformly distributed over $\{1, \cdots, 2^{nR}\}$ (where R is the transmission rate) that the transmitter wants to send, Wyner's secrecy requires that $\forall \epsilon > 0$, $R_e - \epsilon \leq \frac{1}{n} H(S|Z^n)$. Where R_e is the equivocation rate or the uncertainty of the wire-tapper on the message S and $\dot{H()}$ represents the entropy function.

PLS can be subdivided into two main area of research. The first is secret key generation

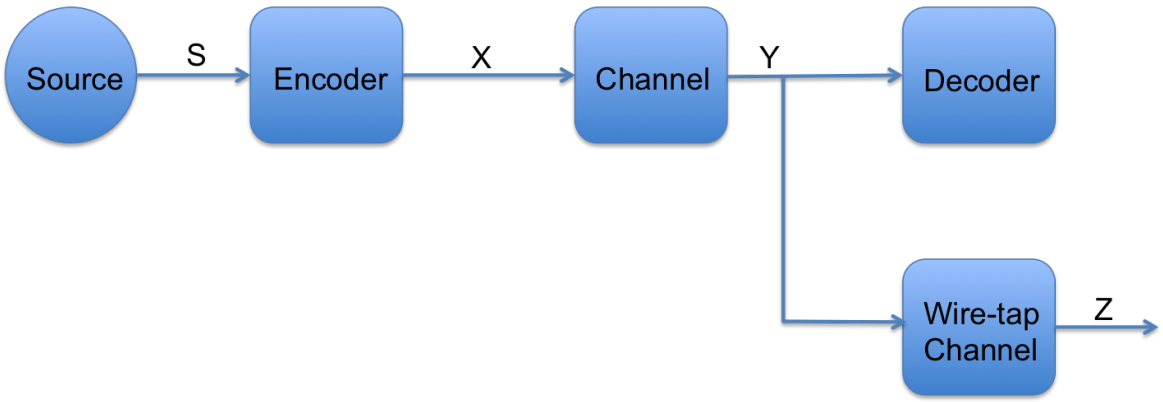


Figure 2.6: The wire-tap channel introduced by Wyner

based on the channel variations and the second consists in using directly the channel properties to hide the transmitted message.

2.5.1 Secret key generation

Secret key generation dates back to Maurer, Ahlswede and Csiszar [66, 67] in 1993. The strategy is to use the variations of the channel between a transmitter and the intended receiver to generate a secret key that will later on be used to encrypt their transmissions. The main advantage of this technique is that a positive secrecy rate can be achieved even when the main channel to the intended receiver is of worst quality than that of the eavesdropper.

The figure 2.7 shows how the signal received at two different receivers experience different channel conditions. The secret key generation method consists in taking advantage of the difference in the channel condition to generate an encryption key that will be unique to a communication pair.

However, the quality of the keys being generated depends on multiple factors such as the channel variability, the correlation of the channel to the intended receiver with that of the eavesdropper [68–72] and channel reciprocity [73, 74].

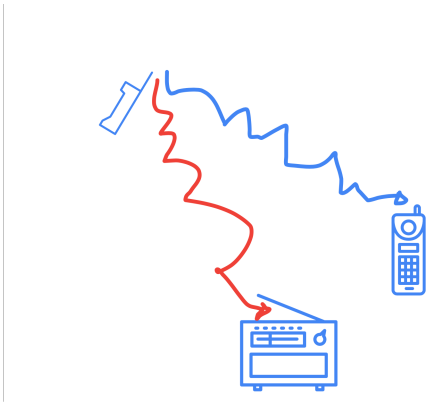


Figure 2.7: Signal taking different path form the transmitter to the intended receiver and eavesdropper

2.5.2 Channel based secrecy

This second category of PLS techniques will be considered in this dissertation to improve secrecy in IoT networks. The fundamental principle is to arrange for the intended receiver to achieve a better channel than the eavesdropper. This strategy comes from the result published in [65] which states that for a degraded wire-tap channel with additive Gaussian noise, the secrecy capacity C_S is given by

$$C_S = C_U - C_E \tag{2.4}$$

Where C_U denotes the capacity of the channel to the intended receiver and C_E represents the capacity of the channel to the eavesdropper. Therefore, in order to increase the secrecy capacity one must increase the channel capacity of the main channel relatively to that of the eavesdropper's channel.
The principal method to achieve this objective is to somehow modify the SINR experienced at both receivers. Several techniques have been developed for that purpose:

- Jamming the eavesdroppers with artificially generated noise (AN). This method was introduced by Goel and Negi in [75, 76].
- Employing directional antennas to limit the signal received by the eavesdroppers [77–79].

- Using beamforming and AN conjointly to increase the SINR at the intended receiver while decreasing it at the eavesdropper [80–83].

The techniques listed above can also be used with other methods such as Interference alignment in the case of artificial noise alignment [84–87].
For a more detailed literature on PLS the reader is referred to the survey paper [88] and the references therein.

Chapter 3

IA with Bounded CSI Error

3.1 Introduction

One major setback for the application of IA in a practical scenario is the need for perfect global channel state information (CSI) at each transmitter.[1] Motivated by this, [11, 58] designed algorithms to perform IA given only local CSI while [18, 19, 89, 90] took into account the errors due to channel estimation and feedback. For example, [19] presented the average achievable rate under a given measurement error power, and [18] established bounds on the average achievable rate with Gaussian CSI errors. Although the results in [18, 19] are indicative, the average rates are operationally unachievable.

In contrast to the previous work, I will derive in this chapter an *achievable* capacity lower bound for IA with imperfect CSI under the model that the CSI errors are bounded. My result reveals several properties that provide guidance in the design of interference networks, and is applicable to any perfect IA methods operating on the imperfect CSI [24, 25]. For example, the case where the Least Square (LS) channel estimation method [91] is used to obtain the CSI will be considered.

[1] Every transmitter needs to possess the CSI for every link in the entire interference network, including those not linking to the transmitter.

3.2 The system Model

Consider an interference channel with K pairs of transmitters and receivers. Each pair is regarded as a user. It is assumed that user i has m_i transmit antennas and n_i receive antennas. Every transmitter is assumed to possess the estimated channel matrices between transmitter j to receiver i, $\hat{\mathbf{H}}_{i,j}$, for all i, j. As in [24, 25], consider that perfect IA is adopted based on the estimated CSI, $\{\hat{\mathbf{H}}_{i,j}\}$, that permits the ith user to transmit d_i data streams. This means that for each user i, the perfect precoder $\mathbf{V}_i$ and interference cancelling matrix $\mathbf{U}_i$ are provided so that to perform IA over all $\hat{\mathbf{H}}_{i,j}$.

In reality, the estimated channels are imperfect and the real channels, $\mathbf{H}_{i,j}$, can be written as

$$\mathbf{H}_{i,j} = \hat{\mathbf{H}}_{i,j} + \Delta\mathbf{H}_{i,j}, \tag{3.1}$$

where $\Delta\mathbf{H}_{i,j}$ denotes the channel measurement errors. In this model the errors are considered bounded [92] such that

$$\delta_{i,j}^2 = \max_k \|(\Delta\mathbf{H}_{i,j})_k\|_2^2, \text{ for some given } \delta_{i,j} \geq 0, \tag{3.2}$$

where $(\Delta\mathbf{H}_{i,j})_k$ denotes the kth row of $\Delta\mathbf{H}_{i,j}$.

The received signals in vector form at user i are given by

$$\mathbf{y}_i = \mathbf{H}_{i,i}\mathbf{V}_i\mathbf{x}_i + \mathbf{H}_{-i}\mathbf{V}_{-i}\mathbf{x}_{-i} + \boldsymbol{\eta}_i, \tag{3.3}$$

where $\mathbf{H}_{-i} \triangleq [\mathbf{H}_{i,1} \cdots \mathbf{H}_{i,i-1}\ \mathbf{H}_{i,i+1} \cdots \mathbf{H}_{i,K}]$,

$$\mathbf{V}_{-i} \triangleq \begin{bmatrix} \mathbf{V}_1 & \mathbf{0} & \cdots & & \cdots & \mathbf{0} \\ \mathbf{0} & \ddots & & \vdots & & \vdots \\ & \mathbf{0} & \mathbf{V}_{i-1} & \mathbf{0} & \cdots & \\ & \cdots & \mathbf{0} & \mathbf{V}_{i+1} & \mathbf{0} & \\ \vdots & & & \vdots & \ddots & \mathbf{0} \\ \mathbf{0} & \cdots & & \cdots & \mathbf{0} & \mathbf{V}_K \end{bmatrix}, \tag{3.4}$$

$\mathbf{x}_{-i} \triangleq [\mathbf{x}_1^T \cdots \mathbf{x}_{i-1}^T \ \mathbf{x}_{i+1}^T \cdots \mathbf{x}_K^T]^T$ in which $\mathbf{x}_j$ is the transmitted data stream vector by user j and $\boldsymbol{\eta}_i$ denotes the additive zero-mean N_0-variance Gaussian noise vector at user i.

For convenience, all users are assumed to have the same average power constraint, $\mathbb{E}(\|\mathbf{x}_i\|_2^2) = \sum_{k=1}^{d_i} \mathbb{E}(|(\mathbf{x}_i)_k|^2) \leq \mathcal{E}$ where $\mathbb{E}(\cdot)$ returns the expectation of the input random entity.

3.3 Definition and derivation of new metrics

This section will carry out the study of the model defined above with the purpose of defining new and insightful metrics to analyse the performance of IA in the bounded CSI case.

3.3.1 Capacity Lower Bound

The first important metric that will be derived is the capacity lower bound of any stream of a given user i in the IA model with imperfect CSI. $\hat{\mathbf{H}}_{-i}$ is defined similarly to $\mathbf{H}_{-i}$ but for the estimated CSI matrix and $\Delta\mathbf{H}_{-i}$ for the CSI error matrix, excluding the direct channel for user i. Hence, $\mathbf{H}_{-i} = \hat{\mathbf{H}}_{-i} + \Delta\mathbf{H}_{-i}$.

Accordingly, the signal model, (3.3) becomes

$$\mathbf{y}_i = \hat{\mathbf{H}}_{i,i}\mathbf{V}_i\mathbf{x}_i + \hat{\mathbf{H}}_{-i}\mathbf{V}_{-i}\mathbf{x}_{-i} + \Delta\mathbf{H}_{i,i}\mathbf{V}_i\mathbf{x}_i + \Delta\mathbf{H}_{-i}\mathbf{V}_{-i}\mathbf{x}_{-i} + \boldsymbol{\eta}_i. \tag{3.5}$$

Applying the interference canceling matrix on (3.5) gives

$$\mathbf{U}_i^*\mathbf{y}_i = \underbrace{\mathbf{U}_i^*\hat{\mathbf{H}}_{i,i}\mathbf{V}_i\mathbf{x}_i}_{\text{Desired Signal}} + \underbrace{\mathbf{U}_i^*\hat{\mathbf{H}}_{-i}\mathbf{V}_{-i}\mathbf{x}_{-i}}_{=0} + \underbrace{\mathbf{U}_i^*\Delta\mathbf{H}_{i,i}\mathbf{V}_i\mathbf{x}_i + \mathbf{U}_i^*\Delta\mathbf{H}_{-i}\mathbf{V}_{-i}\mathbf{x}_{-i}}_{\text{Interference}} + \underbrace{\mathbf{U}_i^*\boldsymbol{\eta}_i}_{\text{Noise}}. \tag{3.6}$$

Being able to bound the powers of the different terms in the expression above will help to derive the capacity lower bound.

First, focus on the interference caused by other users at the ith receiver. The matrix $\Delta\mathbf{H}_{-i}\mathbf{V}_{-i}$ is responsible for that interference. In the general case, $\texttt{span}(\Delta\mathbf{H}_{-i}\mathbf{V}_{-i})$

overlaps with the space designed for the desired signal and also that designed for the interference signal meaning that

$$\Delta\mathbf{H}_{-i}\mathbf{V}_{-i} = \underbrace{\mathbf{U}_i^*\Delta\mathbf{H}_{-i}\mathbf{V}_{-i}}_{\text{span } \subset \text{ desired space}} + \underbrace{(\mathbf{I}-\mathbf{U}_i^*)\Delta\mathbf{H}_{-i}\mathbf{V}_{-i}}_{\text{span } \subset \text{ interference space}}. \tag{3.7}$$

The worst case arises if all the interference goes to the signal space, i.e., $\Delta\mathbf{H}_{-i}\mathbf{V}_{-i} = \mathbf{U}_i^*\Delta\mathbf{H}_{-i}\mathbf{V}_{-i}$. Thus, the interference power caused by other users can be upper bounded by

$$\mathcal{I}_i \leq \mathbb{E}\left(\|\Delta\mathbf{H}_{-i}\mathbf{V}_{-i}\mathbf{x}_{-i}\|_2^2\right), \tag{3.8}$$

where the expectation is taken over the data stream $\mathbf{x}_{-i}$.

Proposition 1. *The upper bound for the received interference power caused by other users at user i is given by:*

$$\mathcal{I}_i \leq n_i\delta_{\max}^2 D(K-1)\mathcal{E}, \tag{3.9}$$

where $D \triangleq \max_i \sum_{\substack{k=1\\k\neq i}}^{K} d_k$ and $\delta_{\max} \triangleq \max_{i,j}\delta_{i,j}$.

Proof. Let $\Delta\tilde{\mathbf{h}}_1$ denote the first column of $\Delta\mathbf{H}_{-i}\mathbf{V}_{-i}$ and $\boldsymbol{v}_1^{(1)}$ be the first column of $\mathbf{V}_1$. Then we have

$$\Delta\tilde{\mathbf{h}}_1 = \begin{bmatrix} (\Delta\mathbf{H}_{i,1})_1\boldsymbol{v}_1^{(1)} \\ (\Delta\mathbf{H}_{i,1})_2\boldsymbol{v}_1^{(1)} \\ \vdots \end{bmatrix}. \tag{3.10}$$

Clearly,

$$|(\Delta\mathbf{H}_{i,1})_k\boldsymbol{v}_1^{(1)}|^2 \leq \underbrace{\|(\Delta\mathbf{H}_{i,1})_k\|_2^2}_{\leq\delta_{i,1}^2}\underbrace{\|\boldsymbol{v}_1^{(1)}\|_2^2}_{\leq 1} \leq \delta_{i,1}^2 \leq \delta_{\max}^2. \tag{3.11}$$

As a result, we get $\|\Delta\tilde{\mathbf{h}}_k\|_2^2 \leq n_i\delta_{\max}^2$ because the same upper bound is valid for any column (say kth column) of $\Delta\mathbf{H}_{-i}\mathbf{V}_{-i}$.

Furthermore, we can write

$$\Delta\mathbf{H}_{-i}\mathbf{V}_{-i}\mathbf{x}_{-i} = \sum_j (\mathbf{x}_{-i})_j\Delta\tilde{\mathbf{h}}_j. \tag{3.12}$$

Now consider

$$\left\| \sum_j (\mathbf{x}_{-i})_j \Delta\tilde{\mathbf{h}}_j \right\|_2 \leq \sum_j |(\mathbf{x}_{-i})_j| \|\Delta\tilde{\mathbf{h}}_j\|_2, \\ \leq \sqrt{n_i}\delta_{\max} \sum_j |(\mathbf{x}_{-i})_j|. \tag{3.13}$$

Note that $\sum_j |(\mathbf{x}_{-i})_j| = \|\mathbf{x}_{-i}\|_1$ and since $\|\mathbf{a}\|_1 \leq \sqrt{N}\|\mathbf{a}\|_2$ (with N being the length of vector $\mathbf{a}$), we have

$$\mathbb{E}\left(\|\Delta\mathbf{H}_{-i}\mathbf{V}_{-i}\mathbf{x}_{-i}\|_2^2\right) \leq n_i\delta_{\max}^2 D\mathbb{E}(\|\mathbf{x}_{-i}\|_2^2), \\ \leq n_i\delta_{\max}^2 D(K-1)\mathcal{E}, \tag{3.14}$$

which completes the proof. □

Next, consider the effects of the uncertainty on the kth stream of the ith user when the transmit power is $E_k^{(i)}$. Denote $\boldsymbol{v}_k^{(i)}$ and $\boldsymbol{u}_k^{(i)}$ as the kth column of $\mathbf{V}_i$ and $\mathbf{U}_i$, respectively. The signal component of the kth stream of user i is

$$\sqrt{E_k^{(i)}}\mathbf{H}_{i,i}\boldsymbol{v}_k^{(i)} = \sqrt{E_k^{(i)}}\hat{\mathbf{H}}_{i,i}\boldsymbol{v}_k^{(i)} + \sqrt{E_k^{(i)}}\Delta\mathbf{H}_{i,i}\boldsymbol{v}_k^{(i)}. \tag{3.15}$$

The worst case occurs if $\Delta\mathbf{H}_{i,i}\boldsymbol{v}_k^{(i)}$ is orthogonal to $\mathbf{H}_{i,i}\boldsymbol{v}_k^{(i)}$. In this case, the signal power in the kth stream at user i is

$$P_k^{(i)} = |\sqrt{E_k^{(i)}}\boldsymbol{u}_k^{(i)*}\hat{\mathbf{H}}_{i,i}\boldsymbol{v}_k^{(i)}|^2 - |\sqrt{E_k^{(i)}}\boldsymbol{u}_k^{(i)*}\Delta\mathbf{H}_{i,i}\boldsymbol{v}_k^{(i)}|^2. \tag{3.16}$$

Also, $|\sqrt{E_k^{(i)}}\boldsymbol{u}_k^{(i)*}\Delta\mathbf{H}_{i,i}\boldsymbol{v}_k^{(i)}|^2 \leq n_i\delta_{\max}^2 E_k^{(i)}$. Define $\sigma_k^{(i)} \triangleq \boldsymbol{u}_k^{(i)*}\hat{\mathbf{H}}_{i,i}\boldsymbol{v}_k^{(i)}$. Therefore, we have

$$P_k^{(i)} \geq \left((\sigma_k^{(i)})^2 - n_i\delta_{\max}^2\right) E_k^{(i)}, \tag{3.17}$$

Where it's assumed that $(\sigma_k^{(i)})^2 \geq n_i\delta_{\max}^2$. This means that the contribution of the error in the channel estimates is less than that of the actual channels.

Proposition 2. *The inter-stream interference power on the kth stream of user i is*

upper bounded by

$$\mathcal{S}_k^{(i)} \leq n_i \delta_{\max}^2 (\mathcal{E} - E_k^{(i)}). \tag{3.18}$$

Proof. Let $\mathbf{V}_i^{(-k)}$ be the precoding matrix $\mathbf{V}_i$ excluding the kth column and $\mathbf{x}_i^{(-k)}$ be the data vector $\mathbf{x}_i$ excluding the kth stream of the ith user. Then the worst case happens if all the power lost by other streams creates interference. That is,

$$\mathcal{S}_k^{(i)} = \|\Delta \mathbf{H}_{i,i} \mathbf{V}_i^{(-k)} \mathbf{x}_i^{(-k)}\|_2^2 = \sum_{l=1}^{n_i} |(\Delta \mathbf{H}_{i,i})_l \mathbf{V}_i^{(-k)} \mathbf{x}_i^{(-k)}|^2, \tag{3.19}$$

which can be upper bounded by

$$\begin{aligned}
\mathcal{S}_k^{(i)} &\leq \sum_{l=1}^{n_i} \|(\Delta \mathbf{H}_{i,i})_l\|_2^2 \|\mathbf{V}_i^{(-k)} \mathbf{x}_i^{(-k)}\|_2^2 && (3.20)\\
&\leq n_i \delta_{i,i}^2 \|\mathbf{V}_i^{(-k)} \mathbf{x}_i^{(-k)}\|_2^2 && (3.21)\\
&= n_i \delta_{i,i}^2 \|\mathbf{x}_i^{(-k)}\|_2^2 && (3.22)\\
&\leq n_i \delta_{\max}^2 \|\mathbf{x}_i^{(-k)}\|_2^2 = n_i \delta_{\max}^2 (\mathcal{E} - E_k^{(i)}), && (3.23)
\end{aligned}$$

which is the desired result and the proof is completed. □

Theorem 1. *A capacity lower bound for the kth stream of the ith user is given by*

$$C_k^{(i)} \geq \log_2 \left(1 + \frac{\left((\sigma_k^{(i)})^2 - n_i \delta_{\max}^2 \right) E_k^{(i)}}{N_0 + n_i \delta_{\max}^2 \left((D(K-1)+1)\mathcal{E} - E_k^{(i)} \right)} \right). \tag{3.24}$$

Proof. Using (3.9), (3.17) and (3.18) gives the result. □

Corollary 1. *If each user has only one stream, the capacity lower bound in (3.24) becomes*

$$\underline{C}_i(\rho) = \log_2 \left(1 + \frac{(\sigma_i^2 - n_i \delta_{\max}^2)\rho}{1 + n_i \delta_{\max}^2 (K-1)^2 \rho} \right), \tag{3.25}$$

where $\rho \triangleq \frac{\mathcal{E}}{N_0}$ *and* $\sigma_k^{(i)}$ *in (3.24) is replaced by* σ_i.

Proof. In this case, (3.18) is not used and $D = K - 1$. □

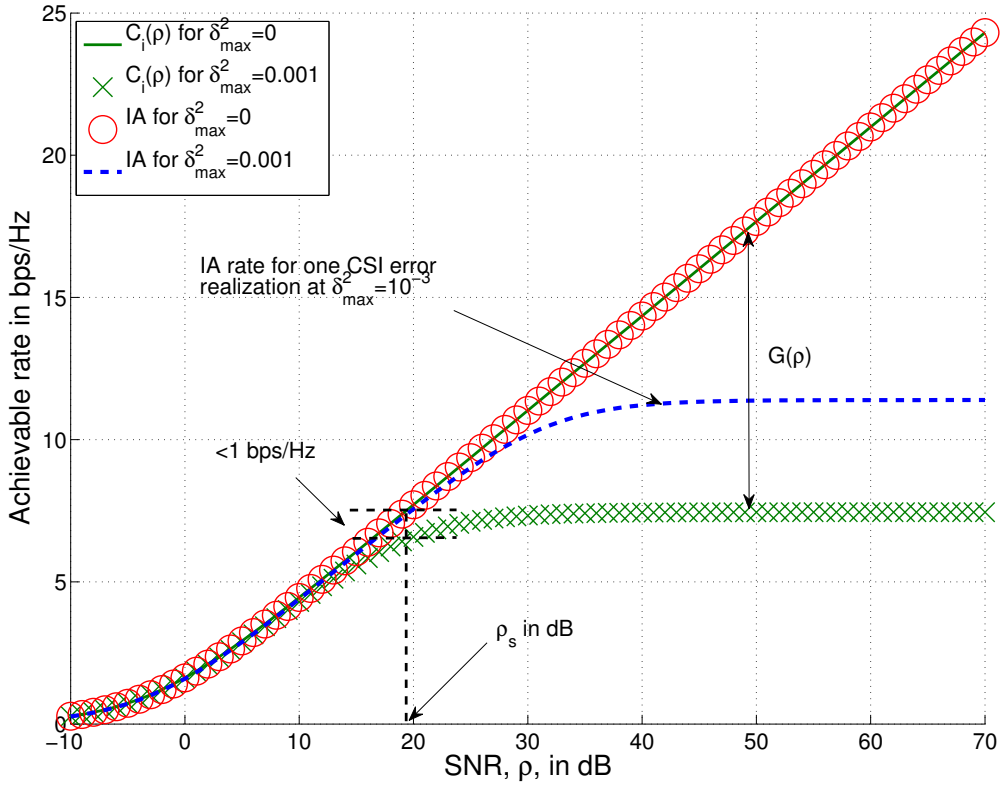


Figure 3.1: The capacity lower bound in the single-stream case.

3.3.2 Saturating SNR and mDoF

In Fig. 3.1, the capacity lower bound $\underline{C}_i$ is plotted for the cases $\delta^2_{\max} = 0$ and $\delta^2_{\max} = 0.001$ assuming that $\sigma_i = 1$. A saturation point in SNR can be seen and one can observe that after this point any further increase in SNR will not lead to a useful increase in the achievable rate due to the CSI errors. This point is referred to as the saturating SNR and will be studied in the following paragraphs.

Theorem 2. *The saturating SNR, ρ_s, is given by*

$$\rho_s = \frac{1}{\sigma_i^2} + \frac{1 - \frac{n_i \delta^2_{\max}}{\sigma_i^2}}{n_i \delta^2_{\max}(K-1)^2} \overset{(a)}{\simeq} \frac{1}{\sigma_i^2} + \frac{1}{n_i \delta^2_{\max}(K-1)^2}, \tag{3.26}$$

where (a) *is due to the fact that typically* $n_i\delta_{\max}^2 \ll \sigma_i^2$.

Proof. Let $A = \sigma_i^2 - n_i\delta_{\max}^2$ and $B = n_i\delta_{\max}^2(K-1)^2$. Hence, we have $\underline{C}_i(\rho) = \log_2(1 + \frac{A\rho}{1+B\rho})$. Further, define the SNR in dB as $\rho_{\text{dB}} = 10\log_{10}\rho$. When $\delta_{\max} = 0$ and at high SNR, the capacity lower bound becomes

$$\begin{aligned}\underline{C}_i(\rho_{\text{dB}})|_{\delta_{\max}=0} &\simeq \log_2(\sigma_i^2 10^{\frac{\rho_{\text{dB}}}{10}}) \\ &= \log_2\sigma_i^2 + \frac{\log_2 10}{10}\rho_{\text{dB}}. \end{aligned} \tag{3.27}$$

The saturating SNR occurs when

$$\underline{C}_i(\rho_{s,\text{dB}})|_{\delta_{\max}=0} = \underline{C}_i(\infty)|_{\delta_{\max}\neq 0}\,, \tag{3.28}$$

which implies that

$$\begin{aligned}\log_2\sigma_i^2 + \frac{\log_2 10}{10}\rho_{s,\text{dB}} &\overset{(a)}{=} \log_2(1+\frac{A}{B}) \\ \rho_{s,\text{dB}} &= 10\log_{10}(\frac{1}{\sigma_i^2} + \frac{A}{B\sigma_i^2}),\end{aligned}$$

where (a) is due to high SNR approximation and (3.27). The desired result in the linear scale is immediately obtained. □

Corollary 2. *At* $\rho = \rho_s$, *if* $n_i\delta_{\max}^2 \ll \sigma_i^2$, *the capacity lower bound is within* 1bps/Hz *of the rate without CSI errors, i.e.,*

$$G(\rho_s) = \underline{C}_i(\rho_s)|_{\delta_{\max}=0} - \underline{C}_i(\rho_s)|_{\delta_{\max}\neq 0} \leq 1\text{bps/Hz}. \tag{3.29}$$

Proof. At the saturating SNR,

$$\begin{aligned} G(\rho_s) &\overset{(a)}{=} \log_2\left(1+\sigma_i^2\rho_s\right) - \log_2\left(1+\frac{A\rho_s}{1+B\rho_s}\right), \\ &\overset{(b)}{=} \log_2\left(2+\frac{A}{B}\right) - \log_2\left(1+\frac{\frac{A}{\sigma_i^2}(1+\frac{A}{B})}{1+\frac{B}{\sigma_i^2}+\frac{A}{\sigma_i^2}}\right), \\ &= \log_2\left(2+\frac{A}{B}\right) - \log_2\left(1+\frac{1+\frac{A}{B}}{\frac{\sigma_i^2}{A}+\frac{B}{A}+1}\right), \end{aligned} \tag{3.30}$$

where (b) uses $\rho_s = \frac{1}{\sigma_i^2}\left(1+\frac{A}{B}\right)$ due to (3.26). Now, consider

$$\frac{A}{\sigma_i^2} \simeq 1, \text{ as } n_i\delta_{\max}^2 \ll \sigma_i^2. \tag{3.31}$$

Substituting this result back into (3.30) gives

$$G(\rho_s) \simeq \underbrace{\log_2\left(2+\frac{A}{B}\right) - \log_2\left(1+\frac{1+\frac{A}{B}}{2+\frac{B}{A}}\right)}_{\in[\log_2(\frac{9}{5}),1] \text{ for } \frac{A}{B}\in[0,+\infty)} \tag{3.32}$$

Therefore, $G(\rho_s) \leq 1$ and we complete the proof. □

In Fig. 3.1, we can see that IA with no CSI errors achieves the same rate of the capacity lower bound if $\delta_{\max} = 0$. In other words, the capacity lower bound is tight and that the saturating SNR, ρ_s, tells exactly where the capacity of IA can be achieved within one bit in the presence of CSI errors.

Corollary 3. *The rate ceiling for $\underline{C}_i$ is given by*

$$\lim_{\rho\to\infty} \underline{C}_i(\rho) = \log_2(\sigma_i^2\rho_s). \tag{3.33}$$

Proof. Taking the limit for $\underline{C}_i(\rho)$ gives the result. □

Corollary 4. *At high SNR ($\geq \rho_s$), the gap between the rate achievable by IA with no*

CSI errors and the capacity lower bound can be approximated by

$$G(\rho) \approx \log_2 \rho - \log_2 \rho_s. \tag{3.34}$$

Proof. This result can be shown by

$$\begin{aligned} G(\rho) &\overset{(a)}{=} \underline{C}_i(\rho)|_{\delta_{\max}=0} - \lim_{\rho\to\infty} \underline{C}_i(\rho)\big|_{\delta_{\max}\neq 0}, \\ &\overset{(b)}{=} \log_2\left(\sigma_i^2\rho\right) - \log_2\left(\sigma_i^2\rho_s\right), \end{aligned} \tag{3.35}$$

where (b) uses the high SNR approximation and the result in *Corollary 3* to reach the desired result. □

Conventionally, the DoF is defined as [12]

$$\text{DoF} = \lim_{\rho\to\infty} \frac{C_\Sigma(\rho)}{\log_{10}\rho}. \tag{3.36}$$

This metric represents the total number of streams achievable by the network but it is only defined at infinite SNR and will be zero with CSI errors. Thus a different metric is defined here, called the modified DoF (mDoF), it is more meaningful in the case of CSI errors and is defined as a function of SNR. The mDoF for user i is defined as

$$\text{mDoF}_i(\rho) = \frac{\underline{C}_i(\rho)}{\min\{m_i, n_i\} \times \log_2(1+\alpha_i^2\rho)}, \tag{3.37}$$

where α_i is the maximum singular value of $\mathbf{H}_{i,i}$. This quantity is the ratio of the capacity lower bound $\underline{C}_i$ derived here and the capacity upper bound for a single-user multiple-input multiple-output (MIMO) channel with the same direct channel $\mathbf{H}_{i,i}$ with no CSI errors. It is defined for any SNR value and characterises the performance of a given user in comparison to the case where this user sees no incoming interference. In a sense the mDoF can be regarded as a lower bound for the DoF when the SNR goes to infinity. Based on this definition, clearly, if $\delta_{\max} \neq 0$, then

$$\lim_{\rho\to\infty} \text{mDoF}_i(\rho) = 0. \tag{3.38}$$

That is, with CSI errors, all DoF is lost at high SNR, as is expected because of the inevitable interference. A network centric metric representing the network mDoF can be defined as, $\text{mDoF}(\rho) = \sum_{\forall i} \text{mDoF}_i(\rho)$ as for the DoF.

3.3.3 Simulation Results

In this section, the capacity lower bound (3.25) is compared to the capacity IA achieves without CSI errors in the 3-user case with $m_i = 3$, $n_i = 2$, $d_i = 1$, and $\delta_i = \delta_{\max}\ \forall i$. In the simulations, all the matrices (including the CSI errors) have random entries drawn from a complex Gaussian distribution with zero mean and unit variance, but the error matrices are normalised to fulfil the δ_i^2 constraint on their norm.

Fig. 3.2shows the achievable rate results including the capacity lower bounds with $\delta_{\max} = 0$ and $\delta_{\max}^2 = 10^{-3}$, the rates achievable by IA with perfect CSI and that by IA with 500 different CSI error realisations. As pointed out earlier, the capacity lower bound stays very close to the rate of IA with perfect CSI initially but they depart as SNR keeps increasing. Also, the actual achievable rate of IA with CSI errors can go anywhere between the bound and the perfect CSI case.
Fig. 3.3 shows the results for the mDoF for a given user of the channel under the cases $\delta_{\max}^2 = 0$ and $\delta_{\max}^2 = 10^{-3}$. Again, the mDoF of the perfect CSI case and that based on the bound, provide a region within which the actual IA with CSI errors achieve. Also, as expected the mDoF approaches 0 at high SNR which is the DoF.

3.4 Effects of LS channel estimation

This section deals with the application of the previous results to the case where the CSI is obtained through the use of the LS estimation method. The influence of the different parameters of the model such as the number of antennas, the length and power of the training signals in the performance of IA will be made more obvious. A single stream per user is assumed throughout.
On the figure 3.4 the system model is shown, one important information in this representation is that the same CSI is available to all the nodes of the network.

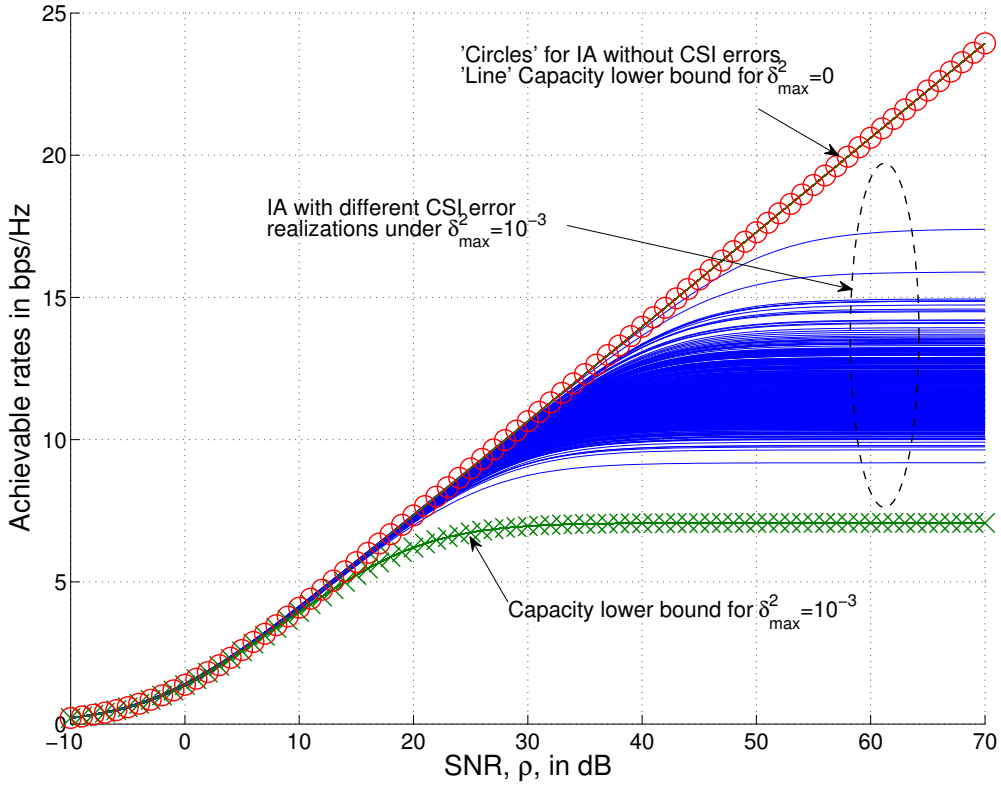


Figure 3.2: Achievable rates for $\delta^2_{\max} = 0$ and 10^{-3}.

3.4.1 LS channel estimation

Assume that during the channel acquisition phase, there is no interference. That is, for a user (say k), the signal at the receiver can be written as

$$\mathbf{y}_{i,k}^{\mathrm{CE}} = \mathbf{H}_{k,i}\mathbf{x}_i^{\mathrm{CE}} + \boldsymbol{\eta}_k^{\mathrm{CE}}, \tag{3.39}$$

where $\mathbf{y}_{i,k}^{\mathrm{CE}}$ denotes the symbol received at the kth receiver from the ith transmitter, and the superscript "CE" specifies the respective parameters in the channel estimation phase.

$\mathbf{H}_{k,i}$ is estimated following the process given in [91]. Consider transmitting $L \geq$

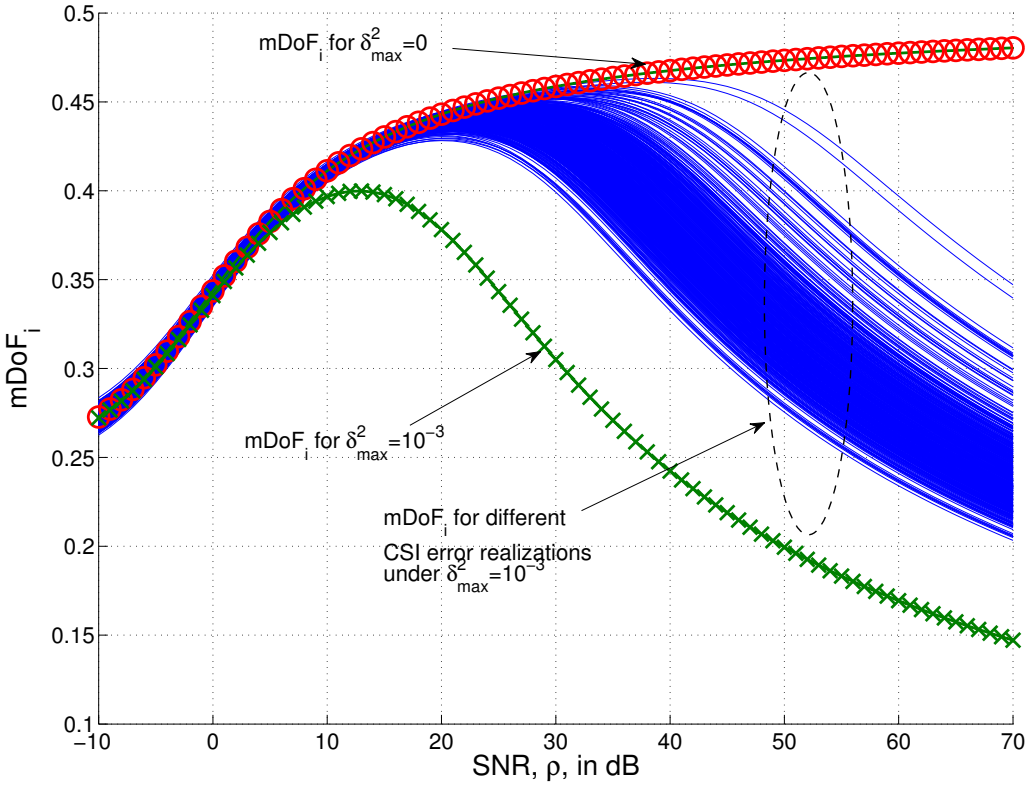


Figure 3.3: mDoF for $\delta^2_{\max} = 0$ and 10^{-3}.

m_i training signal vectors, $\mathbf{p}_i^1, \ldots, \mathbf{p}_i^L$ from the ith transmitter. The collection of the received symbols at the kth receiver from the ith transmitter is given by

$$\mathbf{Y}_{i,k}^{\mathrm{CE}} = \mathbf{H}_{k,i}\mathbf{P}_i + \mathbf{N}_k, \tag{3.40}$$

where $\mathbf{P}_i = [\mathbf{p}_i^1, \ldots, \mathbf{p}_i^L]$ and $\mathbf{N}_k$ is the matrix of size $n_k \times L$ containing the noise vectors $\boldsymbol{\eta}_k^{\mathrm{CE}}$ for each transmission. The power constraint during the estimation phase is defined as $\mathbb{E}\{\|\mathbf{p}_i^j\|_2^2\} = \mathcal{E}_e, \forall(i,j)$.

It's assumed that there is no error in feeding back the channel knowledge to all the users [19]. In the next section, the uncertainty $\delta^2_{\max}$ will be referred to as δ^2 for simplicity, and will be linked to the error of the LS channel estimation method.

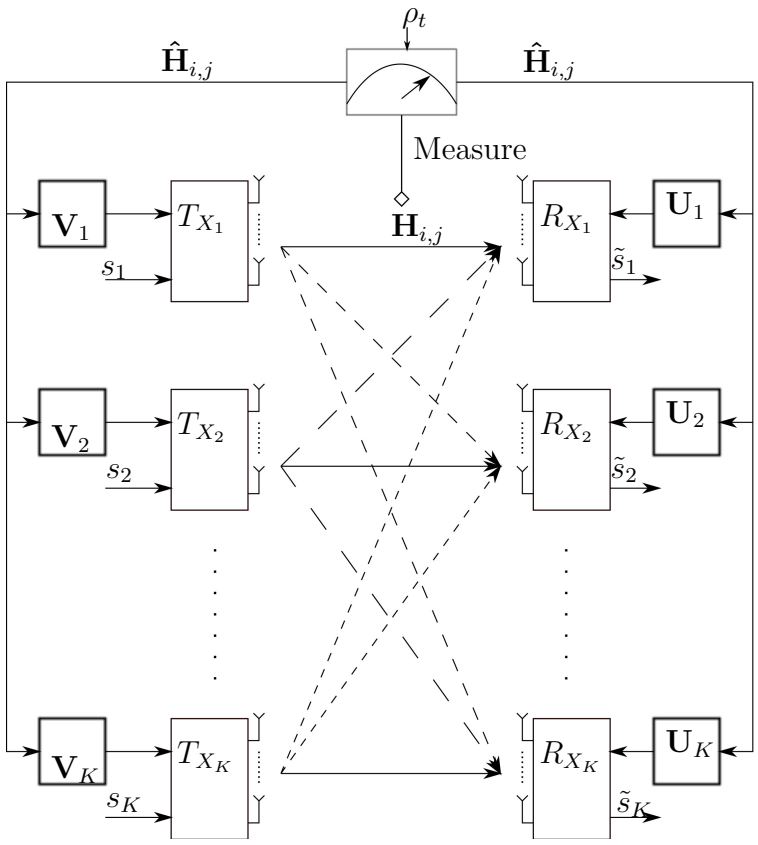


Figure 3.4: The interference channel with K pairs of transmitters and receivers. The channels $\mathbf{H}_{i,j}$ are estimated with a training SNR of ρ_t and the channel estimates $\hat{\mathbf{H}}_{i,j}$ are fed back to all the users to compute the precoders $\mathbf{V}_k$ and the combiners $\mathbf{U}_k$. The transmitted symbols at the ith transmitter are denoted as s_i, while $\tilde{s}_i$ are their estimates at the ith receiver.

3.4.2 δ^2 with LS channel estimation

For notational convenience, all the subscripts and superscripts are dropped in this section since the method is the same for all users and channels. With the knowledge of $\mathbf{Y}^{\mathrm{CE}}$ and $\mathbf{P}$, the channel matrix $\mathbf{H}$ can be estimated using the LS method by

$$\hat{\mathbf{H}} = \mathbf{Y}\mathbf{P}^*(\mathbf{P}\mathbf{P}^*)^{-1}. \tag{3.41}$$

The goal is to find $\mathbf{P}$ such that

$$\min_{\mathbf{P}} \mathbb{E}\left\{\|\mathbf{H} - \hat{\mathbf{H}}_{\mathrm{LS}}\|_{\mathrm{F}}^2\right\} \text{ subject to } \|\mathbf{P}\|_{\mathrm{F}}^2 = L\mathcal{E}_e. \tag{3.42}$$

It is shown in [91] that under optimal training,

$$\min_{\mathbf{P}} \mathbb{E}\left\{\|\mathbf{H} - \hat{\mathbf{H}}_{\mathrm{LS}}\|_{\mathbf{F}}^2\right\} = \frac{N_0 m^2 n}{L\mathcal{E}_e}. \tag{3.43}$$

Now, recalling that $\Delta\mathbf{H} = \mathbf{H} - \hat{\mathbf{H}}_{\mathrm{LS}}$, the follow upper bound is obtained

$$\delta^2 = \max_i \|(\Delta\mathbf{H})_i\|_2^2 \leq \|\mathbf{H} - \hat{\mathbf{H}}_{\mathrm{LS}}\|_{\mathrm{F}}^2, \tag{3.44}$$

and then

$$\min_{\mathbf{P}} \mathbb{E}\{\delta^2\} \leq \min_{\mathbf{P}} \mathbb{E}\left\{\|\mathbf{H} - \hat{\mathbf{H}}_{\mathrm{LS}}\|_{\mathrm{F}}^2\right\} = \frac{N_0 m^2 n}{L\mathcal{E}_e} = \frac{m^2 n}{L\rho_t}, \tag{3.45}$$

where the training SNR is given by definition as $\rho_t \triangleq \frac{\mathcal{E}_e}{N_0}$.

3.4.3 Capacity lower bound and saturating SNR

Now that the relationship between the channel estimation method and the uncertainty on the channel estimates is characterised, this section will be focused on studying the effects of the parameters used during the estimation phase on the capacity lower bound. Even though, the expression obtained in (3.45) provides an upper bound on the average uncertainty yielded by the LS method, It will be used as the actual expression for the

uncertainty. This means

$$\delta^2 \triangleq \frac{m^2 n}{L\rho_t}. \tag{3.46}$$

With this definition, the parameters of the estimation phase are obvious and the trend of the different metrics considered remain the same. For example, with this definition of δ^2, equation (3.25) becomes

$$\underline{C}(\rho) = \log_2\left(1 + \frac{(\sigma^2 - \frac{n^2m^2}{L\rho_t})\rho}{1 + \frac{n^2m^2(K-1)^2\rho}{L\rho_t}}\right). \tag{3.47}$$

If the ratio between the transmit SNR and the training SNR is constant, say $\frac{\rho}{\rho_t} = \mu$, then then the expression above can be rewritten as

$$\underline{C}_\mu(\rho) = \log_2\left(1 + \frac{\sigma^2\rho - \frac{n^2m^2\mu}{L}}{1 + \frac{n^2m^2(K-1)^2\mu}{L}}\right). \tag{3.48}$$

Sometimes it would be useful to express the training SNR in the form of $\rho_t = \rho^\alpha$. In this case, the same expression becomes

$$\underline{C}_\alpha(\rho) = \log_2\left(1 + \frac{\sigma^2\rho - \frac{n^2m^2(\rho)^{1-\alpha}}{L}}{1 + \frac{n^2m^2(K-1)^2(\rho)^{1-\alpha}}{L}}\right). \tag{3.49}$$

The analysis in section 3.3.2 showed that, up to the saturating SNR, the capacity of IA with channel uncertainty is within 1bps/Hz of that of the perfect CSI case. Keeping that in mind, one may want to set a desired saturating SNR that enables to reach a certain rate and then find the training SNR that corresponds to it. To this purpose, use equation (3.26) given by

$$\rho_s = \frac{1}{\sigma^2} + \frac{1 - \frac{n\delta^2}{\sigma^2}}{n\delta^2(K-1)^2}. \tag{3.50}$$

This allows to write the training SNR as a function of the saturating SNR by replacing

δ^2 by its expression,

$$\rho_t = \left[\left(\rho_s - \frac{1}{\sigma^2}\right)(K-1)^2 + \frac{1}{\sigma^2}\right]\frac{m^2n^2}{L}. \tag{3.51}$$

If $\frac{1}{\sigma^2}$ is negligible against ρ_s (i.e., the channel fading is not too bad), then (3.51) becomes

$$\rho_t = \rho_s(K-1)^2\frac{m^2n^2}{L}. \tag{3.52}$$

On this last equation, it is obvious that the saturating SNR is directly proportional to the training SNR, which means that the two quantities will vary at the same time and in the same way. Moreover, the more antennas and users there are, the higher the training SNR or training time (L) needs to be in order to maintain the same performance. In other words, if one were to increase the number of users, they would also need to acquire the CSI with a better accuracy.

3.4.4 mDoF with LS estimation

In this section aim is to investigate the behaviour of the system at high SNR using the mDoF. First of all, let's recall the definition of the DoF of a user

$$\eta \triangleq \lim_{\rho\to\infty}\frac{C_{\text{user}}(\rho)}{\log_2\rho}, \tag{3.53}$$

where C_{user} is the capacity expression for the user against the SNR ρ. In the perfect CSI case with IA, this expression becomes

$$\eta = \lim_{\rho\to\infty}\frac{\log_2(1+\sigma^2\rho)}{\log_2\rho} = 1. \tag{3.54}$$

Now in the imperfect CSI case and using the mDoF, the lower bound of the DoF is defined as

$$\underline{\eta} \triangleq \lim_{\rho\to\infty}\text{mDoF}(\rho) = \lim_{\rho\to\infty}\frac{\underline{C}(\rho)}{\log_2\rho}. \tag{3.55}$$

In itself, $\underline{\eta}$ only provides information on the slope of the capacity when the SNR is high, but no information is given on the performance gap between the capacity in the perfect CSI and ICSI case. Therefore, it becomes difficult to assess the actual impact of ICSI. To obtain more information about that, a new quantity γ is defined that represents the gap between the capacity in the perfect CSI case and the capacity lower bound. It's given as

$$\gamma \triangleq \log_2(1+\sigma^2\rho) - \underline{C}(\rho). \tag{3.56}$$

This value γ is also the upper bound of the difference between the capacity in the perfect CSI case and the capacity achievable with erroneous CSI. It can also characterise the system at all SNR while $\underline{\eta}$ is an asymptotic performance metric. However, here the focus will mostly be on its behaviour at infinite SNR since it provides supplementary information over the DoF lower bound $\underline{\eta}$.

Let's examine $\underline{\eta}$ in the case where the training SNR is a fixed value. In this case, it is easily shown that

$$\underline{\eta} = \lim_{\rho\to\infty} \frac{\log_2\left(1+\frac{(\sigma^2-\frac{n^2m^2}{L\rho_t})\rho}{1+\frac{n^2m^2(K-1)^2\rho}{L\rho_t}}\right)}{\log_2\rho} = 0. \tag{3.57}$$

This shows that in this case, the DoF vanishes and the capacity of a user may no longer be proportional to the transmit SNR. The gap at infinite SNR is $\gamma^\infty = \infty$.

Now, consider the case where ρ_t and ρ are proportional, or μ is some positive constant. As a consequence,

$$\underline{\eta} = \lim_{\rho\to\infty} \frac{\underline{C}_\mu(\rho)}{\log_2(\rho)} = 1. \tag{3.58}$$

Thus, the DoF is equal to one, meaning that even if the CSI is not perfect one can still achieve the full DoF of the network. What is important to note here is that there is no saturating SNR in this case. Note that this result is similar to that in [93] but the main difference is that here the lower bound is used in the analysis and not the average value of the rate.

Even if $\eta = \underline{\eta}$ in this case, there is a constant gap between the capacity in the perfect CSI case and that of the imperfect CSI case. At high SNR, this gap is upper bounded

by

$$\gamma_{\mu}^{\infty} = \lim_{\rho\to\infty} \left(\log_2(1+\sigma^2\rho) - \underline{C}_{\mu}\rho\right) \tag{3.59}$$

$$= \log_2\left(1 + \frac{n^2m^2(K-1)^2\mu}{L}\right). \tag{3.60}$$

This means that the capacity with imperfect CSI at high SNR is within γ_{μ}^{∞}bps/Hz of the capacity in the perfect CSI case.

In addition, if $\rho_t = \rho^{\alpha}$, the DoF lower bound is given by

$$\underline{\eta} = \lim_{\rho\to\infty} \frac{\underline{C}_{\alpha}(\rho)}{\log_2\rho}. \tag{3.61}$$

There are two different behaviours depending on the value of α, which can be seen by

$$\underline{\eta} = \begin{cases} \alpha & \text{for } 0 < \alpha < 1, \\ 1 & \text{for } 1 \leq \alpha. \end{cases} \tag{3.62}$$

Remark that as in [93] we find that fractional numbers of DoF can be achieved.
Let's have a look at the behaviour of the gap for different values of α. Note that

$$\gamma_{\alpha}^{\infty} = \lim_{\rho\to\infty} \left(\log_2(1+\sigma^2\rho) - \underline{C}_{\alpha}(\rho)\right). \tag{3.63}$$

It can be easily shown that

$$\gamma_{\alpha}^{\infty} = \begin{cases} \infty & \text{for } 0 < \alpha < 1, \\ \log_2\left(1 + \frac{n^2m^2(K-1)^2}{L}\right) & \text{for } \alpha = 1, \\ 0 & \text{for } 1 < \alpha. \end{cases} \tag{3.64}$$

Note that the case $\alpha = 1$ is the same as if ρ_t is proportional to ρ with $\mu = 1$. The case $\alpha > 1$ is interesting because the capacity tends to the capacity in the perfect CSI scenario. This can be explained by the fact that the interference power caused by the estimation errors will increase at a much slower pace than the signal power.

3.4.5 Numerical Results

In this section, numerical results are provided to show the behaviour of the capacity lower bound for various ρ_t, μ and α with $m = 2$, $n = 2$, $L = 2$, $K = 3$ and $\sigma^2 = 1$.

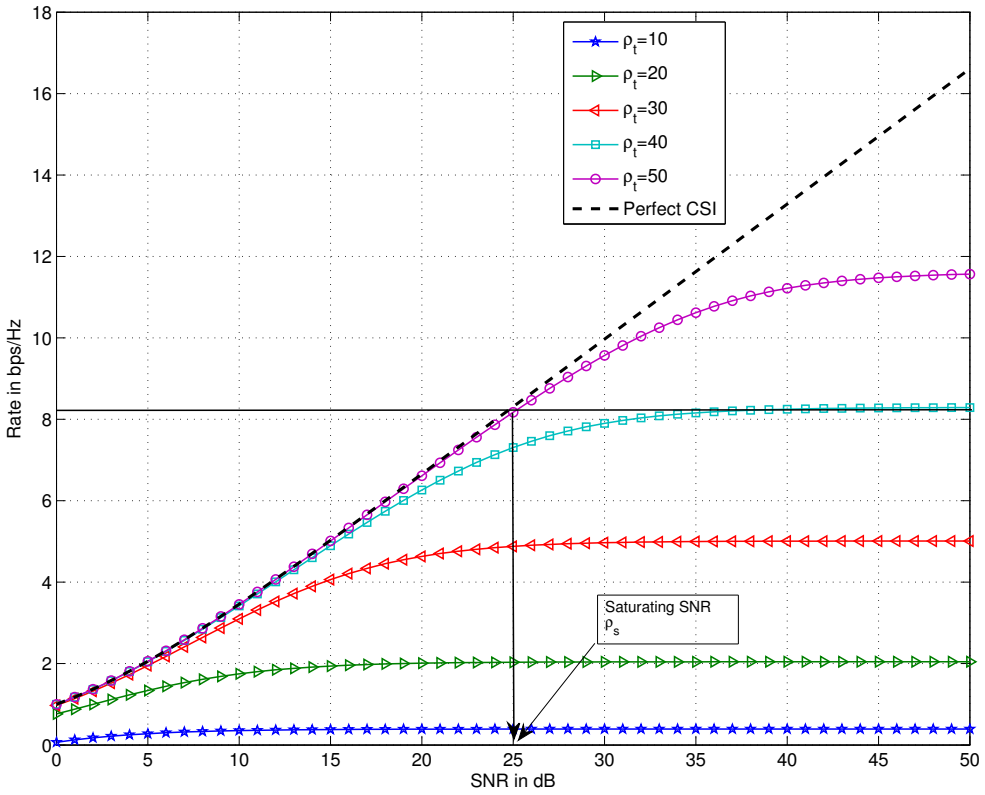


Figure 3.5: Capacity lower bound against SNR for various training SNR ρ_t. The saturating SNR ρ_s is also shown if $\rho_t = 40$dB.

Fig. 3.5, shows the evolution of the capacity lower bound when the training SNR ρ_t is increased. For comparison, the capacity in the perfect CSI case is also added to the plot. One can see that when ρ_t increases, the lower bound stays close to the perfect CSI case for a wider range of transmit SNR ρ and then the rate saturates. This is consistent with the increase of the saturating SNR ρ_s with the training SNR ρ_t. On that figure, the saturating SNR is also indicated for the case $\rho_t = 40$.

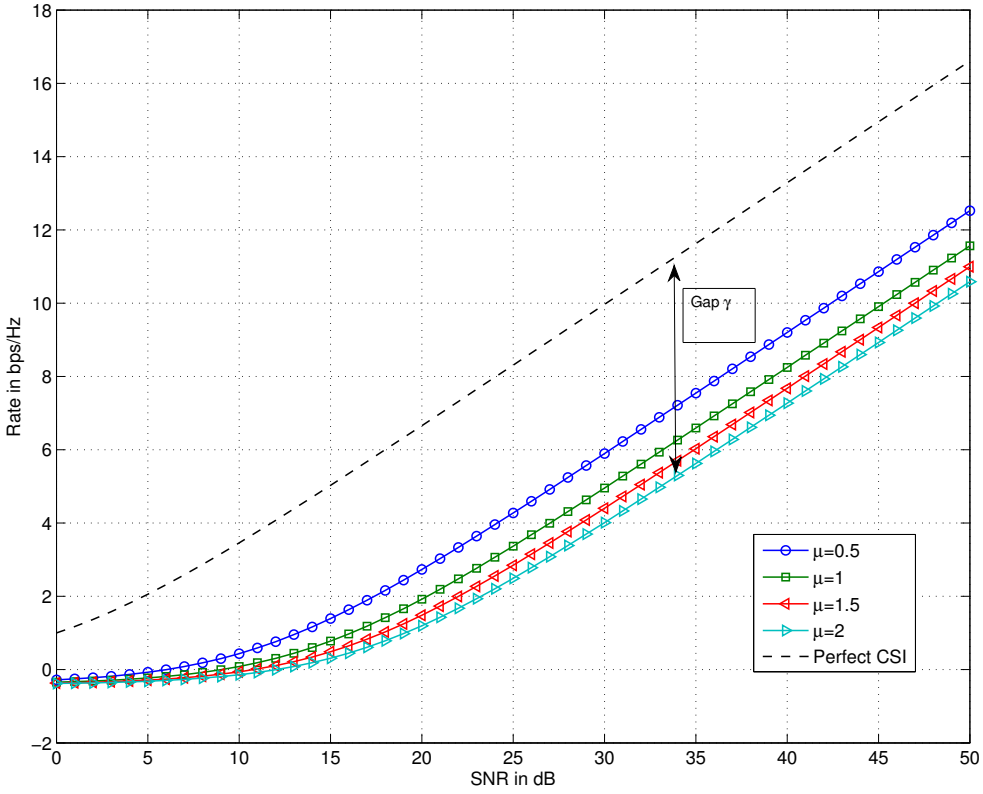


Figure 3.6: Capacity lower bound against SNR for various μ.

Fig. 3.6 shows that when the training SNR ρ_t is proportional to the transmit SNR ρ then the capacity lower bound shows no sign of saturation and increases linearly with the transmit SNR. The gap between the capacity with perfect CSI and the lower bound with corrupted CSI depends on the value for μ and also the numbers of users and antennas as given by (3.60).

3.5 Conclusion

In this chapter, a capacity lower bound is derived for the MIMO interference channel using IA in the presence of bounded CSI errors, a new metric called saturating SNR

is introduced to measure the performance of IA given the CSI quality. It's shown that the performance of IA with CSI errors is within 1bps/Hz of the perfect case for a range of SNR less than the saturating SNR. Following this, the special case where the CSI is acquired using LS estimation is investigated. It's also revealed how the capacity lower bound for each user varies according to the system parameters such as the training signal-to-noise ratio. It's shown that the gap between the performance in the perfect CSI case and the imperfect CSI case is constant when the transmit SNR, is proportional to the training SNR. In addition, the saturating SNR is derived as a function of the training SNR. An interesting result is that one can achieve the full DoF with imperfect CSI and also get very close the capacity of the perfect CSI case using IA. However, it's shown that asymptotically perfect CSI does not guarantee that the capacity achievable at infinite SNR is the same as the capacity achievable in the perfect CSI case.

Chapter 4

Distribution of the Capacity with Gaussian CSI error

4.1 Introduction

In the previous chapter, I have studied the performance of IA in the IC when the CSI of all the channels is affected by some bounded error. In practice, the CSI of the crosstalk channels is likely to be far from perfect, although the CSI of the direct links may be estimated rather accurately. Moreover, the error affecting the channel estimates may follow some probability distribution. For these reasons, there is strong desire to characterise the statistics of the achievable performance limit for IA under such practical scenarios. In this chapter, the main interest is to analyse the performance of the IA methods designed for global perfect CSI in the presence of CSI uncertainties. My emphasis is again on the "achievable" performance, rather than the average performance.[1] Note that there exist robust IA techniques exploiting imperfect CSI, e.g., [18, 19, 89, 94] but in that case, analysing the achievable performance is usually not possible. Further to chapter 3 which provides the capacity lower bound for IA with CSI errors, this chapter's aim is to provide a complete statistical characterisation for the achievable rate.

[1] Achievable performance is the performance that has an operational meaning but average performance is only an average indicator for the performance. For example, an average rate is not achievable because the actual channel rate for a given error instantiation may not meet the average rate.

Specifically, the main contribution is the statistical distribution for the rate per stream achievable by perfect IA based on imperfect CSI. I will also derive metrics such as outage probability and the saturating signal-to-noise ratio (SNR) that can be useful in the design of a practical system using perfect IA with imperfect CSI. Two applications are then presented to demonstrate that the results can be applied to (i) optimise the number of streams per user in the interference network for maximising the sum-rate, and (ii) analyse the outage performance of IA in block-fading channels with degrading CSI over time.

4.2 IA with Imperfect Crosstalk CSI

The system model considered here is the K-user multiple-input multiple-output (MIMO) interference channel where each user k consists of a transmitter equipped with n_k antennas communicating with a receiver equipped with m_k antennas. Hence, at a given time instant, the signal received at the kth user is given by

$$\mathbf{y}_k = \mathbf{H}_{k,k}\mathbf{x}_k + \sum_{\substack{\ell=1 \\ \ell \neq k}}^{K} \mathbf{H}_{k,\ell}\mathbf{x}_\ell + \boldsymbol{\eta}_k, \tag{4.1}$$

where $\boldsymbol{\eta}_\ell$ denotes the additive white Gaussian noise (AWGN) vector with elements distributed as $\mathcal{CN}(0, \sigma_\eta^2)$, $\mathbf{H}_{k,\ell}$ denotes the deterministic MIMO channel between the ℓth transmitter and the kth receiver and $\mathbf{x}_\ell$ is the message sent by the ℓth transmitter with the power constraint $\mathbb{E}\{\|\mathbf{x}_\ell\|_2^2\} = P_0 \ \forall \ell$.

In practice, IA will operate under imperfect knowledge of the channel state, since CSI is estimated and will change over time [19]. Although the main channel CSI can be accurately estimated, the estimation of crosstalk CSI involves other user receivers, and will be less accurate and updated less frequently. Also, the bound in chapter 3 demonstrates that the uncertainty in the main channel CSI tends to have less effect on the capacity performance than that in the crosstalk CSI. For this reason, in this chapter, the scenario where the only main channel CSI is perfect but the crosstalk CSI is in errors will be considered.

The error on the channel knowledge is still modelled as an additive term to the channel measurement, i.e.,

$$\mathbf{H}_{k,\ell} = \hat{\mathbf{H}}_{k,\ell} + \Delta\mathbf{H}_{k,\ell}, \tag{4.2}$$

where $\hat{\mathbf{H}}_{k,\ell}$ represents the measurement or the estimate of the channel matrix and $\Delta\mathbf{H}_{k,\ell}$ is the difference between the real channel and the channel estimate and will be referred to as the measurement error. It is assumed that each entry of $\Delta\mathbf{H}_{k,\ell}$ is complex Gaussian distributed as $\mathcal{CN}(0, \sigma_e^2)$.

If the uncertainty on the CSI is taken into account, then (4.1) can be rewritten as

$$\mathbf{y}_k = \mathbf{H}_{k,k}\mathbf{x}_k + \sum_{\substack{\ell=1 \\ \ell\neq k}}^{K} \hat{\mathbf{H}}_{k,\ell}\mathbf{x}_\ell + \sum_{\substack{\ell=1 \\ \ell\neq k}}^{K} \Delta\mathbf{H}_{k,\ell}\mathbf{x}_\ell + \boldsymbol{\eta}_k, \tag{4.3}$$

where I have separated the interference due to the channel estimates and those due to the measurement errors.
Using the channel estimates to design the IA precoders, the conditions on the precoders can then be expressed as

$$\begin{cases} \text{rank}(\mathbf{U}_k^*\mathbf{H}_{k,k}\mathbf{V}_k) = d_k, \text{ for } k = 1, 2, \ldots, K, \\ \mathbf{U}_\ell^*\hat{\mathbf{H}}_{\ell,k}\mathbf{V}_k = 0, \text{ for all } \ell \neq k. \end{cases} \tag{4.4}$$

Note that the second condition is now on the channel estimates instead of the real channels because of the measurement errors. The first condition remains the same as the main channel CSI is assumed to be perfect. I consider that $\mathbf{V}_k^*\mathbf{V}_k = \mathbf{I}_{d_k}\ \forall k$, and that $\mathbf{V}_k$ is given by an IA solution that does not take into account the direct links $\mathbf{H}_{k,k}$ as in [10, 95, 96].
With these new IA conditions reflecting the practical scenarios, I apply the interference cancelling matrix to the receive signal and get

$$\mathbf{U}_k^*\mathbf{y}_k = \mathbf{U}_k^*\mathbf{H}_{k,k}\mathbf{V}_k\mathbf{x}_k + \sum_{\substack{\ell=1 \\ \ell\neq k}}^{K} \mathbf{U}_k^*\Delta\mathbf{H}_{k,\ell}\mathbf{V}_\ell\mathbf{x}_\ell + \mathbf{U}_k^*\boldsymbol{\eta}_k. \tag{4.5}$$

From the above, the term $\sum_{\substack{\ell=1 \\ \ell \neq k}}^{K} \mathbf{U}_k^* \Delta \mathbf{H}_{k,\ell} \mathbf{V}_\ell \mathbf{x}_\ell$ can be identified as being the interference from the other users to user k due to the imperfect knowledge of the channel.
In the next section, I focus on the effects of this term on the maximum rate achievable per stream of each user.

4.3 Probability Distribution of the Rates

In this section, I provide the statistical description of the achievable rate per stream in relation to the distribution of the CSI error. Thus, the focus is on the interference created by the CSI error on the received signal. I will investigate this interference term prior to applying the interference cancelling matrix. I denote this term at the kth receiver by

$$\boldsymbol{i}_k = \sum_{\substack{\ell=1 \\ \ell \neq k}}^{K} \Delta \mathbf{H}_{k,\ell} \mathbf{V}_\ell \mathbf{x}_\ell. \tag{4.6}$$

Let us consider only the jth component of $\boldsymbol{i}_k$ given by

$$(\boldsymbol{i}_k)_j = \sum_{\substack{\ell=1 \\ \ell \neq k}}^{K} (\Delta \mathbf{H}_{k,\ell})_j \mathbf{V}_\ell \mathbf{x}_\ell, \tag{4.7}$$

where $(\cdot)_j$ returns the jth row of the input matrix.

(4.7) can be adapted to compute the instantaneous interference power contained in the jth component of $\boldsymbol{i}_k$ as

$$|(\boldsymbol{i}_k)_j|^2 = \left(\sum_{\substack{\ell=1 \\ \ell \neq k}}^{K} (\Delta \mathbf{H}_{k,\ell})_j \mathbf{V}_\ell \mathbf{x}_\ell \right) \left(\sum_{\substack{l=1 \\ l \neq k}}^{K} \mathbf{x}_l^* \mathbf{V}_l^* (\Delta \mathbf{H}_{k,l})_j^* \right) \tag{4.8}$$

$$= \sum_{\substack{\ell=1 \\ \ell \neq k}}^{K} \sum_{\substack{l=1 \\ l \neq k}}^{K} (\Delta \mathbf{H}_{k,\ell})_j \mathbf{V}_\ell \mathbf{x}_\ell \mathbf{x}_l^* \mathbf{V}_l^* (\Delta \mathbf{H}_{k,l})_j^*. \tag{4.9}$$

I now take the ensemble average of $|(\boldsymbol{i}_k)_j|^2$ over all possible transmit messages $(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_K)$

under the assumption that they can be treated as uncorrelated sources of multivariate Gaussian random variables with mean 0 and covariance matrix $P_0\mathbf{I}_{d_k}$, where d_k denotes the number of streams of the kth user. In other words, the transmit messages are independent and all the users have the same power constraint. That average value will be denoted $\mathcal{I}_{k,j}$ and can be evaluated as

$$\begin{aligned}\mathcal{I}_{k,j} &= \mathbb{E}_{\mathbf{x}_1,\ldots,\mathbf{x}_k}\left[|(\boldsymbol{i}_k)_j|^2\right] \\ &= \mathbb{E}_{\mathbf{x}_1\ldots,\mathbf{x}_k}\left[\sum_{\substack{\ell=1\\ \ell\neq k}}^{K}\sum_{\substack{l=1\\ l\neq k}}^{K}(\Delta\mathbf{H}_{k,\ell})_j\mathbf{V}_\ell\mathbf{x}_\ell\mathbf{x}_l^*\mathbf{V}_l^*(\Delta\mathbf{H}_{k,l})_j^*\right],\end{aligned} \tag{4.10}$$

where the expectation is conditioned on $\Delta\mathbf{H}_{k,\ell}\ \forall(k,\ell)$.

The expression above can be further found as

$$\mathcal{I}_{k,j} = P_0\sum_{\substack{\ell=1\\ \ell\neq k}}^{K}(\Delta\mathbf{H}_{k,\ell})_j\mathbf{V}_\ell\mathbf{V}_\ell^*(\Delta\mathbf{H}_{k,\ell})_j^*. \tag{4.11}$$

The aim is to investigate the distribution of $\mathcal{I}_{k,j}$ but since the summation in the expression (4.11) contains lots of similar terms, I will focus on only one element, and for simplicity of notation I drop all the subscripts and we replace any term such as $(\Delta\mathbf{H}_{k,\ell})_j$ by $\mathbf{h}$. Furthermore, let's define

$$\delta \triangleq \mathbf{h}\mathbf{V}\mathbf{V}^*\mathbf{h}^*. \tag{4.12}$$

For this, I denote the number of streams as d, the number of transmit antennas n and the number of receive antennas m.

The matrix $\mathbf{V}\mathbf{V}^*$ is hermitian by definition. Therefore, using the spectral theorem it can be decomposed into

$$\mathbf{V}\mathbf{V}^* = \mathbf{U}\mathbf{D}\mathbf{U}^*, \tag{4.13}$$

where $\mathbf{U}$ is a unitary matrix and $\mathbf{D}$ is a diagonal matrix with real entries. Using the

spectral decomposition of $\mathbf{VV}^*$, I can then rewrite (4.12) as

$$\delta = \mathbf{hUDU}^*\mathbf{h}^*. \tag{4.14}$$

Now, if I define

$$\tilde{\mathbf{h}} \triangleq \mathbf{U}^*\mathbf{h}^*, \tag{4.15}$$

then $\tilde{\mathbf{h}}$ has a multivariate complex Gaussian distribution with covariance matrix $\sigma_e^2\mathbf{I}_n$, where σ_e^2 is the variance of each entry of $\mathbf{h}$. Recalling from (4.14), I now have

$$\delta = \tilde{\mathbf{h}}^*\mathbf{D}\tilde{\mathbf{h}}. \tag{4.16}$$

Obviously, δ is random because of the random CSI uncertainties and if I consider this as a random variable Δ, then the structure in (4.16) illustrates that Δ is drawn from a generalised Chi-square distribution [97]. In the following section, the aim is to determine precisely the parameters of that distribution.

4.3.1 DoF of the χ^2 Distribution

I will now focus on the matrix $\mathbf{D}$ as this matrix determines the parameters of the distribution I am looking for.

Theorem 3. *The matrix* $\mathbf{D}$ *is diagonal with exactly* d *ones and* $n-d$ *zeros on its diagonal, where* d *is the number of transmit streams and* n *is the number of transmit antennas.*

Proof. $\mathbf{VV}^*$ and $\mathbf{V}^*\mathbf{V}$ have the same non-zero eigenvalues and since $\mathbf{V}^*\mathbf{V} = I_d$ we deduce that $\mathbf{VV}^*$ has d non-zero eigenvalues all equal to 1, which shows the desired result and completes the proof. □

Corollary 5. *The random variable* $\frac{2}{\sigma_e^2}\Delta$ *is Chi-square distributed with* $2d$ *DoFs, i.e.,* $\frac{2}{\sigma_e^2}\Delta \sim \chi^2_{2d}$.

Proof. From (4.16), we can rewrite δ as

$$\delta = \sigma_e^2 \left(\frac{\tilde{\mathbf{h}}^*}{\sigma_e}\right) \mathbf{D} \left(\frac{\tilde{\mathbf{h}}}{\sigma_e}\right), \tag{4.17}$$

so that $\frac{\tilde{\mathbf{h}}^*}{\sigma_e}$ has unit variance. Now, using (4.17) and Theorem 3 gives the desired result. Note that the factor 2 in $\frac{2}{\sigma_e^2}\Delta$ comes from the fact that I am using complex valued numbers. □

Corollary 6. *The probability density function (pdf) of Δ is given by*

$$f_\Delta(\delta, d) = \begin{cases} \frac{1}{\sigma_e^2 \Gamma(d)} \left(\frac{\delta}{\sigma_e^2}\right)^{d-1} e^{-\frac{\delta}{\sigma_e^2}} & \text{for } \delta \geq 0, \\ 0 & \text{for } \delta < 0. \end{cases} \tag{4.18}$$

Proof. We recall that the pdf of a random variable X following a χ_k^2 distribution is given by

$$f_X(x, k) = \begin{cases} \frac{1}{2^{\frac{k}{2}} \Gamma\left(\frac{k}{2}\right)} x^{\frac{k}{2}-1} e^{-\frac{x}{2}} & \text{for } x \geq 0, \\ 0 & \text{for } x < 0. \end{cases} \tag{4.19}$$

Since $\Delta = \frac{\sigma_e^2}{2} X$, we can give the pdf of Δ as

$$f_\Delta(\delta, d) = \frac{2}{\sigma_e^2} f_X\left(\frac{2}{\sigma_e^2}\delta, 2d\right). \tag{4.20}$$

Therefore, we obtain (4.18) and complete the proof. □

4.3.2 Probability Distribution of the Achievable Rate per Stream

In this subsection, I will link the probability distribution of the interference, to that of the maximum achievable rate, for any stream of any given user. Putting the subscripts back in the notations, δ becomes

$$\delta_{k,\ell}^j = (\Delta \mathbf{H}_{k,\ell})_j \mathbf{V}_\ell \mathbf{V}_\ell^* (\Delta \mathbf{H}_{k,\ell})_j^* \tag{4.21}$$

and the random variable associated is $\Delta_{k,\ell}^j$.

With this notation, (4.11) can be written as

$$\mathcal{I}_{k,j} = P_0 \sum_{\substack{\ell=1 \\ \ell \neq k}}^{K} \delta_{k,\ell}^{j}. \tag{4.22}$$

Now, I define the following random variable

$$\Delta_k^j \triangleq \sum_{\substack{\ell=1 \\ \ell \neq k}}^{K} \Delta_{k,\ell}^{j}. \tag{4.23}$$

Therefore, if $\mathcal{I}_{k,j}$ is considered as a random variable, then

$$\mathcal{I}_{k,j} = P_0 \Delta_k^j. \tag{4.24}$$

At this stage, it should be reminded that I have not specified a precise vector space basis at the receiver side. Thus, every result obtained is true in any given basis. Let's then choose a basis in which d of the basis vectors are independent unitary vectors from the desired signal space and the remaining basis vectors are any unitary vectors that can complete the set to form a basis.
I define the basis in this manner so that the interference cancelling matrices $\mathbf{W}_k$ can be found to simply zero-force the inter-user and inter-stream interference and that the interference power received along any stream is given by $\mathcal{I}_{k,j}$. Note that statistically Δ_k^j and therefore $\mathcal{I}_{k,j}$ are the same $\forall j$. Henceforth, I denote them, respectively, Δ_k and $\mathcal{I}_k$.

The achievable rate for the lth stream of the kth user is given by

$$R_{k,l}(P_0, \mathcal{I}_k) = \log_2 \left(1 + \frac{\left(\frac{P_0}{d_k}\right) |(\mathbf{U}_k^*)_l \mathbf{H}_{k,k} [\mathbf{V}_k]_l|^2}{\mathcal{I}_k + \sigma_n^2} \right). \tag{4.25}$$

From now on, I define $z_{k,l} = |(\mathbf{U}_k^*)_l \mathbf{H}_{k,k} [\mathbf{V}_k]_l|^2$ and write the achievable rate of the lth

stream of the kth user as

$$R_{k,l}(P_0, \mathcal{I}_k) = \log_2 \left(1 + \frac{\left(\frac{P_0}{d_k}\right) z_{k,l}}{\mathcal{I}_k + \sigma_n^2} \right). \tag{4.26}$$

This rate expression will be used in the following form:

$$R_{k,l}(\rho, \Delta_k) = \log_2 \left(1 + \frac{z_{k,l}}{d_k \left(\Delta_k + \frac{1}{\rho} \right)} \right), \tag{4.27}$$

where $\rho = \frac{P_0}{\sigma_n^2}$ and I have used (4.24).

In order to obtain the pdf of $R_{k,l}$, I first express Δ_k as a function of $R_{k,l}$ with ρ fixed so that

$$\Delta_k(\rho, R_{k,l}) = \frac{z_{k,l}}{d_k(2^{R_{k,l}} - 1)} - \frac{1}{\rho}. \tag{4.28}$$

From this, I get

$$\frac{\partial \Delta_k(\rho, R_{k,l})}{\partial R_{k,l}} = -\frac{z_{k,l}(\log_e 2) 2^{R_{k,l}}}{d_k(2^{R_{k,l}} - 1)^2}. \tag{4.29}$$

I can therefore write the pdf, $f_{R_{k,l}}$, of the rate as

$$f_{R_{k,l}}(\rho, r_{k,l}) = \frac{z_{k,l}(\log_e 2) 2^{r_{k,l}}}{d_k(2^{r_{k,l}} - 1)^2} \times f_{\Delta_k} \left(\frac{z_{k,l}}{d_k(2^{r_{k,l}} - 1)} - \frac{1}{\rho} \right). \tag{4.30}$$

Based on this, the pdf of $R_{k,l}$ can be characterised given that of Δ_k. To do so, I recall that $\Delta_k = \sum_{\substack{\ell=1 \\ \ell \neq k}}^{K} \Delta_{k,\ell}$ (I omit the superscripts since the expression is the same for all streams of the same user) and therefore, since $\frac{2}{\sigma_e^2}\Delta_{k,\ell}$ $\forall (k, \ell)$ are independent and $\chi^2(2d_\ell)$ distributed, I have that $\frac{2}{\sigma_e^2}\Delta_k$ is χ^2 distributed with $2(D - d_k)$ DoFs where $D = \sum_{\ell=1}^{K} d_\ell$ denotes the total number of streams in the network.
Therefore,

$$f_{\Delta_k}(\delta) = \begin{cases} \frac{1}{\sigma_e^2 \Gamma(D - d_k)} \left(\frac{\delta}{\sigma_e^2} \right)^{D - d_k - 1} e^{-\frac{\delta}{\sigma_e^2}} & \text{for } \delta \geq 0, \\ 0 & \text{for } \delta < 0. \end{cases} \tag{4.31}$$

If every user has the same number of streams d, then this expression can be written as

$$f_{\Delta_k}(\delta) = \begin{cases} \frac{1}{\sigma_e^2 \Gamma(d(K-1))} \left(\frac{\delta}{\sigma_e^2}\right)^{d(K-1)-1} e^{-\frac{\delta}{\sigma_e^2}} & \text{for } \delta \geq 0, \\ 0 & \text{for } \delta < 0. \end{cases} \tag{4.32}$$

4.4 Saturating SNR and Outage Probability

In this section, I study two performance metrics, namely, *saturating SNR* and outage probability. Saturating SNR was first introduced in chapter 3 for worst-case scenarios (with bounded CSI errors). Here, I emphasise on its statistics. On the other hand, the outage probability is defined to be a metric that will allow to assess the performance of each user despite the randomness of the channel estimates.

4.4.1 PDF of the Saturating SNR

The saturating SNR can be seen as a non-asymptotic performance metric that accounts for estimation errors. It is defined as the SNR where the rate in the perfect CSI case is equal to that of the imperfect CSI case at infinite SNR. Here the saturating SNR is defined for each stream of any given user.
I will first give the pdf of the saturating SNR then, show that up to the saturating SNR, the achievable rate of the IA with corrupted CSI is within 1bps/Hz of the achievable rate of the IA in the perfect CSI case.

From equation (4.27) I deduce that the rate at $\rho = \infty$ is given by

$$R_{k,l}(\infty, \Delta_k) = \log_2\left(1 + \frac{z_{k,l}}{d_k \Delta_k}\right). \tag{4.33}$$

By definition, at the saturating SNR $\rho_s^{k,l}$,

$$\log_2\left(1 + \frac{\rho_s^{k,l} z_{k,l}}{d_k}\right) = R_{k,l}(\infty, \delta_k^{(l)}) \tag{4.34}$$

$$= \log_2\left(1 + \frac{z_{k,l}}{d_k \delta_k^{(l)}}\right), \tag{4.35}$$

which gives

$$\rho_s^{k,l} = \frac{1}{\delta_k^{(l)}}. \tag{4.36}$$

The superscript (l) in $\delta_k^{(l)}$ is there to remind that $\delta_k^{(l)}$ is one realisation of Δ_k for the lth stream of the kth user.

As a result, the saturating SNR is a random variable $\wp_s^k = \frac{1}{\Delta_k}$ (note that I drop the superscript l because it is the same distribution for all the streams of the kth user) and the pdf of the saturating SNR can be derived as

$$f_{\wp_s^k}(\rho_s^k) = \frac{1}{(\rho_s^k)^2} f_{\Delta_k}\left(\frac{1}{\rho_s^k}\right). \tag{4.37}$$

Theorem 4. *Given the saturating SNR $\rho_s^{k,l}$, the achievable rate can be approximated within* 1bps/Hz *by*

$$\tilde{R}_{k,l}(\rho) = \begin{cases} \log_2\left(1 + \frac{\rho z_{k,l}}{d_k}\right) & \text{for } 0 \le \rho \le \rho_s^{k,l}, \\ \log_2\left(1 + \frac{\rho_s^{k,l} z_{k,l}}{d_k}\right) & \text{for } \rho_s^{k,l} \le \rho, \end{cases} \tag{4.38}$$

where $\log_2(1 + \frac{\rho z_{k,l}}{d_k})$ *is the rate in the perfect CSI case.*

Proof. Define the function $G(\rho) \triangleq \tilde{R}_{k,l}(\rho) - R_{k,l}(\rho, \delta_k^{(l)})$ that represents the gap between $R_{k,l}$ and $\tilde{R}_{k,l}$. For $0 \le \rho \le \rho_s^{k,l}$, I have that

$$G(\rho) = \log_2\left(\frac{1 + \frac{\rho}{d_k} z_{k,l}}{1 + \frac{\rho}{d_k(\delta_k^{(l)}\rho + 1)} z_{k,l}}\right). \tag{4.39}$$

One can notice that $G(0) = 0$ and G is an increasing function of ρ. I can now evaluate

G at the saturating SNR, i.e., $\rho_s^{k,l} = \frac{1}{\delta_k^{(l)}}$. Then,

$$G(\rho_s) = G\left(\frac{1}{\delta_k^{(l)}}\right) \tag{4.40}$$

$$= \log_2\left(\frac{1+\frac{\frac{1}{\delta_k^{(l)}}}{d_k} z_{k,l}}{1+\frac{\frac{1}{\delta_k^{(l)}}}{2d_k} z_{k,l}}\right) \tag{4.41}$$

$$= \log_2\left(\frac{\delta_k^{(l)} + \frac{z_{k,l}}{d_k}}{\delta_k^{(l)} + \frac{z_{k,l}}{2d_k}}\right). \tag{4.42}$$

The expression $\frac{\delta_k^{(l)}+\frac{z_{k,l}}{d_k}}{\delta_k^{(l)}+\frac{z_{k,l}}{2d_k}}$ is a decreasing function of $\delta_k^{(l)}$ that goes from 2 to 1 therefore $G(\rho_s^{k,l}) \in [0,1]$ and finally $\forall \rho \in [0, \rho_s^{k,l}]$ $G(\rho) \in [0,1]$.

On the other hand, for $\rho > \rho_s^{k,l}$, by definition of the saturating SNR, $R_{k,l}(\rho, \delta_k^{(l)}) \to \tilde{R}_{k,l}(\rho)$. This concludes that $\tilde{R}_{k,l}(\rho)$ is an approximation of $R_{k,l}(\rho, \delta_k^{(l)})$ within 1bps/Hz $\forall \rho$. □

4.4.2 Outage Probability

In the case of fading channels, one often uses outage capacity as a metric to assess the performance of the communication system. Outage capacity is linked to a parameter called "outage probability", $\mathcal{P}_{\mathsf{out}}$, which represents the probability that *error-free* communications cannot be achieved at a given rate. This can be translated to a minimum SNR $\rho_{\min}$ below which the information rate is not supported, or $\mathcal{P}_{\mathsf{out}} = \mathbb{P}(\rho < \rho_{\min})$. Define the outage probability of the ℓth stream of a user k as the probability that that stream cannot support any rate equal or above $C_{\mathsf{out}}^{k,l}$ at infinite SNR, i.e., $\mathcal{P}_{\mathsf{out}}^{k,l} = \mathbb{P}(R_{k,l}^{\infty} < C_{\mathsf{out}}^{k,l})$, with $R_{k,l}^{\infty}(\Delta_k) \triangleq R_{k,l}(\Delta_k, \infty)$, and $C_{\mathsf{out}}^{k,l}$ being the outage capacity for the ℓth stream of the kth user. Then

$$\mathbb{P}(R_{k,l}^{\infty} < C_{\mathsf{out}}^{k,l}) = \frac{z_{k,l}(\log_e 2)}{d_k} \times \int_0^{C_{\mathsf{out}}^{k,l}} \frac{2^r}{(2^r-1)^2} f_{\Delta_k}\left(\frac{z_{k,l}}{d_k(2^r-1)}, d_k\right) dr, \tag{4.43}$$

which can be further expressed as

$$\mathbb{P}(R_{k,l}^{\infty} < C_{\mathsf{out}}^{k,l}) = \int_{\frac{z_{k,l}}{d_k(2^{C_{\mathsf{out}}^{k,l}}-1)}}^{\infty} f_{\Delta_k}(x, d_k)dx. \tag{4.44}$$

If I define the outage SNR $\rho_{\mathsf{out}}^{k,l}$ so that $C_{\mathsf{out}}^{k,l} = \log_2(1 + \frac{\rho_{\mathsf{out}}^{k,l} z_{k,l}}{d_k})$, then

$$\mathcal{P}_{\mathsf{out}}^{k,l} = \int_{\frac{1}{\rho_{\mathsf{out}}^{k,l}}}^{\infty} f_{\Delta_k}(x, d_k)dx = \mathbb{P}(\rho_s^{k,l} < \rho_{\mathsf{out}}^{k,l}). \tag{4.45}$$

This indicates that the outage probability equals the probability that the saturating SNR is lower than the outage SNR.

I can use (4.31) and (4.45) to give the outage probability as

$$\mathcal{P}_{\mathsf{out}}^{k,l} = \frac{1}{\Gamma(D-d_k)}\Gamma\left(D-d_k, \frac{1}{\rho_{\mathsf{out}}^{k,l}\sigma_e^2}\right) \tag{4.46}$$

$$= \tilde{\Gamma}\left(D-d_k, \frac{1}{\rho_{\mathsf{out}}^{k,l}\sigma_e^2}\right), \tag{4.47}$$

where

$$\tilde{\Gamma}(a,x) = \frac{\Gamma(a,x)}{\Gamma(a)} \tag{4.48}$$

is the regularised upper incomplete Gamma function.

Note that the relation between $\mathcal{P}_{\mathsf{out}}^{k,l}$ and $\rho_{\mathsf{out}}^{k,l}$ does not involve $z_{k,l}$ but does involve d_k. Hence, that relation is the same for all the streams of the same user in accordance with the fact that all those streams transmit the same power. I can therefore define the outage probability (respectively outage SNR) of the user (say k) as $\mathcal{P}_{\mathsf{out}}^{k} = \mathcal{P}_{\mathsf{out}}^{k,l}$ (respectively $\rho_{\mathsf{out}}^{k} = \rho_{\mathsf{out}}^{k,l}$).

In (4.47), the effect of the other users on the performance of user k manifests itself through the total number of streams D in the network. The outage probability will decrease if the contribution of user k in the total number of streams is high, because $D - d_k$ in this case is smaller and also because there is no interference between the streams of the same user.

4.5 Applications

In this section, I give two application examples for utilising the previous analytical results in the MIMO interference channel.

4.5.1 Degrading CSI in Block Fading Channels

For block fading channels, the channels are often considered as constant for a period of time, say T_D, but vary from one block to another. Moreover, the transmit power is normalised such that $\frac{1}{T_D}\mathbb{E}\{\|\mathbf{x}_\ell\|_2^2\} = P_0 \ \forall \ell$. A typical scenario is that the channels are estimated at the first block only and all the IA matrices are obtained from the estimated channels. The direct link channels vary from one block to the next but are tracked perfectly while the crosstalk channels are not tracked (due to high overheads), so the crosstalk CSI degrades over time.

Let us denote $\mathbf{H}(t_0)$ as the actual state of a channel matrix at time t_0. The estimated channel is denoted by $\hat{\mathbf{H}}(t_0)$, which is modelled as

$$\mathbf{H}(t_0) = \hat{\mathbf{H}}(t_0) + \Delta\mathbf{H}(t_0), \tag{4.49}$$

where $\Delta\mathbf{H}(t_0)$ is the deviation of the estimate from the actual channel at time t_0. For the block fading channels, I have

$$\mathbf{H}(t_0 + k \times T_D) \neq \mathbf{H}(t_0), \text{ for } k = 1, 2, \ldots, \tag{4.50}$$

with probability one. I define a new matrix $\mathbf{E}$ that represents the variation of the channel between two different times as

$$\mathbf{E}(k) \triangleq \mathbf{H}(t_0 + k \times T_D) - \mathbf{H}(t_0) \tag{4.51}$$

$$= \mathbf{H}(t_0 + k \times T_D) - \hat{\mathbf{H}}(t_0) - \Delta\mathbf{H}(t_0). \tag{4.52}$$

Hence,

$$\underbrace{\mathbf{E}(k) + \Delta\mathbf{H}(t_0)}_{\triangleq \Delta\mathbf{H}(k)} = \mathbf{H}(t_0 + k \times T_D) - \hat{\mathbf{H}}(t_0) \tag{4.53}$$

represents the deviation from the channel estimate to the actual channel at the $(k+1)$th block for the crosstalk.

I assume that $\Delta\mathbf{H}(k) \sim \mathcal{CN}(0, \sigma_e^2(k))$ with $\sigma_e^2(0) = \sigma_e^2$ being the power of the measurement. Based on this model, if I consider one stream of a user transmitting d_0 streams, and provided that the user is transmitting at the same outage SNR over each block, I can express the evolution of the outage probability in each block as

$$\mathcal{P}_{\mathsf{out}}(k) = \tilde{\Gamma}\left(D - d_0, \frac{1}{\rho_{\mathsf{out}}\sigma_e^2(k)}\right). \tag{4.54}$$

Instead of transmitting at a fixed SNR the user may want to insure a preset outage probability over each block in which case the SNR at which it should transmit over that stream is given by

$$\rho_{\mathsf{out}}(k) = \frac{1}{\sigma_e^2(k)\tilde{\Gamma}^{-1}\left(D - d_0, \mathcal{P}_{\mathsf{out}}\right)} \tag{4.55}$$

$$= \frac{\sigma_e^2}{\sigma_e^2(k)}\rho_{\mathsf{out}}, \tag{4.56}$$

where

$$\rho_{\mathsf{out}} \triangleq \frac{1}{\sigma_e^2\tilde{\Gamma}^{-1}\left(D - d_0, \mathcal{P}_{\mathsf{out}}\right)}, \tag{4.57}$$

and $\tilde{\Gamma}^{-1}$ is the inverse of function $\tilde{\Gamma}$.

Employing the result of Theorem 4, the maximum achievable rate per stream for the MIMO interference channel using IA under the block fading channel at outage probability of $\mathcal{P}_{\mathsf{out}}$ can be given within 1bps/Hz by

$$\tilde{R}(k) = \log_2\left(1 + \frac{\rho_{\mathsf{out}}(k)}{d_0}z(k)\right) \tag{4.58}$$

$$= \log_2\left(1 + \frac{\sigma_e^2}{\sigma_e^2(k)}\frac{\rho_{\mathsf{out}}}{d_0}z(k)\right), \tag{4.59}$$

where $z(k)$ is the effect that the channel has on that stream over the kth block. The

achievable rate for that stream over B consecutive blocks can therefore be found as

$$R_B = \sum_{k=0}^{B-1} \log_2 \left(1 + \frac{\sigma_e^2}{\sigma_e^2(k)} \frac{\rho_{\mathsf{out}}}{d_0} z(k)\right). \tag{4.60}$$

Under the conditions $\frac{\sigma_e^2}{\sigma_e^2(k)} \frac{\rho_{\mathsf{out}}}{d_0} z(k) \gg 1 \ \forall k$, e.g., if the power of the channel variations over the measurement noise power is very small or if the outage SNR is sufficiently big or also if there is no overly deep fading over any block, then that rate becomes

$$R_B \approx \sum_{k=0}^{B-1} \log_2 \frac{\sigma_e^2}{\sigma_e^2(k)} \frac{\rho_{\mathsf{out}}}{d_0} z(k) \tag{4.61}$$

$$= \underbrace{B \log_2 \frac{\rho_{\mathsf{out}}}{d_0}}_{(a)} + \underbrace{\log_2 \prod_{k=0}^{B-1} z(k)}_{(b)} - \underbrace{\log_2 \prod_{k=0}^{B-1} \frac{\sigma_e^2(k)}{\sigma_e^2}}_{(c)}. \tag{4.62}$$

In the equation above,

- (a) represents the rate achievable per stream with perfect IA and no fading at SNR $= \rho_{\mathsf{out}}$ over B blocks.
- (b) represents the effect that the channel variations of the direct link has on the rate; it could be positive or negative depending on the fading coefficients.
- (c) represents the effect of the crosstalk CSI uncertainty on the rate; this effect is negative because there is at least the uncertainty from the measurement.

Let us have a look at the following example.

Recall from the definition of $\mathbf{E}(k)$ in (4.51), if we say $\mathbf{E}(k) \sim \mathcal{CN}(0, \sigma^2) \ \forall k$, then we can get

$$\sigma_e^2(k) = \begin{cases} \sigma_e^2 + \sigma^2 & \text{for } k > 0, \\ \sigma_e^2 & \text{for } k = 0, \end{cases} \tag{4.63}$$

and

$$R_B = B\log_2\frac{\rho_{\mathsf{out}}}{d_0} + \log_2\prod_{k=0}^{B-1} z(k) - \log_2\left(1+\frac{\sigma^2}{\sigma_e^2}\right)^{B-1}, \quad \text{for } B \geq 1 \quad (4.64)$$

In the above, we see that if the power of the channel variation is smaller than the measurement noise power (i.e., $\frac{\sigma^2}{\sigma_e^2} \ll 1$), the channel variations have little effect on the IA performance.

4.5.2 Optimising the Number of Streams

In an IA system with K users and imperfect crosstalk CSI, unsurprisingly, every user would want to increase the number of signal streams for enhancing its achievable rate but doing so may harm the sum-rate because of the additional interference due to imperfect IA resulting from imperfect CSI. If all users are assumed to have the same number of streams d, it would be important to determine the optimal number of streams per user of the interference network for maximising the sum-rate, for a given measurement noise power σ_e^2.

To do so, I first set an outage probability of $\mathcal{P}_{\mathsf{out}}$ that must remain the same for every user. Then I obtain the required outage SNR for all users as

$$\rho_{\mathsf{out}} = \frac{1}{\sigma_e^2\tilde{\Gamma}^{-1}(d(K-1),\mathcal{P}_{\mathsf{out}})}. \quad (4.65)$$

I define the outage SNR per stream as $\bar{\rho}_{\mathsf{out}} = \frac{\rho_{\mathsf{out}}}{d}$.

For most applications, the outage probability is chosen to be a very small value, and thus the probability of the saturating SNR being lower than the outage SNR is equally small (see (4.45)). In that case, I can use Theorem 4 and the function $\tilde{R}$ defined in Section 4.4.1 to approximate the rate per stream at SNR $= \rho_{\mathsf{out}}$ with a confidence given by the choice of $\mathcal{P}_{\mathsf{out}}$ as

$$\tilde{R}_{k,l}(\bar{\rho}_{\mathsf{out}}) = \log_2\left(1+\bar{\rho}_{\mathsf{out}}z_{k,l}\right), \quad (4.66)$$

where $z_{k,l}$ has the same meaning as in the previous section.
Hence, the sum-rate for the network is found as

$$\bar{R}(\bar{\rho}_{\mathsf{out}}) = \sum_{k=1}^{K} \sum_{l=1}^{d} \tilde{R}_{k,l}(\bar{\rho}_{\mathsf{out}}). \tag{4.67}$$

The optimal number of streams per user can be found by

$$\max_{d} \bar{R}(\bar{\rho}_{\mathsf{out}}). \tag{4.68}$$

One may also want to optimise the number of streams per user in average over all possible realisations of $z_{k,l}$. This means multiple realisations of IA with different channel gains must be considered and averaged over all possible achievable sum-rates. To do so, assume that the direct channels $\mathbf{H}_{k,k}$ are independent across users and have their entries independent and identically distributed (i.i.d.) from $\mathcal{CN}(0,1)$. Also, the crosstalk channels do not matter since their effects are cancelled out by IA. Under that condition Lemma 1 in [19] can be applied to derive the average sum-rate as

$$\mathcal{R}(\bar{\rho}_{\mathsf{out}}) = \sum_{k=1}^{K} \sum_{l=1}^{d} \mathbb{E}\left[\tilde{R}_{k,l}(\bar{\rho}_{\mathsf{out}})\right] \tag{4.69}$$

$$= Kd \log_2(e) e^{\frac{1}{\bar{\rho}_{\mathsf{out}}}} E_1\left(\frac{1}{\bar{\rho}_{\mathsf{out}}}\right), \tag{4.70}$$

where $E_1(x) = \int_1^\infty t^{-1} e^{-xt} dt$ is an exponential integral.

Since the approximation of the rate given by Theorem 2 was used, the expectation does not involve the measurement error matrices. The price to pay for that is however that the result is given within 1bps/Hz precision.
Now the optimal number of streams is found by solving

$$\max_{d} \mathcal{R}(\bar{\rho}_{\mathsf{out}}). \tag{4.71}$$

This second expression depends only on the number of users, the measurement noise power and the outage probability.

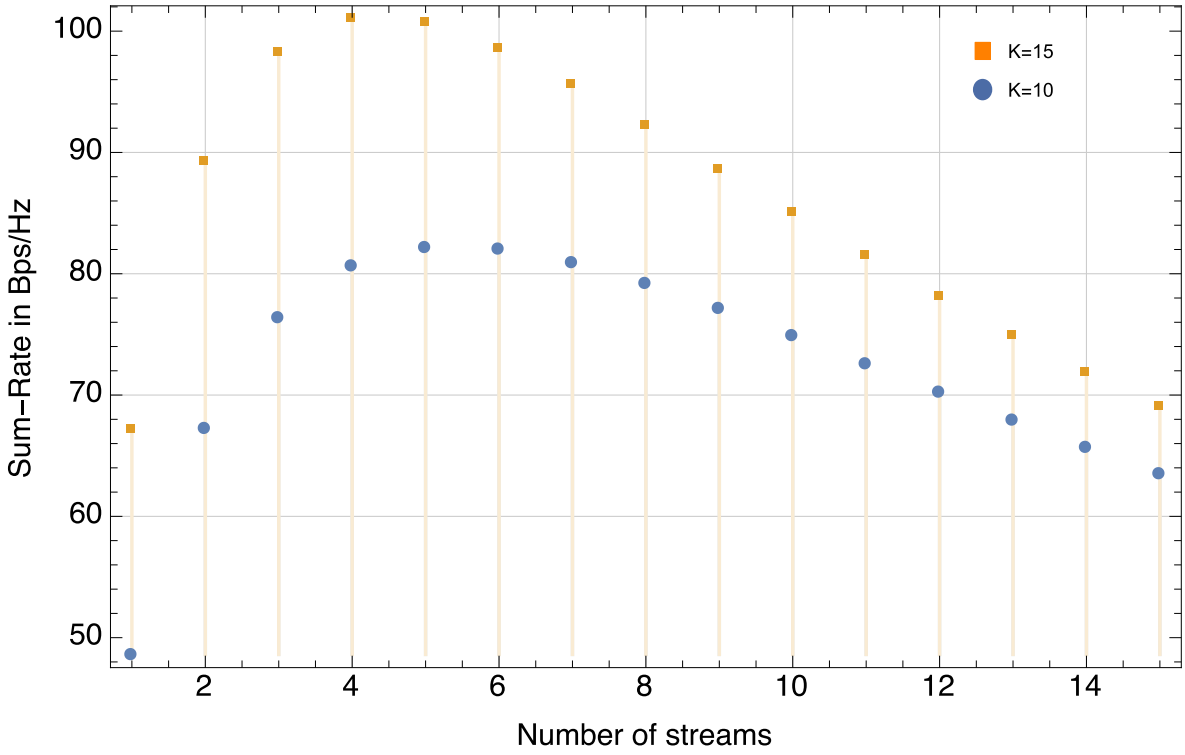
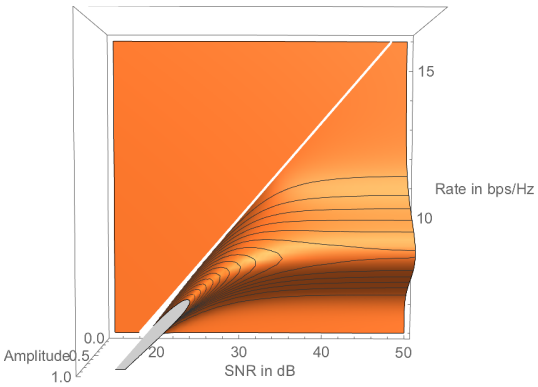
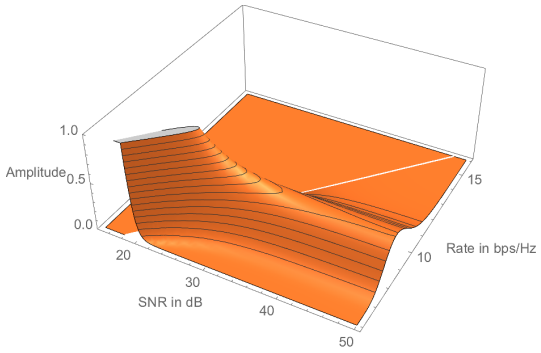


Figure 4.1: The sum-rate $\mathcal{R}$ against the number of streams per user, with its maximum achieved when $d = 5$ for 10 users and $d = 4$ for 15 users.

In Figure 4.1, I provide the numerical results for the sum-rate $\mathcal{R}$ against the number of signal streams, when $K = 10$ and $K = 15$, $\sigma_e^2 = 10^{-3}$ and $\mathcal{P}_{\text{out}} = 10^{-3}$. The results demonstrate the concavity of the sum-rate so the optimal number of streams can be easily identified to be $d = 5$ with $K = 10$ and $d = 4$ with $K = 15$. The results also imply that it is counter-productive to increase the number of streams further due to excessive interference. In addition, note that there is a significant gain in the total rate to go from one signal stream to the optimal number of streams (up 35bps/Hz for $K = 10$). This figure also demonstrates that the number of streams allowed per user decreases with the number of user due to CSI uncertainty.



(a) Top view



(b) Side view

Figure 4.2: The pdf of the achievable rate per stream with $K = 3$, $d = 1$, and $\sigma_e^2 = 10^{-3}$. The white line represents the limiting case where there is no CSI uncertainty.

4.6 Simulations versus Theory

In this section, I present the predictions of the model and compare these predictions to the results obtained from the simulations. In these simulations, I focus on the 3-user case as it allows to compute the perfect precoders for IA. The parameters for the simulations are set to $K = 3$ and $d = 1$.

First adapt (4.32) to the parameters above which yields

$$f_{\Delta_k}(\delta_k, 1) = \begin{cases} \frac{1}{\sigma_e^4}\delta_k e^{-\frac{\delta_k}{\sigma_e^2}} & \text{for } \delta_k \geq 0, \\ 0 & \text{for } \delta_k < 0. \end{cases} \tag{4.72}$$

Figure 4.2 shows the pdf of the achievable rate per stream for the case $\sigma_e^2 = 10^{-3}$ based on the theory. It is a three-dimensional plot with the x-axis showing the SNR in dB, the y-axis the rate in bps/Hz and the z-axis the pdf value.

To compare the theoretical predictions to the simulations, I ran the simulations, in which channel matrices were drawn randomly from $\mathcal{CN}(0, 1)$ which represent the perfect CSI, and the erroneous channel matrices were set to be the sum of the channel matrices and the error matrices drawn randomly from $\mathcal{CN}(0, \sigma_e^2)$. Moreover, all the users were assumed to have $n = 3$ transmit antennas and $m = 2$ receive antennas, and

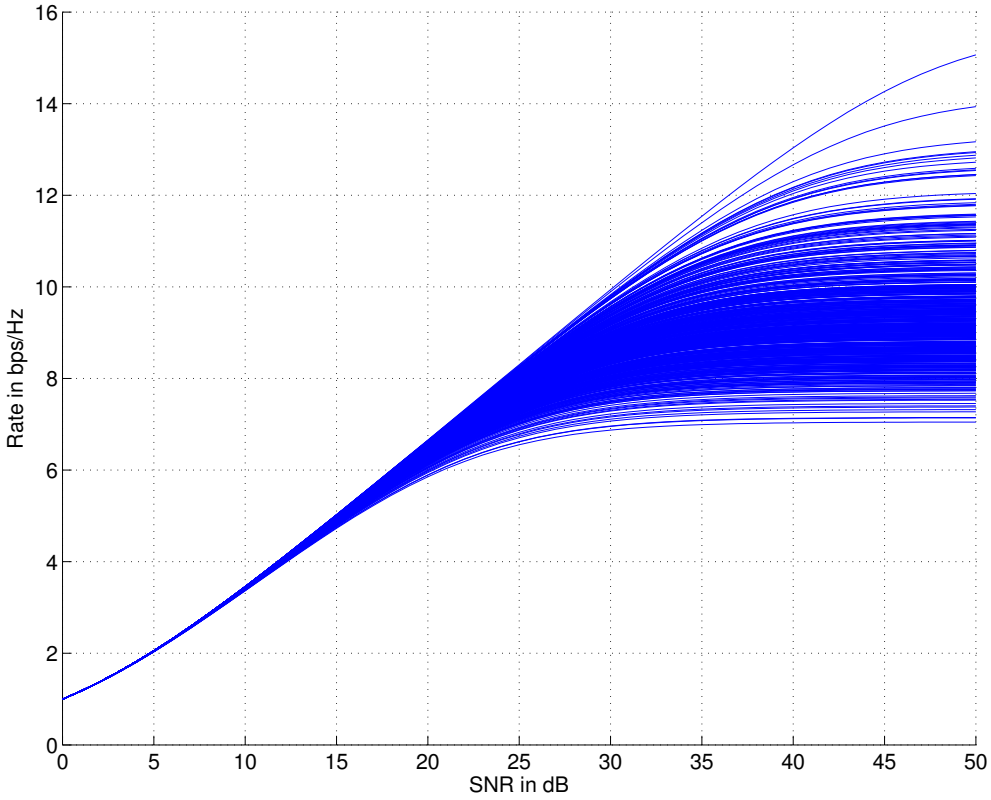


Figure 4.3: The achievable rates with IA for a given MIMO interference channel with 500 independent measurement errors.

these matrices were used to perform IA at various SNR. I also set the fading coefficients on the direct links ($z_{k,l}$) to 1 so that only the effects of the measurement error can be seen and not that of the fast fading.

In Figure 4.3, I provide the results for the rates achievable by IA for a given MIMO channel for 500 independent error realisations. As can be seen, the rates appear to saturate at high SNR as predicted by the theory. To compare theory and simulations further, I also provide the results for the case at SNR = 80dB, as shown in Figure 4.4, where the theoretical pdf and the simulations fit almost perfectly.

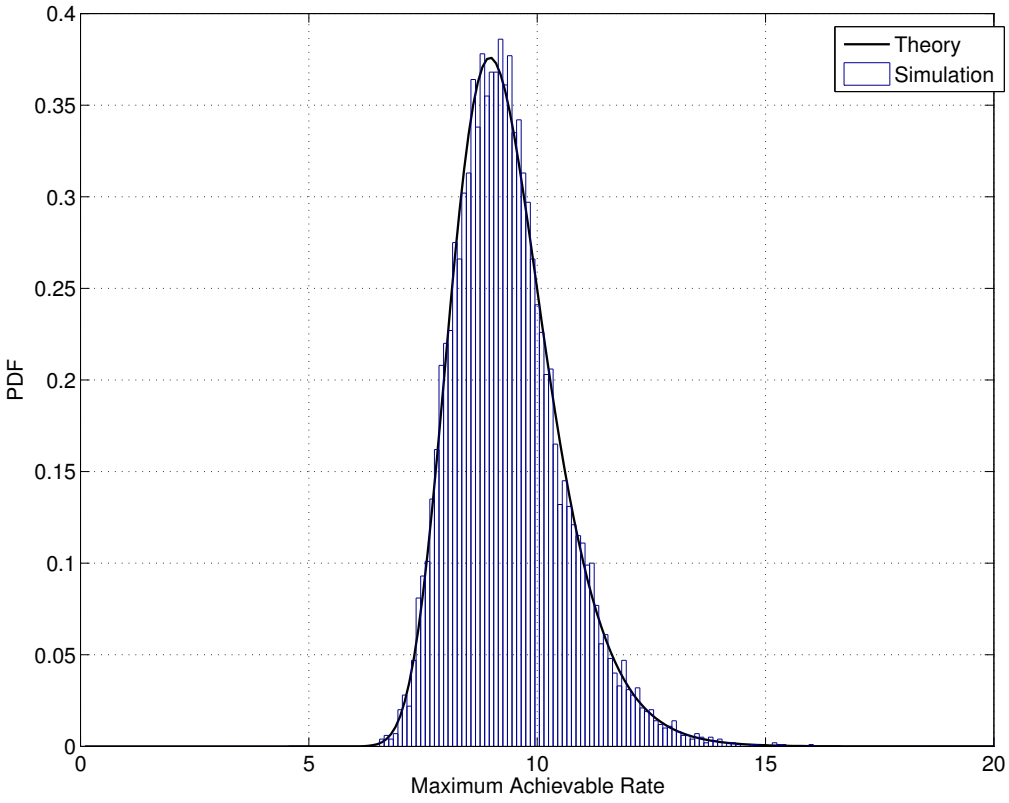


Figure 4.4: The pdfs of the achievable rates when $K = 3$, $d = 1$, $\sigma_e^2 = 10^{-3}$ at $SNR = 80dB$ from the simulations and the theory.

4.7 Conclusion

This chapter presents a full statistical characterisation for the maximum achievable rate per user using IA in the interference channel, when cross-talk CSI are imperfect. I've proposed two metrics to evaluate the performance of the interference network despite the randomness of CSI errors. The first metric is the saturating SNR that was already introduced in chapter 3, in this case it is stochastic. However, it allows the definition of a powerful new metric namely, the outage probability. With this new tool, the study of the performance of IA with random CSI errors is greatly simplified.
In order to show the relevance of the newly defined metric, two different examples are shown. The first one shows how to investigate the performance of IA in block fading channels with degrading CSI, while the second one shows how to use the results on the outage probability in order to optimise the number of streams per user and maximise the sum-rate using IA in the presence of CSI errors. Simulation results are provided to confirm the accuracy of the analysis.

Chapter 5

Coverage probability

5.1 Introduction

This chapter considers the use of IA in cellular networks under imperfect CSI conditions. While similar objectives have been pursued in [18, 98, 99], the novelty of this work lies in that the analysis includes the randomness of base station (BS) deployment and that the coverage probability of such IA-assisted cellular network is derived. Note that although coverage probability analysis has been addressed in [100] where the authors developed new general models for the multi-cell signal-to-interference-plus-noise ratio (SINR) using stochastic geometry, no ways of mitigating the inter-cell interference was considered in the analysis except by changing the frequency reuse factor in the network. To the best of my knowledge there is no such study including IA with imperfect CSI in their analysis.

5.2 System Model

Let's consider a cellular network model that consists of BSs located randomly in a Euclidean plane according to some point process. Also consider multiple user equipments (UE) distributed randomly in the network according to an independent point process. Each UE is assumed to be associated with a serving BS which may or may not be the nearest one. For example, if the association policy is to pair the UE with the BS with

the highest SNR, then this BS may or may not be the closest one because of propagation issues (e.g., shadowing). The focus is on the downlink i.e. the link from the base station to the users. Intra-cell interference is assumed is non-existent or dealt with perfectly by orthogonalising the same cell users over time or frequency. As a result, at each time or frequency slot, the network can be modelled as an interference channel with multiple transmitter-receiver pairs. The inter-cell interference is then mitigated using IA.

In particular, IA is applied in the network under the assumption that every node in the network (BSs and UEs) has access to perfect CSI between a BS and its associated UE but imperfect CSI between a BS and the UEs that the BS is creating interference at. Note that a given UE in the network will not suffer interference from every BS in the network due to the high path-loss to some BSs. Therefore, there exist a maximum distance R_M to the UE within which a non-serving BS will be considered as an interferer and above which it is invisible to the UE. A simple example of this is when the power received from some base station is below the noise floor.

Let us focus our attention onto a circle of radius R_M in the network and denote by G the numbers of serving BSs and UEs in each time/frequency slot in that circle. Both the BSs and the UEs are equipped with multiple antennas for spatial IA. The number of antennas at each node is determined so as to fulfil the feasibility conditions for IA [23, 24]. $\mathbf{H}_{i,j}$ denotes the channel matrix related to the scattering and multipath effect of the environment between the jth transmitter and the ith receiver. The estimate of $\mathbf{H}_{i,j}$, denoted as $\hat{\mathbf{H}}_{i,j}$, is such that

$$\mathbf{H}_{i,j} = \hat{\mathbf{H}}_{i,j} + \Delta\mathbf{H}_{i,j}, \ \forall i \neq j \tag{5.1}$$

where $\Delta\mathbf{H}_{i,j}$ is the estimation error with entries drawn from a complex Gaussian distribution $\mathcal{CN}(0, \sigma_e^2)$. As in the previous chapter, the direct links are assumed to be known perfectly since their estimation is easier than that of the interfering links and is typically highly accurate. The path-loss and shadowing will be represented by the quantities ℓ_i for the interfering links and ℓ_d for the direct link. The assumption that is made here is that all the interferers have the same coefficients ℓ_i which in practice is not true. However this case can provide some meaningful insights in the study of IA

applied at the cell edge. The channel matrices are assumed constant for at least the time of communication over a time or frequency slot. The precoders $\mathbf{V}_k$ and decoding matrices $\mathbf{U}_k$ are obtained following the IA conditions below:

$$\begin{cases} \text{rank}(\mathbf{U}_k^* \mathbf{H}_{k,k} \mathbf{V}_k) = d_k, \text{ for } k = 1, 2, \ldots, K, \\ \mathbf{U}_\ell^* \hat{\mathbf{H}}_{\ell,k} \mathbf{V}_k = 0, \text{ for all } \ell \neq k, \end{cases} \tag{5.2}$$

where d_k represents the number of streams for the kth user.

5.3 Coverage Probability Analysis

In this section, the aim is to derive the coverage probability for a user taken randomly in the network. It is defined as the probability that a given user can achieve some target rate. The coverage probability can be viewed as the complementary of the outage probability given in chapter 4. In order to provide a mathematical definition of the coverage probability, I will first need to adapt the equation (4.47) of the outage probability to the current model.

5.3.1 Statistics of the Achievable Rate

Consider a typical user (say user o) and the set $\mathcal{S}_o$ of the BSs that create interference at this user. The received signal at this user can be written as

$$\mathbf{y}_o = \sqrt{\ell_d} \mathbf{H}_{o,o} \mathbf{V}_o \mathbf{x}_o + \sum_{s \in \mathcal{S}_o} \sqrt{\ell_i} \mathbf{H}_{o,s} \mathbf{V}_s \mathbf{x}_s + \boldsymbol{\eta}_o, \tag{5.3}$$

where $\boldsymbol{\eta}_o$ is the additive noise drawn from $\mathcal{CN}(0, \sigma_n^2)$ and $\mathbf{x}_k$ denotes the data stream for the kth user. After applying the decoding matrix, the expression (5.3) becomes

$$\mathbf{U}_o^* \mathbf{y}_o = \sqrt{\ell_d} \mathbf{U}_o^* \mathbf{H}_{o,o} \mathbf{V}_o \mathbf{x}_o + \mathbf{U}_o^* \sum_{s \in \mathcal{S}_o} \sqrt{\ell_i} \Delta \mathbf{H}_{o,s} \mathbf{V}_s \mathbf{x}_s + \mathbf{U}_o^* \boldsymbol{\eta}_o, \tag{5.4}$$

where the term $\mathbf{U}_o^* \sum_{s \in \mathcal{S}_o} \sqrt{\ell_i} \Delta \mathbf{H}_{o,s} \mathbf{V}_s \mathbf{x}_s$ arises from the IA conditions (5.2) and the CSI error model (5.1).

If the BSs are assumed to have the same transmit power P_o, then according to (4.24), the received interference at any stream of user o can be expressed as a r.v.

$$\mathcal{I} = \ell_i P_o \Delta, \tag{5.5}$$

in which $\frac{2}{\sigma_e^2}\Delta$ is a r.v. drawn from the χ^2 distribution with $2(D - d_o)$ DoFs where D is the total number of streams sent by the interferers in $\mathcal{S}_o$ plus that of the serving BS and d_o is the number of streams sent by the serving BS only.

The probability density function (pdf) of Δ is given as

$$f_\Delta(\delta) = \begin{cases} \frac{1}{\sigma_e^2 \Gamma(D-d_o)} \left(\frac{\delta}{\sigma_e^2}\right)^{D-d_o-1} e^{-\frac{\delta}{\sigma_e^2}} & \text{for } \delta \geq 0, \\ 0 & \text{for } \delta < 0, \end{cases} \tag{5.6}$$

and the achievable rate for the lth stream of the UE is

$$R_l(P_o, \mathcal{I}) = \log_2 \left(1 + \frac{\left(\ell_d \frac{P_o}{d_o}\right) |(\mathbf{U}_o^*)_l \mathbf{H}_{o,o} [\mathbf{V}_o]_l|^2}{\mathcal{I} + \sigma_n^2} \right). \tag{5.7}$$

As in the previous chapter, I define $z_l \triangleq |(\mathbf{U}_o^*)_l \mathbf{H}_{o,o} [\mathbf{V}_o]_l|^2$ and write the achievable rate of the lth stream of the UE as

$$R_l(P_o, \mathcal{I}) = \log_2 \left(1 + \frac{\left(\ell_d \frac{P_o}{d_o}\right) z_l}{\mathcal{I} + \sigma_n^2} \right). \tag{5.8}$$

This rate expression will be used in the following form:

$$R_l(\rho, \Delta) = \log_2 \left(1 + \frac{\ell_d z_l}{d_o \left(\ell_i \Delta + \frac{1}{\rho}\right)} \right), \tag{5.9}$$

where $\rho = \frac{P_o}{\sigma_n^2}$.

5.3.2 Outage Probability

Let recall and adapt the definition of the outage probability. The outage probability of a user sending d_o streams is defined for each of its streams (say for the ℓth stream) as the probability that that stream cannot support any rate equal or above a target rate R^l_{out} at infinite SNR, i.e., $\mathcal{P}^l_{\mathsf{out|D}} = \mathbb{P}(R^\infty_l < R^l_{\mathsf{out}}|D)$, with $R^\infty_l(\Delta) \triangleq R_l(\infty, \Delta)$ and

$$R^\infty_l(\Delta) = \log\left(1 + \frac{\beta z_l}{d_o \Delta}\right), \tag{5.10}$$

where $\beta = \frac{\ell_d}{\ell_i}$.

I define the outage SNR ρ^l_{out} so that

$$R^l_{\mathsf{out}} = \log\left(1 + \frac{\rho^l_{\mathsf{out}} z_l}{d_o}\right). \tag{5.11}$$

As I will show later on, this definition of the outage SNR allows to talk about the outage probability without having to worry about the randomness of z_l on the direct link.

The outage probability is then given by

$$\begin{aligned}
\mathcal{P}^l_{\mathsf{out|D},\beta} &= \mathbb{P}(R^\infty_l < R^l_{\mathsf{out}}|D, \beta) && (5.12)\\
&= \mathbb{P}\left(\log\left(1 + \frac{\beta z_l}{d_o \Delta}\right) < \log\left(1 + \frac{\rho^l_{\mathsf{out}} z_l}{d_o}\right) \middle| D, \beta\right) && (5.13)\\
&= \mathbb{P}\left(\Delta > \frac{\beta}{\rho^l_{\mathsf{out}}} \middle| D, \beta\right) && (5.14)\\
&= \int_{\frac{\beta}{\rho^l_{\mathsf{out}}}}^{\infty} f_\Delta(x, d_o) dx && (5.15)\\
&= \frac{1}{\Gamma(D - d_o)} \Gamma\left(D - d_o, \frac{\beta}{\rho^l_{\mathsf{out}} \sigma^2_e}\right) && (5.16)
\end{aligned}$$

Note that z_l does not appear in this expression, but of course it is needed to link the outage SNR to the outage rate.

5.3.3 Coverage Probability

Let's focus on the case where all the users transmit a single stream. In [100] the coverage probability is defined as the probability that a typical mobile user is able to achieve some threshold SINR. Here, that definition will be modified slightly and to say that the coverage probability is the probability that a typical user can achieve some threshold target rate R_{tar}.

Define the target SNR ρ_{tar} as the SNR needed to transmit at the target rate on an interference-free stream with fading z. That is,

$$R_{\mathsf{tar}} = \log_2(1 + \rho_{\mathsf{tar}} z). \tag{5.17}$$

In the case where β and the number S of interferers at the UE are known, the coverage probability can be expressed as

$$\begin{aligned} \mathcal{P}_{\mathsf{C}|\mathsf{S},\beta} &= \mathbb{P}(R^{\infty} \geq R_{\mathsf{tar}}|S,\beta) && (5.18)\\ &= 1 - \mathbb{P}(R^{\infty} < R_{\mathsf{tar}}|S,\beta) && (5.19)\\ &= 1 - \mathcal{P}_{\mathsf{out}|\mathsf{S},\beta}. && (5.20) \end{aligned}$$

Note that here the outage probability $\mathcal{P}_{\mathsf{out}|\mathsf{S},\beta}$ is defined with the target rate as the outage rate. Note also that if there is no interferer ($S = 0$), then $\mathcal{P}_{\mathsf{out}|\mathsf{S},\beta} = 0$ and then $\mathcal{P}_{\mathsf{C}|\mathsf{S},\beta} = 1$.

However, in the current study, the number of interfering BS S is assumed random. Therefore,

$$\begin{aligned} \mathcal{P}_{\mathsf{C}} &= \mathbb{E}_{S,\beta}[1 - \mathcal{P}_{\mathsf{out}|\mathsf{S}}] && (5.21)\\ &= \mathbb{E}_{S,\beta}\left[1 - \frac{1}{\Gamma(S)}\Gamma\left(S, \frac{\beta}{\rho_{\mathsf{tar}}\sigma_e^2}\right)\right] && (5.22)\\ &= \mathbb{E}_{S,\beta}\left[\frac{1}{\Gamma(S)}\gamma\left(S, \frac{\beta}{\rho_{\mathsf{tar}}\sigma_e^2}\right)\right], && (5.23) \end{aligned}$$

where $\gamma(a, x)$ is the lower incomplete gamma function and $\mathbb{E}_{S,\beta}$ means that the average is over β and the number of interfering BS in the vicinity of the UE.

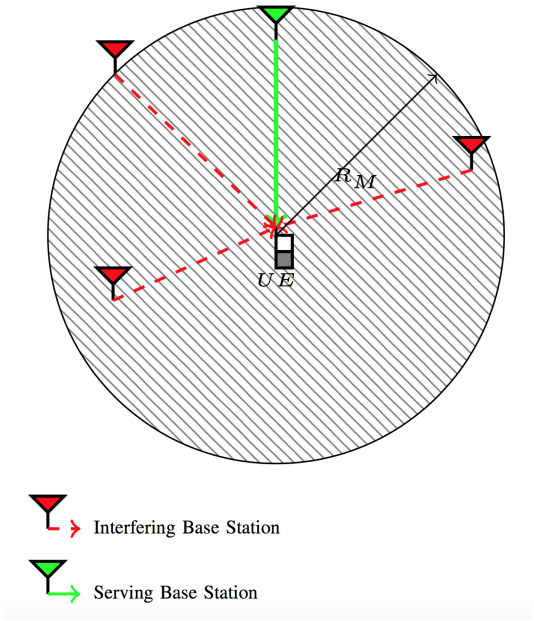


Figure 5.1: Local environment of a user taken randomly, with 3 interferers and 1 serving BS.

5.4 Example

Let us investigate the case where the interfering BSs are distributed according to a PPP Ψ with intensity λ. We can imagine the vicinity of a UE as in Figure 5.1. In this case,

$$\mathbb{P}(S = s|\mathcal{A}) = e^{-\mu}\frac{\mu^s}{s!}, \tag{5.24}$$

where $\mu = \int_{\mathcal{A}} \lambda(r)dr$ is the mean of the Poisson process, and $\mathcal{A}$ is the disc of radius R_M around the UE.

The coverage probability conditioned on β is then given as

$$\mathcal{P}_{\mathsf{C}|\beta} = e^{-\mu} + e^{-\mu}\sum_{s=1}^{\infty}\frac{\mu^s}{s!}\frac{1}{\Gamma(s)}\gamma\left(s, \frac{\beta}{\rho_{\mathsf{tar}}\sigma_e^2}\right). \tag{5.25}$$

This expression can be expressed in terms of an easy to compute integral

$$\mathcal{P}_{\mathsf{C}|\beta} = e^{-\mu} + e^{-\mu} \sum_{s=1}^{\infty} \frac{\mu^s}{s!} \frac{1}{(s-1)!} \int_0^{\frac{\beta}{\rho_{\mathsf{tar}}\sigma_e^2}} t^{s-1} e^{-t} dt \tag{5.26}$$

$$= e^{-\mu} + \mu e^{-\mu} \int_0^{\frac{\beta}{\rho_{\mathsf{tar}}\sigma_e^2}} e^{-t} \left(\sum_{s=1}^{\infty} \frac{(\mu t)^{s-1}}{s!(s-1)!} \right) dt \tag{5.27}$$

$$= e^{-\mu} + \mu e^{-\mu} \int_0^{\frac{\beta}{\rho_{\mathsf{tar}}\sigma_e^2}} e^{-t} \frac{\mathcal{I}_1(2\sqrt{t\mu})}{\sqrt{t\mu}} dt \tag{5.28}$$

$$= e^{-\mu} \left(1 + \int_0^{2\sqrt{\frac{\beta\mu}{\rho_{\mathsf{tar}}\sigma_e^2}}} e^{\frac{-x^2}{4\mu}} \mathcal{I}_1(x) dx \right), \tag{5.29}$$

where $\mathcal{I}_1(\cdot)$ is the modified Bessel function of the first kind. The final expression (5.29) can be computed easily knowing only the four parameters in this expression.

Let us perform a quick analysis of the effects of the different parameters in the expression of $\mathcal{P}_{\mathsf{C}|\beta}$.

- β can be viewed as the signal-to-interference ratio (SIR) at the UE. Increasing it means that the power of the signal at the receiver is getting higher than that of the interference, and therefore it is normal that increasing it would also increase the coverage probability. (5.25) shows that β increases to infinity then the coverage probability becomes.

$$\begin{aligned} \mathcal{P}_{\mathsf{C}|\beta=\infty} &= e^{-\mu} + e^{-\mu} \sum_{K=2}^{\infty} \frac{\mu^{K-1}}{(K-1)!} \\ &= e^{-\mu} + e^{-\mu}(e^{\mu} - 1) \\ &= 1. \end{aligned}$$

- In the same way decreasing σ_e^2 makes $\mathcal{P}_{\mathsf{C}}$ bigger which makes sense since the channel estimates are more accurate. In the limiting case where $\sigma_e^2 = 0$, $\mathcal{P}_{\mathsf{C}} = 1$.

- Regarding ρ_{tar}, increasing its value means that we require a higher rate to be achievable by the UE and thus the coverage probability decreases. The more the

target requirements are decreased, the better the coverage probability.

- The last parameter μ represents the average number of interferers. As a result, when μ is close to zero, $\mathcal{P}_{\mathsf{C}|\beta}$ is close to one and as the density of interferers increases the coverage probability drops.

A closed-form approximation of the coverage probability can be given by truncating the infinite sum in expression (5.25) after the first few terms. In practice, the number of terms to keep will depend on the value of μ.

5.5 Numerical Results

In this section, numerical results are provided based on Monte Carlo simulations of the model studied in this paper and the results are compared with the theory. The channel estimation errors are generated randomly from a complex Gaussian distribution of mean 0 and variance $\sigma_e^2 = 10^{-1}$. This value corresponds to the performance of channel estimation techniques with training SNR $\simeq$ 20dB and up to 8 antennas at the UE and the BS [91]. The number of interfering BS is drawn from a Poisson distribution with expected value $\mu = 3$. In order to consider the case where the user is at the cell edge, I choose $\beta = 1$ so that the strength of the desired signal is comparable to that of the interfering signals. The results with $\beta = 10$ are also shown for comparison. The fading coefficient z on the direct link is assumed exponentially distributed with rate 1 according to [90, Lemma 1].

Figure 5.2 shows the evolution of the coverage probability against the target SNR. The simulation curves are obtained by first computing the coverage probability for a given target rate and realisation of z then the target rate is linked to the target SNR using equation (5.17). In so doing, the effects of the randomness of z are removed. Every point is averaged over ten thousand iterations. There's a perfect match between the theoretical predictions and the simulations. As expected, the coverage probability drops faster when $\beta = 1$ than when $\beta = 10$ because the received SIR is much stronger with $\beta = 10$. This result can be used to obtain the coverage probability for a given target knowing the value of the fading on the communication link.

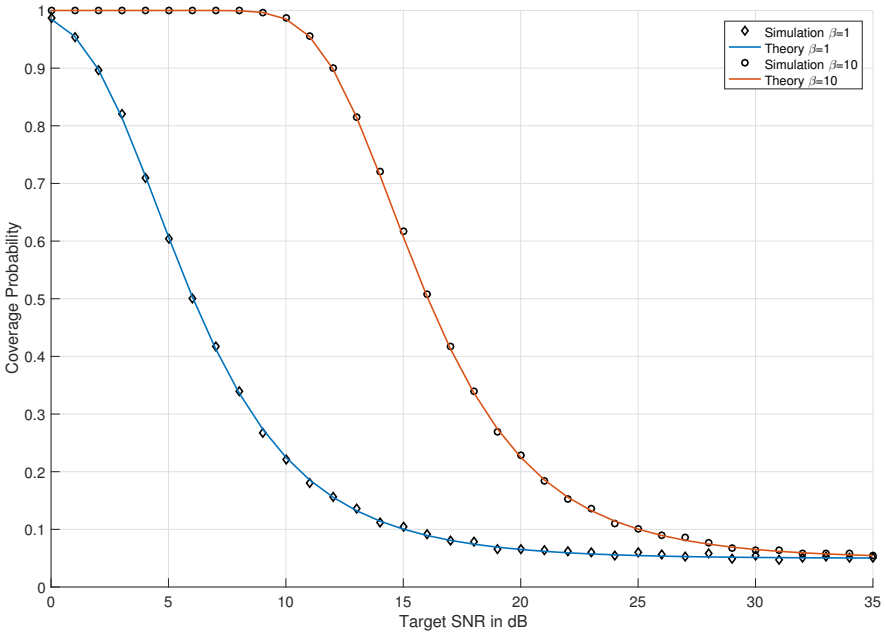


Figure 5.2: Coverage probability of the network against the target SNR in dB with $\mu = 3$, $\sigma_e^2 = 10^{-1}$.

Figure 5.3 shows the coverage probability against the target rate. In this case, I look at two different scenarios in order to see the effect of the fading on the coverage probability. The first scenario is with a fixed fading coefficient $z = 1$ and the second scenario is with z drawn according to the exponential distribution with rate 1. In this second scenario I plot the average of the coverage probability over the fading coefficient. See that the curve for the average coverage probability is lower, which means that on average there is some performance loss due to fading.

5.6 Conclusion

This chapter presented the study of cellular networks using IA to mitigate inter-cell interference. The structure of practical BS deployments is taken into account by considering a random point process to model the BS locations. The coverage probability is derived and given as an easy to compute integral. Simulation results are provided

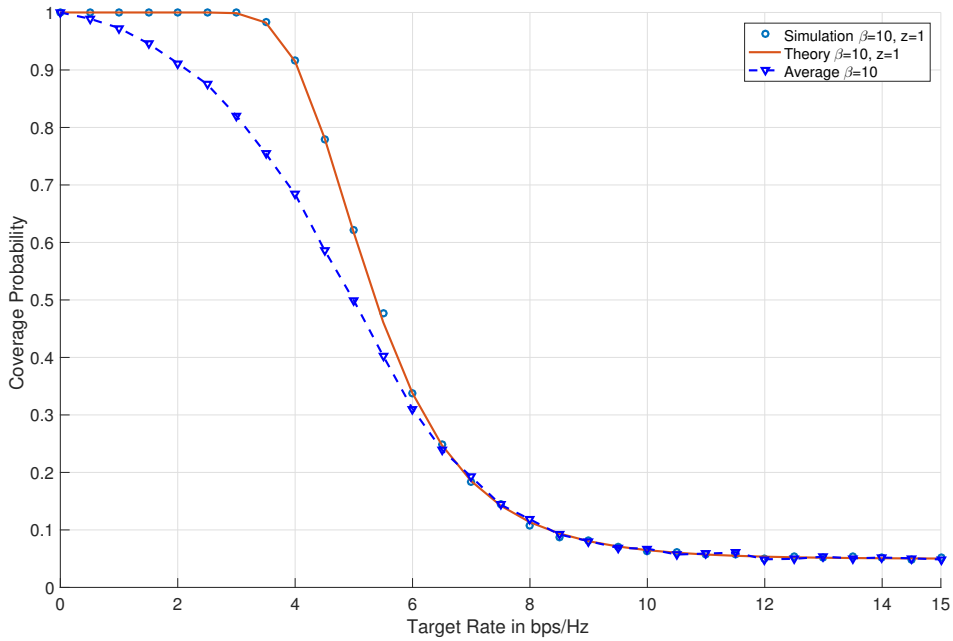


Figure 5.3: Coverage probability of the network against the target rate in bps/Hz with $\mu = 3$, $\sigma_e^2 = 10^{-1}$ for $z = 1$.

and agree with the theoretical results. Throughout this analysis I assumed that the interfering BSs had the same path-loss towards to the UE in consideration. Modifying this assumption to consider different path-loss per BS is left for future work.

Chapter 6

PLS in IoT Networks

6.1 Introduction

This chapter addresses the problem of protecting IoT delay-tolerant uplink data, consisting of users' private information, from eavesdropping. Because of the IoT nature of the network considered here, it is assumed that not every device possesses the necessary power for implementing complex cryptographic protocols such as RSA or other elliptic curves based techniques. The methods considered in this chapter in order to secure IoT networks are based on Physical Layer Security techniques that can be implementing without relying heavily on a device own capabilities. PLS consists in utilising or modifying the properties of the communication channel in order to give an information advantage to the legitimate communication nodes in the network, hence enabling them to perform secure communications. PLS techniques have been around for many years and have been greatly advanced since the work of Wyner [101] in 1975 introducing the degraded wiretap channel and the fundamental notion of secrecy capacity. However, implementing PLS is made more practical today by the development and maturation of technologies such as Full-Duplex communications and phased array antennas. In this chapter the advantages provided by these new technologies will be put into use in securing IoT networks. The work presented in this chapter has been done collaboratively with Dr. Stefano Iellamo at ICS-FORTH Greece. My contribution consists of the section 6.4 and the related simulation results and focuses on cooperative approaches.

6.2 Model and Problem Statement

6.2.1 Network Model

Let us first precise the notations that will be used throughout this chapter.

- The index $i > 1$ will be used when referring to the IoT-devices.
- $k > 1$ will be used when referring to helper nodes.
- $e > 1$ will be used when referring to the eavesdroppers.
- j is a dummy index.
- 0 is always the index of the IoT-GW

The variable x is used to represent a location or a point in the 2D plane and if followed by a subscript it then represents the location of a specific type of device in the network. For example x_i (respectively x_e, x_k and x_0) is the location of an IoT device (respectively an eavesdropper, a helper and the IoT-GW).
Let's also define $\mathcal{B}(x, \rho)$ to be a disk centred at node position x with radius ρ.
We define our network over a disc $\mathcal{B}(x_0, R)$, where x_0 is the location of the IoT-GW and also corresponds to the origin of the 2D plane and R is the radius of the network. The different devices in the network are regrouped into different sets :

- $\mathcal{X} = \{x_i\} \subset \mathcal{B}(0, R)$ denotes the set of IoT devices.
- $\mathcal{E} = \{x_e\} \subset \mathcal{B}(0, 2R)$ denotes the set of eavesdroppers.
- $\mathcal{K} = \{x_k\} \subset \mathcal{B}(0, 2R)$ denotes the set of helpers.

The IoT devices transmit data to the IoT-GW located at x_0 and it is assumed that the IoT-GW features IBFD (In-Band Full Duplex) technology and is therefore able to receive and transmit on the same frequency band.
All operations occur on the same frequency band B_1 centred at f_1 and characterised by background noise power $N_1 = N_0 B_1$. The resulting network is sketched in Fig. 6.1. The sets $\mathcal{E}$, $\mathcal{K}$ and $\mathcal{X}$ are finite with size $\#\mathcal{E}$, $\#\mathcal{K}$ and $\#\mathcal{X}$ respectively and the points they

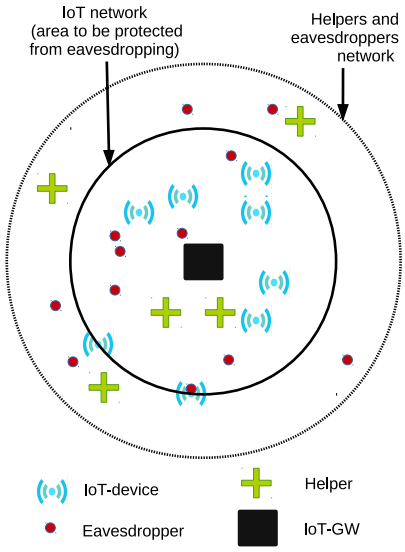


Figure 6.1: Sketch of the considered IoT network.

contain are distributed according to an independent Poisson Point Process (PPP) [102] with intensities λ_E, λ_K and λ_X respectively across a disk of radius R centred at the IoT-GW.

The Euclidean distance between two nodes x and y is denoted by d_{xy} and the channel gain g_{xy} is assumed to be strictly decreasing with the distance d_{xy} and not dependent on the considered nodes.

All nodes are assumed to be static and independant, so there is also no collusion amongst eavesdroppers.

6.2.2 Secure communications

In order for the data transmission from an IoT device i to be securely received at a destination node j in the presence of an eavesdropper e, the signal to interference plus noise ratio (SINR) ie at the eavesdropper's location x_e should be smaller than the SINR experienced at the destination node x_j, i.e., $SINR_{ie} < SINR_{ij}$. In particular, given SINR $ij \geq \gamma_j$ and $SINR_{ie} < \gamma_e$, where $\gamma_e < \gamma_j$ and γ_e can be arbitrarily small,

the secrecy capacity [103, 104] of the communication between i and j at each separate transmission can be determined by:

$$\mathbf{C}_{ij} = \max\{0, \log_2(1 + SINR_{ij}) - \log_2(1 + SINR_{ie})\} \tag{6.1}$$

That is, i and j can achieve secure communication with secrecy rate $\mathbf{R}_{ij} < \mathbf{C}_{ij}$ by agreeing on a code.
Recalling that the eavesdroppers follow a PPP process $\mathcal{E}$, a secure data link can be defined as follows [105]:

Definition 1 (Secure Data Link)**.** *The data link from x_i to x_j is secure if and only if*

$$SINR_{ij} \geq \gamma_j \qquad and \qquad SINR_{ie} < \gamma_e, \qquad \forall e \leq \#\mathcal{E}. \tag{6.2}$$

In our model, the above security conditions are met thanks to *jamming operations* which generate *neutralisation zones*.

Definition 2 (Neutralisation zone)**.** *A neutralisation zone is an area across which conditions* (6.2) *are satisfied, i.e., where no eavesdropper is able to overhear transmissions performed by any IoT device of the network .*

We model the neutralisation zones by disks $\mathcal{B}(x, \rho)$, $x \subset \mathcal{B}(0, 2R), \rho > 0$. The jamming operation are performed by the IBFD IoT-GWs emitting artificial noise (AN) with power P_0 and/or a set of cooperative helpers which are capable of steering their jamming signal away of the IoT-GW (by means of multiple antenna techniques such as beamforming). The IBFD IoT-GW is then able to partially cancel the related self-interference from its in-band receive antenna. We say partially because self-interference cancellation is a complex operation and so far it has only been proven the possibility to cancel up to 110dB [106].

6.2.3 Problem Formulation

We formulate the problem of minimising the IoT-GW transmit power while securing the uplink IoT data in the case of unknown eavesdroppers location. We focus on the

case where all IoT devices transmit with the same power P and all the helpers transmit with the same power Q and set-up the following optimisation problem:

$$\textbf{minimize} \quad P_0 \tag{6.3}$$

$$\textbf{s.t.} \quad SINR_{i0} \geq \gamma_0 \qquad \forall i \leq \#\mathcal{X} \tag{6.4}$$

$$SINR_{ie} < \gamma_E \qquad \forall i \leq \#\mathcal{X}, \forall e \leq \#\mathcal{E} \tag{6.5}$$

$$P_0 \leq P_0^{max} \tag{6.6}$$

where

$$SINR_{i0} = \frac{Pg_{i0}}{N_1 + P_0 h_0}, \tag{6.7}$$

$$SINR_{ie} = \frac{Pg_{ie}}{N_1 + P_0 g_{0e} + \sum_{k \in \mathcal{K}} Q g_{ke}} \tag{6.8}$$

where h_0 denotes the IoT-GW self-interference reduction factor, P_0^{max} denote the maximum power the IoT-GW can use for jamming operations. Note that $\gamma_E = \min_e\{\gamma_e\}$, meaning that no eavesdropper is able to decode messages if the experienced SINR is less than γ_E.

6.3 Jamming from the IoT-GW only

Let us firstly focus on the case where there are no cooperative jamming nodes. This is equivalent to setting $Q = 0$ in (6.8). In this scenario a worst case communication can be defined as follows:

Definition 3 (Worst case communication)**.** *The worst case communication is the one occurring from the farthest IoT-device (from the IoT-GW) when an eavesdropper e^* is co-located with it.*

The following proposition is straightforward.

Proposition 3. *An IoT network is fully secure (i.e., all of its data links are secure) if all IoT-devices transmit at a secrecy rate which is less than the secrecy capacity calculated wrt to the worst case communication.*

From the Proposition, a solution to the optimisation problem (6.3)-(6.6) exists if the IoT-GW can guarantee secure data links to all of its associated IoT-devices. This is possible by generating a neutralisation zone covering the whole IoT network.

Theorem 5. *Assume $g_{xy} = f(d_{xy})$ is a monotone function (strictly decreasing in Euclidean distance d_{xy} and not dependent on the position of x and y). Further, assume i^* is the farthest IoT-device from the IoT-GW and e^* is its co-located eavesdropper. Then:*

1. *The IoT-GW can guarantee a positive secrecy rate to all its associated IoT-devices if*

$$h_0 < \frac{\gamma_E g_{i^*0}(P g_{i^*0} - N_1\gamma_0)}{\gamma_0(P - N_1\gamma_E)} \tag{6.9}$$

2. *When such inequality holds, there exists a solution to the optimisation problem* (6.3)-(6.6). *Such solution is*

$$P_0 = \frac{P - N_1\gamma_E}{g_{i^*0}\gamma_E} + \epsilon \tag{6.10}$$

where ϵ is the smallest power increasing step.

Proof. Recall that the secrecy rate capacity of IoT-device i with respect to the eavesdropper e is $\mathbf{C}_{i0} = \max\{0, \log_2(1 + SINR_{i0}) - \log_2(1 + SINR_{ie})\}$, where

$$SINR_{i0} = \frac{P g_{i0}}{N_1 + P_0 h_0}$$

Assuming reciprocal channel gains (i.e., e.g., $g_{i0} = g_{0i}$) and for the worst case where an eavesdropper e^* is co-located with a transmitting IoT-device i (i.e., $g_{i0} = g_{e^*0} = g_{0e^*}$), $SINR_{ie^*}$ can be written as follows:

$$SINR_{ie^*} = \frac{P}{N_1 + P_0 g_{i0}}$$

According to constraints (6.4) and constraints (6.5) (which reflect conditions (6.2)) an IoT-device experiences positive secrecy rate if $SINR_{i0} \geq \gamma_0$ and $SINR_{ie^*} < \gamma_E$, i.e.,

$$\begin{cases} \frac{P g_{i0}}{N_1 + P_0 h_0} \geq \gamma_0 \\ \frac{P}{N_1 + P_0 g_{i0}} < \gamma_E \end{cases}$$

It is easy to verify that the system of inequalities above is solved for $\frac{P-N_1\gamma_E}{g_{i0}\gamma_E} < P_0 \leq \frac{Pg_{i0}-N_1\gamma_0}{h_0\gamma_0}$.
Thus a finite P_0 exists only if $\frac{Pg_{i0}-N_1\gamma_0}{h_0\gamma_0}$ is strictly greater than $\frac{P-N_1\gamma_E}{g_{i0}\gamma_E}$, which holds for $h_0 < \frac{\gamma_E g_{i0}(Pg_{i0}-N_1\gamma_0)}{\gamma_0(P-N_1\gamma_E)}$ (point 1 of the Theorem). From this one can easily infer that 1) if g(.) is strictly decreasing as a function of the distance d_{xy} between positions x and y, the most stringent condition for h is with respect to the farthest IoT-device i^* from the IoT-GW. Thus, if the inequality holds for such worst case, then it holds for all the IoT devices of the network (point 1 of the Theorem 2) The minimum feasible P_0 is $\frac{P-N_1\gamma_E}{g_{i0}\gamma_E} + \epsilon$, where ϵ is the smallest possible power increasing step (point 2 of the Theorem). □

However, as shown in the numerical section (Section 6.5) fully secure communications even in small areas come at the cost of extremely high IoT-GW AN transmit power. This reduces drastically the business potential of the proposed technique (for instance, it would be unrealistic to install such power-hungry IoT-GW at the users' premises) and motivates us to seek other ways to improve the IoT network secrecy capacity while reducing the IoT-GW power consumption. Thus, we now study the cases with protected surroundings and with helpers.

6.3.1 Protected surroundings

In some scenarios, each legitimate IoT-node may be able to physically inspect its surroundings and deactivate the eavesdroppers falling inside some neutralisation region. With each node, we associate a neutralisation region inside which all eavesdroppers have been deactivated. This can be the case for indoor IoT nodes (e.g., within the smart home walls).

For finite neutralisation regions, we need to define a new worst case communication case:

Definition 4 (Worst case communication with neutralisation areas)**.** *In the presence of finite neutralisation areas around each IoT-device the worst case communication occurs*

when an eavesdropper e^* is located just outside the neutralisation region, on the farthest point from the IoT-GW.

Theorem 6. *Consider a neutralisation region around each IoT-node of minimum radius $d_{x_i x_e^*} - \epsilon$, where ϵ is a very small constant. Assume $g_{xy} = f(d_{xy})$ is a monotone function (strictly decreasing in Euclidean distance d_{xy} and not dependent on the position of x and y). Let i^* be the farthest IoT-device from the IoT-GW and e^* be the eavesdropper located on the farthest point from the IoT-GW which is just outside the neutralisation region. Then,*

1. *the IoT-GW can guarantee a positive secrecy rate to all its associated IoT-devices if*

$$h_0 < \frac{\gamma_E g_{0e^*}(P g_{i^*0} - N_1\gamma_0)}{\gamma_0(P g_{i^*e^*} - N_1\gamma_E)} \tag{6.11}$$

2. *When such inequality holds, there exists a solution to the optimisation problem* (6.3)-(6.6). *Such solution is*

$$P_0 = \frac{P g_{i^*e^*} - N_1\gamma_E}{g_{i^*0}\gamma_E} + \epsilon \tag{6.12}$$

where ϵ is the smallest power increasing step.

We will show in the simulation section how even a neutralisation region of limited size allows to greatly reduce the IoT-GW power consumption.

6.4 Cooperative approaches

A simple and yet powerful strategy for lowering the IoT-GW transmit power while guaranteeing a certain degree of secrecy is cooperative jamming [107]. In cooperative jamming, the IoT-GW artificial noise is complemented by the jamming signal(s) emitted by a set of of friendly jammers or helpers. We propose in the following subsections two cooperative jamming strategies and provide a systematic study of their performance.

6.4.1 Based on the location of eavesdroppers

In this section we consider a cooperative model where the IoT network is populated by helpers which are able to neutralise potential eavesdroppers located within a certain radius. The resulting IoT network is sketched in Fig. 6.2, where the white areas are the neutralisation zones generated by the helpers.
Note that the considered model with neutralisation regions is general enough to include different sorts of physical realisations. For example, the helpers can be radio transceivers able to sense even passive eavesdroppers from their leaked local oscillator power as described in [108] then, using directional antennas they can send a jamming signal towards these eavesdroppers. Using the same model, the neutralisation regions can be viewed as trusted areas where no eavesdropper can be found, for example this could be locations where physical security measures dissuades the eavesdroppers.

In the following, we will rate the level of confidentiality of an IoT network by its Average number of Secure Connections (ASC) to the IoT-GW. However, due to the fact that a practical IoT network is envisioned to comprise thousands of IoT devices, running a Monte Carlo simulation to obtain the ASC can be very daunting and could take days. Therefore, we aim to obtain a closed-form expression of the ASC lower bound as this can indeed provide a powerful tool to analyse IoT networks within shorter terms and limited resources.

Let us recall that helpers, eavesdroppers and IoT devices are PPP distributed with intensities λ_K, λ_E and λ_X respectively. And let us adapt a few definitions from graph theory and from [109] to our case:

Definition 5 (Poisson iS-Graph for IoT networks)**.** *The Poisson intrinsically Secure graph ($i\mathcal{S}-graph$) for IoT networks*[1] *is the directed graph* $G = \{\mathcal{X} \cup \{x_0\}, \mathcal{T}\}$ *with vertex set* $\mathcal{X} \cup \{x_0\}$ *and edge set*

$$\mathcal{T} = \{\overrightarrow{x_i x_0} : \boldsymbol{C}_{i0} > 0\}. \tag{6.13}$$

[1]The $i\mathcal{S}$-graph was defined in [109] in a setting where every node in the network could potentially want to talk to any other node.

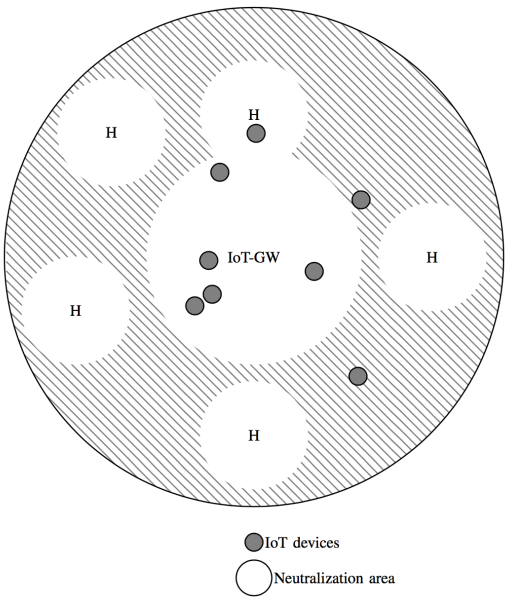


Figure 6.2: Neutralisation region in IoT networks. Note that the eavesdroppers and the helpers can be in an area much larger than the IoT network itself.

Definition 6 (IoT-GW in-degree N_{in})**.** *In the Poisson iS-Graph for IoT networks, the IoT-GW in-degree N_{in} is the number of edges entering the IoT-GW vertex. In other words, it is the average number of secure connections in the IoT network.*

Definition 7 (IoT-GW In-isolation)**.** *In the Poisson iS-Graph for IoT networks, the IoT-GW In-isolation is the probability that the IoT-GW cannot receive from anyone with positive secrecy rate.*

By the definitions above, we want the IoT-GW to be the least In-isolated possible by letting each helper generate a neutralisation zone of finite size.

We approximate the neutralisation zones as in [109] by associating to each helper x_k a neutralisation zone Θ_k inside of which all eavesdroppers will be neutralised. Thus the total neutralisation region Θ is given as

$$\Theta \approx \bigcup_{k=1}^{\#\mathcal{K}} (x_k + \Theta_k) \tag{6.14}$$

The area around the IoT-GW is most sensitive because, the closer an eavesdropper

is to the IoT-GW the higher the probability of In-isolation. Therefore, we assume that the IoT-GW is protected inside a neutralisation region of radius ρ_{IoT}. With this model, no protection for the IoT-GW is equivalent to $\rho_{IoT} = 0$.

Considering generic path losses g_{xy}, we provide a full characterisation of the proposed cooperative model with the following theorem.

Theorem 7. *The average number of secure communication connections in the Poisson iS-Graph for IoT networks is lower bounded by*

$$\mathbb{E}\{N_{in}\} \geq \frac{\lambda_x}{\lambda_e}\left(\pi\lambda_e\bar{\rho}_{IoT}^2 + \frac{1}{p_{\bar{\Theta}}}\left[\exp(-\lambda_e\pi p_{\bar{\Theta}}\bar{\rho}_{IoT}^2) - \exp(-\lambda_e\pi p_{\bar{\Theta}}R^2)\right]\right) \tag{6.15}$$

With $p_{\bar{\Theta}} = e^{-\lambda_k\pi\rho_k^2}$, $\bar{\rho}_{IoT} = \frac{\rho_{IoT}}{2}$ *and* $\bar{\Theta}$ *is the complement of* Θ *in* $\mathcal{B}(0, 2R)$.

Proof. In order for a device (say x) to be able to establish a secure communication link to the IoT-GW there must not be any eavesdropper within a disc of radius d_{xx_0} around the device.
If there is an eavesdropper within $\mathcal{B}(x, d_{xx_0})$ then to keep the link secure that eavesdropper must be neutralised by a helper or by the IoT-GW.
Hence, the set of users able to achieve a secure communication link to the IoT-GW is given as

$$\mathcal{S} = \left\{x \ ; \ x \in \mathcal{X} \text{ and } \overset{\circ}{\mathcal{B}}(x, d_{xx_0}) \cap \bar{\Theta} \cap \mathcal{E} = \emptyset\right\} \tag{6.16}$$

Where $\overset{\circ}{\mathcal{B}}(x, d_{xx_0}) = \mathcal{B}(x, d_{xx_0})/\mathcal{B}(0, \rho_{IoT})$ is the disc centred on x of radius d_{xx_0} without the zone neutralised by the IoT-GW.

We can write the number of secure links from the IoT devices to the IoT-GW as

$$\begin{aligned} N_{in} &= \sum_{x\in\mathcal{X}} \mathbb{1}\{x \in \mathcal{S}\} \\ &= \iint_{\mathcal{B}(0,R)} \mathbb{1}\{x \in \mathcal{S}\}\,\mathcal{X}(dx) \end{aligned}$$

Therefore

$$\mathbb{E}\left\{N_{in}\right\} = \lambda_x \iint_{\mathcal{B}(0,R)} \mathbb{P}_x\left\{x \in \mathcal{S}\right\} dx \tag{6.17}$$

$$= \lambda_x \left(\pi \bar{\rho}_{IoT}^2 + \iint_{\mathcal{D}(\bar{\rho}_{IoT},R)} \mathbb{P}_x\left\{x \in \mathcal{S}\right\} dx\right) \tag{6.18}$$

Where $\mathcal{D}(\bar{\rho}_{IoT}, R)$ is the annulus centred at the origin with inner radius $\bar{\rho}_{IoT}$ and outer radius R with $0 \leq \bar{\rho}_{IoT} \leq R$.
Now let's find the palm probability $\mathbb{P}_x\left\{x \in \mathcal{S}\right\}$

$$\mathbb{P}_x\left\{x \in \mathcal{S}\right\} = \mathbb{P}_{\Theta,\mathcal{K}}\left\{\mathring{\mathcal{B}}\left(x, d_{xx_0}\right) \cap \bar{\Theta} \cap \mathcal{E} = \emptyset\right\} \tag{6.19}$$

$$= \mathbb{E}_{\Theta}\left\{\exp(-\lambda_e \mathbb{A}(\mathring{\mathcal{B}}\left(x, d_{xx_0}\right) \cap \bar{\Theta})\right\} \tag{6.20}$$

$$\geq \exp\left(-\lambda_e \mathbb{E}_{\Theta}\left\{\mathbb{A}(\mathring{\mathcal{B}}\left(x, d_{xx_0}\right) \cap \bar{\Theta})\right\}\right) \tag{6.21}$$

Where (6.21) is obtained using Jensen's inequality, $\mathbb{E}_X$ is the average according to the random variable X, $\mathbb{A}()$ gives the area of a specified random region.

$$\mathbb{E}_{\Theta}\left\{\mathbb{A}(\mathring{\mathcal{B}}\left(x, d_{xx_0}\right) \cap \bar{\Theta})\right\} = \iint_{\mathring{\mathcal{B}}(x,d_{xx_0})} \mathbb{P}\left\{y \in \bar{\Theta}\right\} dy \tag{6.22}$$

$$\leq \iint_{\mathcal{B}(x,d_{xx_0})} \mathbb{P}\left\{y \in \bar{\Theta}\right\} dy \tag{6.23}$$

$$= \pi d_{xx_0}^2 \underbrace{e^{-\lambda_k \pi \rho_k^2}}_{\triangleq p_{\bar{\Theta}}} \tag{6.24}$$

Therefore

$$\mathbb{P}_x\left\{x \in \mathcal{S}\right\} \geq \exp(-\lambda_e \pi p_{\bar{\Theta}} d_{xx_0}^2) \tag{6.25}$$

And finally we can obtain equation (6.15) by plugging this last result back into equation (6.18). □

This result shows how the network parameters are linked to the number of secure connections. Compared to the result shown in [109] our result takes into account the physical size of the network, the presence of helpers, as well as generic channel gains.

6.4.2 Blind Jamming Strategies

We now turn our attention to the case where jamming operations are performed by the IoT-GW in cooperation with a set of helpers in the form of multi-antenna friendly jammers. This could model a 5G LTE small cell network (5G) where each small cell base station additionally operates as an IoT-GW and each served multi-antenna LTE terminal additionally operates as an IoT helper by steering the jamming beam away of the IoT-GW.

In a first approach, we can assume that each eavesdropper is jammed only by the closest helper node to its location. This approximation is realistic in the case where the IoT-devices use the technique Divide-and-Conquer [105] for their data transmission, provided that the messages are encoded across a sufficiently large number of blocks and the helpers are sending jamming signals sporadically. The technique Divide-and-Conquer consists in encoding a secret message into say M different blocks that are all required to recover the original message, then sporadically send a jamming signal at different locations of the network via some helper nodes that are located randomly inside the network. The jamming happens while each of the M blocks are being transmitted, thus increasing the chances that no eavesdropper will get all M blocks error free.

A second approach is to assume that all the eavesdroppers are receiving a jamming signal from all the helpers at the same time. In this scenario also, we consider that the helpers are able to steer their interference away from the IoT-GW.
The performance of the two approaches above will be shown and compared in the numerical section (Section 6.5). A more detailed analysis of this work is left for future work.

6.5 Numerical analysis

For the simulation we consider a NB-IoT network whose IoT devices transmit with constant power $P = 0$dBm across a bandwidth B_1 which is $200kHz$ wide and is centred at $900MHz$. We calculate the channel gains according to $\frac{1}{g_{xy}(d)} = A\log(d) + B + C\log(f_c)$

with $A = 22$, $B = 28$, $C = 20$ (typical urban LOS [110]) and we set in all simulations $\gamma_0 = 6$ and $\gamma_E = 3$.

In this real world scenario, we want to analyse the results presented in the form of Theorem 5 and Theorem 6. In Fig. 6.3 and Fig. 6.4 we show the minimum required IoT-GW performance (in terms respectively of dB to be canceled from the self-interference signal and artificial noise transmit power) needed in order to fully secure a disk area of radius R around the IoT-GW. From the figures it is easy to notice that the case with co-located eavesdropper is very unrealistic in practice as a state-of-the-art self-interference cancellation mechanism and 50 dBm of AN transmit power are required to fully secure a disk area of only 20m radius. On the other hand, by considering even a small neutralisation region it is possible to secure much wider areas with much less resources. For instance a 70m radius area can be fully secured by means of a 70 dB self-interference cancellation mechanism and 36 dBm AN transmit power for the 1m protected surroundings case.

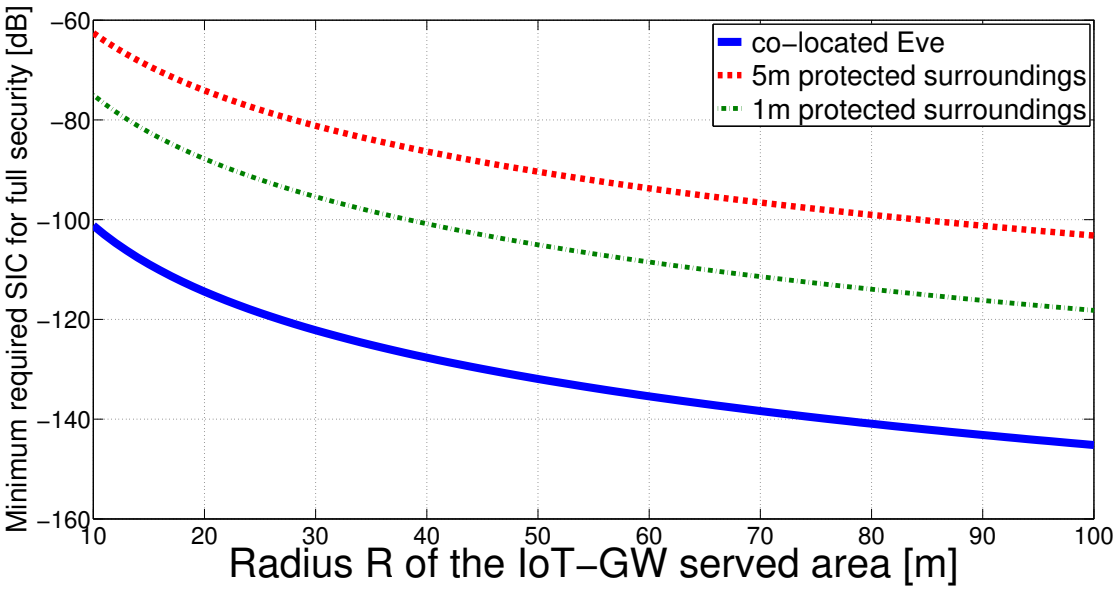


Figure 6.3: Minimum self-interference cancellation (SIC) performance required at the IoT-GW in order to achieve fully secure NB-IoT communications across a disk-shaped area of radius R around the IoT-GW.

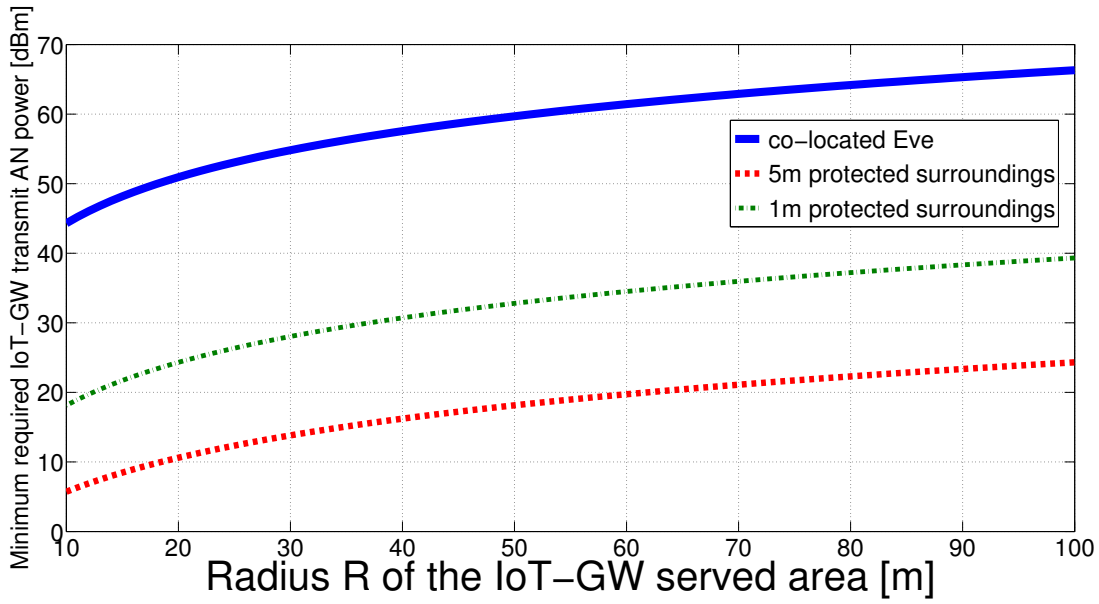


Figure 6.4: Minimum required IoT-GW transmit power performance to achieve fully secure NB-IoT communications across a disk-shaped area of radius R around the IoT-GW.

Fig. 6.5 shows the ASC from the IoT devices to the IoT-GW in percentage of the total number of IoT-devices against the size of the neutralisation regions generated by the helpers. The neutralisation region of the IoT-GW is fixed at $\rho_{IoT} = 0m$ and the network size is $R = 100m$. The Monte Carlo simulation and theoretical curves are shown for $\lambda_x = 0.1$, which corresponds to an average number of 3141 IoT devices. We see that the simulation curves and the lower bounds are very close.

In Fig. 6.6 we show the ASC when the eavesdroppers are jammed by the closest helper only. Three different cases are shown, first, when the IoT-GW is not sending jamming signal in the network we see that with helpers power of -5dBm only 40% of the IoT devices are secured in average. This number grows to almost 60% when the IoT-GW sends a 0dBm jamming signal and 90% when the IoT-GW jamming signal power is 15dBm. However, even without IoT-GW jamming, the helpers are able to secure 90% of the IoT-devices with a power of just 5dBm whereas the IoT-GW would need at least 15dBm to obtain the same results.

In Fig. 6.7 we compare the scenario where an eavesdropper is jammed by its closest helper to the one where the eavesdropper is jammed by all the helpers. The first ob-

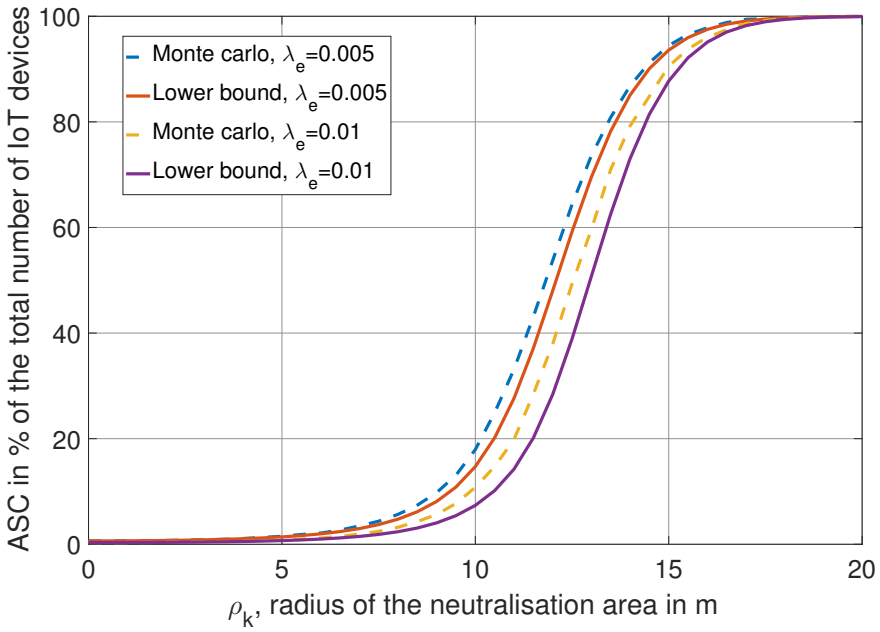


Figure 6.5: Average number of secure connections to the IoT-GW against the size of de neutralisation regions of the helpers. Settings: $\rho_{IoT} = 0m$, $\lambda_x = 0.1$, $\lambda_k = 1.10^{-2}m^{-2}$, $R = 100m$.

vious result is that the performance is higher when all the helpers are considered at the same time. However, the gap between the two scenario is smaller if the helpers are transmitting at higher power, and the aggregate interference created by the network to potential neighbouring networks is much less if only one helper is jamming at one time.

6.6 Conclusion

In this chapter we have studied the confidentiality of the communications flowing from a network of IoT devices to a reference IoT-GW when the position of the potential eavesdropper(s) is unknown with precision. By building on the concepts of jamming by artificial noise (AN) and In band full duplex we have proposed smart jamming strategies aimed at minimising the IoT-GW AN power consumption while guaranteeing a positive secrecy rate across the IoT-GW served region. To study the proposed jamming strategies, we have used the concept of neutralisation regions, which are areas within the IoT

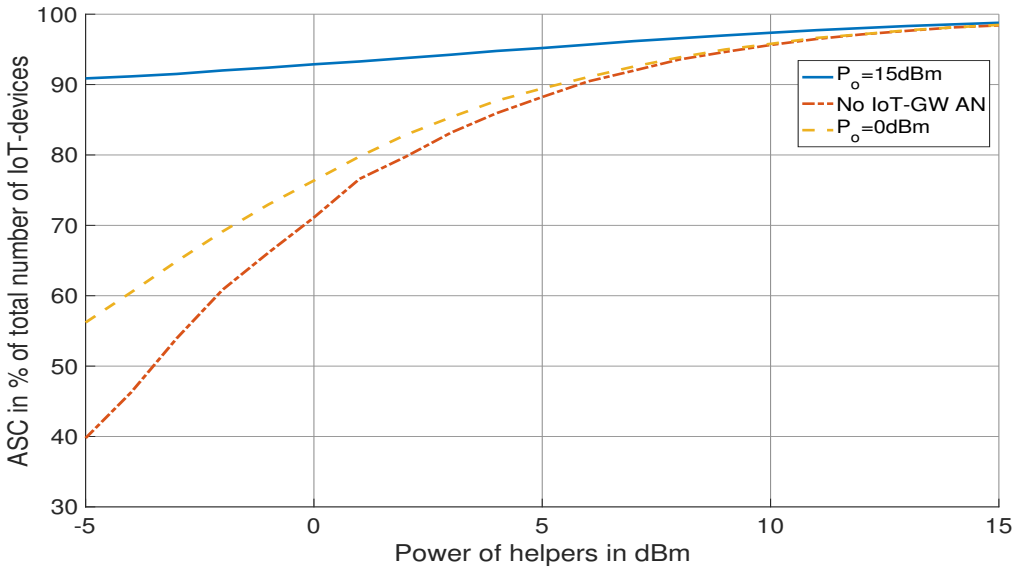


Figure 6.6: Average number of secure connections to the IoT-GW against the transmit power of the helpers and for different transmit AN power at the IoT-GW, settings: $\lambda_x = 0.1$, $\lambda_e = 5.10^{-4}m^{-2}$, $\lambda_k = 5.10^{-4}m^{-2}$, $R = 100m$, $\gamma_E = 3$, $\gamma_0 = 6$, $h_0 = 10^{-10}$.

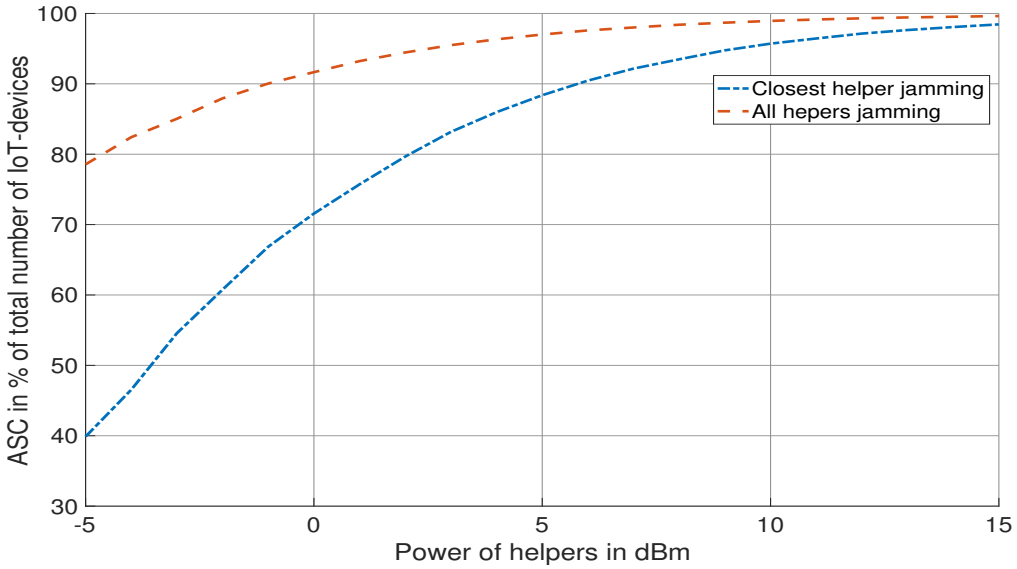


Figure 6.7: Comparison of the ASC against the transmit power of the helpers in the case where only the closest helper AN is considered with the case where all helpers AN are considered, settings: $\lambda_x = 0.1$, $\lambda_e = 5.10^{-4}m^{-2}$, $\lambda_k = 5.10^{-4}m^{-2}$, $R = 100m$, $\gamma_E = 3$, $\gamma_0 = 6$.

network where all eavesdroppers are deactivated (i.e., they are not able to decode information). We have shown that the solution where only the IBFD IoT-GW generates AN is viable in the smart-home use case, i.e., when a neutralisation zone around each IoT-device is assumed. In the case with helpers and punctual jamming instead, we have shown that the Average number of Secure Connections (ASC) increases at least exponentially with the density of the helpers.

A major limitation in the applicability of our results are in the case where multiple networks have to cohabitate on the same frequencies as for example in the unlicensed bands. In this case jamming would disrupt communications for legitimate parties nearby. In networks where the frequencies used are proprietary and/or managed by a central entity -for example one can imagine a sensor network in a sensitive power plant- the full potential of the techniques described here and of our analysis can be applied. More about this issue is mentioned in the future work section.

Chapter 7

Conclusion and future work

7.1 Conclusion

Throughout this work we have focused on analysing the performance of Interference Alignment with imperfect channel knowledge. In comparison to the existing literature, this work is novel because we do not only give some average performance but go further and provide some achievable performance and complete statistical description of the rate of the network.

In Chapter 3 we have studied IA with bounded CSI knowledge, we have seen that we could obtain a lower bound on the capacity achievable in that case, and how this lower bound depends on the number of user in the network the number streams and more importantly on the uncertainty on the CSI. We have defined the saturating SNR and showed that up to that SNR, the real performance of the network is going to be within 1bps/Hz of the lower bound.

The results of chapter 3 are then applied to the case where the channel estimation is done using the Least-square method, we show how the capacity lower bound varies according to different parameters of the estimation method especially the training SNR. We show the variation of the DoF with the parameters.

Chapter 4 gives a statistical description of the rate given that the channel matrices entries are Complex Gaussian random variables, with this statistical description we are able to define a parameter called outage probability and which gives the probability

of not achieving a certain rate with a certain channel uncertainty. Using the outage probability we were also able optimise the number of streams in the network and to extend our analysis to block fading channel and not only constant channels.
Chapter 5 Introduces IA in cellular networks in order to mitigate the inter-cell interference. The main objective is to analyse the performance of users locate at the cell-edge where the desired signal and the interference are received at the mobile user with similar intensities. The base stations locations are modelled after a Poisson point process. Using stochastic geometry and the results developed in the previous chapters, the coverage probability of the networks is derived.
Chapter 6 considers physical layer security in IoT network, smart jamming is utilised to prevent eavesdroppers from listening in on communications and the concept of neutralisation regions is used to study the performance of helpers in securing IoT networks. The work presented throughout this dissertation was published in the ChinaSIP conference in Chengdu China, in Wireless Communications letters, in Transaction on Wireless Communications and in a special issue of the Journal of Communications and Networks.

7.2 Future Work

Different aspects of the work presented in this thesis can be improved. The aim of this section is to point out where these improvements can be made and provide some guidance as to how to approach them and which techniques might be appropriate to use in such and such context.

7.2.1 Coverage probability with IA

The model presented in chapter 5 depicts a scenario where the interference and the desired signal strength at the mobile user are equivalent. While this model provides a good representation of what happens at the cell edge, it is not accurate over the entire network. A better system model would consider heterogeneous path-loss coefficients for every signal received by the mobile user.

Using similar notation as in chapter 5 this means that the received signal at a given user (say o) can be written as

$$\mathbf{y}_o = \sqrt{\ell_d}\mathbf{H}_{o,o}\mathbf{V}_o\mathbf{x}_o + \sum_{s\in\mathcal{S}_o}\sqrt{\ell_s}\mathbf{H}_{o,s}\mathbf{V}_s\mathbf{x}_s + \boldsymbol{\eta}_o, \tag{7.1}$$

Where ℓ_s is the signal attenuation from the interfering BS s to the user o due to the path-loss and shadowing.

In order to adopt the same approach used in chapter 5, the expression of the outage probability needs to be updated. This means that the derivations of chapter 4 must be modified. To do so, one must consider IA with heterogeneous path-loss coefficients [111]. The literature on this topic is very slim and appears indirectly when IA and power allocation are considered together [112–114] in this case there is never an analytical solution to characterise the performance of IA but different forms of iterative algorithms are proposed to design the precoders that optimise the performance of the system. It appears more directly in clustering approaches [115–117] where clusters of users to which to apply IA are defined based on the strength of the interference they generate or receive from their neighbours. This latter case the effects of heterogeneous path-loss matters more for the clustering than for analysis of IA itself. This lack of literature can be explained by the fact that initial developments of IA where focus on the infinite SNR case where the path-loss has no effect on the performance. However this is an important result to get because obviously practical networks operate at finite SNR.

Obtaining the coverage probability of cellular network in a more general setting that that of chapter 5 would allow for a better comparison between the performance of IA and other existing techniques for interference mitigation.

7.2.2 Jamming in the unlicensed spectrum

In chapter 6 the issue of securing IoT networks is raised, the main problem with IoT networks is that they are populated with a wide variety of devices some of which might not have the resources necessary for complex encryption protocols. The solution that was proposed consisted in using jamming to protect vulnerable devices from eavesdroppers.

While this solution can be implemented to successfully reduce the eavesdropper's capabilities to overhear transmission, it is not attractive for application in public networks especially on the unlicensed spectrum. Indeed, jamming the frequencies might be efficient to protect the secrecy of the messages in one subnetwork, However the neighbouring networks might suffer from the same jamming signal.
An interesting result would be to measure the effect of different sort of jamming protocol in the unlicensed spectrum to see how different devices and transmission standards respond. This sort of tests have been done for example in [118]. Note that the jamming strategy can be to sporadically jam some parts of the network for very short period of time using a technique such as divide and conquer [105, 119] leaving enough room for other devices to transmit, therefore it's not obvious that jamming is not a viable option in the unlicensed spectrum. The goal here is then to devise a jamming protocol that is efficient to provide security to one network while leaving the neighbours unaffected.

7.2.3 Securing the backhaul of an IoT network

In order to completely secure IoT networks, one must not only insure that the uplink from the IoT devices is secure but also the downlink and the backhaul link from the gateway to the data processing part of the network. In the following section the focus is on the latter. It's assumed that the backhaul consists of a wireless link to an access point to the cloud that is denoted cloud receiver (C-Rx). It's also assumed that the IoT-GW is equipped with $M \geq 2$ antennas and the C-Rx with $N \geq 2$. Moreover, Maximum Ratio Transmission (MRT) and Maximum Ration Combining (MRC) are used as the transmission and reception strategy for the link. In order to secure this communication link, artificial noise can be transmitted along with the desired signal from the IoT-GW. This idea is not novel and was investigated in 2010 in [120], however, as we will see later there's no complete analysis of the performance of such system especially in the case of imperfect CSI.
With this model, the strategy of the IoT-GW is to transmit the useful signal along the strongest stream available while sending AN along all other weaker streams and because the eavesdropper doesn't know the channel between the IoT-GW and the C-

Rx it cannot remove the AN from the desired signal efficiently.
In the following sections we will consider different scenarios of communication between the IoT network and the C-Rx building gradually towards more and more realistic and perhaps more secure scenarios.

Single IoT-Gateway

In this subsection I assume that the IoT devices transmit their data to a single IoT-Gateway that forwards it to the C-Rx. We'll look at two cases, first let's assume that perfect knowledge of the CSI is available to both IoT-GW and C-Rx and second that only imperfect CSI is available to them. The eavesdropper has no access to that CSI and both the IoT-GW and the C-Rx are unaware of the presence of the eavesdropper.
Case 1 : Perfect CSI.
We denote $\mathbf{H}$ the channel matrix between the IoT-GW and the C-Rx whose entries are iid $\mathcal{CN}(0,1)$ and $\mathbf{x}$ the data vector sent by the IoT-GW so that the received vector $\mathbf{y}$ at the C-Rx writes as

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n}. \tag{7.2}$$

With $\mathbf{n}$ the noise vector with entries iid $\mathcal{CN}(0, \sigma_n^2)$.
The IoT-GW wants to design $\mathbf{x}$ so as to send a useful signal to the C-Rx and at the same time jam eventual eavesdroppers. Therefore it designs three vectors $\mathbf{v}$, $\mathbf{w}$ and $\mathbf{r}$ such that

$$\begin{cases} \mathbf{r}^*\mathbf{H}\mathbf{v} = \lambda_M \\ \mathbf{r}^*\mathbf{H}\mathbf{w} = 0 \\ \|\mathbf{v}\|^2 = 1 \end{cases} \tag{7.3}$$

Where λ_M is the highest eigenvalue of $\mathbf{H}^*\mathbf{H}$.
To fulfil the conditions above it suffices to take for $\mathbf{v}$ the eigen-vector of $\mathbf{H}^*\mathbf{H}$ corresponding to the eigen-value λ_M, $\mathbf{r} = \mathbf{H}\mathbf{v}$ and $\mathbf{w} = \sqrt{\frac{P_S^{AN}}{M-1}}\mathbf{P}\mathbf{f}$, where $\mathbf{P}$ is the matrix containing the eigen-vectors of $\mathbf{H}^*\mathbf{H}$ except $\mathbf{v}$ and $\mathbf{f} \in \mathcal{CN}(\mathbf{0}, \mathbf{I})$. P_S^{AN} is the artificial noise power send by the IoT-GW.
The received signal at the C-Rx can be written as

$$\mathbf{y} = \mathbf{H}(\mathbf{v}s + \mathbf{w}) + \mathbf{n}. \tag{7.4}$$

Where s is the desired signal and $|s|^2 = P_S$ is the signal power.
The estimate of the signal at the C-Rx is given by

$$\hat{s} = \mathbf{r}^*\mathbf{y} = \underbrace{\mathbf{r}^*\mathbf{H}\mathbf{v}s}_{=\lambda_M s} + \underbrace{\mathbf{r}^*\mathbf{H}\mathbf{w}}_{=0} + \mathbf{r}^*\mathbf{n}. \tag{7.5}$$

Therefore the SINR at the C-Rx is given by

$$\gamma_C = \frac{E\left\{|\lambda_M s|^2\right\}}{E\left\{|\mathbf{r}^*\mathbf{n}|^2\right\}} = \frac{E\left\{\lambda_M^2\right\} P_S}{N\sigma_n^2} \tag{7.6}$$

There's one important term that appears here $E\left\{|\lambda_M s|^2\right\}$ that limits the complete characterisation of γ_C, to my knowledge, there is not yet a closed form expression for that term even though its statistical properties have been very well studied as can be seen in [121] and the references therein. Finding an analytical solution to this problem would be a very good contribution in different fields of research from pure mathematics to telecommunications and atomic physics. Luckily, for a given small number of antennas, the value of $E\left\{|\lambda_M s|^2\right\}$ can be approximated very accurately by simple methods such as Monte Carlo simulations. For very large values there are also good analytical approximations [122].
Let's now consider the eavesdropper side. Denote by $\mathbf{H}_e$ the channel matrix between the IoT-GW and the eavesdropper, which is equipped with K antennas. the received signal at the eavesdropper is given by

$$\mathbf{z} = \mathbf{H}_e(\mathbf{v}s + \mathbf{w}) + \mathbf{n}_e. \tag{7.7}$$

Where $\mathbf{n}_e$ is the noise vector at the eavesdropper with entries iid $\mathcal{CN}(0, \sigma_{ne}^2)$.
Because the eavesdropper doesn't know $\mathbf{H}$ the CSI between the IoT-GW and C-Rx it uses equal gain combining to decode the message with the decoder $\mathbf{r}_e^* = \frac{1}{K}[1, 1, ...1]$.

$$\hat{s}_e = \mathbf{r}_e^*\mathbf{H}_e\mathbf{v}s + \mathbf{r}_e^*\mathbf{H}_e\mathbf{w} + \mathbf{r}_e^*\mathbf{n}_e \tag{7.8}$$

Hence, the SINR at the eavesdropper can be expressed as

$$\gamma_E = \frac{E\left\{|\mathbf{r}_e^* \mathbf{H}_e \mathbf{v}|^2\right\} P_S}{E\left\{|\mathbf{r}_e^* \mathbf{H}_e \mathbf{w}|^2\right\} + \sigma_{ne}^2} \tag{7.9}$$

$E\left\{|\mathbf{r}_e^* \mathbf{H}_e \mathbf{v}|^2\right\} = 1$ and $E\left\{|\mathbf{r}_e^* \mathbf{H}_e \mathbf{w}|^2\right\} = P_S^{AN}$ therefore

$$\gamma_E = \frac{P_S}{P_S^{AN} + \sigma_{ne}^2} \tag{7.10}$$

And finally the secrecy capacity is given by

$$C_s = [\log(1 + \gamma_C) - \log(1 + \gamma_E)]^+ \tag{7.11}$$

Where $[\cdot]^+$ means the maximum between 0 and the value in the brackets.
The equations (7.11) and (7.10) together show that increasing the artificial noise power increases the secrecy capacity of the communication link.
Remark : This does not take into account the distance related path-loss or any form of self-interference.
Case 2 : Imperfect CSI
Let's now assume that the channel knowledge is imperfect. That's represented as [123]

$$\mathbf{H} = \rho\hat{\mathbf{H}} + \Delta\mathbf{H} \tag{7.12}$$

With $\rho = \frac{1}{1+\sigma_e^2}$, $\hat{\mathbf{H}}$ is the channel estimate whose entries are i.i.d drawn from $\mathcal{CN}(0, 1 + \sigma_e^2)$, $\Delta\mathbf{H}$ is the error matrix with entries i.i.d drawn from $\mathcal{CN}(0, \frac{\sigma_e^2}{1+\sigma_e^2})$.
In this case the precoding vector $\hat{\mathbf{v}}$ is the eigenvector of $\hat{\mathbf{H}}$ corresponding to the highest eigenvalue $\hat{\lambda}_M$ and the artificial noise vector is $\hat{\mathbf{w}}$. The received vector at the C-Rx is now

$$\mathbf{y} = (\rho\hat{\mathbf{H}} + \Delta\mathbf{H})(\hat{\mathbf{v}}s + \hat{\mathbf{w}}) + \mathbf{n}. \tag{7.13}$$

and the estimated signal

$$\hat{s} = \rho\hat{\lambda}_M s + \hat{r}^* \Delta\mathbf{H}\hat{\mathbf{v}}s + \hat{r}^* \Delta\mathbf{H}\hat{\mathbf{w}} + \hat{\mathbf{r}}^* \mathbf{n}. \tag{7.14}$$

Therefore the SINR at the C-Rx is given as

$$\hat{\gamma}_C = \frac{\rho^2 E\left\{\hat{\lambda}_M^2\right\} P_S}{E\left\{|\hat{r}^* \Delta\mathbf{H}\hat{\mathbf{v}}s|^2\right\} + E\left\{|\hat{r}^* \Delta\mathbf{H}\hat{\mathbf{w}}|^2\right\} + N\sigma_n^2} \tag{7.15}$$

$$= \frac{\rho^2 E\left\{\hat{\lambda}_M^2\right\} P_S}{N(\sigma_e^2 P_S + \frac{1}{M-1} P_S^{AN} \sigma_e^2 + \sigma_n^2)} \tag{7.16}$$

In order to obtain (7.16) the terms representing averaging on the denominator have been simplified. I show below how this is done on one of the terms. Let's show that $E\left\{|\hat{r}^* \Delta\mathbf{H}\hat{\mathbf{w}}|^2\right\} = \frac{N}{M-1} P_S^{AN} \sigma_e^2$.

Proof. First, rewrite the left-hand side term $E\left\{|\hat{r}^* \Delta\mathbf{H}\hat{\mathbf{w}}|^2\right\} = E\left\{\hat{\mathbf{w}}^* \Delta\mathbf{H}^* \hat{r}\hat{r}^* \Delta\mathbf{H}\hat{\mathbf{w}}\right\}$
By construction $E\left\{\hat{r}\hat{r}^*\right\} = (1 + \sigma_e^2)\mathbf{I}_M$
Because $\hat{\mathbf{w}} = \sqrt{\frac{P_S^{AN}}{M-1}}\hat{\mathbf{P}}\mathbf{f}$ with $\|f\| = 1$ and $\hat{\mathbf{P}}$ is a matrix of unitary vectors, $\Delta\mathbf{H}\hat{\mathbf{w}}$ entries are drawn from $\mathcal{CN}(0, \frac{P_S^{AN}}{M-1}\frac{\sigma_e^2}{1+\sigma_e^2})$ that means $E\left\{\hat{\mathbf{w}}^* \Delta\mathbf{H}^* \Delta\mathbf{H}\hat{\mathbf{w}}\right\} = \frac{N\sigma_e^2}{(M-1)(1+\sigma_e^2)} P_S^{AN}$.
Therefore, $E\left\{\hat{\mathbf{w}}^* \Delta\mathbf{H}^* \hat{r}\hat{r}^* \Delta\mathbf{H}\hat{\mathbf{w}}\right\} = \frac{N\sigma_e^2}{M-1} P_S^{AN}$. □

On the eavesdropper side, the expression of the SINR remains the same

$$\gamma_E = \frac{E\left\{|\mathbf{r}_e^* \mathbf{H}_e \hat{\mathbf{v}}|^2\right\} P_S}{E\left\{|\mathbf{r}_e^* \mathbf{H}_e \hat{\mathbf{w}}|^2\right\} + \sigma_{ne}^2} = \frac{P_S}{P_S^{AN} + \sigma_{ne}^2} \tag{7.17}$$

The secrecy capacity in this case is similar with γ_C replaced with $\hat{\gamma}_C$.

$$\hat{C}_s = [\log(1 + \hat{\gamma}_C) - \log(1 + \gamma_E)]^+ \tag{7.18}$$

In this case, the artificial noise decreases the reception quality at the eavesdropper but also at the C-Rx. Equation (7.16) shows how the SINR at the C-Rx is affected by the AN sent by the IoT-GW. We see that the number of transmit and receive antennas count as well as the CSI quality.

Single IoT-GW + C-Rx jamming

In this section I will expand the results developed in the case 2 of the previous section. We are going to consider that the C-Rx helps to increase the secrecy rate by sending artificial noise in the network. Let's also assume that the self-interference cancellation is not perfect at the C-Rx then add the effects of path-loss in the analysis.
Let's denote $\mathbf{H}_{SI}$ the self-interference channel at the C-Rx after imperfect self-interference cancellation it's entries are drawn from $\mathcal{CN}(0, \sigma_{SI}^2)$, $\mathbf{H}_{CE}$ the channel from the C-Rx to the eavesdropper with entries drawn from $\mathcal{CN}(0, 1)$ and P_D^{AN} the artificial noise power sent by the C-Rx.
The received signal at the C-Rx is now

$$\mathbf{y} = (\rho\hat{\mathbf{H}} + \Delta\mathbf{H})(\hat{\mathbf{v}}s + \hat{\mathbf{w}}) + \mathbf{H}_{SI}\mathbf{e} + \mathbf{n}. \tag{7.19}$$

Where $\mathbf{e}$ is the artificial noise vector sent by C-Rx, $\mathbf{e}$ is drawn from $\mathcal{CN}(0, \frac{P_C}{N}\mathbf{I})$.
Following the same derivation as in the previous section, the SINR is given as

$$\hat{\gamma}_{Cs} = \frac{\rho^2 E\left\{\hat{\lambda}_M^2\right\} P_S}{E\left\{|\hat{r}^*\Delta\mathbf{H}\hat{\mathbf{v}}s|^2\right\} + E\left\{|\hat{r}^*\Delta\mathbf{H}\hat{\mathbf{w}}|^2\right\} + E\left\{|\hat{r}^*\mathbf{H}_{SI}\mathbf{e}|^2\right\} + N\sigma_n^2} \tag{7.20}$$

$$= \frac{\rho^2 E\left\{\hat{\lambda}_M^2\right\} P_S}{N(\sigma_e^2 P_S + \frac{1}{M-1}P_S^{AN}\sigma_e^2 + \sigma_n^2) + (1+\sigma_e^2)\sigma_{SI}^2 P_D^{AN}} \tag{7.21}$$

On this new expression for the SINR at the C-Rx we see that quality of the signal at the C-Rx now depends on the performance of the self-interference cancellation technique.
At the eavesdropper side the received signal can be written as

$$\mathbf{z} = \mathbf{H}_e(\mathbf{v}s + \mathbf{w}) + \mathbf{H}_{CE}\mathbf{e} + \mathbf{n}_e. \tag{7.22}$$

In this case the SINR of the eavesdropper is

$$\gamma_E = \frac{E\left\{|\mathbf{r}_e^*\mathbf{H}_e\hat{\mathbf{v}}|^2\right\} P_S}{E\left\{|\mathbf{r}_e^*\mathbf{H}_e\hat{\mathbf{w}}|^2\right\} + E\left\{|\mathbf{r}_e^*\mathbf{H}_{CE}\mathbf{e}|^2\right\} + \sigma_{ne}^2} = \frac{P_S}{P_S^{AN} + P_D^{AN} + \sigma_{ne}^2} \tag{7.23}$$

The C-Rx successfully decreases the reception quality of the eavesdropper. But this is a double edge sword since the AN also affect its own decoding performance.
However, this picture is not complete since in a real system, signal attenuation play an important role. For example if the signal getting to the C-Rx is very weak it is not advisable to transmit AN as the self-interference will probably cover the signal. In the next paragraph, the path-loss is added to form a more complete picture.
With path-loss : The expressions above can be easily modified to take into account the path-loss.
Let's first define the gains on the different links.
g_{De} is the channel gain between the C-Rx and the eavesdropper, g_{Se} is the channel gain between the IoT-GW and the eavesdropper, g_{SD} is the channel gain between the IoT-GW and the C-Rx.
With that the SINR expression of the C-Rx and the eavesdropper can be given as

$$\hat{\gamma}_{Cs} = \frac{\rho^2 E\left\{\hat{\lambda}_M^2\right\} g_{SD} P_S}{N(\sigma_e^2 g_{SD} P_S + \frac{1}{M-1}\sigma_e^2 g_{SD} P_S^{AN} + \sigma_n^2) + (1+\sigma_e^2)\sigma_{SI}^2 P_D^{AN}} \tag{7.24}$$

And

$$\gamma_E = \frac{g_{Se} P_S}{g_{Se} P_S^{AN} + g_{De} P_D^{AN} + \sigma_{ne}^2} \tag{7.25}$$

The parameter $E\left\{\hat{\lambda}_M^2\right\}$ can be approximated numerically once the number of transmit and receive antennas and σ_e are specified.
With the expression of the SINR at the C-Rx and at the eavesdropper, the secrecy capacity of the backhaul link can be analysed for different sets of parameters. An interesting direction would be to find the optimal transmit power for the signal and AN to maximise the secrecy capacity in realistic scenarios.

Bibliography

[1] M. He, C. Ren, Q. Wang, B. Shao, and J. Dong, "The internet of things as an enabler to supply chain innovation," in *2010 IEEE 7th International Conference on E-Business Engineering*, Nov 2010, pp. 326–331.

[2] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787 – 2805, 2010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128610001568

[3] A. Scarf, "Internet of things, the smart x enabler," in *2014 International Conference on Intelligent Networking and Collaborative Systems*, Sept 2014, pp. 569–574.

[4] S. C. Hung, D. Liau, S. Y. Lien, and K. C. Chen, "Low latency communication for internet of things," in *2015 IEEE/CIC International Conference on Communications in China (ICCC)*, Nov 2015, pp. 1–6.

[5] S. S. Prasad and C. Kumar, "An energy efficient and reliable internet of things," in *2012 International Conference on Communication, Information Computing Technology (ICCICT)*, Oct 2012, pp. 1–4.

[6] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the internet of things: A survey of existing protocols and open research issues," *IEEE Communications Surveys Tutorials*, vol. 17, no. 3, pp. 1294–1312, thirdquarter 2015.

[7] K. Zhang, D. Han, and H. Feng, "Research on the complexity in internet of things," in *2010 International Conference on Advanced Intelligence and Awarenss Internet (AIAI 2010)*, Oct 2010, pp. 395–398.

[8] R. Rom and M. Sidi, *Multiple Access Protocols: Performance and Analysis*. New York, NY, USA: Springer-Verlag New York, Inc., 1990.

[9] S. Jafar and S. Shamai, "Degrees of freedom region of the mimo x channel," *Information Theory, IEEE Transactions on*, vol. 54, no. 1, pp. 151–170, Jan 2008.

[10] V. Cadambe and S. Jafar, "Interference alignment and spatial degrees of freedom for the k user interference channel," in *Communications, 2008. ICC '08. IEEE International Conference on*, May 2008, pp. 971–975.

[11] K. Gomadam, V. Cadambe, and S. Jafar, "Approaching the capacity of wireless networks through distributed interference alignment," in *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, Nov 2008, pp. 1–6.

[12] S. Jafar and M. Fakhereddin, "Degrees of freedom for the mimo interference channel," *Information Theory, IEEE Transactions on*, vol. 53, no. 7, pp. 2637–2642, July 2007.

[13] R. Etkin and E. Ordentlich, "The degrees-of-freedom of the k -user gaussian interference channel is discontinuous at rational channel coefficients," *Information Theory, IEEE Transactions on*, vol. 55, no. 11, pp. 4932–4946, Nov 2009.

[14] O. El Ayach, S. Peters, and J. Heath, R.W., "The practical challenges of interference alignment," *Wireless Communications, IEEE*, vol. 20, no. 1, pp. 35–42, February 2013.

[15] S. Jafar, "Topological interference management through index coding," *Information Theory, IEEE Transactions on*, vol. 60, no. 1, pp. 529–568, Jan 2014.

[16] ——, "Blind interference alignment," *Selected Topics in Signal Processing, IEEE Journal of*, vol. 6, no. 3, pp. 216–227, June 2012.

[17] G. Bresler, D. Cartwright, and D. Tse, "Feasibility of interference alignment for the mimo interference channel," *Information Theory, IEEE Transactions on*, vol. 60, no. 9, pp. 5573–5586, Sept 2014.

[18] R. Tresch and M. Guillaud, "Cellular interference alignment with imperfect channel knowledge," in *Communications Workshops, 2009. ICC Workshops 2009. IEEE International Conference on*, June 2009, pp. 1–5.

[19] O. El Ayach, A. Lozano, and R. Heath, "On the overhead of interference alignment: Training, feedback, and cooperation," *Wireless Communications, IEEE Transactions on*, vol. 11, no. 11, pp. 4192–4203, November 2012.

[20] P. Aquilina and T. Ratnarajah, "Performance analysis of ia techniques in the mimo ibc with imperfect csi," *Communications, IEEE Transactions on*, vol. 63, no. 4, pp. 1259–1270, April 2015.

[21] J. H. Lee and W. Choi, "On the achievable dof and user scaling law of opportunistic interference alignment in 3-transmitter mimo interference channels," *Wireless Communications, IEEE Transactions on*, vol. 12, no. 6, pp. 2743–2753, June 2013.

[22] ——, "Interference alignment by opportunistic user selection in 3-user mimo interference channels," in *Communications (ICC), 2011 IEEE International Conference on*, June 2011, pp. 1–5.

[23] O. Gonzalez, C. Beltran, and I. Santamaria, "A feasibility test for linear interference alignment in mimo channels with constant coefficients," *Information Theory, IEEE Transactions on*, vol. 60, no. 3, pp. 1840–1856, March 2014.

[24] G. Bresler, D. Cartwright, and D. Tse, "Feasibility of interference alignment for the mimo interference channel: The symmetric square case," in *Information Theory Workshop (ITW), 2011 IEEE*, Oct 2011, pp. 447–451.

[25] C. Yetis, T. Gou, S. Jafar, and A. Kayran, "On feasibility of interference alignment in mimo interference networks," *Signal Processing, IEEE Transactions on*, vol. 58, no. 9, pp. 4771–4782, Sept 2010.

[26] S. Jacobs, "Optimizing cryptographically based security in wireless networks," in *2015 International Conference on Information Systems Security and Privacy (ICISSP)*, Feb 2015, pp. 39–45.

[27] J. Goodman and A. P. Chandrakasan, "An energy-efficient reconfigurable public-key cryptography processor," *IEEE Journal of Solid-State Circuits*, vol. 36, no. 11, pp. 1808–1820, Nov 2001.

[28] K. Somsuk, "The improving decryption process of rsa by choosing new private key," in *2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE)*, Oct 2016, pp. 1–4.

[29] N. M. S. Iswari, "Key generation algorithm design combination of rsa and elgamal algorithm," in *2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE)*, Oct 2016, pp. 1–5.

[30] K. Lauter, "The advantages of elliptic curve cryptography for wireless security," *IEEE Wireless Communications*, vol. 11, no. 1, pp. 62–67, Feb 2004.

[31] M. Amara and A. Siad, "Elliptic curve cryptography and its applications," in *International Workshop on Systems, Signal Processing and their Applications, WOSSPA*, May 2011, pp. 247–250.

[32] M. A. S. Eldeen, A. A. Elkouny, and S. Elramly, "Des algorithm security fortification using elliptic curve cryptography," in *2015 Tenth International Conference on Computer Engineering Systems (ICCES)*, Dec 2015, pp. 335–340.

[33] S. R. Singh, A. K. Khan, and T. S. Singh, "A critical review on elliptic curve cryptography," in *2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT)*, Sept 2016, pp. 13–18.

[34] J. Wu, I. Detchenkov, and Y. Cao, "A study on the power consumption of using cryptography algorithms in mobile devices," in *2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, Aug 2016, pp. 957–959.

[35] J. M. Liang, J. J. Chen, H. H. Cheng, and Y. C. Tseng, "An energy-efficient sleep scheduling with qos consideration in 3gpp lte-advanced networks for internet of things," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 3, no. 1, pp. 13–22, March 2013.

[36] Ericsson, "Lte release 13, white paper," *Online*, 2015.

[37] N. Namvar, W. Saad, N. Bahadori, and B. Kelley, "Jamming in the internet of things: A game-theoretic perspective," in *2016 IEEE Global Communications Conference (GLOBECOM)*, Dec 2016, pp. 1–6.

[38] A. Mukherjee, "Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1747–1761, Oct 2015.

[39] C. Shannon, "A mathematical theory of communication," *Bell System Technical Journal, The*, vol. 27, no. 3, pp. 379–423, July 1948.

[40] H. Sato, "The capacity of the gaussian interference channel under strong interference (corresp.)," *Information Theory, IEEE Transactions on*, vol. 27, no. 6, pp. 786–788, Nov 1981.

[41] A. Carleial, "A case where interference does not reduce capacity (corresp.)," *IEEE Transactions on Information Theory*, vol. 21, no. 5, pp. 569–570, Sep 1975.

[42] M. Costa and A. E. Gamal, "The capacity region of the discrete memoryless interference channel with strong interference (corresp.)," *IEEE Transactions on Information Theory*, vol. 33, no. 5, pp. 710–711, Sep 1987.

[43] T. Han and K. Kobayashi, "A new achievable rate region for the interference channel," *IEEE Transactions on Information Theory*, vol. 27, no. 1, pp. 49–60, Jan 1981.

[44] T. Cover, "Broadcast channels," *Information Theory, IEEE Transactions on*, vol. 18, no. 1, pp. 2–14, Jan 1972.

[45] P. Bergmans, "Random coding theorem for broadcast channels with degraded components," *IEEE Transactions on Information Theory*, vol. 19, no. 2, pp. 197–207, Mar 1973.

[46] ——, "A simple converse for broadcast channels with additive white gaussian noise (corresp.)," *IEEE Transactions on Information Theory*, vol. 20, no. 2, pp. 279–280, Mar 1974.

[47] C. Nair and A. E. Gamal, "An outer bound to the capacity region of the broadcast channel," in *2006 IEEE International Symposium on Information Theory*, July 2006, pp. 2205–2209.

[48] C. Nair, "Capacity regions of two new classes of two-receiver broadcast channels," *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4207–4214, Sept 2010.

[49] A. Motahari and A. Khandani, "To decode the interference or to consider it as noise," *Information Theory, IEEE Transactions on*, vol. 57, no. 3, pp. 1274–1283, March 2011.

[50] M. Ebrahimi, M. A. Maddah-Ali, and A. K. Khandani, "Throughput scaling laws for wireless networks with fading channels," *IEEE Transactions on Information Theory*, vol. 53, no. 11, pp. 4250–4254, Nov 2007.

[51] R. Etkin, A. Parekh, and D. Tse, "Spectrum sharing for unlicensed bands," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 3, pp. 517–528, April 2007.

[52] P. Jung and P. Baier, "Cdma and spread spectrum techniques versus fdma and tdma in cellular mobile radio applications," in *Microwave Conference, 1991. 21st European*, vol. 1, Sept 1991, pp. 404–409.

[53] M. Costa, "Writing on dirty paper (corresp.)," *Information Theory, IEEE Transactions on*, vol. 29, no. 3, pp. 439–441, May 1983.

[54] M. Maddah-Ali, A. Motahari, and A. Khandani, "Communication over mimo x channels: Interference alignment, decomposition, and performance analysis," *Information Theory, IEEE Transactions on*, vol. 54, no. 8, pp. 3457–3470, Aug 2008.

[55] R. Tresch, M. Guillaud, and E. Riegler, "On the achievability of interference alignment in the k-user constant mimo interference channel," in *Statistical Signal Processing, 2009. SSP '09. IEEE/SP 15th Workshop on*, Aug 2009, pp. 277–280.

[56] P. Mohapatra, K. E. Nissar, and C. R. Murthy, "Interference alignment algorithms for the k user constant mimo interference channel," *IEEE Transactions on Signal Processing*, vol. 59, no. 11, pp. 5499–5508, Nov 2011.

[57] G. Bresler, D. Cartwright, and D. Tse, "Interference alignment for the mimo interference channel," *CoRR*, vol. abs/1303.5678, 2013.

[58] S. Peters and R. Heath, "Interference alignment via alternating minimization," in *Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on*, April 2009, pp. 2445–2448.

[59] G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," *Transactions of the American Institute of Electrical Engineers*, vol. XLV, pp. 295–301, Jan 1926.

[60] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct 1949.

[61] M. Hellman, "An extension of the shannon theory approach to cryptography," *IEEE Transactions on Information Theory*, vol. 23, no. 3, pp. 289–294, May 1977.

[62] P. R. Geffe, "Secrecy systems approximating perfect and ideal secrecy," *Proceedings of the IEEE*, vol. 53, no. 9, pp. 1229–1230, Sept 1965.

[63] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct 1975.

[64] A. Carleial and M. Hellman, "A note on wyner's wiretap channel (corresp.)," *IEEE Transactions on Information Theory*, vol. 23, no. 3, pp. 387–390, May 1977.

[65] S. Leung-Yan-Cheong and M. Hellman, "The gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, Jul 1978.

[66] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[67] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. i. secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, Jul 1993.

[68] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Transactions on Communications*, vol. 43, no. 1, pp. 3–6, Jan 1995.

[69] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *IEEE Transactions on Mobile Computing*, vol. 12, no. 5, pp. 917–930, May 2013.

[70] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *2013 Proceedings IEEE INFOCOM*, April 2013, pp. 3048–3056.

[71] F. Graziosi and F. Santucci, "A general correlation model for shadow fading in mobile radio systems," *IEEE Communications Letters*, vol. 6, no. 3, pp. 102–104, March 2002.

[72] S. T. B. Hamida, J. B. Pierrot, B. Denis, C. Castelluccia, and B. Uguen, "On the security of uwb secret key generation methods against deterministic channel prediction attacks," in *2012 IEEE Vehicular Technology Conference (VTC Fall)*, Sept 2012, pp. 1–5.

[73] A. Mahmood and M. A. Jensen, "Assessing and removing the impact of non-reciprocal transceiver circuitry for channel-based key establishment," in *2015 9th European Conference on Antennas and Propagation (EuCAP)*, May 2015, pp. 1–4.

[74] Y. Han, J. Ni, and G. Du, "The potential approaches to achieve channel reciprocity in fdd system with frequency correction algorithms," in *2010 5th International ICST Conference on Communications and Networking in China*, Aug 2010, pp. 1–5.

[75] R. Negi and S. Goel, "Secret communication using artificial noise," in *VTC-2005-Fall. 2005 IEEE 62nd Vehicular Technology Conference, 2005.*, vol. 3, Sept 2005, pp. 1906–1910.

[76] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[77] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in mimo wiretap channels with imperfect csi," *IEEE Transactions on Signal Processing*, vol. 59, no. 1, pp. 351–361, Jan 2011.

[78] J. Li and A. P. Petropulu, "Optimality of beamforming for secrecy capacity of mimo wiretap channels," in *2012 IEEE International Workshop on Information Forensics and Security (WIFS)*, Dec 2012, pp. 276–281.

[79] N. Valliappan, R. W. Heath, and A. Lozano, "Antenna subset modulation for secure millimeter-wave wireless communication," in *2013 IEEE Globecom Workshops (GC Wkshps)*, Dec 2013, pp. 1258–1263.

[80] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas part i: The misome wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3088–3104, July 2010.

[81] ——, "Secure transmission with multiple antennas part ii: The mimome wiretap channel," *IEEE Transactions on Information Theory*, vol. 56, no. 11, pp. 5515–5532, Nov 2010.

[82] Q. Li and W. K. Ma, "Spatially selective artificial-noise aided transmit optimization for miso multi-eves secrecy rate maximization," *IEEE Transactions on Signal Processing*, vol. 61, no. 10, pp. 2704–2717, May 2013.

[83] P. H. Lin, S. H. Lai, S. C. Lin, and H. J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1728–1740, September 2013.

[84] Z. Wang, M. Xiao, M. Skoglund, and H. V. Poor, "Secure degrees of freedom of wireless x networks using artificial noise alignment," *IEEE Transactions on Communications*, vol. 63, no. 7, pp. 2632–2646, July 2015.

[85] A. Khisti and D. Zhang, "Artificial-noise alignment for secure multicast using multiple antennas," *IEEE Communications Letters*, vol. 17, no. 8, pp. 1568–1571, August 2013.

[86] N. Zhao, F. R. Yu, M. Li, and V. C. M. Leung, "Secure transmission in interference alignment (ia)-based networks with artificial noise," in *2016 IEEE 83rd Vehicular Technology Conference (VTC Spring)*, May 2016, pp. 1–5.

[87] S. A. A. Fakoorian, H. Jafarkhani, and A. L. Swindlehurst, "Secure space-time block coding via artificial noise alignment," in *2011 Conference Record of the Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, Nov 2011, pp. 651–655.

[88] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 16, no. 3, pp. 1550–1573, Third 2014.

[89] B. Nosrat-Makouei, J. Andrews, and R. Heath, "Mimo interference alignment over correlated channels with imperfect csi," *Signal Processing, IEEE Transactions on*, vol. 59, no. 6, pp. 2783–2794, June 2011.

[90] O. Ayach and R. Heath, "Interference alignment with analog channel state feedback," *Wireless Communications, IEEE Transactions on*, vol. 11, no. 2, pp. 626–636, February 2012.

[91] M. Biguesh and A. Gershman, "Training-based mimo channel estimation: a study of estimator tradeoffs and optimal training signals," *Signal Processing, IEEE Transactions on*, vol. 54, no. 3, pp. 884–893, March 2006.

[92] G. Zheng, K.-K. Wong, and B. Ottersten, "Robust cognitive beamforming with bounded channel uncertainties," *Signal Processing, IEEE Transactions on*, vol. 57, no. 12, pp. 4871–4881, Dec 2009.

[93] S. Razavi and T. Ratnarajah, "Asymptotic performance analysis of interference alignment under imperfect csi," in *Wireless Communications and Networking Conference (WCNC), 2014 IEEE*, April 2014, pp. 532–537.

[94] H. Shen, B. Li, Y. Luo, and F. Liu, "A robust interference alignment scheme for the mimo x channel," in *Communications, 2009. APCC 2009. 15th Asia-Pacific Conference on*, Oct 2009, pp. 241–244.

[95] S. Peters and R. Heath, "Cooperative algorithms for mimo interference channels," *Vehicular Technology, IEEE Transactions on*, vol. 60, no. 1, pp. 206–218, Jan 2011.

[96] K. Gomadam, V. Cadambe, and S. Jafar, "A distributed numerical approach to interference alignment and applications to wireless interference networks," *Information Theory, IEEE Transactions on*, vol. 57, no. 6, pp. 3309–3322, June 2011.

[97] M. Koutras, "On the generalized noncentral chi-squared distribution induced by an elliptical gamma law," *Biometrika*, vol. 73, no. 2, pp. pp. 528–532, 1986. [Online]. Available: http://www.jstor.org/stable/2336235

[98] C. Suh and D. Tse, "Interference alignment for cellular networks," in *Communication, Control, and Computing, 2008 46th Annual Allerton Conference on*, Sept 2008, pp. 1037–1044.

[99] B. Zhuang, R. A. Berry, and M. L. Honig, "Interference alignment in MIMO cellular networks," in *2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, May 2011, pp. 3356–3359.

[100] J. G. Andrews, F. Baccelli, and R. K. Ganti, "A tractable approach to coverage and rate in cellular networks," *IEEE Transactions on Communications*, vol. 59, no. 11, pp. 3122–3134, November 2011.

[101] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[102] S. N. Chiu, D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic Geometry and Its Applications*. John Wiley & Sons, Jun. 2013.

[103] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[104] F. Oggier and B. Hassibi, "The Secrecy Capacity of the MIMO Wiretap Channel," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[105] Z. Liu, J. Liu, N. Kato, J. Ma, and Q. Huang, "Divide-and-conquer based cooperative jamming: Addressing multiple eavesdroppers in close proximity," in *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications*, Apr. 2016, pp. 1–9.

[106] D. Kim, H. Lee, and D. Hong, "A Survey of In-Band Full-Duplex Transmission: From the Perspective of PHY and MAC Layers," *IEEE Communications Surveys Tutorials*, vol. 17, no. 4, pp. 2017–2046, 2015.

[107] M. Atallah, G. Kaddoum, and L. Kong, "A Survey on Cooperative Jamming Applied to Physical Layer Security," in *2015 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB)*, Oct. 2015, pp. 1–5.

[108] A. Mukherjee and A. L. Swindlehurst, "Detecting passive eavesdroppers in the MIMO wiretap channel," in *2012 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Mar. 2012, pp. 2809–2812.

[109] P. C. Pinto, J. Barros, and M. Z. Win, "Secure Communication in Stochastic Wireless Networks #x2014;Part I: Connectivity," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 125–138, Feb. 2012.

[110] r. G. P. Project, "3gpp 36tr 36 .814 V 9.0.0 (20 10 - 03)," 3GPP, Tech. Rep., 2010. [Online]. Available: http://www.qtc.jp/3GPP/Specs/36814-900.pdf

[111] X. Rao, L. Ruan, and V. K. N. Lau, "Limited feedback design for interference alignment on mimo interference networks with heterogeneous path loss and spatial correlations," *IEEE Transactions on Signal Processing*, vol. 61, no. 10, pp. 2598–2607, May 2013.

[112] F. H. Panahi, T. Ohtsuki, W. Jiang, Y. Takatori, and K. Uehara, "Interference alignment and power allocation for multi-user mimo interference channels," in *2016 IEEE International Conference on Communications (ICC)*, May 2016, pp. 1–7.

[113] F. H. Panahi, T. Ohtsuki, W. Jiang, Y. Takatori, and T. Nakagawa, "Joint interference alignment and power allocation for multi-user mimo interference channels under perfect and imperfect csi," *IEEE Transactions on Green Communications and Networking*, vol. PP, no. 99, pp. 1–1, 2017.

[114] F. Shu, X. You, M. Wang, Y. Han, Y. Li, and W. Sheng, "Hybrid interference alignment and power allocation for multi-user interference mimo channels," *Science China Information Sciences*, vol. 56, no. 4, pp. 1–9, 2013. [Online]. Available: http://dx.doi.org/10.1007/s11432-012-4549-z

[115] S. Chen and R. S. Cheng, "Clustering for interference alignment in a multiuser interference channel," in *2012 IEEE 75th Vehicular Technology Conference (VTC Spring)*, May 2012, pp. 1–5.

[116] R. Tresch and M. Guillaud, "Clustered interference alignment in large cellular networks," in *2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications*, Sept 2009, pp. 1024–1028.

[117] R. Seno, T. Ohtsuki, W. Jiang, and Y. Takatori, "Interference alignment in heterogeneous networks using pico cell clustering," in *2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall)*, Sept 2015, pp. 1–5.

[118] I. Harjula, J. Pinola, and J. Prokkola, "Performance of ieee 802.11 based wlan devices under various jamming signals," in *2011 - MILCOM 2011 Military Communications Conference*, Nov 2011, pp. 2129–2135.

[119] A. Sheikholeslami, M. Ghaderi, H. Pishro-Nik, and D. Goeckel, "Energy-efficient secrecy in wireless networks based on random jamming," *IEEE Transactions on Communications*, vol. PP, no. 99, pp. 1–1, 2017.

[120] S. Ma, M. Hempel, Y. Yang, and H. Sharif, "A new approach to null space-based noise signal generation for secure wireless communications in transmit-receive diversity systems," in *2010 IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS)*, Jun. 2010, pp. 406–410.

[121] M. Kang and M. S. Alouini, "Largest eigenvalue of complex wishart matrices and performance analysis of mimo mrc systems," *IEEE Journal on Selected Areas in Communications*, vol. 21, no. 3, pp. 418–426, Apr 2003.

[122] G. Akemann, J. Baik, and P. Di Francesco, *The Oxford handbook of random matrix theory.* Oxford; New York: Oxford University Press, 2011.

[123] Y. Chen and C. Tellambura, "Performance analysis of maximum ratio transmission with imperfect channel estimation," *IEEE Communications Letters*, vol. 9, no. 4, pp. 322–324, April 2005.