Spontaneous and Self-Organizing Networks: from Space-Time Coding to Network Coding

Ali Osmane

ParisTech
INSTITUT DES SCIENCES ET TECHNOLOGIES
PARIS INSTITUT OF TECHNOLOGY

TELECOM ParisTech

Doctorat ParisTech

T H È S E

pour obtenir le grade de docteur délivré par

Télécom ParisTech

Spécialité " Communications et Électronique "

présentée et soutenue publiquement par

ALi OSMANE

le 7 décembre 2011

Réseaux Spontanés et Auto-Organisants: du Codage Spatio-Temporel au Codage de Réseaux

Directeur de thèse : **Jean-Claude Belfiore**

Jury

M. Ezio BIGLIERI, Professeur, Universitat Pompeu Fabra	Président
M. Mérouane DEBBAH, Professeur, Supélec	Rapporteur
M. Jean-Marie GORCE, Professeur, INSA - Lyon	Rapporteur
M. Cong LING, Maître de conférence, Imperial College	Examinateur
M. Sheng YANG, Maître de conférence, Supélec	Examinateur
M. Jean-Claude BELFIORE, Professeur, Télécom ParisTech	Directeur de thèse

T H È S E

Télécom ParisTech
Grande école de l'Institut Télécom – membre fondateur de ParisTech
46, rue Barrault – 75634 Paris Cedex 13 – Tél. + 33 (0)1 45 81 77 77 – www.telecom-paristech.fr

To my family and Laurie

Acknowledgements

I would like to start by thanking Prof. Jean-Claude Belfiore for giving me the opportunity to do a PhD under his supervision. His suggestions and fruitful ideas provided me exciting topics to work on, and guided me along the three years of my research work.

I am very grateful to Dr. Sheng Yang for his supervision at the beginning of my PhD, and for the many discussions we have had. Special thanks go to Dr. Lina Mroueh for our valuable discussions on topics that go beyond the PhD context but are essential to better understand the communication systems.

Many thanks go to all the members of the Communications and Electronics Department at Telecom ParisTech, and to the administrative staff for their kindness and assistance. A thought goes also to all my friends in and outside Telecom ParisTech.

I want to express my deep gratitude to my parents, Mohamad and Maha Osmane, for their unconditional love, their prayers, their advices and unlimited support. They worked hard to guarantee for me and my sisters, a better future despite all the difficulties. They give me the motivation and the strength to advance in life. I owe the person I am to them. I also express my gratitude for my sisters for their understanding and endless support. Finally, I would like to mention the one person who becomes during this PhD, a part of me - Laurie Marrauld, for her daily love, patience and support.

Abstract

WIRELESS communication systems are limited in data rate and reliability. In order to overcome this limitation, two fundamentals aspects of the wireless communication channel are often considered. The first aspect is the signal attenuation that is described by three phenomena: channel fading, shadowing and path loss. The second aspect is related to the interference problem resulting from the fact that the transmitter-receiver pairs share the same communication medium.

With the rapid development of the web 2.0 and the wireless personal devices, the demand for wireless access increases rapidly. In the Third-Generation (and beyond) of wireless communication systems, advanced algorithms and techniques are employed to increase both reliability and spectral efficiency. Among these techniques, diversity is of major importance due to its connection to the physical nature of the wireless environment.

In this scope, cooperative diversity techniques are attractive candidates for improving the throughput and reliability of wireless networks. The idea behind the cooperative systems is to emulate the Multiple-Input Multiple-Output (MIMO) systems to take benefits from the spatial diversity.

In the first part of this thesis, we study the two-hop MIMO relay networks without a direct source-destination link. In particular, we are interested in the rotate-and-forward (RF) relaying protocol proposed by Yang and Belfiore in [1]. We consider different network configurations and we study the performance of the RF in terms of a new metric called outage gain and defined in [2]. This gain gives us an exact characterization of the outage probability's behavior at moderate and high signal-to-noise ratio (SNR). Using this metric, we compare the performance of the RF scheme to the performance of other schemes considered in literature and having the same diversity order. Finally, we assume that a feedback channel exists between the destination and the relays, and we use the channel knowledge to improve the performance of the RF scheme in terms of outage probability.

On another hand, the physical layer network coding (PLNC) presents an alternative way to deal with interference in wireless communication systems. While interference is commonly seen as nuisance, PLNC uses interference in order to increase the transmission rates between the users in the network. More precisely, the users help to relay each other's messages by exploiting the broadcast and multiple-access properties of the wireless medium.

Motivated by this issue, Bobak and Gastpar have proposed a new PLNC relaying strategy known as compute-and-forward (CF) protocol [3]. In summary, the CF relays decode linear functions of transmitted messages rather than ignoring the interference as noise. Once these linear functions are decoded, the relays send them to the next relays or destination. This later, given enough equations, can recover the original messages. In order to insure that integer combinations of codewords remain in the set of codewords, the CF messages are coded using structured codes, particularly nested lattice codes.

In the second part of the thesis, we analyze the practical aspects of the compute-and-forward scheme as proposed by Nazer and Gastpar. We first implement this protocol for real Gaussian channels and one-dimensional lattices. Then, we consider the transmission rate maximization problem and we relate it to the lattice shortest vector problem. We derive the maximum likelihood (ML) criterion and we propose a quasi-ML decoding technique and show that it can be implemented by using an Inhomogeneous Diophantine Approximation algorithm. Finally, we generalize some of these results to the complex Gaussian multi-dimensional lattices, and introduce the flatness factor as a design criterion for lattice codes.

Résumé de la Thèse

LES SYSTÈMES de communication sans fil sont connus pour avoir une fiabilité variable et un débit limité. Afin de surmonter ces limites, deux aspects fondamentaux du canal de communication sans fil sont souvent pris en compte. Le premier est l'atténuation du signal qui est décrit par trois phénomènes : l'évanouissement, l'effet de masque et l'atténuation du canal. Le second aspect est lié au probème d'interférence résultant du fait que les paires de transmetteur-receveur partagent le même canal de communication.
Avec le développement rapide du web 2.0 et des outils personnels de communication sans fil, la demande d'accès au sans fil augmente considérablement. Dans les systèmes de communication sans fil de troisième génération (et au-delà), des algorithmes et des techniques avancés sont utilisés pour améliorer à la fois la fiabilité et l'efficacité spectrale. Parmi ces techniques, la diversité est d'une importance majeure en raison de son lien à la nature physique de l'environnement sans fil.
Dans ce cadre, les techniques de diversité coopérative sont des candidats attractifs pour l'amélioration du débit et de la fiabilité des réseaux sans fil. Les systèmes coopératifs sont une imitation des systèmes à plusieurs entrées et plusieurs sorties (MIMO), et ceci pour profiter de la diversité spaciale.

Dans la première partie de cette thèse, nous étudions les réseaux MIMO à deux sauts. Dans ces réseaux, la source et la destination ne communiquent pas via un lien direct mais à travers une couche de relais. Nous nous intéressons en particulier au protocole rotate-and-forward (RF) proposé par Yang et Belfiore dans [1]. Nous considérons des configurations différentes de réseaux et nous étudions la performance du protocole RF à partir d'une nouvelle métrique appelée gain de coupure et définie dans [2]. Ce gain nous permet de décrire le comportement de la probabilité de coupure à des valeurs du rapport signal à bruit (SNR) moyennes et élevées. En utilisant le gain de coupure, nous comparons la performance du RF aux performances d'autres protocoles définis dans la littérature et ayant le même ordre de diversité que le RF. Nous supposons aussi qu'une voie de retour existe entre la destination et les relais et nous donnons un algorithme qui permet d'améliorer les performances du RF en termes de probabilité de coupure en se basant sur la connaissance des gains du canal.

D'autre part, le codage de réseaux au niveau physique (PLNC) représente une autre vision pour le traitement de l'interférence dans les systèmes de communications sans fil. Bien

qu'elle soit communément considérée comme une nuisance, le PLNC utilise l'interférence pour augmenter les débits de transmission entre les utilisateurs d'un réseau. Plus précisément, tout utilisateur relaie les messages des autres utilisateurs en exploitant les caractéristiques de diffusion et d'accès-multiple du canal sans fil.
Se fondant sur ce principe, Bobak et Gastpar ont proposé un nouveau protocole PLNC appelé compute-and-forward (CF) dans [3]. En quelques mots, un relai décode une fonction linéaire entière de tous les messages transmis au lieu de les ignorer et les considérer comme du bruit. Une fois décodée, le relai envoie cette fonction linéaire à un autre relai ou à la destination. Cette dernière, ayant reçu plusieurs équations, peut récupérer les messages d'origine. Les auteurs du CF proposent de coder les messages avec des codes en réseaux de points pour s'assurer que toute combinaison entière de deux mots de code est aussi un mot de code en réseaux de points.

Dans la deuxième partie de la thèse, nous analysons les aspects pratiquent du protocole compute-and-forward. Nous nous intéressons à la maximisation du débit de calcul et nous montrons que le problème est équivalent à la recherche du vecteur le plus court dans un réseau de points bien déterminé. Dans une première étape, nous implémentons le protocole utilisant des réseaux de points uni-dimensionnels et des gains de canal réels. Nous nous basons sur la fonction de maximum de vraisemblance (ML) pour proposer une technique de décodage quasi-ML et nous montrons que le décodage s'effectue par une approximation Diophantienne inhomogène. Dans une deuxième étape, nous généralisons certains de ces résultats au cas des réseaux de points multi-dimensionnels et des gains de canal complexes, et nous proposons un critère de construction des codes en réseaux de points qu'on appelle le facteur de platitude.

Contents

List of Figures

Résumé Détaillé de la Thèse

Dans le premier chapitre de cette synthèse détaillée, nous introduisons la communication coopérative et les principales métriques de mesure utilisées pour étudier la performance des systèmes coopératifs. Dans le deuxième chapitre, nous étudions les performances du protocole rotate-and-forward dans les réseaux à deux-sauts. Nous présentons, dans le troisième chapitre, le principe du codage de réseaux en multicast pour des réseaux à plusieurs sources et plusieurs destinations, ainsi que le codage de réseaux au niveau physique. Nous proposons, dans le quatrième chapitre, une technique de décodage pour le protocole compute-and-forward pour des réseaux de points uni-dimensionnels et nous traitons les réseaux de points multi-dimensionnels dans le cinquième chapitre. Pour finir, nous donnons quelques perspectives pour des recherches futures.

Chapitre 1: La Communication Coopérative: Modèles et Outils

Les systèmes de communication sans fil doivent répondre à la rapide augmentation de demande d'accès à internet en particulier avec le développement actuel des applications du web 2.0 et des appareils de communication personnels. Le principal défi du développement de ces systèmes est de combattre l'atténuation du signal et l'intérference dûes au canal. Dans ce contexte, une nouvelle technique de communication a émérgé: la coopération, consistant à supporter la destination lors de la réception de l'information de la source et lui relayant cette information par une troisième entité coopératrice, le relai. La technique de communication coopérative a reçu une attention particulière car c'est un moyen efficace pour augmenter la fiabilité et le débit dans les systèmes de communication sans fil.

Ce chapitre résume succintement les principaux modèles et notions de la communication coopérative. Tout d'abord, nous définissons la diversité qui se traduit par la réception de la même information par plusieurs voies indépendantes. Nous détaillons aussi les principaux schémas de coopération présents dans la littérature: l'amplify-and-forward (AF), le decode-and-forward (DF) et le compress-and-forward. Le protocole de coopération définit ainsi l'action du relai et son rôle dans le schéma coopératif.

Nous donnons aussi une classification générale des réseaux les plus étudiés. Nous remarquons qu'une grande partie des résultats concernent les réseaux composés d'une source et d'une destination qui communiquent via un lien direct et assistées par un ou plusieurs relais.

Les réseaux multi-sauts sont aussi étudiés. Dans ces réseaux, la source et la destination n'ont pas de lien direct et communiquent via des relais classés en couches de relais. Dans le cadre de cette thèse, nous sommes intéressés par les réseaux à deux-sauts où la source et la destination communiquent via des relais ordonnés en une seule couche de relais.

Ensuite, nous présentons les principaux outils de mesure de performance utilisés dans la littérature: la capacité du canal sans fil, la probabilité de coupure et le degré de diversité. La probabilité de coupure mesure le taux de faillite du canal à assurer une communication entre la source et la destination à un débit fixé. De cette probabilité, les chercheurs dérivent deux mesures: le compromis diversité-multiplexage (DMT) et le gain de coupure. Dans le cadre de cette thèse, nous utilisons le gain de coupure pour étudier la performance des réseaux à deux-sauts. Le gain de coupure est calculé par rapport à une fonction f comme,

$$\xi = \lim_{\mathrm{SNR}\to\infty} f(\mathrm{SNR}) P_{out}.$$

La valeur de ξ nous permet de bien décrire la probabilité de coupure du canal à des valeurs du rapport signal à bruit (SNR) élevées et à un débit fixé R. Nous détaillons le modèle de canal de ces réseaux sous le protocole amplify-and-forward.

Enfin, nous faisons une briève bibliographie des différents protocoles de coopération proposés pour les réseaux mutli-sauts. Dans le chapitre suivant, nous étudions le rotate-and-forward proposé par Yang et Belfiore dans [1]. Ce protocole de coopération est attractif en raison de sa faible complexité et de sa bonne performance.

Chapitre 2: Performance du Protocole Rotate-and-Forward dans les Réseaux à Deux-Sauts

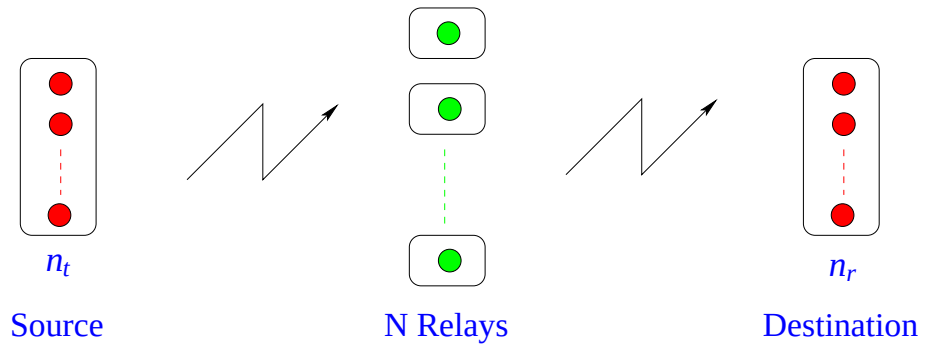


Figure 1: Coopération dans un réseau à deux-sauts.

Le Modèle de Canal

Ce chapitre est consacré à l'étude de la performance du protocole rotate-and-forward (RF) dans les réseaux à deux-sauts. Dans ces réseaux, la source dotée de n_t antennes communique avec la destination dotée de n_r antennes via une couche de N relais mono-antennaires et half-duplex. Le réseau à deux-sauts est ainsi désigné par le triplet (n_t, N, n_r) et représenté dans la Figure 1. Les relais sont indépendants et synchronisés, ils n'échangent aucune information entre eux ni sur l'état du canal ni sur les messages à transmettre. Le canal est à évanouissement Rayleigh.

Le Protocole Rotate-and-Forward

Chaque saut de ce réseau est un canal MIMO. Les signaux transmis par les relais dépendent du protocole de relayage. Dans le cadre du protocole RF [1], chaque relai applique une rotation aléatoire au signal qu'il reçoit avant de le retransmettre vers la destination. Ainsi le signal reçu à la destination peut s'écrire comme,

$$\boldsymbol{y}_D[i+1] = \boldsymbol{H}_2\boldsymbol{F}_i\boldsymbol{H}_1\boldsymbol{x}[i] + \boldsymbol{H}_2\boldsymbol{F}_i\boldsymbol{z}_R[i] + \boldsymbol{z}_D[i+1],$$

où $\boldsymbol{x} \in \mathbb{C}^{n_t \times 1}$ est le signal de la source et $\boldsymbol{y}_D \in \mathbb{C}^{n_r \times 1}$ est le signal reçu à la destination. $\boldsymbol{z}_R \sim \mathcal{CN}(0, \boldsymbol{I}_N)$ et $\boldsymbol{z}_D \sim \mathcal{CN}(0, \boldsymbol{I}_{nr})$ représentent le bruit Gaussien additif (AWGN) aux relais et à la destination respectivement. $\boldsymbol{H}_1 \in \mathbb{C}^{N \times n_t}$ et $\boldsymbol{H}_2 \in \mathbb{C}^{n_r \times N}$ sont les matrices des canaux MIMO. Les rotations effectuées par les relais à l'instant i sont représentées par la matrice diagonale $\boldsymbol{F}_i$ définie par $\boldsymbol{F}_i \triangleq \mathrm{diag}\big(e^{j\theta_{i,1}}, \ldots, e^{j\theta_{i,N}}\big)$.

Ainsi, dans un canal quasi-statique, chaque mot de code $\boldsymbol{X}$, envoyé sur T temps symbole, voit un canal équivalent, variant dans le temps, et défini à l'instant i par $\boldsymbol{H}_2\boldsymbol{F}_i\boldsymbol{H}_1$. Pour un grand T, l'information mutuelle de ce canal converge vers,

$$I_{\mathsf{moy}} = \mathbb{E}_{\theta_i}\left\{\log\det\left(\boldsymbol{I} + \mathrm{SNR}\left(\boldsymbol{H}_2\boldsymbol{F}_i\boldsymbol{H}_1\right)\left(\boldsymbol{H}_2\boldsymbol{F}_i\boldsymbol{H}_1\right)^{\dagger}\right)\right\}$$

avec $\boldsymbol{\theta}_i \triangleq (\theta_{i,1}, \ldots, \theta_{i,N})$. Le rotate-and-forward est optimal dans le sens du DMT dans les réseaux à deux-sauts avec un nombre arbitraire d'antennes à la source, à la destination et aux les relais [1], [4].

Performance du Protocole RF dans les Réseaux (1, N, 1)

On considère les réseaux (1, N, 1) composés d'une source et d'une destination mono-antennaire et N relais half-duplex indépendants. Les relais appliquent le protocole RF. Nous considérons que les liaisons source-relais ne sont pas bruitées. A très hautes valeurs du rapport signal à bruit (SNR), l'information mutuelle de ce canal dépend d'un terme a indépendant des rotations effectuées par les relais θ_j. La probabilité de coupure devient alors,

$$\mathsf{Prob}\left\{\mathbb{E}_{\theta}\left\{\log\det(\boldsymbol{I} + \mathrm{SNR}\boldsymbol{H}\boldsymbol{H}^{\dagger})\right\} < R\right\} \doteq \mathsf{Prob}\left\{\log(a) < R\right\}$$

où $a = 1 + \mathrm{SNR} \sum_{l=1}^{N} g_{1l} g_{2l}$ et $g_{ij} = |h_{ij}|^2$ sont les gains du canal de variances σ_{ij}^2.

Pour ce type de réseau, on définit la fonction f nécessaire pour calculer le gain de coupure comme étant égale à $f(\mathrm{SNR}) = \dfrac{\mathrm{SNR}^N}{(\ln \mathrm{SNR})^N}$. Ainsi, le gain de coupure dans un réseau (1, N, 1) opérant sous le protocole RF est donné en fonction du nombre de relais N, le débit R et les variances des canaux à évanouissements σ_{ij}^{-2} par:

$$\xi_{(1,N,1),RF} = \frac{(2^R - 1)^N}{N!} \prod_{l=1}^{N} \sigma_{1l}^{-2} \sigma_{2l}^{-2}.$$

Nous considérons maintenant le protocole rotate-and-forward orthogonal dans les réseaux (1, N, 1). Pour ce schéma, on définit la fonction f, comme pour le rotate-and-forward, par $f(\mathrm{SNR}) = \dfrac{\mathrm{SNR}^N}{(\ln \mathrm{SNR})^N}$. Ainsi, le gain de coupure pour le protocole RF orthogonal est obtenu par la forme récursive suivante:

$$\xi_{(1,N,1),ORF} = \mathcal{I}_N(N, R) \prod_{l=1}^{N} \sigma_{1l}^{-2} \sigma_{2l}^{-2},$$

$\mathcal{I}_N(N, R)$ est une forme récursive donnée par

$$\mathcal{I}_n(N, R) \;=\; \frac{2^{NR}}{(N-1)!} \left(\ln 2^{NR}\right)^{N-1} - \mathcal{I}_{n-1}(N, R), \qquad n = 1, \ldots N,$$

Nous considérons toujours les réseaux (1, N, 1) mais opérant, cette fois-ci, sous le protocole Selection-Relais RF. Pour ce schéma, on définit la fonction f par $f(\mathrm{SNR}) = \dfrac{\mathrm{SNR}^N}{(\ln \mathrm{SNR})^N}$ comme dans les deux cas précédents, et le gain de coupure est alors

$$\xi_{(1,N,1),RS} = (2^R - 1)^N \prod_{l=1}^{N} \sigma_{1l}^{-2} \sigma_{2l}^{-2}.$$

Ayant défini la même fonction f, les trois protocoles de relayage ont ainsi le même ordre de diversité. Par contre, pour comparer la performance de ces protocoles, il suffit de comparer les gains de coupure respectifs. Il est facile de voir que le protocole ayant le gain de coupure le plus petit a la meilleure performance;

$$\xi_{(1,N,1),RF} < \xi_{(1,N,1),RS} < \xi_{(1,N,1),ORF}.$$

Le rotate-and-forward est le protocole le plus performant.

Performance du Protocole RF dans les Réseaux (M, 1, M)

Nous considérons un réseau (M, 1, M) opérant sous le protocole RF. Pour ce schéma, l'information mutuelle peut s'écrire sous la forme suivante:

$$I = \log(1 + \mathrm{SNR} \times G_1 \times G_2)$$

où $G_1 = g_{11} + \ldots + g_{1M} \sim \mathcal{X}^2_{2M}$ et $G_2 = g_{21} + \ldots + g_{2M} \sim \mathcal{X}^2_{2M}$ sont deux variables aléatoires ayant une distribution Chi-2 à 2M degrés de liberté.

Nous définissons la fonction f par $f(\mathrm{SNR}) = \dfrac{\mathrm{SNR}^M}{\ln \mathrm{SNR}}$. Le gain de coupure est alors

$$\xi_{(M,1,M),RF} = \frac{M(2^R - 1)^M}{(M!)^2} \prod_{l=1}^{M} \sigma_{1l}^{-2} \sigma_{2l}^{-2}$$

Le Protocole RF avec Voie de Retour

Dans cette section, nous expliquons comment on peut améliorer la performance du protocole RF si une voie de retour existe entre la destination et les relais pour les réseaux (n_t, N, n_r). L'idée est basée sur le fait que, dans le cadre du protocole RF, les relais choisissent aléatoirement les angles de rotations. Ces angles ne sont pas toujours optimaux pour une réalisation de canal donnée. Alors la destination, ayant une parfaite connaissance du canal, peut trouver les angles de rotation optimaux et les transmettre aux relais via la voie de retour. Ainsi, le canal équivalent devient $\boldsymbol{H}_2 \boldsymbol{F}_{opt} \boldsymbol{H}_1$.

La recherche des rotations optimales $\boldsymbol{\theta}_{opt} = (\theta_{1,opt}, \ldots, \theta_{N,opt})$ peut se faire par une recherche exhaustive, certes optimales mais d'une complexité de calcul exponentielle en fonction du nombre de relais N. Alternativement, nous proposons un algorithme qui permet de trouver les rotations optimales avec une complexité linéaire en N. L'idée de cet algorithme est de pouvoir écrire l'information mutuelle pour un angle donné θ_j de la façon suivante:

$$I(\boldsymbol{\theta}) = \log\left(\boldsymbol{A}_j + \boldsymbol{B}_j \cos(\theta_j + \phi_j)\right)$$

où $\boldsymbol{A}_j$, $\boldsymbol{B}_j$, and ϕ_j sont fonctions des matrices de canal $\boldsymbol{H}_1$ and $\boldsymbol{H}_2$ et les angles θ_i, $\forall i \neq j$. Alors, pour cet angle

$$\theta_{j,opt} = -\phi_j$$

La destination peut ainsi maximiser l'information mutuelle par rapport aux angles de rotations l'un après l'autre. Ayant obtenu tous les angles, la destination itère pour affiner les résultats.

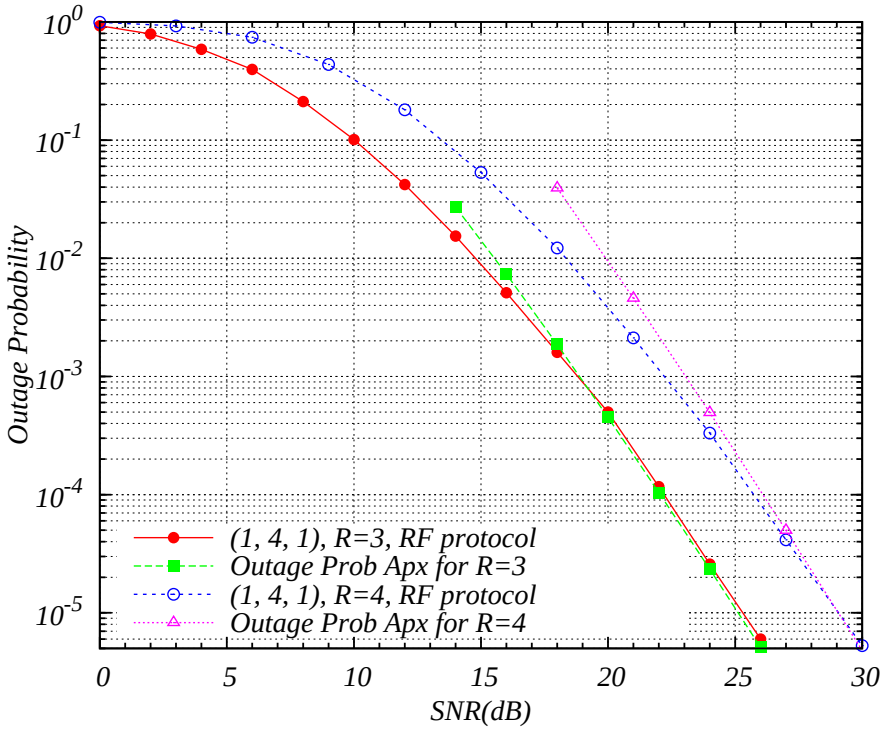


Figure 2: Probabilité de coupure pour les réseaux (1, 4, 1) opérant sous le protocole RF, $\sigma_{1l}^2 = \sigma_{2l}^2 = 1$.

Résultats de Simulations

Nous avons vérifié les gains de coupure obtenus dans les réseaux (1, 4, 1) pour le protocole RF dans des canaux à évanouissements Rayleigh, Figure 2. On remarque que les valeurs théoriques et les valeurs expérimentales sont très proches, ce qui valide notre calcul. De la même façon, on a vérifié les gains de coupure pour le protocole RF orthogonal dans les réseaux (1, 2, 1) et (1, 3, 1), Figure 3, ainsi que pour les réseaux (M, 1, M), Figure 4.

Nous avons aussi vérifié la performance de notre algorithme itératif et avons trouvé que cet algorithme a des performances optimales, Figure 5. Par ailleurs, nous avons étudié l'effet de la limitation de la voie de retour sur les performances du protocole RF. Nous concluons que nous n'avons pas besoin d'une précision très fine dans le calcul des rotations optimales et que le nombre d'itérations nécessaires est petit. Il est de l'ordre de 3 itérations dans les simulations, Figure 6.

Chapitre 3: Introduction à la Théorie de Codage de Réseaux

Dans ce chapitre, nous introduisons le codage de réseaux proposé pour atteindre la borne supérieure sur l'information mutuelle dans les réseaux à plusieurs sources et plusieurs destinations. La façon traditionnelle de transport des données, en gardant séparés les flux

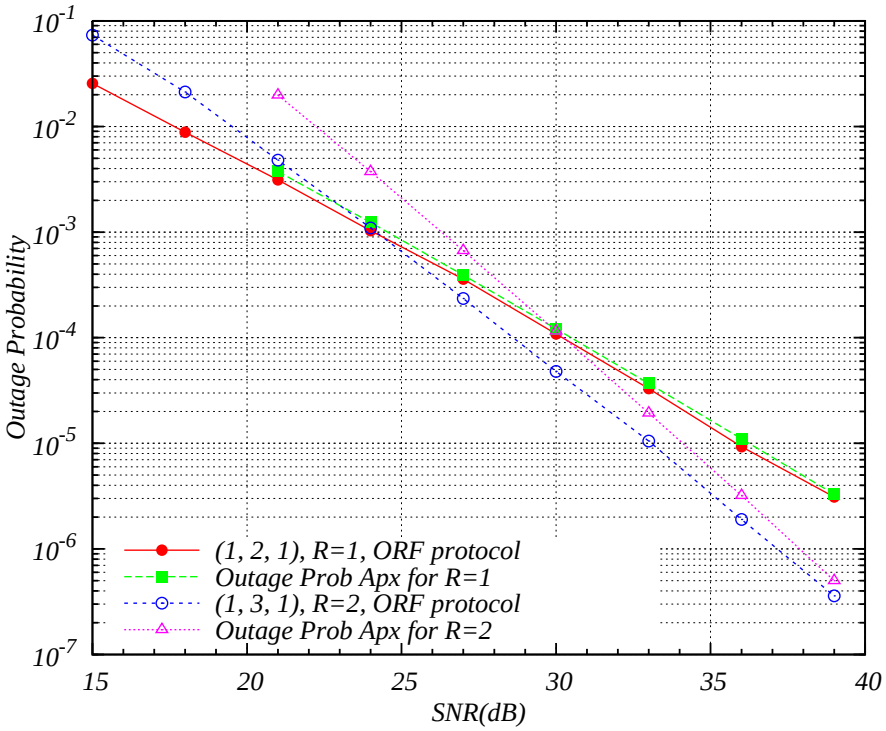


Figure 3: Probabilité de coupure pour les réseaux (1, N, 1) opérant sous le protocole RF orthogonal, $\sigma_1^2 = \sigma_2^2 = 1$.

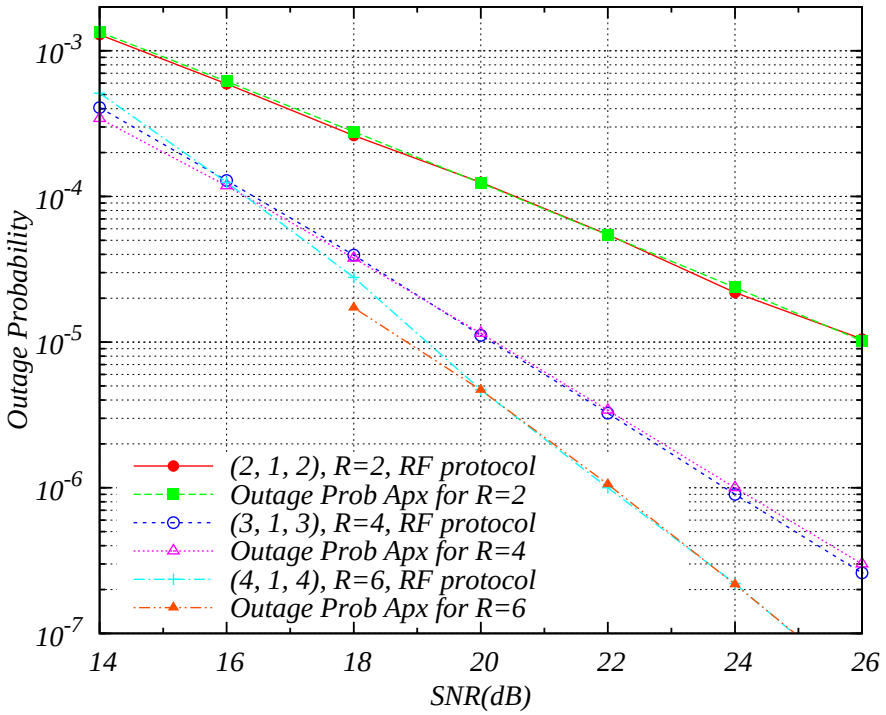


Figure 4: Probabilité de coupure pour les réseaux (M, 1, M) opérant sous le protocole RF, $\sigma_1^2 = \sigma_2^2 = 2$.

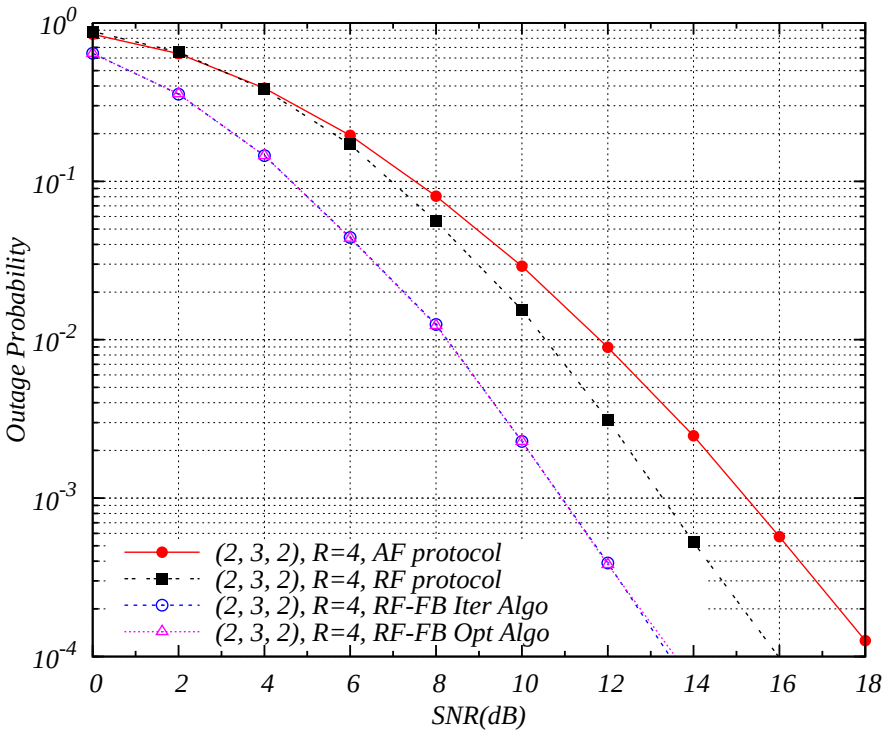


Figure 5: Probabilité de coupure pour le réseau (2, 3, 2) sous les protocoles AF, RF, et RF avec voie de retour.

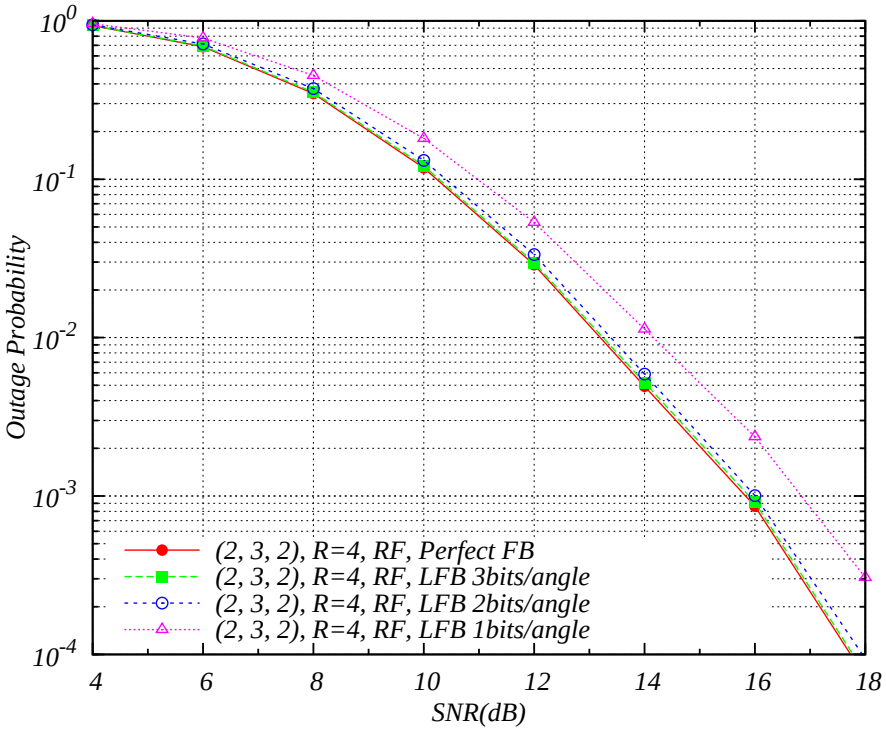


Figure 6: Probabilité de coupure pour le réseau (2, 3, 2) avec voie de retour limitée.

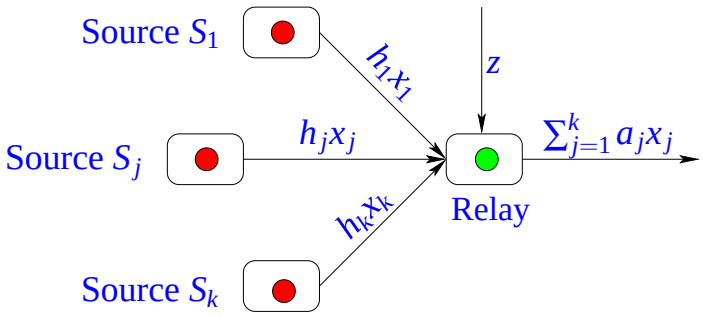


Figure 7: Modèle de système: k sources et un relay.

indépendants, résulte en une sous-exploitation de la capacité du réseau. Ainsi, le codage de réseaux consiste à combiner les flux d'information indépendants et d'envoyer des combinaisons de ces informations sur le réseau. La destination, ayant reçu plusieurs combinaisons d'informations, peut ainsi récupérer ces flux indépendants.

Nous utilisons le réseau papillon, bien connu dans ce contexte, pour expliquer les différents avantanges du codage de réseaux: débit, exploitation du canal sans fil, sécurité, ainsi que les principaux défits: complexité, sécurité et compatibilité avec l'infrastructure existante. Nous introduisons aussi le théorème de base de codage de réseaux qui stipule l'existence, pour tout réseau, d'un schéma de codage linéaire permettant d'atteindre la borne supérieure sur l'information mutuelle pour toute paire source-destination. Une version algébrique équivalente de ce théorème est aussi présentée.

Le codage de réseaux au niveau physique recopie le principe du codage de réseaux aux niveaux supérieurs (les bits) et l'applique aux ondes électromagnétiques. Dans cette optique, le canal sans fil est un combinateur naturel d'ondes électromagnétiques en raison du phénomène d'interférence. Le principe du codage de réseaux au niveau physique est d'exiger de la part d'un relai, recevant une combinaison linéaire évanouie et bruitée de plusieurs signaux, de décoder une combinaison linéaire non bruitée des symboles reçus. Nous sommes intéressés, dans le cadre de cette thèse, par le protocole compute-and-forward (CF) récemment proposé par Nazer et Gastpar [3]. Nous donnons à la fin de ce chapitre une courte bibliographie sur tous les protocoles de codage de réseaux au niveau physique traités dans la littérature.

Chapitre 4: Codage de Réseaux au niveau Physique: Le Protocole Compute-and-Forward

Le codage de réseaux au niveau physique consiste à diffuser dans le réseau des combinaisons des messages transmis. Nous traitons dans ce chapitre un protocole de codage de réseaux au niveau physique appelé compute-and-forward (CF) proposé par Nazer et Gastpar dans [3]. Le relai, qui reçoit une combinaison évanouie et bruitée de symboles indépendants transmis par

plusieurs sources, doit décoder une combinaison linéaire entière non bruitée de ces symboles. Cette combinaison est retransmise vers un autre relai ou vers la destination. Cette dernière, à son tour, ayant reçu plusieurs combinaisons entières, peut résoudre ce système d'équations pour en extraire les symboles des sources.

Compute-and-Forward: Débit de Calcul

Le modèle du système est donné dans la Figure 7. Le signal reçu au relai est

$$\boldsymbol{y} = \sum_{j=1}^{k} h_j \boldsymbol{x}_j + \boldsymbol{z}.$$

Le relai doit décoder à partir de $\boldsymbol{y}$, et sans décoder les symboles $\boldsymbol{x}_j$, la combinaison linéaire

$$\boldsymbol{\lambda} = \sum_{j=1}^{k} a_j \boldsymbol{x}_j,$$

où les coefficients $a_j \in \mathbb{Z}[i]$.

Les auteurs du CF propose d'utiliser les codes en réseaux de points afin de garantir que toute combinaison linéaire de mots de code est aussi un mot de code en réseaux de points. Les auteurs indiquent que tout relai est capable de décoder toute combinaison linéaire de messages transmis tant que les débits de toutes les sources sont inférieurs au débit de calcul. Ils définissent le débit de calcul par,

$$R_{\mathsf{comp}}(\boldsymbol{h}, \boldsymbol{a}) = \log \left(\left(\|\boldsymbol{a}\|^2 - \frac{\mathsf{SNR}|\boldsymbol{h}^\dagger \boldsymbol{a}|^2}{1 + \mathsf{SNR}\|\boldsymbol{h}\|^2} \right)^{-1} \right).$$

Dans le cadre de cette thèse, nous cherchons à maximiser le débit de calcul, proposer une technique de décodage qui a une meilleure performance que le décodage à distance Euclidienne minimale et donner des critères de construction de codes en réseaux de points.

Maximiser le Débit de Calcul

Nous cherchons le vecteur de coefficients $\boldsymbol{a}$ qui maximise le débit de calcul. Nous montrons que ceci est équivalent à trouver le vecteur $\boldsymbol{a}$ qui maximise

$$\boldsymbol{a} = \arg\min_{\boldsymbol{a} \neq \boldsymbol{0}} \left(\boldsymbol{a}^\dagger \boldsymbol{G} \boldsymbol{a} \right)$$

où

$$\boldsymbol{G} = \boldsymbol{I} - \frac{\mathsf{SNR}}{1 + \mathsf{SNR}\|\boldsymbol{h}\|^2} \boldsymbol{H}.$$

$\boldsymbol{H} = [H_{ij}]$, $H_{ij} = h_i h_j^\star$, $1 \leq i, j \leq k$. $\dagger$ est pour le transposé conjugué (Hermitien).

Nous montrons aussi que ce problème est équivalent à la recherche du vecteur de plus petit module dans le réseau de points ayant $\boldsymbol{G}$ comme matrice de Gram.

Réseau de Points Uni-Dimensionnel: Cas Réel

Dans la perspective de proposer une technique de décodage basée sur le maximum de vraisemblance (ML), nous considérons le cas uni-dimensionnel avec des canaux à gains réels. Notre réseau est ainsi formé par deux sources transmettant deux messages indépendants, x_1 et x_2, et un relai décodant une combinaison linéaire à coefficients entiers et premiers entre eux:

$$\lambda = a_1 x_1 + a_2 x_2.$$

Le signal reçu au relai peut s'écrire comme suit:

$$y = a_1 x_1 + a_2 x_2 + q + z$$

$x_j \in \mathcal{S}$, appartient à une constellation PAM définie par $|x_j| \leq x_{\mathsf{max}}$. $a_j \in \mathbb{Z}$. Noter que $\lambda \in \mathbb{Z}$.

La Métrique de Décodage

Notons que $\lambda = a_1 x_1 + a_2 x_2$ est une équation Diophantienne qui a une infinité de solutions données par:

$$\begin{cases} x_1 = u_1 \lambda + a_2 k \\ x_2 = u_2 \lambda - a_1 k. \end{cases}$$

où (u_1, u_2) est une solution particulière et $k \in \mathbb{Z}$. Le décodeur à maximum de vraisemblance maximize la probabilité conditionnelle $p(y|\lambda)$,

$$\hat{\lambda} = \arg\max_{\lambda} \Omega(\lambda) := \sum_{\substack{(x_1,x_2) \\ a_1 x_1 + a_2 x_2 = \lambda}} \exp\left[-\frac{(y - h_1 x_1 - h_2 x_2)^2}{2\sigma^2}\right] = \sum_{k=-\infty}^{+\infty} \exp\left[-\frac{(y - \beta\lambda + k\alpha)^2}{2\sigma^2}\right]$$

où $\beta = h_1 u_1 + h_2 u_2$, $\alpha = h_2 a_1 - h_1 a_2$.

Approximation Diophantienne Inhomogène

Nous montrons que le problème est équivalent à

$$\min_{(\lambda,k)} F(k,\lambda) = \min_{\substack{(\lambda,k) \\ x_1, x_2 \in \mathcal{S}}} \left| k\alpha' - \lambda + y' \right|$$

où $\alpha' = \alpha/\beta$ et $y' = y/\beta$. Cette minimisation est une approximation Diophantienne inhomogène qui peut être résolue par l'algorithme de Cassel. Ainsi, λ peut être trouvé par une approximation Diophantienne inhomogène.

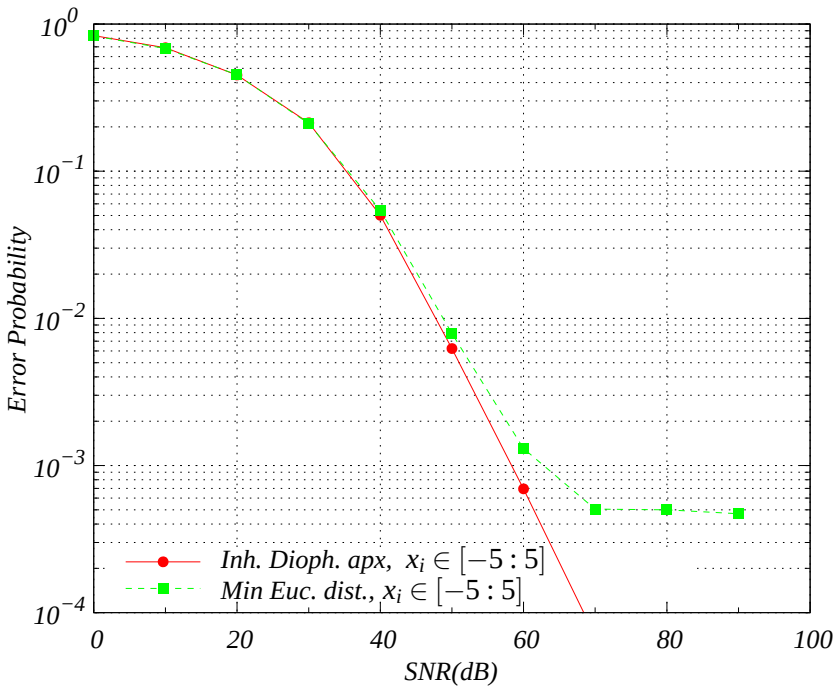


Figure 8: Probabilité d'erreur sur le décodage de λ utilisant l'approximation Diophantienne inhomogène et la distance Euclidiène minimale.

Résultats de Simulations

Tout d'abord, nous comparons la performance de notre technique de décodage basée sur l'approximation Diophantienne à celle basée sur la distance minimale, Figure 8. On peut voir que la technique de la distance minimale représente un palier dû au bruit de quantification q. Ce bruit résulte de la représentation du gain réel du canal par un coefficient entier. Ce palier est inévitable avec la technique de décodage de distance minimale. Par contre, notre technique basée sur l'approximation Diophantienne ne représente aucun palier.

Dans la Figure 9, nous traçons la probabilité d'erreur sur le décodage de λ avec des constellations PAM de tailles différentes. Nous remarquons que pour $x_{\mathsf{max}} = 5$, la diversité est égale à 1, ce qui correspond à une diversité égale à 2 avec des symboles complexes. Par contre, pour $x_{\mathsf{max}} > 5$, la diversité est de $1/2$. Nous traçons la fonction de vraisemblance pour comprendre cette perte de diversité, Figure 10. Nous remarquons que pour des constellations de grande taille, la fonction de vraisemblance devient plate et est maximisée pour plusieurs valeurs de λ, ce qui crée une ambiguité dans le choix de λ. Pour des constellations de petite taille, cette fonction est maximisée pour une seule valeur de λ. En dimension 1, le seul réseau de points est l'anneau des entiers $\mathbb{Z}$ et donc cette perte de diversité est inévitable. Nous devons faire une étude plus approfondie dans le cas multi-dimensionnel pour pouvoir contrer cette platitude.

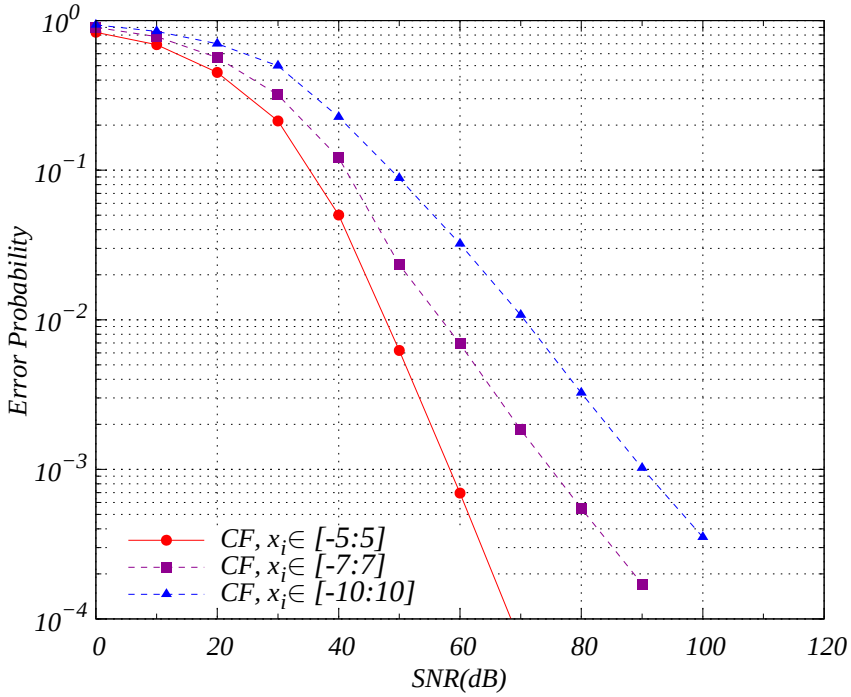


Figure 9: Probabilité d'erreur sur le décodage de λ utilisant l'approximation Diophantienne inhomogène.

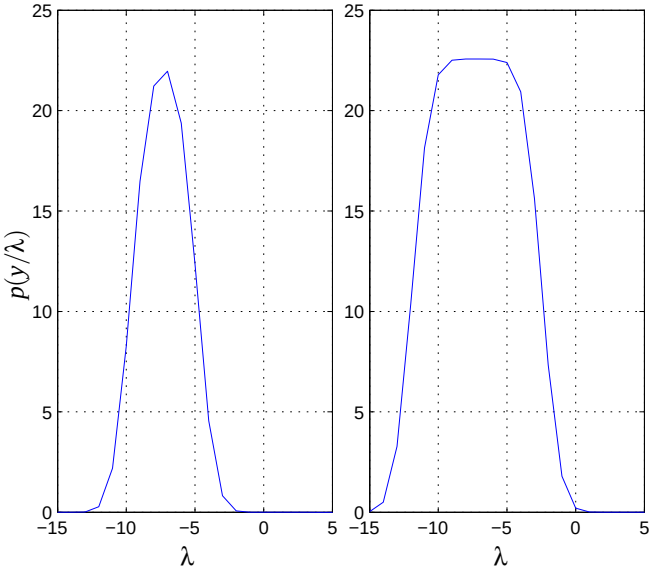


Figure 10: $p(y/\lambda)$ pour $\boldsymbol{h} = [-1.274\ 0.602]^T$, $\boldsymbol{a} = [2\ \ -1]^T$, $\mathsf{SNR} = 40dB$, $x_1 = -2$ and $x_2 = 3$. $p(y/\lambda)$ est maximale pour une seule valeur $\lambda = -7$ à gauche tandis qu'elle est maximisée pour plusieurs valeurs de λ à droite.

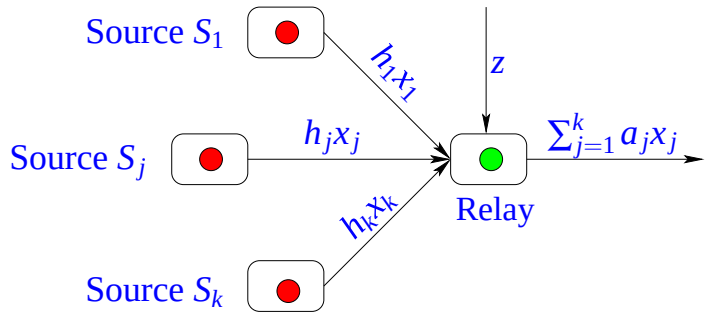


Figure 11: System model: k sources and one relay.

Chapitre 5: Le Compute-and-Forward: Cas Multi-Dimensionnel

Dans ce chapitre, nous considérons des réseaux de points multi-dimensionnels et des gains de canal complexes. Dans le chaptire précedent, avec des réseaux de points uni-dimensionnels et des gains de canal réels, nous avons proposé une technique de décodage quasi-ML basée sur une approximation Diophantienne inhomogène. Nous avons aussi constaté que la fonction ML est plate pour des constellations de grande taille ce qui mène à des ambiguités au décodage. En se basant sur ces résultats, nous étudions, dans ce chapitre, la fonction de maximum de vraisemblance (ML) pour généraliser la technique de décodage et donner des critères de construction des codes en réseaux de points.

Modèle de Système

Nous considérons k sources envoyant k symboles indépendants. Le symbole $\boldsymbol{x}_j$ transmis par la source j est tiré d'un réseau de points $\Lambda_j \subset \mathbb{Z}[i]^n$. Le signal reçu au relai est

$$\boldsymbol{y} = \sum_{j=1}^{k} h_j \boldsymbol{x}_j + \boldsymbol{z},$$

où $h_j \in \mathbb{C}$ sont les gains du canal et $\boldsymbol{z}$ est le bruit additif Gaussien. Le relai décode $\boldsymbol{\lambda}$, une combinaison linéaire des messages $\boldsymbol{x}_j$ avec des coefficients entiers, $a_j \in \mathbb{Z}[i]$, et donnée par

$$\boldsymbol{\lambda} = \sum_{j=1}^{k} a_j \boldsymbol{x}_j.$$

Décodage ML

En suivant le même calcul du chapitre précedent, nous montrons que la métrique du décodage ML peut s'écrire sous la forme suivante:

$$\hat{\boldsymbol{\lambda}} = \arg \max_{\boldsymbol{\lambda}|\boldsymbol{\lambda}=\sum_{j=1}^{k} a_j \boldsymbol{x}_j} p(\boldsymbol{y}|\boldsymbol{\lambda}) = \arg \max_{\boldsymbol{\lambda}\in\Lambda} \sum_{\{\boldsymbol{x}_j\}|\sum_{j=1}^{k} a_j \boldsymbol{x}_j=\boldsymbol{\lambda}} \exp\left[-\frac{\|\boldsymbol{y}-\sum_{j=1}^{k} h_j \boldsymbol{x}_j\|^2}{2\sigma_z^2}\right].$$

Afin d'expliciter l'expression des $\boldsymbol{x}_j$ en fonction de $\boldsymbol{\lambda}$, nous devons résoudre un système d'équations Diophantiennes. Ceci est possible en utilisant la forme Normale de Hérmit (HNF) qui s'appliquent à toute matrice à éléments entiers. La solution du système d'équations est donc

$$\boldsymbol{x}_j = \boldsymbol{M}_j \boldsymbol{V}_j \boldsymbol{B}^{-1} \boldsymbol{\lambda} + \boldsymbol{s}_j,$$

où $\boldsymbol{s}_j$ est un point quelconque du réseau de points L_j généré par $\boldsymbol{M}_j \boldsymbol{U}_j$. Les matrices $\boldsymbol{V}_j$, $\boldsymbol{M}_j$ et $\boldsymbol{B}$ sont données par la HNF.

En combinant la fonction ML et la solution $\boldsymbol{x}_j$, nous obtenons la métrique de décodage sous la forme suivante

$$\hat{\boldsymbol{\lambda}} = \arg\max_{\boldsymbol{\lambda}\in\Lambda} \Omega(\boldsymbol{\lambda}) := \sum_{u\in\mathcal{L}} \exp\left[-\frac{\|\boldsymbol{y} - w(\boldsymbol{\lambda}) - \boldsymbol{u}\|^2}{2\sigma_z^2}\right],$$

où $w(\boldsymbol{\lambda})$ est une fonction linéaire de $\boldsymbol{\lambda}$ et $\mathcal{L}$ est un réseau de points de matrice génératrice $\sum_{j=1}^{k} h_j \boldsymbol{M}_j \boldsymbol{U}_j$ sachant que $\sum_{j=1}^{k} a_j \boldsymbol{M}_j \boldsymbol{U}_j = 0$.

Le problème est que $\varrho(\boldsymbol{\lambda})$ peut être plate en fonction de $\boldsymbol{\lambda}$. Nous introduisons alors le facteur de platitude d'une somme de mesures Gaussiennes.

Le facteur de Platitude

Considérons la fonction suivante,

$$\begin{cases} \phi : \mathbb{R}^n \to \mathbb{R} \\ \phi : \boldsymbol{y} \mapsto \sum\limits_{\boldsymbol{x}\in\Lambda} e^{-\frac{\|\boldsymbol{y}-\boldsymbol{x}\|^2}{2\sigma^2}} \end{cases}$$

où Λ est un réseau de points Euclidéen d'ordre n. ϕ est une somme de mesure Gaussiennes et est périodique. Nous définissons le facteur de platitude de cette fonction par le rapport de sa valeur moyenne sur sa valeur maximale dans un intervalle donné. Nous montrons que pour un réseau de points Λ Euclidéen d'ordre n, ce facteur est égale à

$$\epsilon_\Lambda(\mu) = \frac{(2\pi)^{\frac{n}{2}}}{\mu^{\frac{n}{2}} \Theta_\Lambda\left(e^{-\frac{\mu}{2} vol(\Lambda)^{-\frac{2}{n}}}\right)}.$$

μ est le signal rapport à bruit généralisé (GSNR) et $\Theta_\Lambda(q)$ est la série théta du réseau de points Λ. Le facteur de platitude est compris entre 0 et 1. Nous le voulons le plus petit possible.

Dans la Figure 12, nous traçons le facteur de platitude de plusieurs réseaux de points en dimension 8. En particulier, le réseau de points E_8, qui est le plus dense en dimension 8, a le plus grand facteur de platitude, tandis que le réseau de points $\mathbb{Z}^4 \oplus 2\mathbb{Z}^4$, qui est un mauvais réseau de points, a le plus petit facteur de platitude. Puisque nous cherchons à minimiser le

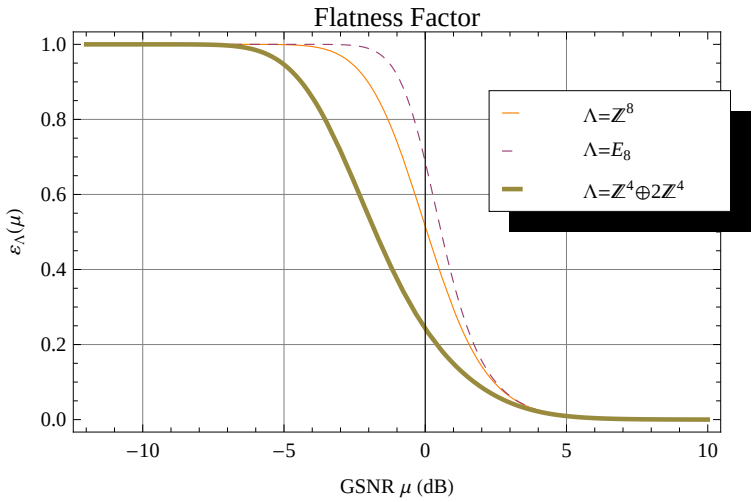


Figure 12: Some flatness factors in dimension 8.

facteur de platitude, nous sommes davantage intéressés par le réseau de points $\mathbb{Z}^4 \oplus 2\mathbb{Z}^4$.

Bon Réseau de Points, Mauvais Réseaux de Points

Dans la métrique de décodage, deux réseaux de points entrent en jeu. Le réseau de points Λ, dans lequel on décode $\boldsymbol{\lambda}$, est défini par,

$$\Lambda = \sum_{j=1}^{k} a_j \Lambda_j.$$

Ce réseau de points doit être dense, il est ainsi un “Bon” réseau de points.

Le réseau de points $\mathcal{L}$, dans lequel on effectue la somme des mesures Gaussiennes, est généré par la matrice $\boldsymbol{M}_{\mathcal{L}} = \sum_{k=1}^{j} h_j \boldsymbol{M}_j \boldsymbol{U}_j$, sachant que $\sum_{k=1}^{j} a_j \boldsymbol{M}_j \boldsymbol{U}_j = 0$ (HNF). Dans le but de minimiser le facteur de platitude de ce réseau de points, la matrice génératrice $\sum_{j=1}^{k} h_j \boldsymbol{M}_j \boldsymbol{U}_j$ doit avoir une déficience de rang. Ainsi, nous devons aligner $\boldsymbol{a}$ avec $\boldsymbol{h}$ le plus possible. Donc, $\mathcal{L}$ est un “Mauvais” réseau de points.

Il nous reste à trouver des algorithmes de décodage efficaces, capables de décoder des systèmes d’approximations Diophantiennes inhomogènes.

Perspectives

Comme perspectives pour les travaux futurs, nous proposons les directions suivantes:

- *Degrés de liberté offerts par le décodage quasi-ML:* Dans [5], les auteurs montrent que le schéma du compute-and-forward et le décodage basé sur la minimisation de la distance Euclidienne atteint au plus 2 degrés de liberté avec k utilisateurs, loin de $k/2$ degrés de liberté que peut atteindre l'alignement d'interférence et la borne supérieure de k degrés de liberté donnée par les systèmes MIMO. Il serait intéressant de trouver le nombre de degrés de liberté que peut atteindre notre système basé sur l'approximation Diophantienne inhomogène.

- *Alignement de réseau de points pour le canal à interférence:* Donnons un exemple. Supposons que nous avons trois transmetteurs et trois récepteurs utilisant le même environnement de transmission. Le symbole transmis $\boldsymbol{x}_i \in \Lambda_i \subset \mathbb{Z}[i]^n$ est un point de réseau de points. Le récepteur R_1 reçoit une combinaison linéaire bruitée des symboles transmis,

$$\boldsymbol{y}_1 = h_{11}\boldsymbol{x}_1 + h_{21}\boldsymbol{x}_2 + h_{31}\boldsymbol{x}_3 + \boldsymbol{z}.$$

  Au lieu de considérer $h_{21}\boldsymbol{x}_2 + h_{31}\boldsymbol{x}_3$ comme du bruit, le récepteur R_1 l'évalue par une combinaison entière $a_{21}\boldsymbol{x}_2 + a_{31}\boldsymbol{x}_3$ qui, a son tour, est un point d'un réseau de points $\Lambda_1 \subset \mathbb{Z}[i]^n$. R_1 quantifie le signal reçu modulo Λ_1 et retrouve ainsi le message x_1. Une étude détaillée pour ce schéma peut être menée.

- *Décodage de plusieurs combinaisons entières:* Nous avons montré que le relai décode la combinaison linéaire avec le vecteur de coefficients entiers du plus petit module. Le relai peut décoder autant de combinaisons linéaires qu'il a des variables inconnues et ceci en choisissant les vecteurs successifs de plus petits modules. Ces vecteurs étant indépendants, le relai peut ainsi décoder tous les symboles. Une analyse fine de cette technique de décodage est à faire.

Introduction and Outline

MORE and always more: that is how we can qualify the demand for wireless ressources drift by the rapid development of wireless personal gadgets and web-based applications. The challenge of the new generations of wireless communication systems (Third-Generation and beyond) is to provide to the users high data rates with the best quality of service.

While traditional point-to-point communication fails to satisfy this increasing wireless demand, cooperative modes of communication such as relaying are attractive to improve both the reliability and the spectral efficiency in wireless networks. In a cooperative scheme, a relay helps the source in delivering the messages to the destination. This system creates an equivalent distributed Multiple-Input Multiple-Output (MIMO) channel that provides additional spatial dimension for communication and yields a degree-of-freedom gain. In the recent years, the cooperative communication has received a great interest to answer an essential question: "How to cooperate at the best?". In other words, what is the best thing that the relay should do to improve the reliability of a communication scheme? To date, most proposed cooperative schemes in the literature have relied on one of the following three relaying strategies: the amplify-and-forward (AF), the decode-and-forward (DF), and the compress-and-forward (CF).

In the first part of the thesis, we are interested in the study of the two-hop MIMO relay networks without a direct source-destination link. In particular, we consider the rotate-and-forward (RF) protocol proposed by Yang and Belfiore in [1]. In this linear protocol based on AF, the relays rotate randomly their received signals before amplify-forwarding them. The RF scheme is shown to be DMT-achievable in the two-hop relay networks in [1] and [4]. Motivated by the low complexity and good performance of the RF scheme, we use the outage gain metric defined in [2] to characterize the outage probability at moderate and high signal-to-noise ratio. Using the outage gain, we compare the performance of the RF scheme to that of other schemes having the same diversity order. In case of the existing of a limited feedback channel between the destination and the relays, we give a simple algorithm to find the optimal rotations by the destination. These rotations are then fed back to the relays. We show that this enhances the performance of the RF scheme in terms of channel outage probability.

In multiple source-destination pairs networks, the physical layer network coding (PLNC) approach takes benefits from the interference to increase the transmission rates between the users in the network. Instead of just forwarding, the relays process the incoming independent information flows. In this scope, Bobak and Gastpar have proposed a PLNC protocol called the compute-and-forward (CF) protocol [3]. In the CF scheme, the relays decode a linear functions of the received signals and transmit them to the next relay or destination. The destination collecting enough linear functions, recovers the original messages. In the second part of this thesis, we analyze the practical implementation aspects of the CF scheme, and we propose a decoding technique based on the maximum likelihood (ML) criterion for the real one-dimensional lattices. Then, we generalize some of our results to the complex multi-dimensional lattices.

Outline and Contributions

This dissertation is organized as follows. Chapter 1 introduces the cooperative communication and the theoretic tools used to study the performance of the cooperative systems. Chapter 2 studies the performance of the rotate-and-forward scheme in the two-hop MIMO networks. Chapter 3 presents the principle of network coding for multicasting in multiple source-destination networks, and the principle of the physical layer network coding which is the equivalent of the classical network coding at the physical layer. Chapter 4 is devoted to the compute-and-forward scheme in the real one-dimensional lattices. Finally, Chapter 5 is the generalization of our results for the RF protocol to the complex multi-dimensional lattices.

The chapters of this thesis are summarized in the following.

1. **Cooperative Communication: System and Tools (Chapter 1)** We introduce the cooperative communication and the three core relaying strategies and cooperative protocols studied in the literature. We present a general classification of wireless cooperative networks, and then we detail the system model of our interest. Moreover, we give the theoretical tools used to study the performance of wireless communication systems, namely the channel capacity, the outage probability, and the diversity-multiplexing tradeoff (DMT). We introduce the outage gain metric that we will use later to study the performance of the rotate-and-forward scheme in the two-hop relay networks. Finally, we provide a brief state of the art on the cooperative protocols proposed for the multi-hop networks.

2. **Rotate-and-Forward: Performance in the Two-Hop Relay Networks (Chapter 2)** We consider the (1, N, 1)[1] and the (N, 1, N) networks. We use the outage

[1] (n_t, N, n_r) designates a two-hop network with a n_t antennas source, n_r antennas destination, and N single antenna relays.

gain metric as a performance measure. For the (1, N, 1) networks, we extract the outage gains for the rotate-and-forward, orthogonal rotate-and-forward, and relay selection schemes. For the (N, 1, N) networks, we extract the outage gain for the RF scheme. The outage gain values allow us to exactly characterize the outage probability at moderate and high signal-to-noise ratio, and to compare the performance of protocols having the same diversity order. We also assume that a limited feedback channel exists between the destination and the relays. We give a low complexity algorithm to find the optimal rotations based on the channel knowledge. This algorithm enhances the performance of the RF scheme in terms of outage probability.

3. **Introduction to Network Coding Theory (Chapter 3)** We introduce the principle of network coding for multicast in multiple source-destination networks. Based on the basic butterfly network, we give the main challenges and benefits of the network coding, namely throughput, wireless resources, security, and complexity. Then, we develop the min-cut max-flow theorem, and the main network coding theorem in both network and algebraic approaches. Finally, we present the physical-layer network coding which is the equivalent of the classical network coding at the physical layer.

4. **Physical Layer Network Coding: The Compute-and-Forward Protocol (Chapter 4)** We study the implementation and practical aspects of the CF scheme in the real one-dimensional lattices in a system composed of two sources and one relay. We determine how to maximize the computation rate across the network in relating this problem to the shortest vector problem in a lattice. Then, we propose a decoding technique based on the maximum likelihood (ML) expression. We show that decoding a linear combination of the received signal can be viewed as an inhomogeneous Diophantine approximation problem. Numerically, we show that the error probability of our decoding technique is less than that of minimum Euclidian distance decoding proposed in the original work [3].

5. **Compute-and-Forward Protocol: Multi-Dimensional Case (Chapter 5)** We extend the previous work to the general complex multi-dimensional lattices. We analyze the maximum likelihood function and the lattices that intervene in it. In the ML function, we find a system of linear Diophantine equation. Moreover, the decoding error probability depends on the ML function that can be flat. We introduce then the flatness factor as a tool to study and design the lattices involved in this function. Finally, we state that the decoding technique should be based on simultaneous Diophantine approximations.

Finally, we conclude this thesis and give some general perspectives.

Chapter 1

Cooperative Communication: System and Tools

WIRELESS communication systems are limited in data rate and reliability. This limitation is directly related to the wireless channel's nature. There are two fundamental aspects of the wireless communication channels. First is the signal attenuation described by three phenomena: channel fading, shadowing, and path loss. Second is the interference since several transmitter-receiver pairs share the same communication medium.

The demand for wireless access increases rapidly especially with the development of the web 2.0 and the wireless personal devices. In the Third-Generation (and beyond) wireless communication systems, advanced algorithms and techniques are employed to increase both reliability and spectral efficiency. Among these techniques, diversity is of major importance due to the connection to the physical nature of the wireless environment.

This chapter serves as an introduction on the cooperative communication. In Section 1.1, we introduce the cooperative diversity and present the core relaying strategies and cooperative protocols developed in the literature. We then give a general classification of wireless relay networks in Section 1.2, and detail the multi-hop channel model, which is the model of our interest in Section 1.3. We provide a review of most important information theory tools that yield important theoretic evaluation measures: the channel capacity in Section 1.4, the outage probability in Section 1.5, and the diversity-multiplexing tradeoff in Section 1.6. These measures are mainly used as a basis to compare and evaluate the performance of the cooperative protocols and to develop optimal coding schemes. Finally, we give a general overview about the cooperative algorithms proposed in the literature for the multi-

hop networks in Section 1.7.

1.1 Cooperative Communication

1.1.1 Cooperation Diversity

The reliability of a communication scheme depends on the strength of the channel path between the transmitter and the receiver. When this channel is in deep fade, any communication scheme suffers from errors. In order to enhance the performance of a communication system, a solution is to allow the information symbols to reach the destination through different independently fading paths. This technique is called *diversity*, and it can dramatically improve performance over fading channels.

The well-known forms of diversity are **time** diversity, **frequency** diversity, and **space** diversity. Space diversity relies on the principle that the information symbols transmitted by geographically separated transmitters, and/or received by geographically separated receivers, experience independent fading. The multi-antenna, MIMO systems are an example provided that antennas are sufficiently far apart. Actually, though it is possible to increase the number of transmitting antennas, it is often practically hard to do the same at the reception. This is due to the small size of the receiving terminals that does not guarantee enough separation between antennas and then the independence of the different received versions. In order to overcome this limitation, Sendonaris *et al.* [6], [7] introduced a new form of spatial diversity, the *cooperation* diversity, in which the diversity gain is achieved via the cooperation of different users.

Originally, cooperation was proposed for the mobile systems. In each cell, each user has a *partner*. Each of the two partners is responsible for transmitting his own information and that of his partner. Apart from the cellular systems, cooperation can be used in wireless ad-hoc networks.

In general, a cooperative system model is composed of three entities: a *source* node transmitting the useful information, a *destination* node receiving this information, and a *relay* node relaying the information of the source to the destination.

Since the work of Sendonaris *et al.* [6], [7], a number of cooperation protocols have been proposed. In the following, we present the most important relaying strategies and some of the proposed cooperation protocols.

1.1.2 Relaying Strategies

The relaying strategy defines the nature of the processing performed by the relay node. There are three core families of relaying strategies.

Amplify and Forward

The relay simply acts like a repeater and retransmits a scaled version of what he observed. The amplify-and-forward (AF) is a linear transformation. The low complexity of the AF makes it very attractive for implementation and ships industry. That is why, the AF is the most relaying strategy studied in the literature. However, the major drawback of this strategy is that noise builds up with every retransmission.

Decode and Forward

The relay decodes the hole or a part of the source message. The decoded bits are then re-encoded and re-transmitted to the destination. The decode-and-forward (DF) is a non-linear transformation. It requires more processing at the relay. The DF offers significant advantages, it guarantees an error-free retransmission. However, the relay is interference limited as the number of transmitted messages increases.

Compress-and-Forward

The relay quantizes the received signal form the source and forwards it to the destination without decoding. Unfortunately, noise builds up in the network since no decoding is performed by the relay.

Other relaying strategies were proposed in the literature such as quantize-and-forward, and compute-and-forward. In this thesis, we are particularly interested in the rotate-and-forward (RF) as a linear strategy based on AF, and in the compute-and-forward (CF) as a non-linear strategy. These two strategies will be developed in the upcoming chapters.

1.1.3 Cooperative Protocols

Once the relaying strategy is determined, a cooperation protocol is defined by the transmission frame for a given network topology. The transmission frame states what node is transmitting/receiving at each time slot. The network topology defines the number of sources, destinations, and relaying nodes in a network. The cooperative protocols are named according to the relaying strategies as amplify-and-forward or decode-and-forward protocol.
We note that, in this thesis, we are considering the cooperation protocols on the physical layer.

1.2 Wireless Cooperative Networks

A wireless cooperative network can be build up from a collection of spatially distributed nodes. We connect the source to the destination through a series of nodes. The network is then a set of paths from the source to the destination. We can further impose the constraint

that these paths do not interfere with each other, *i.e.*, they do not have nodes in common.

Any wireless network can be represented by a directed graph. The vertices represent the nodes, and the edges the connectivity between nodes. An edge connecting two nodes points in the transmission direction or in both directions if backflow exists.

A wireless network is characterized by two constraints: broadcast and interference. Under the *broadcast* constraint, all nodes connected to a transmitting node receive the same information. Under the *interference* constraint, the receiving signal at a listinning node is the sum of the signals simultaneously transmitted by all connected transmitting nodes.

In wireless networks, the relay nodes can operate in either full or half-duplex mode. Full-duplex nodes can receive and transmit at the same time. This property allows the nodes to transmit continuously so the data rate is maximized. On the other side, half-duplex nodes can not receive and transmit simultaneously, and the data rate drop down. However, the half-duplex nodes are more considered in the literature and in industrial applications.

1.2.1 Classification of Networks

Throughout the literature, two class of networks are mostly studied. We present here a general classification of these networks. We first consider the two-hop relay network with a direct link between the source and the destination, and second the multi-hop generalizations of the two-hop networks: the KPP and the layered networks. We present a brief review on the prior work concerning these networks. We note that, unless otherwise stated, all networks possess a single source and a single destination.

Two-Hop Networks

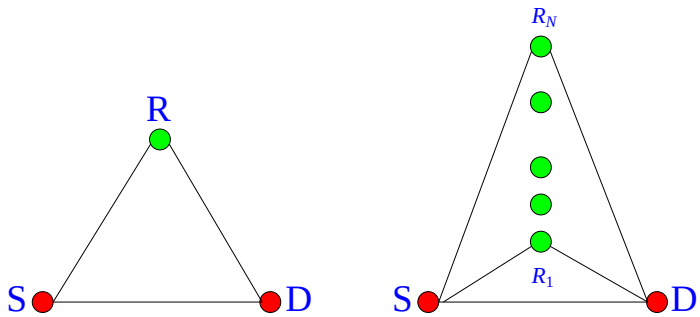


Figure 1.1: Two-hop cooperative relay networks with source-destination link.

Cooperative diversity protocols were first discussed in [8] for the two-hop single-relay network represented in Figure 1.1(a), and then generalized for N relays in [9], Figure 1.1(b).

The authors have proposed an orthogonal amplify-and-forward (OAF) protocol where the source and the relays do not transmit simultaneously.

However, the source should transmit constantly to maximize the multiplexing gain [10]. For this reason the non-orthogonal amplify-and-forward (NAF) has been proposed in [11] for the one-relay case, and then generalized in [10] to the multiple-relay case.

In [12], the authors have proposed the slotted amplify-and-forward (SAF) in order to protect a larger part of the signal. They have shown that these protocols improve upon the performance of the NAF protocols and are optimal if the relays are isolated.

The protocols based on DF are less studied in the literature than the protocols based on AF because they require more processing at the relays, and hence, they are practically more complex. In [8], the authors have proposed a DF protocol whose transmission frame is similar to that of the OAF protocol except for the processing at the relays: the relay decodes and forwards a decoded version of the received signal.

In [11], the authors have proposed another DF protocol to solve the problem of low rate of the previous one. This protocol has the same transmission frame as that of the NAF protocol. The source transmits information during the whole transmission frame. Only half of the source information is decoded and retransmitted by the relays.

In [10], the authors have introduced the dynamic decode-and-forward (DDF) protocol wherein the source transmits during the whole transmission frame, and the listening time duration of the relays depends on the source-relays channel gain.

Several other protocols based on AF and DF have been proposed for these networks. It is worth noting that in the compress-and-forward protocols family, the relays are assumed to know all the fading coefficients in the system [13] [14].

K-Parallel-Path Networks

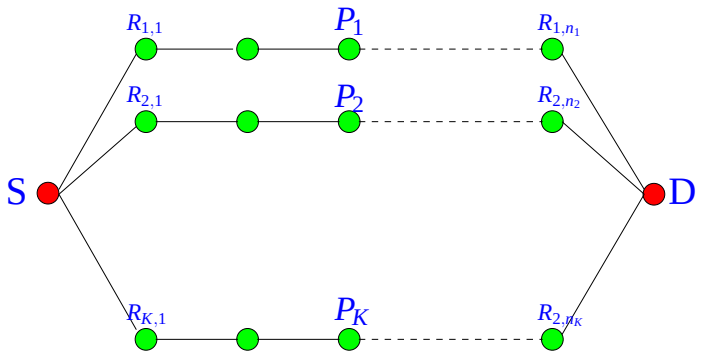


Figure 1.2: The KPP network.

One way of generalizing the two-hop relay network is to consider the network composed of k parallel paths connecting the source to the destination via relays. The communication

takes place through K paths, labeled $P_1, \ldots, P_K$ of lengths $n_1, \ldots, n_K$. The KPP networks can also be considered either with direct source-destination link or with interference between paths.

The authors in [15], [16] have studied these networks in half-duplex mode, and have proposed cooperative protocols based on edge coloring and path-selection strategies. They have also treated the back-flow case, and gave code constructions for all cases.

Layered Networks

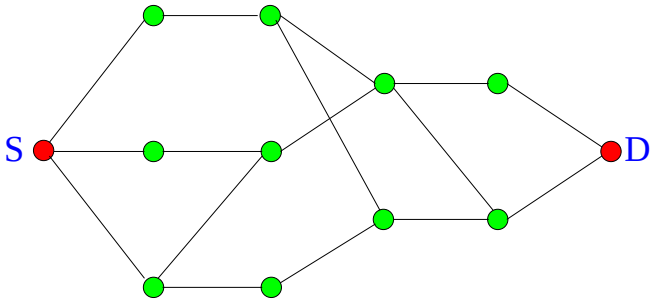


Figure 1.3: A layered network with 4 relaying layers.

An alternative way to generalize the two-hop relay network is to view the two-hop network as a network composed of a single layer of relays. The immediate generalization is to allow for more layers of relays between the source and the destination. In these networks, the links are either between nodes in the same layer or between nodes in adjacent layers. In particular, we are interested in *regular* layered networks having an equal number of relay nodes in all layers.

A quick review on the relaying strategies for these networks will be developed later in Section 1.7.

1.3 System Model

Consider a two-hop relay network composed of one source equipped with n_t transmit antennas, one destination equipped with n_r receive antennas, and one relaying layer. The relaying layer contains N half-duplex relays, each equipped with one antenna. The two-hop network is then denoted by (n_t, N, n_r).

In this model, there is no direct link between the source and the destination. The source transmits its signal to the relays, and the relays retransmit a processed version of the signal to the destination. The processing at the relays depends on the relaying strategy.

Remark 1.1 *In all this thesis, we focus on distributed relaying scheme. A distributed scheme means that the relays are independent and isolated. They don't exchange any information neither about the source's signal nor about the channel state information (CSI).*

Remark 1.2 *$\mathcal{CN}(\mu, \sigma^2)$ represents a complex circular Gaussian distribution with mean μ and variance σ^2.*

1.3.1 Signal Model

Let $\boldsymbol{x}_S \in \mathbb{C}^{n_t \times 1}$ and $\boldsymbol{x}_R \in \mathbb{C}^{N \times 1}$ denote the signals transmitted by the source and the relays respectively. $\boldsymbol{y}_R \in \mathbb{C}^{N \times 1}$ and $\boldsymbol{y}_D \in \mathbb{C}^{n_r \times 1}$ denote the signals received at the relays and the destination respectively.

Let $\boldsymbol{H}_1 \in \mathbb{C}^{N \times n_t}$ and $\boldsymbol{H}_2 \in \mathbb{C}^{n_r \times N}$ be the random matrices modeling the source-relays and relays-destination channels respectively. The channel matrices have Rayleigh statistics. The channel coefficients are independent and identically distributed with zero mean, unit variance, circularly symmetric, with complex Gaussian density, $\mathcal{CN}(0, 1)$. They remain constant during a coherence interval of length L and change independently from one coherence interval to another. The coherence time interval L is large enough in the non-ergodic case. Furthermore, the relays are considered perfectly synchronized. Under these assumptions, the signal model can be written as

$$\boldsymbol{y}_R = \sqrt{\mathrm{SNR}}\boldsymbol{H}_1\boldsymbol{x}_S + \boldsymbol{z}_R \tag{1.1}$$

$$\boldsymbol{y}_D = \sqrt{\mathrm{SNR}}\boldsymbol{H}_2\boldsymbol{x}_R + \boldsymbol{z}_D \tag{1.2}$$

where $\boldsymbol{z}_R \in \mathbb{C}^{N \times 1}$ and $\boldsymbol{z}_D \in \mathbb{C}^{n_r \times 1}$ are the additive white Gaussian noise (AWGN) at the relays and destination respectively. The noise entries are independent and identically distributed with unit variance, *i.e.*, $\boldsymbol{z}_R \sim \mathcal{CN}(0, \boldsymbol{I}_N)$ and $\boldsymbol{z}_D \sim \mathcal{CN}(0, \boldsymbol{I}_{n_r})$. We assume that the transmission is subject to the following power constraint on the source and the relays,

$$\mathbb{E}\left\{\|\boldsymbol{x}_{S/R}\|_F^2\right\} \leq \mathrm{SNR}. \tag{1.3}$$

with SNR being the average signal-to-noise ratio (SNR) per layer, and $\|\boldsymbol{x}\|_F$ is the Frobenius norm of vector $\boldsymbol{x}$. The channel state information is only available at the receivers, no CSI at the transmitters.

1.3.2 Signal Model: Amplify-and-Forward Case

For the two-hop networks, we are interested in linear schemes based on AF. We consider herein the naive AF scheme. In this scheme, each antenna node normalizes the received signal to the same power level and retransmits it. We recall that SNR is the per layer signal-to-noise ratio. The normalization operation can be expressed as,

$$\boldsymbol{x}_R = \boldsymbol{\Delta}\boldsymbol{y}_R \tag{1.4}$$

The power constraint (1.3) gives

$$\mathbb{E}\left\{|\boldsymbol{x}_R(j)|^2\right\} \leq \frac{\mathrm{SNR}}{N}, \quad j = 1, \ldots, N \tag{1.5}$$

the scaling matrix $\boldsymbol{\Delta} \in \mathbb{C}^{N \times N}$ is diagonal. The normalization factors are then

$$\boldsymbol{\Delta}(j,j) = \sqrt{\frac{1}{\frac{\mathrm{SNR}}{n_t}\left(\sum_{k=1}^{n_t} |\boldsymbol{H}_1(j,k)|^2\right) + 1}} \cdot \sqrt{\frac{\mathrm{SNR}}{N}}. \tag{1.6}$$

Therefore, the end-to-end signal model of the channel is

$$\boldsymbol{y}_D = (\boldsymbol{H}_2 \boldsymbol{\Delta} \boldsymbol{H}_1)\, \boldsymbol{x}_S + \boldsymbol{H}_2 \boldsymbol{\Delta} \boldsymbol{z}_R + \boldsymbol{z}_D. \tag{1.7}$$

The whitened form of the channel is

$$\boldsymbol{y} = \boldsymbol{R}^{1/2} \boldsymbol{H}_2 \boldsymbol{\Delta} \boldsymbol{H}_1 \boldsymbol{x}_0 + \boldsymbol{z} \tag{1.8}$$

where $\boldsymbol{z}$ is the whitened noise and $\boldsymbol{R}^{1/2}$ is the whitening matrix with $\boldsymbol{R}^{-1}$ being the covariance matrix of the noise in (1.7).

1.4 Channel Capacity

In a point-to-point scenario, the channel *capacity* dictates the maximum data rate that can be transmitted over a wireless channel with asymptotically small error probability, assuming no constraints on delay or complexity of the encoder and decoder. Channel capacity was settled by Claude Shannon in [17], using the theory of communication based on the mutual information between the input and the output of a channel. Shannon defined capacity C as the mutual information maximized over all input distributions,

$$C = \max_{p(X)} I(X;Y) \tag{1.9}$$

where X is the channel input, Y is the channel output, and $p(X)$ is the channel input distribution. The capacity is measured in bits per channel use (bpcu). It depends only on the channel characteristics.

Shannon have proved the existence of codes that could achieve data rate R close to the capacity with negligible probability of error, and that any data rate higher than capacity could not be achieved without an error probability bounded away from zero.

For a MIMO channel (n_t, n_r), with CSI at the receiver, the instantaneous channel capacity is given by

$$C(\boldsymbol{H}) = \log_2 \det\left(\boldsymbol{I} + \frac{\mathrm{SNR}}{n_t} \boldsymbol{H}\boldsymbol{H}^{\dagger}\right) \tag{1.10}$$

in bpcu, for a given channel realization $\boldsymbol{H} \in \mathbb{C}^{n_r \times n_t}$.

1.4.1 Fast Fading Channel

In a *fast fading* channel, when the channel coherence time is short compared to the delay requirement, the transmission is done over a number of independently faded channel realizations. The capacity can be obtained by averaging the instantaneous capacity (1.10) over all channel realizations. We obtain the *ergodic* capacity as

$$C(\text{SNR}) = \mathbb{E}_{\boldsymbol{H}} \left[C(\boldsymbol{H}) \right]. \tag{1.11}$$

Asymptotically in SNR, it is shown that this equation satisfies [18]

$$C(\text{SNR}) = \min(n_t, n_r) \log(\text{SNR}) + \mathcal{O}(1) \tag{1.12}$$

where $r = \min(n_t, n_r)$ is the maximum number of degrees of freedom available for data transmission. r is called the *multiplexing gain*.

1.4.2 Slow Fading Channel

The situation when the delay requirement is short compared to the channel coherence time, models the *slow fading* channel. In this situation, the channel gain is random but remains constant for all the transmission time. This is also called the *quasi-static* scenario.

If the channel realization $\boldsymbol{H}$ is such that the capacity is less than the transmission rate R, then whatever code that was used by the transmitter, the decoding error probability cannot be made arbitrarily small. Therefore, there is a non-zero probability that the channel is in fade and cannot guarantee a reliable transmission at rate R. Thus, the capacity of the slow fading channel in the strict sense is zero. Alternatively, we can study the probability that the channel capacity falls below the transmission rate R, we call it the *outage probability*..

1.5 Outage Analysis

In a point-to-point channel, the *outage event* occurs when the channel capacity C is lower than the data transmission rate R. The outage probability is defined as

$$\mathrm{P}_{\mathsf{out}}(R) = \mathrm{P}\left\{ C(\boldsymbol{H}) < R \right\} \tag{1.13}$$

The outage probability is a powerful theoretical tool to study the performance of a communication system. However, it is often hard to give an exact characterization of it for each SNR value. As an alternative, we go customarily to characterize the outage probability at high SNR by retrieving two measures: the *diversity order* and the *outage gain* of a channel.

1.5.1 Diversity Order

Definition 1.1 *The diversity order of a channel is defined as the* SNR *exponent of the asymptotic expression of the outage probability. In a log-log scale plot, the diversity order indicates the negative value of the slope of the outage probability curve in function of* SNR *in the high signal-to-noise ratio regime.*

For convenience, we give the following definition.

Definition 1.2 *For each quantity q,*

$$q \doteq \mathrm{SNR}^{\alpha} \quad \textit{means} \quad \lim_{\mathrm{SNR}\to\infty} \frac{\log q}{\log \mathrm{SNR}} = \alpha$$

and similarly for $\dot{\leq}$ and $\dot{\geq}$.

Example: MIMO Channel

For a MIMO channel with capacity given in (1.10), the outage probability is

$$\mathrm{P}_{\mathsf{out},\mathrm{MIMO}}(R) = \mathrm{P}\left\{\log_2 \det\left(\boldsymbol{I} + \frac{\mathrm{SNR}}{n_t}\boldsymbol{H}\boldsymbol{H}^{\dagger}\right) < R\right\} \tag{1.14}$$

Asymptotically in SNR, the outage probability of the MIMO channel decays as

$$\mathrm{P}_{\mathsf{out},\mathrm{MIMO}}(R) \doteq \frac{1}{\mathrm{SNR}^{n_t n_r}} \tag{1.15}$$

$n_t n_r$ is the maximum diversity order of the MIMO channel. The proof is given in Appendix 1.A.1.

1.5.2 Outage Gain

While the diversity order only indicates the slope of the outage probability curve at high SNR, we need to know, sometimes in some applications, the exact outage probability value for a given SNR and data rate R.

Though the outage probability is a natural benchmark for evaluating the performance of communication schemes, the exact characterization of the outage probability remains a difficult task. Instead, a simpler task is to extract the outage gain as SNR goes to infinity, $\mathrm{SNR} \to \infty$, at a given rate R. The outage gain is defined as,

Definition 1.3 *[2] For a given communication scheme with outage probability P_{out} , and a given data rate R, the outage gain with respect to a function $f(\mathrm{SNR})$ is defined as*

$$\xi = \lim_{\mathrm{SNR}\to\infty} f(\mathrm{SNR}) P_{\mathsf{out}}. \tag{1.16}$$

The positive constant ξ, called outage gain, provides useful information on the behavior of $\mathrm{P}_{\mathsf{out}}$ at high SNR.

The outage probability value for a specified SNR and a given rate R is given by the approximation $\mathrm{P}_{\mathsf{out}} \approx \xi f(\mathrm{SNR})$.

In this thesis, we compute the outage gains of different relaying schemes in order to study and compare their performance. For example, if two relaying protocols have the same diversity gain, *i.e.*, the same $f(\mathrm{SNR})$, the one having the smallest outage gain, has the smallest outage probability, and then performs better.

1.6 The Diversity-Multiplexing Tradeoff

1.6.1 Definition and Converse

The Diversity-Multiplexing Tradeoff (DMT) is an approximation that captures the dual benefits of MIMO communication in the high SNR regime: increased data rate and increased reliability. The dual benefits are captured as a fundamental *tradeoff* between these two types of gain.

Let $\mathcal{P}$ be the protocol used across the network. Consider a coding scheme defined by the family of codes, indexed by the signal-to-noise ratio SNR, $\mathcal{X}(\mathrm{SNR})$ with data rate $R(\mathrm{SNR})$ bpcu. The data rate scales with SNR as $R(\mathrm{SNR}) = r \log \mathrm{SNR}$.

Definition 1.4 *The multiplexing gain r and the diversity gain d of a fading channel are defined as follows*

$$r \triangleq \lim_{\mathrm{SNR}\to\infty} \frac{R(\mathrm{SNR})}{\log \mathrm{SNR}}$$

and

$$d(\mathcal{P}, r) \triangleq -\lim_{\mathrm{SNR}\to\infty} \frac{P_{\mathsf{out}}(\mathcal{P}, r \log \mathrm{SNR})}{\log \mathrm{SNR}}$$

$d(\mathcal{P}, r)$ is the diversity-multiplexing tradeoff of the channel and can be indicated as the SNR *exponent of the outage probability in the high* SNR *regime,*

$$P_{\mathsf{out}}(\mathcal{P}, r \log \mathrm{SNR}) \doteq \mathrm{SNR}^{-d(\mathcal{P}, r)} \tag{1.17}$$

The outage exponent $d(r)$ of the network associated to a multiplexing gain r is defined as the supremum of the outage exponents taken over all possible protocols, *i.e.*,

$$d(r) \triangleq \sup_{\mathcal{P}} d(\mathcal{P}, r). \tag{1.18}$$

A coding scheme $\mathcal{X}(\mathrm{SNR})$, operating under a protocol $\mathcal{P}$, is said to achieve multiplexing

gain r and diversity gain $d_{\mathcal{X}}(\mathcal{P}, r)$ if

$$\mathrm{P}_{e,\mathcal{X}}(\mathcal{P}, r \log \mathrm{SNR}) \doteq \mathrm{SNR}^{-d_{\mathcal{X}}(\mathcal{P},r)} \tag{1.19}$$

where $\mathrm{P}_{e,\mathcal{X}}(\mathcal{P}, r \log \mathrm{SNR})$ is the average error probability of the code $\mathcal{X}(\mathrm{SNR})$ with a Maximum Likelihood (ML) decoder.

Using Fano's inequality, it can be shown that for a given protocol (Converse of the DMT [19])

$$d_{\mathcal{X}}(\mathcal{P}, r) \leq d(\mathcal{P}, r). \tag{1.20}$$

The DMT of the channel $d(r)$ is called the *optimal DMT* because it is the supremum of all achievable diversity gains across all possible protocols and coding schemes.

1.6.2 Cut-Set bound on DMT

In any network, the cut-set upper-bound on the mutual information translates into an upper-bound on the achievable DMT [14],

$$d(r) < \min_{w \in \Omega} \{d_w(r)\}. \tag{1.21}$$

where w is a given cut, and Ω is the set of all cuts between the source and the destination. Let $\boldsymbol{H}_w$ be the transfer matrix between nodes on the source-side of the cut and those on the destination-side, $d_w(r)$ is the DMT associated with $\boldsymbol{H}_w$.

An example is given in the Figure 1.4. Using the max-flow min-cut algorithm [20], w_3 corresponds to the minimum cut for which no flow can pass from the source to the destination. As a consequence, the DMT of the transfer channel corresponding to the cut w_3 is the upper-bound on the achievable DMT of the network.

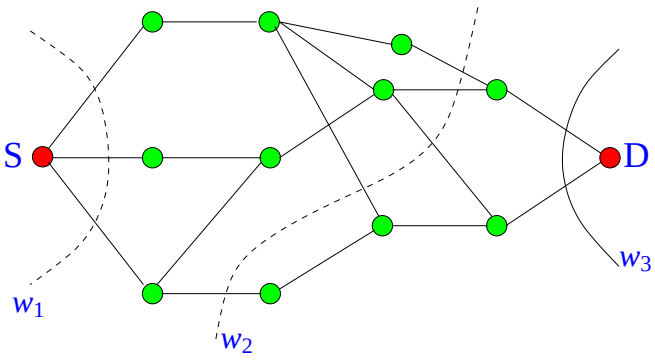


Figure 1.4: Cuts in a network. Here, the min-cut is w_3

1.6.3 Examples of DMT

DMT of the MIMO Channel

Theorem 1.1 *The DMT of a Rayleigh (n_t, n_r) MIMO channel 1.1 is a piece-wise linear function connecting the points $(r, d_{(n_t,n_r)}(r))$ for*

$$r = 0, 1, \ldots, \min(n_t, n_r) \tag{1.22}$$

and

$$d_{(n_t,n_r)}(r) = (n_t - r)(n_r - r). \tag{1.23}$$

Proof: A sketch of the DMT derivation of the MIMO channel is given in Appendix 1.A.2.

The maximum diversity gain and the maximum multiplexing gain are defined by

$$d_{\max} \triangleq d(0) \tag{1.24}$$

$$r_{\max} \triangleq \sup\{r : d(r) > 0\}. \tag{1.25}$$

The maximum diversity gain is obtained for $r = 0$. Thus, the maximum reliability is obtained at a constant data rate R. In addition, the maximum multiplexing gain is obtained for $d = 0$ when no additional protection is provided for the symbols. Between these two extrema, the DMT $d(r)$ is a decreasing function of r (Figure 1.5), hence, increasing the data rate comes at the expense of diversity.

In MIMO case, $d_{\max} = n_t n_r$ and $r_{\max} = \min(n_t, n_r)$.

Remark 1.3 *To achieve the maximum diversity gain, one needs to communicate at a constant data rate R which becomes vanishingly small compared to the fast fading capacity at high* SNR *(which grows like 1.12). Thus, all spatial multiplexing benefits of the MIMO channel are sacrificed to maximize the reliability. To reclaim some benefits, one would instead want to communicate at a rate $R = r \log \mathrm{SNR}$ which is a fraction of the fast fading capacity. Thus, it makes sense to formulate the DMT for a slow fading channel.*

DMT of the Two-Hop (n_t, N, n_r) Channel

Theorem 1.2 *The optimal DMT of a Rayleigh two-hop (n_t, N, n_r) MIMO channel is equivalent to the DMT of a Rayleigh $(N, \min(n_t, n_r))$ MIMO channel.*

Proof: Two channels are said to be DMT-*equivalent* or *equivalent* if they have the same DMT. Applying the cut-set upper-bound Eq.1.21, the optimal DMT of the two-hop channel is equal to

$$d_{(n_t,N,n_r)}(r) = \min\left\{d_{(n_t,N)}(r), d_{(N,n_r)}(r)\right\} \tag{1.26}$$

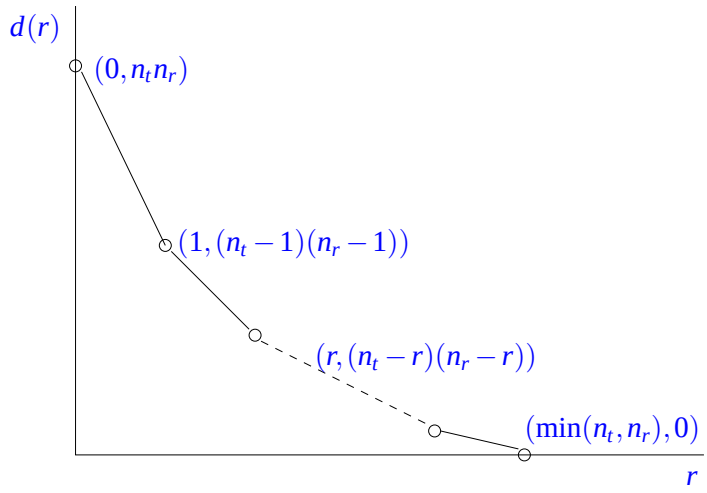


Figure 1.5: DMT of the MIMO Channel

DMT of the AF in the Two-Hop (n_t, N, n_r) Channel

The two-hop relay channel operating under the AF protocol is identified as the *Rayleigh Product* (RP) channel [21]. For convenience, we define the ordered version of a multi-hop channel.

Definition 1.5 *[21] The ordered version of a MIMO multi-hop channel* $(n_0, n_1, \ldots, n_N)$ *is* $\tilde{\boldsymbol{n}} \triangleq (\tilde{n}_0, \tilde{n}_1, \ldots, \tilde{n}_N)$ *with* $\tilde{n}_0 \leq \tilde{n}_1 \leq \ldots \leq \tilde{n}_N$.

The DMT of the RP channel is given in the following theorem.

Theorem 1.3 *[21] The DMT of a Rayleigh Product* (n_t, N, n_r) *channel given in Eq.1.8 is a piecewise linear function connecting the points* $(r, d_{RP}(r))$, $r = 0, 1, \ldots, n_{\min}$, *where*

$$d_{RP}(r) = \sum_{i=r+1}^{n_{\min}} c_i \tag{1.27}$$

with $n_{\min} = \tilde{n}_0$ *and* c_i *given by*

$$c_i \triangleq 1 - i + \min_{k=1,2} \left\lfloor \frac{\sum_{l=0}^{k} \tilde{n}_l - i}{k} \right\rfloor, \quad i = 1, \ldots, n_{\min} \tag{1.28}$$

As it was shown in [15] that the colored noise for all AF protocols can be treated as white as long as the DMT is of our interest, the covariance matrix $\boldsymbol{R}$ in Eq.1.8 can be neglected in the DMT analysis and the RP channel is equivalent to the MIMO channel defined by the matrix $\boldsymbol{H}_2\boldsymbol{H}_1$. A consequence of Theorem 1.3 is summarized in Corollary 1.1.

Corollary 1.1 *(Permutation invariance [21]). The DMT of a RP channel depends only on the ordered version* $\tilde{\boldsymbol{n}}$.

1.7 Relaying Strategies for Multi-Hop Networks

In multi-hops settings, cooperative diversity was first studied by Jing and Hassibi in [22] for the two-hop networks with single-antenna nodes and without a direct link between source and destination, and then in [23] for multi-antenna case, with distributed space-time coding. They have studied protocols where the relays apply linear transformations on the received signals before retransmission.

In [24], Rao and Hassibi have considered the two-hop half-duplex multi-antenna cooperative networks and have provided an AF scheme and compute the DMT achieved by this scheme. Their scheme incurs a rate loss of a factor of two compared to the cut-set bound.

In [21], Yang and Belfiore have considered the MIMO multi-hop networks operating under the Amplify-and-Forward (AF) protocol. They have proved that the AF channel is equivalent, in the DMT sense, to the Rayleigh product (RP) channel and have given an exact characterization of the DMT of the AF scheme in multi-hop networks of arbitrary size. While the AF scheme achieves the maximum multiplexing gain, it fails in achieving the maximum diversity gain in all the multi-hop networks. The Flip-and-Forward (FF) protocol, also proposed in [21], allows to achieve both the maximum diversity and multiplexing gains in multi-hop networks.

Borade, Zheng and Gallager in [25] have considered AF schemes on a class of layered multi-hop networks where each layer has the same number of relays. They showed that AF strategies are optimal in terms of multiplexing gain. They also computed lower bounds on the DMT of the Rayleigh product channel.

Gharan, Bayesteh, and Khandani in [26] have proposed the multiplication by a random unitary matrix at the relay nodes. This multiplication used in a Random-Sequential (RS) scheme, proposed in [27], allows to achieve the optimal DMT in multi-antenna multi-hop networks consisting of one source, one destination, and full-duplex relays with exactly one relay in each hop.

Avestimehr, Diggavi and Tse have proposed a non-linear scheme called Quantize-and-Forward (QF) in [28]. This scheme is shown to achieve any rate within a constant gap to the capacity of the channel and thus attains the optimal DMT of the considered channel.

Recently, Yang and Belfiore have proposed a linear relaying scheme called Rotate-and-Forward in [1]. The idea is to convert the spatial diversity into time diversity by creating an artificial fast fading channel using time-varying distributed rotations. They have shown that time-varying distributed rotations can recover spatial diversity. This scheme is shown to achieve the optimal DMT in the two-hop relay networks with an arbitrary number of

antennas at the source, destination and relays [4]. RF is a distributed relaying scheme, the relays are independent and act in a distributed fashion. On the contrary, in the RS scheme proposed in [26], full cooperation is needed where the restriction to one relay in each layer.

1.8 Conclusion

In this chapter, we gave a general overview on the cooperative communication. We introduce the cooperative diversity techniques and the major families of relaying strategies as seen in the literature. We also present the major classifications of the cooperative network and the proposed cooperative protocols. Moreover, we gave the information theoretic tools used to evaluate and compare the performance of these protocols, namely, the outage probability, the outage gain, and the diversity-multiplexing tradeoff.

In the next chapter, we are particularly interested in the two-hop relay networks. For this, we examine the linear rotate-and-forward protocol (RF). We evaluate the performance of this protocol in terms of outage gain for some network configurations. We compare its performance to that of other protocols having the same diversity gain. Furthermore, we assume the existence of a limited feedback channel between the destination and the relays and show how to use this feedback channel to improve the performance of the RF scheme.

1.A Proofs

1.A.1 Proof of Example 1.5.1

The MIMO channel matrix $\boldsymbol{H}$ is a $n_r \times n_t$ matrix with complex zero-mean unit-variance Gaussian *i.i.d* components. Let $q = \min(n_t, n_r)$. The outage probability is given by

$$\begin{aligned} \mathrm{P}_{\mathsf{out},\mathrm{MIMO}}(R) &= \mathrm{P}\left\{\log_2 \det\left(\boldsymbol{I} + \frac{\mathrm{SNR}}{n_t}\boldsymbol{H}\boldsymbol{H}^\dagger\right) < R\right\} \\ &= \mathrm{P}\left\{\sum_{i=1}^{q} \log\left(1 + \frac{\mathrm{SNR}}{n_t}\mu_i^2\right) < R\right\} \end{aligned} \tag{1.29}$$

where μ_i's are the singular values of the matrix $\boldsymbol{H}$. The MIMO channel exhibits q modes of transmission, each corresponding to an instantaneous SNR equal to $\left(\mathrm{SNR}\mu_i^2\right)/n_t$. Depending on the instantaneous SNR, a transmission mode can be *effective* if $(\mathrm{SNR}\mu_i^2)/n_t$ is of order SNR, or *not effective* if $(\mathrm{SNR}\mu_i^2)/n_t$ is of order 1 or less.

An outage event occurs when none of the q channel modes is effective which means that all μ_i^2 are of order $1/SNR$ or less. Since

$$\sum_{i=1}^{q} \mu_i^2 = \mathrm{Tr}(\boldsymbol{H}\boldsymbol{H}^\dagger) = \sum_{i,j} |h_{i,j}|^2 \tag{1.30}$$

an outage event can be equivalently defined as the event where each $|h_{i,j}|^2$ is of order $1/\mathrm{SNR}$ or less. Since all $|h_{i,j}|^2$ are independent and $\mathrm{P}\left\{|h_{i,j}|^2 < 1/\mathrm{SNR}\right\} \approx 1/\mathrm{SNR}$ [19], the corresponding outage probability is

$$\begin{aligned} \mathrm{P}_{\mathsf{out},\mathrm{MIMO}}(R) &= \mathrm{P}\left\{\bigcap_{i,j}\left(|h_{i,j}|^2 < 1/\mathrm{SNR}\right)\right\} \\ &\doteq \frac{1}{\mathrm{SNR}^{n_t n_r}} \end{aligned} \tag{1.31}$$

The channel diversity order of the MIMO channel is $n_t n_r$.

1.A.2 Proof of Theorem 1.1

The procedure of [29] is followed. The transmission rate R scales with SNR as $R = r \log \mathrm{SNR}$. At high SNR, (1.29) gives

$$\mathrm{P}_{\mathsf{out},\mathrm{MIMO}}(r\log \mathrm{SNR}) = \underbrace{\mathrm{P}\left\{\log_2 \det\left(\boldsymbol{I}_{n_r} + \mathrm{SNR}\boldsymbol{H}\boldsymbol{H}^\dagger\right) < r\log \mathrm{SNR}\right\}}_{\mathcal{O}_{\boldsymbol{H}}(r,\mathrm{SNR})} \tag{1.32}$$

$$\doteq \underbrace{\mathrm{P}\left\{\sum_{i=1}^{q}\log\left(1+\mathrm{SNR}\lambda_i\right) < r\log\mathrm{SNR}\right\}}_{\mathcal{O}_{\boldsymbol{\lambda}(r,\mathrm{SNR})}} \tag{1.33}$$

$$\doteq \mathrm{P}\left\{\sum_{i=1}^{q}(1-\alpha_i)^{+} < r\right\} \tag{1.34}$$

$$\doteq \underbrace{\mathrm{P}\left\{\sum_{i=1}^{k}\alpha_i > k-r,\ \forall k=1,\ldots,q\right\}}_{\mathcal{O}_{\boldsymbol{\alpha}}(r,\mathsf{SNR})} \tag{1.35}$$

where $\boldsymbol{\lambda}$ is the vector of eigenvalues of the matrix $\boldsymbol{H}\boldsymbol{H}^{\dagger}$ in a decreasing order, and $\boldsymbol{\alpha}$ the vector of the eigen-exponents corresponding to $\boldsymbol{\lambda}$, *i.e.*, $\lambda_i = \mathsf{SNR}^{-\alpha_i}$. q is the rank of the channel matrix. $\mathcal{O}_{\boldsymbol{H}}$, $\mathcal{O}_{\boldsymbol{\lambda}}$, and $\mathcal{O}_{\boldsymbol{\alpha}}$ are three representations of the outage region of the channel. The DMT is calculated on the region $\mathcal{O}_{\boldsymbol{\alpha}}$:

$$\begin{aligned}\mathrm{P}_{\mathsf{out},\mathrm{MIMO}}(r\log\mathrm{SNR}) &= \mathrm{P}\left\{\mathcal{O}_{\alpha}(r,\mathrm{SNR})\right\}\\ &= \int_{\mathcal{O}_{\alpha}} p(\boldsymbol{\alpha})d\boldsymbol{\alpha}\\ &\doteq \mathrm{SNR}^{-\inf_{\mathcal{O}_{\boldsymbol{\alpha}}}E(\boldsymbol{\alpha})}\end{aligned} \tag{1.36}$$

where, for a (n_t, n_r) Rayleigh channel, it can be shown that the SNR exponent of the pdf of $\boldsymbol{\alpha}$, $E(\boldsymbol{\alpha})$, is given by

$$E(\boldsymbol{\alpha}) = \sum_{i=1}^{q}(2k-1+|n_t-n_r|)\alpha_i \tag{1.37}$$

The DMT of the (n_t, n_r) MIMO channel can be calculated as

$$d(r) = \inf_{\mathcal{O}_{\boldsymbol{\alpha}(r)}} E(\boldsymbol{\alpha}) \tag{1.38}$$

$\mathcal{O}_{\boldsymbol{\alpha}(r)}$ being the outage region with

$$\mathcal{O}_{\boldsymbol{\alpha}(r)} \triangleq \{\boldsymbol{\alpha} : f(\boldsymbol{\alpha}) < r\} \tag{1.39}$$

The solution of (1.38) gives the equation (1.23) and concludes the proof.

Chapter 2

Rotate-and-Forward: Performance in the Two-Hop Relay Networks

COOPERATIVE diversity techniques are attractive candidates for improving the throughput and reliability of wireless networks in the new generations of wireless communication systems. The idea behind the cooperative systems is to emulate the Multiple-Input Multiple-Output (MIMO) systems to take benefits from the spatial diversity.

The cooperative protocols proposed in the literature, were compared in terms of diversity-multiplexing-tradeoff (DMT). This tool was introduced by Zheng and Tse in [19] to evaluate the point-to-point MIMO schemes in slow fading scenarios at high signal-to-noise ratio (SNR). In a given network, the question is whether a cooperative protocol can achieve the optimal DMT for all the range of multiplexing gain.

This chapter is devoted to the two-hop MIMO relay networks where no direct source-destination link is present. For these networks, a general overview of the proposed relaying strategies is given in Section 1.7. In particular, we consider the rotate-and-forward (RF) relaying protocol proposed by Yang and Belfiore in [1]. The chapter is organized as follows. The Section 2.1 introduces the system model. The Section 2.2 gives a general idea about the RF protocol. In Section 2.3, we consider different networks and we study the performance of the RF using the outage gain criterion. We compare the performance of the RF to that of other relaying protocols having the same diversity. Finally, in Section 2.4, we assume that a feedback channel exists between the destination and the relays, and we use this channel to improve the performance of the RF scheme.

2.1 Network and System Model

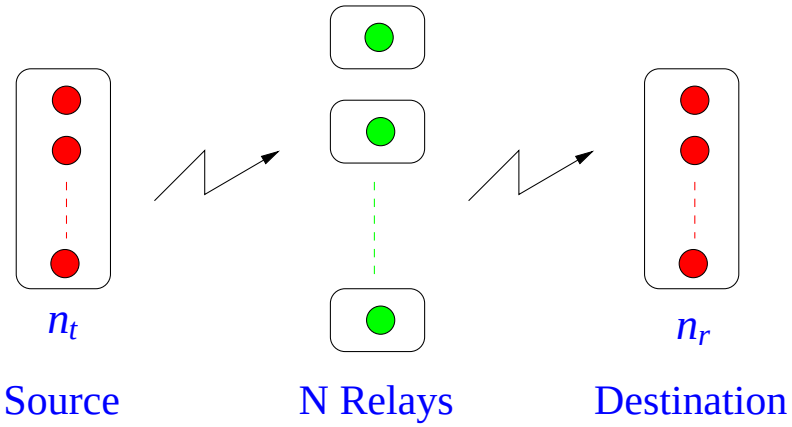


Figure 2.1: Two-hop cooperative relay networks without source-destination link.

Consider one source with n_t transmitting antennas, one destination with n_r receiving antennas, and N half-duplex single-antenna relays, clustered in one layer between the source and the destination. The system is denoted by (n_t, N, n_r), where N becomes the number of antennas at the relaying layer.

The relays are assumed to be isolated. The source signal is then the only signal received by a relay. The relay retransmits the received signal to the destination. There is no information exchange concerning the message or the channel state information (CSI) between relays. The CSI are only available at the receiver side, no transmitter CSI at all. All terminals are considered perfectly synchronized. We assume that the destination knows the topology of the network, *i.e.*, it knows the number of *active* relays: relays who are rotate-forwarding the source signal.

2.1.1 Fading Channel

The faded sub-channels have Rayleigh statistics. The channel coefficients are flat, quasi-static. Let $\boldsymbol{H}_1$ and $\boldsymbol{H}_2$ be the respective channel matrices of the source-relays and relays-destination links. $\boldsymbol{H}_1$ and $\boldsymbol{H}_2$ are independent, and have i.i.d. complex circular Gaussian entries, h_k, with mean zero and variance σ_k^2. For convenience, we give the following definitions.

Definition 2.1 *For a random variable x, $f_X(x)$ is the probability density function.*

Definition 2.2 *Let $u : \mathbb{R}^N \to \mathbb{R}$ be a real function and $\mathcal{S}$ be a subset of $\mathbb{R}$. We denote by $\mathbf{1}\{u \in \mathcal{S}\}$ the indicator function of the subset $\left\{x \in \mathbb{R}^N : u(x) \in \mathcal{S}\right\}$.*

We associate to each channel coefficient h_k a power gain defined as $g_k = |h_k|^2$. The power gain g_k is a random variable with density function $f_{G_k}(g_k)$ which is right continuous at zero and admits a positive limit denoted by $c_k = f_{G_k}(0^+)$. For example, in the Rayleigh case, if h_k

is complex Gaussian with mean 0 and variance σ_k^2, then g_k has the exponential distribution $f_{G_k}(g_k) = \sigma_k^{-2} \exp\left\{-g_k/\sigma_k^{-2}\right\} \mathbf{1}\left\{g_k > 0\right\}$, and then $c_k = \sigma_k^{-2}$.

We assume an additive white Gaussian noise (AWGN) at the receiving nodes. Depending on the settings, we might sometimes consider that the relays are noiseless.

2.2 The Rotate-And-Forward Protocol

In relay networks, the distributed space-time processing at the relays is a conventional way to exploit spatial diversity. Interestingly, Yang and Belfiore showed in [1] than even simple time-varying distributed rotations can recover spatial diversity. The idea is to convert the spatial diversity into time diversity by creating an artificial fast fading channel using time-varying distributed rotations.

This framework is quite general and can be applied to a wide range of linear and nonlinear relaying strategies. In particular, the authors applied this strategy to multi-antenna two-hop layered networks. They called their scheme the rotate-and-forward (RF).

The RF is a linear relaying strategy based on AF. Its attractiveness is due to its low complexity. In this relaying protocol, each relay rotates the received signal and retransmits it to the destination. The rotation angles are chosen f on a distributed rotation sequence (DRS) defined hereafter,

Definition 2.3 *[1] Define a set of L equally spaced angles in $[0, 2\pi)$ and the corresponding set of complex rotations as follows,*

$$\mathcal{A}_L \triangleq \left\{0, \frac{2\pi}{L}, \ldots, \frac{2(L-1)\pi}{L}\right\}$$

$$\mathcal{R}_L \triangleq \{e^{j\theta} | \theta \in \mathcal{A}_L\}.$$

A sequence of diagonal matrices Δ_t, $t = 1, \ldots, L^N$ is said to be a distributed rotation sequence (DRS) if

1. $\Delta_t = diag\{\xi_t\}$ *with* $\xi_t \in \mathcal{R}_L^{N\times 1}$,
2. $\Delta_t \neq \Delta'_t, \forall t \neq t'$.

A sequence of rotation vectors $\boldsymbol{\theta}_1, \ldots, \boldsymbol{\theta}_T$ is defined based on a distributed rotation sequence where $\boldsymbol{\theta}_i \triangleq [\theta_{i,1}, \ldots, \theta_{i,N}]^T$. For two time instants $i \neq i', \forall i, i'$, we have that $\boldsymbol{\theta_i} \neq \boldsymbol{\theta_{i'}}$. A codeword $\boldsymbol{X} \in \mathbb{C}^{n_t \times T}$ is transmitted by the source over T symbol times. At symbol time i, the relay j rotates the signal received at symbol time $i-1$ by the angle $\theta_{i,j}$. Thus, by ignoring the power normalization terms in Eq.1.7 and introducing the time index i, the end-to-end input-output relation is

$$\boldsymbol{y}_D[i+1] = \boldsymbol{H}_2 \boldsymbol{F}_i \boldsymbol{H}_1 \boldsymbol{x}[i] + \boldsymbol{H}_2 \boldsymbol{F}_i \boldsymbol{z}_R[i] + \boldsymbol{z}_D[i+1], \tag{2.1}$$

$\boldsymbol{x} \in \mathbb{C}^{n_t \times 1}$ is the transmitted signal from the source, and $\boldsymbol{y}_D \in \mathbb{C}^{n_r \times 1}$ is the received signal at the destination. $\boldsymbol{z}_R \sim \mathcal{CN}(0, \boldsymbol{I}_N)$, and $\boldsymbol{z}_D \sim \mathcal{CN}(0, \boldsymbol{I}_{nr})$ are the additive white Gaussian noise (AWGN) at the relays and destination respectively. $\boldsymbol{H}_1 \in \mathbb{C}^{N \times n_t}$ and $\boldsymbol{H}_2 \in \mathbb{C}^{n_r \times N}$ are the channel matrices. The rotations performed by the relays at a symbol time i, can be presented by a diagonal matrix $\boldsymbol{F}_i$ defined as $\boldsymbol{F}_i \triangleq \text{diag}\big(e^{j\theta_{i,1}}, \ldots, e^{j\theta_{i,N}}\big)$.

In this setting, the transmitted codeword $\boldsymbol{X}$ goes through an equivalent time-varying fading channel and the equivalent channel of the RF scheme is the sequence $\boldsymbol{H}_2\boldsymbol{F}_1\boldsymbol{H}_1, \ldots,$ $\boldsymbol{H}_2\boldsymbol{F}_T\boldsymbol{H}_1$. The covariance matrix of the equivalent noise in Eq.2.1 is $\boldsymbol{\Sigma}_{\boldsymbol{z}}[i] = \boldsymbol{I} + \boldsymbol{H}_2\boldsymbol{F}_i\boldsymbol{F}_i^H\boldsymbol{H}_2^H$.

The eigenvalues of $\boldsymbol{\Sigma}_{\boldsymbol{z}}$ satisfy $\lambda_{\max}(\boldsymbol{\Sigma}_{\boldsymbol{z}}[t]) \doteq \lambda_{\min}(\boldsymbol{\Sigma}_{\boldsymbol{z}}[t]) \doteq \mathsf{SNR}^0$. It was proven in [15], that the colored noise for all AF protocols can be treated as white as long as the DMT is of our interest. Therefore, the DMT of the RF protocol depends uniquely on the time-variant equivalent channel matrix $\boldsymbol{H} \triangleq \boldsymbol{H}_2\boldsymbol{F}_i\boldsymbol{H}_1$.

The average mutual information for a given channel realization is

$$\frac{1}{T}\sum_{i=1}^{T} \log\det\Big(\boldsymbol{I} + \mathsf{SNR}(\boldsymbol{H}_2\boldsymbol{F}_i\boldsymbol{H}_1)(\boldsymbol{H}_2\boldsymbol{F}_i\boldsymbol{H}_1)^\dagger\Big).$$

With a large T, the average mutual information converges to the following term,

$$I_{\mathsf{avg}} = \mathbb{E}_{\theta_i}\left\{\log\det\Big(\boldsymbol{I} + \text{SNR}\left(\boldsymbol{H}_2\boldsymbol{F}_i\boldsymbol{H}_1\right)\left(\boldsymbol{H}_2\boldsymbol{F}_i\boldsymbol{H}_1\right)^\dagger\Big)\right\} \tag{2.2}$$

The RF scheme is a DMT-optimal cooperative protocol in the two-hop relay networks. This scheme is shown to achieve the optimal DMT in a two-hop relay network with two antennas at the relay node in [1], and for an arbitrary number of antennas at the source, relay and destination nodes in [4]. The optimal DMT is a piece-wise linear function connecting the points $(k, d^{(RF)}(k))$ for $k = 1, \ldots, \min(n_{min}, N)$ and

$$d^{(RF)}(k) = (N-k)(n_{min}-k), \tag{2.3}$$

where $n_{min} = \min\{n_t, n_r\}$, k is the multiplexing gain and d is the diversity gain.

2.3 Outage Gains in the Two-Hop Networks

The aim of this section is to study the performance of the rotate-and-forward protocol in the two-hop relay networks. We take the outage gain as a performance measure. In particular, we study the outage probability behavior as the signal-to-noise ratio tends to infinity, and extract the outage gains for some relaying protocols in some networks.

We consider two network configurations: the (1, N, 1) and the (M, 1, M) networks, and we compute the outage gains in function of the number of relays N, the number of antennas

M, the transmission rate R, and the channel variances σ^2's. The outage gain gives us useful information to obtain the outage probability asymptotically at high signal to noise ration SNR.

We consider the (1, N, 1) network under three different relaying protocols; RF, orthogonal RF and relay-selection protocols. The (M, 1, M) is only considered under the RF protocol. As a beginning, and for sake of simplicity, we assume that the source-relays links are noiseless. This assumption could be motivated as if the relays are close to the source and benefit from a high signal to noise ratio. Then, the second term in Eq.2.1 is ignored, and the input-output relation becomes,

$$\boldsymbol{y}_D[i+1] = \boldsymbol{H}_2\boldsymbol{F}_i\boldsymbol{H}_1\boldsymbol{x}[i] + \boldsymbol{z}_D[i+1]. \tag{2.4}$$

Later in this paper, the RF protocol with noisy source-relays links is reconsidered for the (1, N, 1) networks. In the following, we omit the time index for simplicity.

2.3.1 The RF Protocol in the Two-Hop (1, N, 1) Network

Consider a two-hop (1, N, 1) relay network operating under the rotate-and-forward protocol. We give the outage gain of this scheme at high signal-to-noise ration (SNR) in Theorem 2.1.

Theorem 2.1 *Consider a (1, N, 1) relay network operating under the rotate-and-forward protocol, the outage gain at high signal-to-noise ration and a given transmission rate R is*

$$\xi_{(1,N,1),RF} = \frac{(2^R-1)^N}{N!}\prod_{k=1}^{N}\sigma_{1k}^{-2}\sigma_{2k}^{-2}. \tag{2.5}$$

σ_{1k}^{-2} and σ_{2k}^{-2} are the variances of the channel coefficients in the first and second hops respectively.

Proof: Let the channel matrices of the first and second hops be $\boldsymbol{H}_1 = [h_{11}\dots h_{1N}]^T$ and $\boldsymbol{H}_2 = [h_{21}\dots h_{2N}]$ respectively. Let $\boldsymbol{F} = \text{diag}\{e^{i\theta_1},\dots,e^{i\theta_N}\}$ be the rotation matrix. The equivalent channel matrix is $\boldsymbol{H} = \boldsymbol{H}_2\boldsymbol{F}\boldsymbol{H}_1$. Using Eq.2.2, the mutual information of the channel can be written as,

$$I_{\mathsf{avg}} = \mathbb{E}_{\boldsymbol{\theta}}\left\{\log\left\{a + \sum_{k=1}^{N-1}\sum_{l=k+1}^{N} b_{lk}\cos(\theta_k - \theta_l + \varphi_{lk})\right\}\right\}, \tag{2.6}$$

with

$$a = 1 + \text{SNR}\sum_{k=1}^{N} g_{1k}g_{2k}$$

$$b_{lk} = 2\text{SNR}|h_{1l}h_{2l}h_{1k}^*h_{2k}^*|.$$

$g_{lk} = |h_{lk}|^2$ are the channels power gains with variances σ_{lk}^2, and a is independent of θ_k. According to Theorem 1 in [1], the average mutual information satisfies

$$\log(a) - (N-1) < I_{\mathsf{avg}} < \log(a). \tag{2.7}$$

Hence, for a SNR $\to \infty$ and for a large rate R, the mutual information of the channel depends only on a, and the outage probability expression is simplified to

$$P_{\mathsf{out}} = \mathsf{Prob}\left\{\mathbb{E}_{\boldsymbol{\theta}}\left\{\log\det(\boldsymbol{I} + \mathrm{SNR}\boldsymbol{H}\boldsymbol{H}^{\dagger})\right\} < R\right\} \doteq \mathsf{Prob}\left\{\log(a) < R\right\}. \tag{2.8}$$

Using an appropriate function $f(\mathrm{SNR})$, we need to show that $f(\mathrm{SNR})P_{\mathsf{out}}$ converges to a positive constant, the outage gain ξ, as SNR $\to \infty$. The function $f(\mathrm{SNR})$ contains information on the diversity order that can be achieved by the cooperative scheme.

Let $g_{1k}g_{2k} = g_k$. We have

$$P_{\mathsf{out}} = \int \mathbf{1}\left\{(g_1, \ldots, g_N) \in \mathbb{R}_+^N : \log(a) < R\right\} f_{G_1}(g_1) \ldots f_{G_N}(g_N) \prod_{k=1}^{N} dg_k.$$

$f_{G_k}(g_k)$ is the probability density function (pdf) of g_k. By making the change of variables $x_k = \mathrm{SNR}g_k$, the outage probability becomes

$$P_{\mathsf{out}} = \mathrm{SNR}^{-N} \int \mathbf{1}\left\{(x_1, \ldots, x_N) \in \mathbb{R}_+^N : \log(a) < R\right\} f_{G_1}(x_1/\mathrm{SNR}) \ldots f_{G_N}(x_N/\mathrm{SNR}) \prod_{k=1}^{N} dx_k.$$

g_k is the product of 2 independent central chi-square variates of two degrees of freedom each with respective variances σ_{1k}^2 and σ_{2k}^2. Its density function is right continuous at zero and admits a positive limit, c_k. Then, $f_{G_k}(x_k/\mathrm{SNR})$ satisfies as SNR $\to \infty$

$$c_k \triangleq f_{G_k}(g_k \propto \frac{1}{\mathrm{SNR}}) = \sigma_{1k}^{-2}\sigma_{2k}^{-2} \ln \mathrm{SNR}. \tag{2.9}$$

The details are deferred to Appendix 2.A.2. We exchange integration and limits (uniform convergence satisfied), and we obtain the outage gain as

$$\begin{aligned}\xi = \lim_{\mathrm{SNR}\to\infty} f(\mathrm{SNR})\mathrm{SNR}^{-N} \prod_{k=1}^{N} \sigma_{1k}^{-2}\sigma_{2k}^{-2} \ln \mathrm{SNR} \\ \times \int \mathbf{1}\left\{(x_1, \ldots, x_N) \in \mathbb{R}_+^N : \log(a) < R\right\} \prod_{k=1}^{N} dx_k.\end{aligned} \tag{2.10}$$

The integration in Eq.2.10 is described by the following equation set,

$$0 < x_k < 2^R - 1 - \sum_{l=1}^{k-1} x_l, \qquad k = 1, \ldots, N.$$

Thus, after simple derivations

$$\int \mathbf{1}\left\{(x_1,\ldots,x_N)\in\mathbb{R}_+^N : \log(a) < R\right\} \prod_{k=1}^{N} dx_k = \frac{(2^R-1)^N}{N!}. \tag{2.11}$$

We choose $f(\mathrm{SNR}) = \frac{\mathrm{SNR}^N}{(\ln \mathrm{SNR})^N}$. With this, we obtain the outage gain of a (1, N, 1) network operating under the RF protocol in a closed form as in Theorem 2.1 and conclude the proof.

In the (1, N, 1) network, the maximal achievable diversity is N, then one may say that $f(\mathrm{SNR}) = \mathrm{SNR}^N$ is immediate. However, the outage probability expression has a term which decays even slower than SNR^{-N}, and we would ideally want to capture its coefficients to understand the asymptotic behavior of the outage probability. That explain the choice of $f(\mathrm{SNR}) = \frac{\mathrm{SNR}^N}{(\ln \mathrm{SNR})^N}$.

$f(\mathrm{SNR})^{-1}$ gives the negative slope of the outage probability curve as $\mathrm{SNR}\to\infty$. The outage gain ξ is a scaling factor.

As we have mentioned before, the outage gain could be used to compare the performance of different protocols if they have the same diversity. In this scope, we will compute in the next sections, the outage gain values for protocols having the same diversity of that of the RF scheme in order to compare their performances.

2.3.2 The Orthogonal RF Protocol in the Two-Hop (1, N, 1) Network

Reconsider the two-hop (1, N, 1) relay network with the orthogonal RF protocol. At each symbol time, only one relay, chosen arbitrarily, rotate-forwards its received signal. We assume the same power budget at the relays. For this scheme, we derive the outage gain at high signal-to-noise ratio (SNR) as shown in Theorem 2.2.

Theorem 2.2 *Consider a (1, N, 1) relay network operating under the orthogonal rotate-and-forward protocol, the outage gain at high signal-to-noise ration and a given transmission rate R is*

$$\xi_{(1,N,1),ORF} = I_N(N,R)\prod_{k=1}^{N}\sigma_{1k}^{-2}\sigma_{2k}^{-2}. \tag{2.12}$$

σ_{1k}^{-2} and σ_{2k}^{-2} are the variances of the channel coefficients in the first and second hops respectively. $I_N(N,R)$ is given recursively as

$$I_n(N,R) \;=\; \frac{2^{NR}}{(N-1)!}\left(\ln 2^{NR}\right)^{N-1} - I_{n-1}(N,R), \qquad n=1,\ldots N,$$

with

$$\begin{aligned} I_1(N,R) &= 2^{NR}-1 \\ I_2(N,R) &= 2^{NR}\ln(2^{NR}) - I_1(N,R). \end{aligned}$$

Proof: The system is in outage if the average mutual information fall down under the transmission rate. The outage probability expression can be written as,

$$\begin{aligned} \mathbf{P}_{\mathsf{out}} &= \mathsf{Prob}\left\{\frac{1}{N}\sum_{k=1}^{N}\log\left(1+\mathrm{SNR}|h_{1k}|^2|h_{2k}|^2\right) < R\right\} \\ &= \mathsf{Prob}\left\{\prod_{k=1}^{N}(1+\mathrm{SNR}g_k) < 2^{NR}\right\}, \end{aligned} \tag{2.13}$$

where $g_k = |h_{1k}|^2|h_{2k}|^2$ and $h_{lk} \sim \mathcal{CN}(0,\sigma_{lk}^2)$. Let $x_k = \mathrm{SNR}g_k$, the outage gain becomes

$$\begin{aligned} \xi &= \lim_{\mathrm{SNR}\to\infty} f(\mathrm{SNR})\mathrm{SNR}^{-N}\int \mathbf{1}\left\{(x_1,\ldots,x_N)\in\mathbf{R}_+^N : \prod_{k=1}^{N}(1+x_k) < 2^{NR}\right\} \\ &\qquad \times f_{G_1}(x_1/\mathrm{SNR})\ldots f_{G_N}(x_N/\mathrm{SNR})\prod_{k=1}^{N}dx_k. \end{aligned} \tag{2.14}$$

$f_{G_k}(x_k/\mathrm{SNR})$ satisfies Eq.2.9. The integration in Eq.2.14 is described by the following equations set:

$$0 < x_k < \frac{2^{NR}-1-\sum_{l=1}^{k-1}E_l(x_1,\ldots,x_{k-1})}{1+\sum_{l=1}^{k-1}E_l(x_1,\ldots,x_{k-1})}, \qquad k=1,...N.$$

The functions $E_l(x_1,\ldots,x_n)$ are defined as follows:

$$E_l(x_1,\ldots,x_n) = \sum_{\substack{p_1,\ldots,p_l\in\{1,\ldots,n\}\\ p_1<\ldots<p_l}} x_{p_1}\ldots x_{p_l}.$$

In other words, $E_l(x_1,\ldots,x_n)$ is the coefficient of the term x^{n-l} in the polynomial $\prod_{k=1}^{n}(x+x_k)$.

After derivation, the integration in Eq.2.14 can be given in a recursive manner as:

$$I_n(N,R) = \frac{2^{NR}}{(N-1)!}\left(\ln 2^{NR}\right)^{N-1} - I_{n-1}(N,R), \quad n=1,\ldots N, \tag{2.15}$$

with

$$\begin{aligned} I_1(N,R) &= 2^{NR}-1 \\ I_2(N,R) &= 2^{NR}\ln(2^{NR}) - I_1(N,R). \end{aligned}$$

As in the previous case, we choose $f(\mathrm{SNR}) = \dfrac{\mathrm{SNR}^N}{(\ln \mathrm{SNR})^N}$. With this, the outage gain of the (1, N, 1) network operating under the orthogonal rotate-and-forward (ORF) protocol is given in a closed form as in Theorem 2.2. End of the proof.

2.3.3 The Relay Selection Protocol in the Two-Hop (1, N, 1) Network

In this section, we start by establishing a lower bound on the average mutual information of the RF scheme. Based on this lower bound, we extract the outage gain of the relay-selection (RS) scheme in the (1, N, 1) networks. We state the result in Theorem 2.3.

Theorem 2.3 *Consider a (1, N, 1) relay network operating under the relay-selection rotate-and-forward protocol, the outage gain at high signal-to-noise ration and a given transmission rate R is*

$$\xi_{(1,N,1),RS} = (2^R - 1)^N \prod_{k=1}^{N} \sigma_{1k}^{-2}\sigma_{2k}^{-2}. \tag{2.16}$$

σ_{1k}^{-2} and σ_{2l}^{-2} are the variances of the channel coefficients in the first and second hops respectively.

Let $N = 2$, $g_k = |h_{1k}h_{2k}|^2$. The average mutual information of the RF scheme is

$$I_{\mathsf{avg}} = \log\left(\frac{1 + \mathrm{SNR}g_1 + \mathrm{SNR}g_2 + \sqrt{(1 + \mathrm{SNR}g_1 + \mathrm{SNR}g_2)^2 - 4\mathrm{SNR}^2 g_1 g_2}}{2}\right).$$

The mutual information can be lower bounded as follows

$$I_{\mathsf{avg}} \geq \max\left\{\log(1 + \mathrm{SNR}g_1), \log(1 + \mathrm{SNR}g_2)\right\}. \tag{2.17}$$

The logarithm is a monotonic function, then it is easy to show that $I_{\mathsf{avg}} \geq \log(1 + \mathrm{SNR}g_1)$. In the same way, we show that $I_{\mathsf{avg}} \geq \log(1 + \mathrm{SNR}g_2)$ and we can get Eq.2.17. It is straight forward to generalize for $N > 2$. Then

$$I_{\mathsf{avg}} \quad \geq \quad \max_{\substack{k \\ 1\leq k\leq N}} \left\{\log(1 + \mathrm{SNR}g_k)\right\}. \tag{2.18}$$

The RHS of the equation Eq.2.18 represents the mutual information of the relay-selection (RS) scheme. This scheme consists of choosing the best source-relay-destination link to rotate-forward the source signal. Based on Eq.2.18, the RF scheme without CSI is better than the RS scheme. The outage probability of the RS scheme is the product of the outage probabilities of each source-relay-destination link,

$$P_{\mathsf{out}}(R, \sigma_{1k}, \sigma_{2k}, \mathrm{SNR}) = \prod_{k=1}^{N}\left[\frac{(2^R - 1)(1 - 2\gamma - \ln(2^R - 1) + \ln(\sigma_{1k}^2\sigma_{2k}^2) + \ln(\mathrm{SNR}))}{\sigma_{1k}^2\sigma_{2k}^2\mathrm{SNR}}\right]. \tag{2.19}$$

where γ is the Euler's constant.

As in the above two cases, we choose $f(\text{SNR}) = \dfrac{\text{SNR}^N}{(\ln \text{SNR})^N}$. We derive the outage gain of this scheme and the result is given in a closed form as in Theorem 2.3.

2.3.4 Comments

- The RF, the Orthogonal RF and the RS protocols have the same diversity in the (1, N, 1) networks. The respective outage probability curves have asymptotically the same slope since the function $f(\text{SNR})$ is the same for the three protocols. However, one should look to the outage gains to compare the performance of these schemes. It is easy to see that the smaller the outage gain is, the better the scheme performs. Then, the RF which has the smallest outage gain is the best scheme. We have

$$\xi_{(1,N,1),RF} < \xi_{(1,N,1),RS} < \xi_{(1,N,1),ORF} \tag{2.20}$$

- If we reconsider the additive noise on the relays, the average mutual information of the RF scheme can be written in the following form independently of the rotations θ_k,

$$I_{\mathsf{avg}} = \log\left(1 + \text{SNR}\left(1 + \sum_{k=1}^{N} g_{2k}\right)^{-1} \sum_{k=1}^{N} g_{1k}g_{2k}\right), \tag{2.21}$$

  where $g_{lk} = |h_{lk}|^2$ are the channels power gains. By letting $x_k = \text{SNR}g_{1k}g_{2k}$, the outage gain becomes

$$\xi = \lim_{\text{SNR}\to\infty} f(\text{SNR})\text{SNR}^{-N} \int \mathbf{1}\left\{x_k, g_{2k} \in \mathbb{R}_+ : I_{\mathsf{avg}} < R\right\} \prod_{k=1}^{N} f_{G_k}(x_k/\text{SNR}, g_{2k}) dx_k dg_{2k} \tag{2.22}$$

  This integral is complicated to solve, we have to delineate the domain of variation of all the variables. Intuitively, one may conjecture that $f(\text{SNR})$ must be chosen as $f(\text{SNR}) = \dfrac{\text{SNR}^N}{(\ln \text{SNR})^N}$; the noise on the relays does not affect the diversity of the RF scheme, and it is straightforward to say that

$$\xi_{(1,N,1),RF/noise} > \xi_{(1,N,1),RF}. \tag{2.23}$$

  Indeed, the noisy model is worse than the noiseless one. We will further see this inequality in numerical results.

2.3.5 The RF Protocol in the Two-Hop (M, 1, M) Network

Consider a two-hop (M, 1, M) relay network operating under the rotate-and-forward protocol. We compute the outage gain at high signal-to-noise ration (SNR) in Theorem 2.4,

Theorem 2.4 *Consider a (M, 1, M) relay network operating under the rotate-and-forward protocol, the outage gain at high signal-to-noise ration and a given transmission rate R is*

$$\xi_{(M,1,M),RF} = \frac{M(2^R-1)^M}{(M!)^2}\prod_{k=1}^{M}\sigma_{1k}^{-2}\sigma_{2k}^{-2}. \tag{2.24}$$

σ_{1k}^{-2} and σ_{2k}^{-2} are the variances of the channel coefficients in the first and second hop respectively.

Proof: Let $\boldsymbol{H}_1 = [h_{11}\dots h_{1M}]$ and $\boldsymbol{H}_2 = [h_{21}\dots h_{2M}]^T$ be the channel matrices of the first and second hops respectively. The rotation matrix is reduced to $\boldsymbol{F}_i = e^{i\theta_i}$. The equivalent channel matrix is $\boldsymbol{H} = \boldsymbol{H}_2\boldsymbol{F}\boldsymbol{H}_1$. The mutual information of this scheme is

$$I = \log\det(\boldsymbol{I} + \mathrm{SNR}\boldsymbol{H}\boldsymbol{H}^\dagger) = \log(1+\mathrm{SNR}G_1G_2),$$

where $G_1 = g_{11} + \ldots + g_{1M}$ and $G_2 = g_{21} + \ldots + g_{2M}$, $g_{lk} = |h_{lk}|^2$. G_1 and G_2 are two central chi-square variates with 2M degrees of freedem each, *i.e.* $G_1 \sim \mathcal{X}^2_{2M}$ and $G_2 \sim \mathcal{X}^2_{2M}$. Consider $w = G_1G_2$ and its probability density function $f_W(w)$, the outage gain becomes

$$\begin{aligned}\xi &= \lim_{\mathrm{SNR}\to\infty} f(\mathrm{SNR})\int \mathbf{1}\left\{w\in\mathbb{R}_+ : I(w) < R\right\} f_W(w)dw \\ &= \lim_{\mathrm{SNR}\to\infty} f(\mathrm{SNR})\int \mathbf{1}\left\{w < \frac{2^R-1}{\mathrm{SNR}}\right\} f_W(w)dw.\end{aligned}$$

By resolving the equation 2.25, we compute the outage probability of the (M, 1, M) networks operating under the RF protocol,

$$P_{\mathsf{out}}(R,\sigma_1,\sigma_2,\mathrm{SNR}) = \frac{(2^R-1)^M(1-2M\gamma - M\ln(2^R-1) + M\ln(\sigma_1^2\sigma_2^2) + M\ln(\mathrm{SNR}))}{(M!)^2\sigma_1^{2M}\sigma_2^{2M}\mathrm{SNR}^M}, \tag{2.25}$$

γ is the Euler's constant, $\sigma_{1k}^2 = \sigma_1^2$ and $\sigma_{2k}^2 = \sigma_2^2$ are the channel variances of the first and second hops, respectively. The proof is given in Appendix 2.A.1.

We choose $f(\mathrm{SNR}) = \dfrac{\mathrm{SNR}^M}{\ln\mathrm{SNR}}$. We compute the outage gain of a (M, 1, M) network operating under the rotate-and-forward protocol in a closed form as given in Theorem 2.4. End of the proof.

We note that in our work, we have focused on some symmetrical antenna settings. Though the tools to be used and the steps to be followed to extract the outage gains for a more general settings of antennas (n_t, N, n_r) are the same, it is bitter hard to find the corresponding probability density functions and to solve integration equation sets. This could be the subject of a future work.

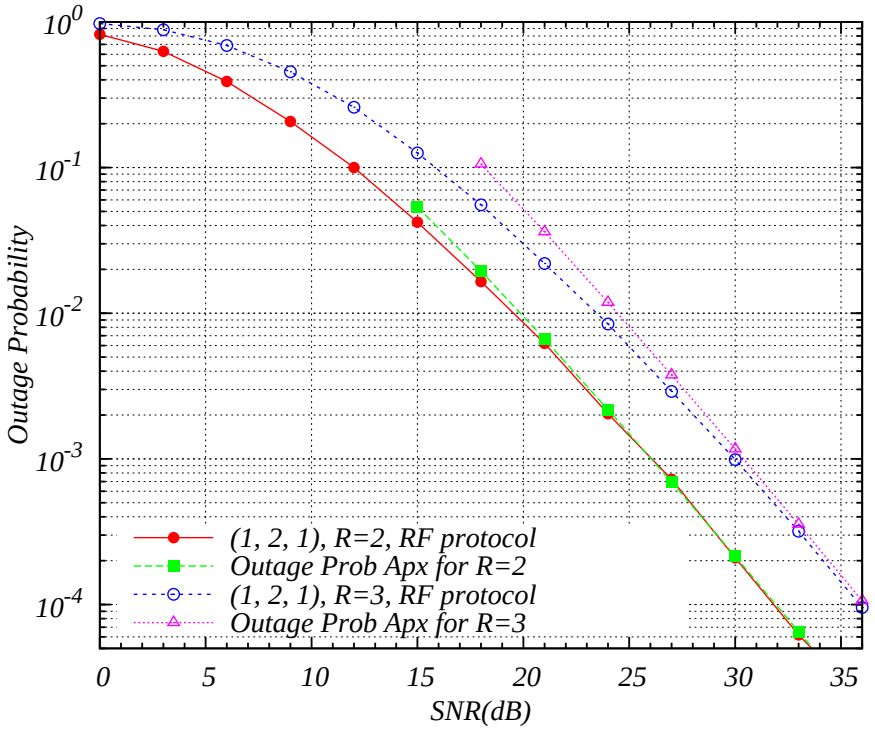


Figure 2.2: Outage Probability approximation of the (1, 2, 1) network operating under the RF protocol, $\sigma_{1l}^2 = \sigma_{2l}^2 = 1$.

2.3.6 Numerical Examples

We verified the outage gain expressions given in Theorems 2.1, 2.2 and 2.4 over Rayleigh faded channels. We noticed that the outage probability values obtained by the approximation $P_o \approx \xi f(\text{SNR})$ and the numerical values are close, and this validate the outage gain expressions. The outage gain in Theorem 2.1 is verified in the (1, 2, 1), (1, 3, 1) and (1, 4, 1) networks for $\sigma_{1l}^2 = \sigma_{2l}^2 = 1$, in Fig.2.2, Fig.2.3 and Fig.2.4 respectively. The outage gain in Theorem 2.2 is verified in the (1, 2, 1) and (1, 3, 1) networks for $\sigma_{1l}^2 = \sigma_{2l}^2 = 1$, in Fig.2.5. The outage gain given in Theorem 2.4 is also verified for $\sigma_1^2 = \sigma_2^2 = 2$, in Fig.2.6. We notice also that the outage gain expressions hold for moderate values of SNR as well. If we consider the additive noise on the relays, we have the same diversity as without noise which validates the choice of $f(\text{SNR})$, and we loose 2dB and 3dB at 10^{-3} for $N = 2, 3$ respectively (Fig.2.7).

2.4 Two-Hop (2, N, 2) Networks with Feedback

In this section, we consider the (2, N, 2) networks operating under the RF protocol, and we want to find the optimal rotations so as to maximize the mutual information. Maximizing the mutual information between the source and destination, and hence, minimizing the outage probability of cooperative schemes has been widely studied in the literature as problems of power allocation, precoding design or network beamforming [30] - [31].

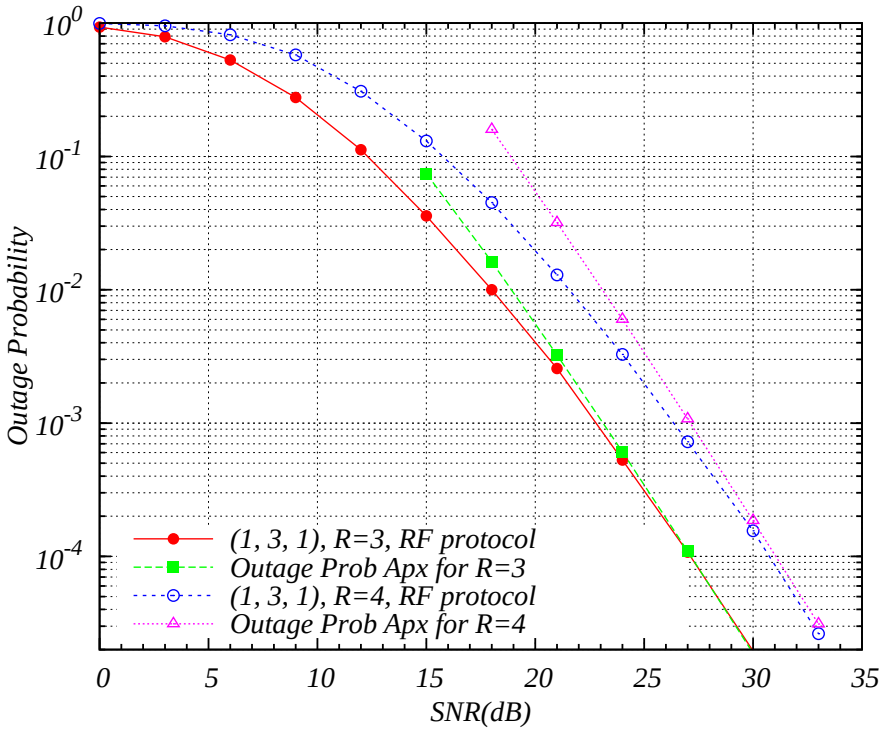


Figure 2.3: Outage Probability approximation of the (1, 3, 1) network operating under the RF protocol, $\sigma_{1l}^2 = \sigma_{2l}^2 = 1$.

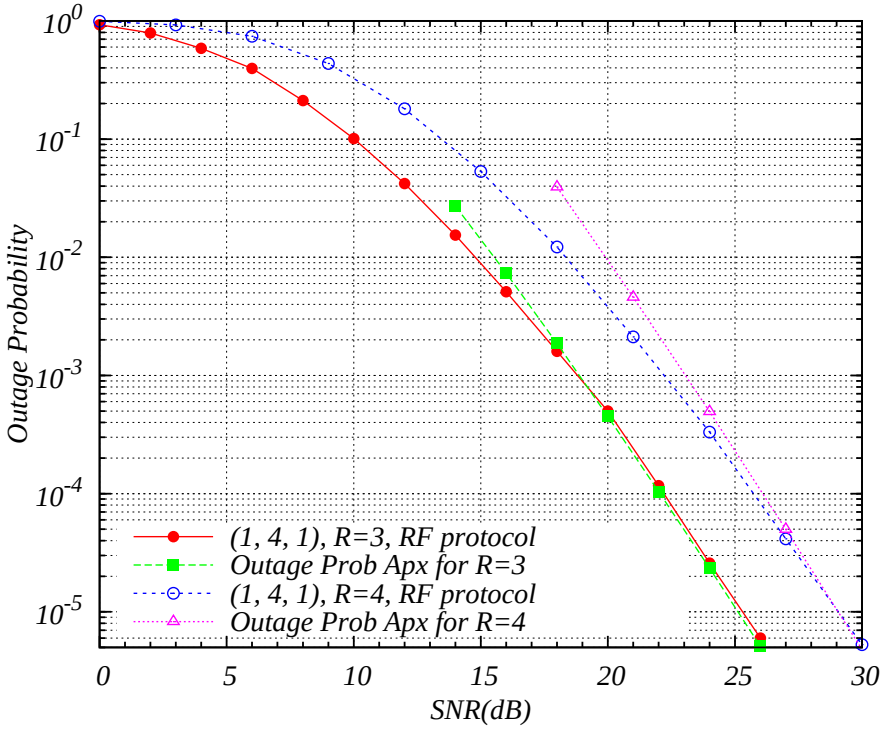


Figure 2.4: Outage Probability approximation of the (1, 4, 1) network operating under the RF protocol, $\sigma_{1l}^2 = \sigma_{2l}^2 = 1$.

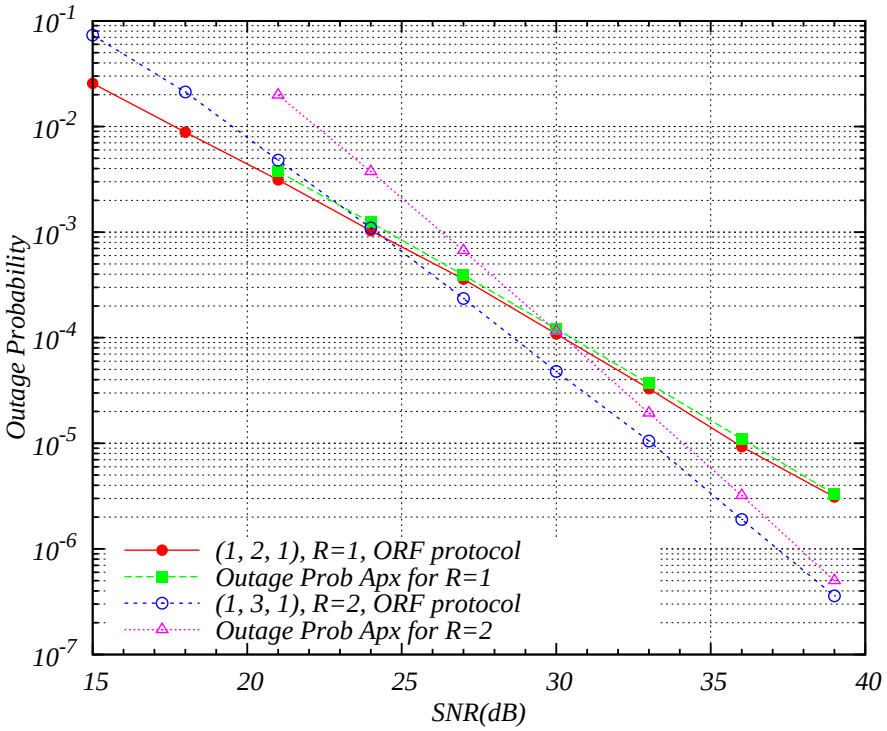


Figure 2.5: Outage Probability approximation of the (1, N, 1) network operating under the orthogonal RF protocol, $\sigma_1^2 = \sigma_2^2 = 1$.

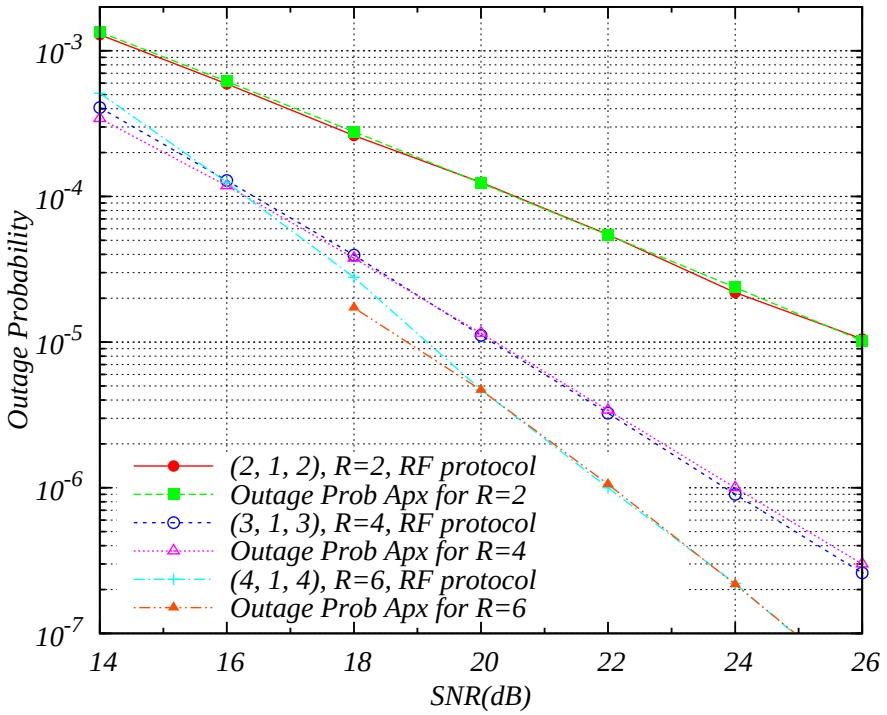


Figure 2.6: Outage Probability approximation of the (N, 1, N) network operating under the RF protocol, $\sigma_1^2 = \sigma_2^2 = 2$.

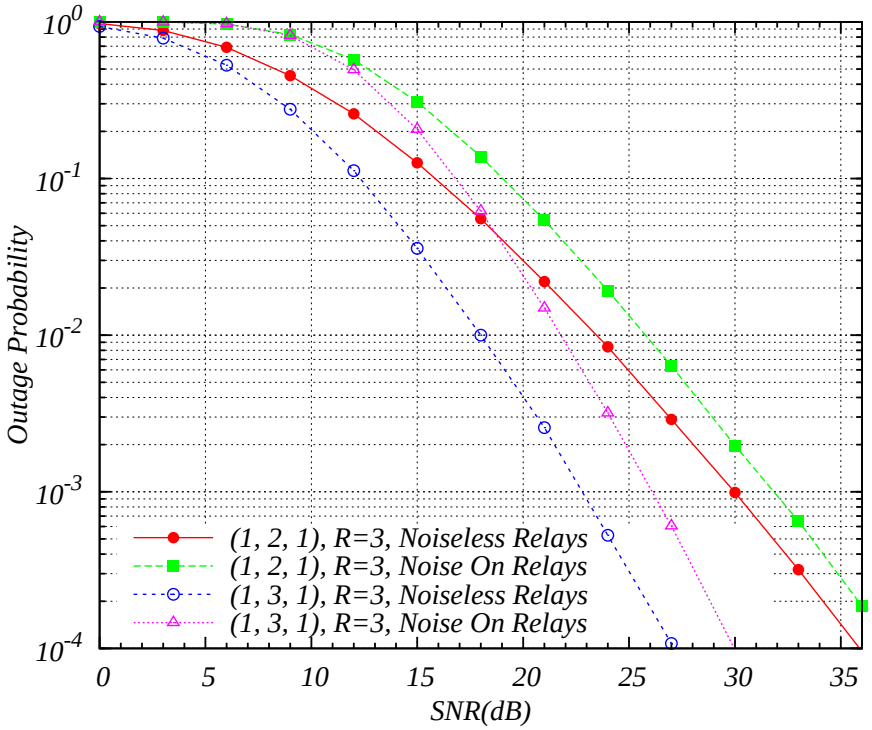


Figure 2.7: Outage probability in the (1, 2, 1) and (1, 3, 1) RF networks with noiseless and noisy relays for R=3, $\sigma_{1l}^2 = \sigma_{2l}^2 = 1$.

In the RF protocol, the relays choose the rotations from a given DRS. These rotations are not optimal for all channel realizations, and then the mutual information is not maximized. However, the destination could use the channel state knowledge to find the optimal rotations, and then to feed them back to the relays via a feedback channel. The optimal rotations $\boldsymbol{\theta}_{\mathsf{opt}}$ are then used by the relays during the transmission of the codeword $\boldsymbol{X}$. Thus, the equivalent channel of the RF scheme is reduced to $\boldsymbol{H}_\theta = \boldsymbol{H}_2\boldsymbol{F}_{\mathsf{opt}}\boldsymbol{H}_1$, and we omit the time index in the input-output relation Eq.2.1

$$\boldsymbol{y}_D = \boldsymbol{H}_2\boldsymbol{F}_{\mathsf{opt}}\boldsymbol{H}_1\boldsymbol{x} + \boldsymbol{z}_D. \tag{2.26}$$

Searching for the optimal rotations is based on a signal model without noise on the relays. In order to do this, the destination can do an optimal global research over all possible N-tuples,

$$\boldsymbol{\theta}_{\mathsf{opt}} \triangleq \arg \max_{\boldsymbol{\theta}, \theta_i \in [0,2\pi)} \log\det(\boldsymbol{I} + \mathrm{SNR}\boldsymbol{H}_{\boldsymbol{\theta}}\boldsymbol{H}_{\boldsymbol{\theta}}^{\dagger}) \tag{2.27}$$

The global research is optimal. However, the computational cost is heavy and grows exponentially in N. Instead, we propose a simple iterative algorithm to find θ_{opt} which complexity is linear in N. This is possible because we are able to separate the angles θ_i's in the mutual information expression. Next, we will show how the destination could find the optimal

rotations; first in case of only one relay performing the RF protocol, and then in case of N relays.

2.4.1 Case: One Active Relay

Consider the network (2, N, 2) in which only one relay is active. This relay rotates its received signal by an angle θ. The remaining $N-1$ relays just amplify and forward their signals. The rotation matrix is $\boldsymbol{F} = \mathrm{diag}\big(1, \ldots, 1, e^{j\theta}\big)$, and the mutual information becomes,

$$I(\theta) = \log\det(\boldsymbol{I}_2 + \mathrm{SNR}\boldsymbol{D}\boldsymbol{W}_2) + \log\{1 - \mathrm{SNR}^2\det(\boldsymbol{P}) + 2\mathrm{SNR}|P_{12}|\cos(\theta + \angle P_{12})\}. \quad (2.28)$$

The computation details are deferred to the Appendix 2.A.3. The matrices $\boldsymbol{D}$, $\boldsymbol{W}_2$, and $\boldsymbol{P}$ are independent of θ and defined in Appendix D. Considering one angle, the mutual information is periodic in θ over $[0, 2\pi)$. The destination feeds back to the relay the value of θ which maximizes (2.28),

$$\theta_{\mathsf{opt}} = -\angle P_{1,2}. \quad (2.29)$$

2.4.2 Case: N Active Relays

Consider N active relays. Our goal is to to separate the considered angle, θ_i, form all the other rotation angles $\theta_j, j \neq i$, so the destination can find all angles consequently. In other words, for a given θ_i, we want to write the mutual information as

$$I(\theta_1, \ldots, \theta_N) = \log\{\boldsymbol{A}_i + \boldsymbol{B}_i\cos(\theta_i + \phi_i)\} \quad (2.30)$$

where $\boldsymbol{A}_i$, $\boldsymbol{B}_i$ and ϕ_i are functions of the channel matrices $\boldsymbol{H}_1$ and $\boldsymbol{H}_2$, and the angles θ_j, $j \neq i$. Hence, the mutual information is maximized in respect to θ_i by choosing $\theta_{i,\mathsf{opt}} = -\phi_i$. In order to make this, we need to do some line and column permutations.

Let us define $\boldsymbol{R}_{i,\theta_i}$ as a $N \times N$ diagonal matrix where $\boldsymbol{R}_{i,\theta_i}(i,i) = e^{j\theta_i}$ and $\boldsymbol{R}_{i,\theta}(k,k) = 1$ $\forall\ k \neq i$. We have the following lemma

Lemma 2.1

$$\det(\boldsymbol{I} + \boldsymbol{R}_{i,\theta_i}\boldsymbol{A}\boldsymbol{R}_{i,\theta_i}^{\dagger}\boldsymbol{B}) = f_i(\boldsymbol{A},\boldsymbol{B}) + \mathcal{R}\left\{g_i(\boldsymbol{A},\boldsymbol{B})e^{j\theta_i}\right\}, \quad (2.31)$$

where f_i and g_i are some functions of $\boldsymbol{A}$ and $\boldsymbol{B}$, $\mathcal{R}$ is the real part of a complex number.

Now, when all the relays are rotate-forwarding their signals, the mutual information is function of $\theta_1, \ldots, \theta_N$ and can be written as,

$$I(\theta_1, \ldots, \theta_N) = \log\det(\boldsymbol{I} + \boldsymbol{F}\boldsymbol{W}_1\boldsymbol{F}^{\dagger}\boldsymbol{W}_2) = \log\det(\boldsymbol{I} + \prod_{i=1}^{N}\boldsymbol{R}_{i,\theta_i}\boldsymbol{W}_1\prod_{i=1}^{N}\boldsymbol{R}_{i,\theta_i}^{\dagger}\boldsymbol{W}_2) \quad (2.32)$$

where $\boldsymbol{W}_1 \triangleq \boldsymbol{H}_1\boldsymbol{H}_1^\dagger$ and $\boldsymbol{W}_2 \triangleq \boldsymbol{H}_2^\dagger\boldsymbol{H}_2$. We define the unitary matrix $\boldsymbol{P}_{i,N}$ such that $\boldsymbol{P}_{i,N}\boldsymbol{A}\boldsymbol{P}_{i,N}^\dagger$ permutes the ith and Nth columns of $\boldsymbol{A}$. Then, for a given θ_i at a position (i,i), the mutual information is,

$$\begin{aligned} I(\theta_1,\ldots,\theta_N) &= \log\det(\boldsymbol{I}+\boldsymbol{R}_{i,\theta_i}\boldsymbol{W}_{1,i}\boldsymbol{R}_{i,\theta_i}^\dagger\boldsymbol{W}_{2,i}) \\ &= \log\det(\boldsymbol{I}+\boldsymbol{P}_{i,N}\boldsymbol{R}_{i,\theta_i}\boldsymbol{W}_{1,i}\boldsymbol{R}_{i,\theta_i}^\dagger\boldsymbol{W}_{2,i}\boldsymbol{P}_{i,N}^\dagger) \\ &= \log\det(\boldsymbol{I}+\boldsymbol{R}_{N,\theta_i}\overline{\boldsymbol{W}}_{1,i}\boldsymbol{R}_{N,\theta_i}^\dagger\overline{\boldsymbol{W}}_{2,i}) \qquad (2.33) \\ &= \log\left(f_N(\overline{\boldsymbol{W}}_{1,i},\overline{\boldsymbol{W}}_{2,i})+\mathcal{R}\left\{g_N(\overline{\boldsymbol{W}}_{1,i},\overline{\boldsymbol{W}}_{2,i})e^{j\theta_i}\right\}\right) \qquad (2.34) \end{aligned}$$

where the last equality is obtained form Eq.2.28, and

$$\boldsymbol{W}_{1,i} \triangleq \prod_{k=1,k\neq i}^{N}\boldsymbol{R}_{k,\theta_k}\boldsymbol{W}_1 \quad \text{and} \quad \boldsymbol{W}_{2,i} \triangleq \prod_{k=1,k\neq i}^{N}\boldsymbol{R}_{k,\theta_k}^\dagger\boldsymbol{W}_2 \qquad (2.35)$$

$$\overline{\boldsymbol{W}}_{l,i} = \boldsymbol{P}_{i,N}\boldsymbol{W}_{l,i}\boldsymbol{P}_{i,N}^\dagger, \text{ for } l=1,2 \quad \text{and} \quad \boldsymbol{R}_{N,\theta_i} = \boldsymbol{P}_{i,N}\boldsymbol{R}_{i,\theta_i}\boldsymbol{P}_{i,N}^\dagger, \ \forall i \qquad (2.36)$$

Arriving at the stage of Eq.2.33, the rotation angle θ_i is at the postion (N, N), then we can solve for the $\theta_{i,\mathsf{opt}}$ as we did for Eq.2.28. Thus, f_i and g_i are obtained as follows

$$\begin{aligned} f_i(\boldsymbol{W}_{1,i},\boldsymbol{W}_{2,i}) &= f_N(\overline{\boldsymbol{W}}_{1,i},\overline{\boldsymbol{W}}_{2,i}) \qquad (2.37) \\ g_i(\boldsymbol{W}_{1,i},\boldsymbol{W}_{2,i}) &= g_N(\overline{\boldsymbol{W}}_{1,i},\overline{\boldsymbol{W}}_{2,i}) \qquad (2.38) \end{aligned}$$

In case of one active relay at the position (N, N), we have found that

$$\begin{aligned} f_N(\boldsymbol{W}_{1,N},\boldsymbol{W}_{2,N}) &= (1-\mathrm{SNR}^2\det(\boldsymbol{P}))\det(\boldsymbol{I}+\mathrm{SNR}\boldsymbol{D}\boldsymbol{W}_2) \qquad (2.39) \\ g_N(\boldsymbol{W}_{1,N},\boldsymbol{W}_{2,N}) &= 2\mathrm{SNR}\det(\boldsymbol{I}+\mathrm{SNR}\boldsymbol{D}\boldsymbol{W}_2)P_{1,2} \qquad (2.40) \end{aligned}$$

2.4.3 Iterative Algorithm

The destination has full CSI and knows the number of active relays N in the network. We propose to calculate the optimal rotations $\boldsymbol{\theta}_{\mathsf{opt}} \triangleq [\theta_{1,\mathsf{opt}},\ldots,\theta_{N,\mathsf{opt}}]$ in an iterative manner. Starting with an initial rotation vector chosen randomly, $\boldsymbol{\theta}_{\mathsf{init}}$, the destination maximizes the mutual information with respect to all the angles one by one by calculating f_i, g_i, ϕ_i and the corresponding $\theta_{i,\mathsf{opt}}$, for $i=1,\ldots N$. Then, the destination can iterate to find accurate rotation angles. This iterative algorithm can be summarized in these steps:

step 1: choose an initial rotation vector $\boldsymbol{\theta}_{\mathsf{init}}$ arbitrarily.

step 2: calculate

$$\begin{aligned} f_1,\ g_1,\ \phi_1, \text{ and compute } \theta_{1,\mathsf{opt}} &= -\phi_1(\theta_2,\ldots,\theta_N), \\ &\vdots \\ f_i,\ g_i,\ \phi_i, \text{ and compute } \theta_{i,\mathsf{opt}} &= -\phi_i(\theta_{1,\mathsf{opt}},\ldots,\theta_{i-1,\mathsf{opt}},\theta_{i+1},\ldots,\theta_N), \\ &\vdots \\ f_N,\ g_N,\ \phi_N, \text{ and compute } \theta_{N,\mathsf{opt}} &= -\phi_N(\theta_{2,\mathsf{opt}},\ldots,\theta_{N-1,\mathsf{opt}}). \end{aligned}$$

step 3: back to step 2 with $\boldsymbol{\theta}_{\mathsf{init}} = \boldsymbol{\theta}_{\mathsf{opt}}$.

Experimentally, we need 3 iterations in order to get an accurate $\boldsymbol{\theta}_{\mathsf{opt}}$. This is interesting when we consider a perfect feedback channel. However, when the feedback is limited, which is the case of real systems, too many iterations don't have any added-value. In this case, one iteration is sufficient.

2.4.4 Numerical Results

We studied the performance of our iterative algorithm with perfect and limited feedback channel. We took the outage probability as a performance criterion. In Fig.2.8 and Fig.2.9, we show the outage probabilities of the (2, 3, 2) network under AF and RF schemes. It is clear that the RF outperforms the AF. In case of feedback, we compare the outage probability of the optimal global algorithm to that of the proposed iterative algorithm. We can see that both algorithms have the same performance. The feedback allows us to have 2.3dB gain over the RF scheme at a target outage probability of 10^{-3} for a rate $R = 4$ BPCU. Indeed, by averaging over $\boldsymbol{\theta}$ in the RF scheme, the second term of the logarithm argument in Eq.2.34 goes to zero, while in case of feedback, this term is maximized.

Now, if the feedback channel is limited, the destination quantizes the rotation angles and send them over limited number of bits, let us say B bits/angle (bpa). In this case, the interval $[0, 2\pi)$ is divided into 2^B levels, and the destination sends back the level index to the corresponding relay. Fig.2.9 shows the gain loss due to limitation on feedback for $B = 2, 1$(bpa); 0.2 and 1dB respectively at an outage probability 10^{-3} and rate $R = 4$. It is worth noting that $B = 1$bpa corresponds to either rotating the signal of π before retransmission or not. The YES/No decision in this case depends on the channel conditions while in the flip-and-forward (FF) protocol, proposed in [21], the rotation is independent of the channel which is not optimal. The $B = 2$bpa is the choice of one out of the four quadrants of a trigonometric circle. Based on the observed performance, we can conclude that exact θ_{opt} values are not needed and then, the number of iterations in the proposed algorithm may be too small. This is the case in the simulations where we did 3 iterations for each $\boldsymbol{\theta}_{\mathsf{opt}}$.

In the (2, 4, 2) network, we have the same observation, Fig.2.10 and Fig.2.11. The optimal

algorithm and our iterative algorithm have the same performance in terms of outage probability. The feedback allows us to have 3.2dB gain over the RF scheme at outage probability 10^{-3} and rate $R = 6$ BPCU. Again, when the feedback channel is limited, Fig.2.11, we loose 0.2 and 1dB for $B = 2, 1$(bpa) respectively at 10^{-3}.

We notice that although the iterative algorithm is based on a noiseless source-relays link model, we have considered the additive noise on the relays in the results with limited feedback,

$$I = \log\det\left\{\boldsymbol{I} + \mathrm{SNR}(\boldsymbol{I} + \boldsymbol{F}_{\mathsf{opt}}^{\dagger}\boldsymbol{W}_2\boldsymbol{F}_{\mathsf{opt}})^{-1}\boldsymbol{F}_{\mathsf{opt}}^{\dagger}\boldsymbol{W}_2\boldsymbol{F}_{\mathsf{opt}}\boldsymbol{W}_1\right\} \tag{2.41}$$

is the mutual information. Fig.2.12 and Fig.2.13 show that the RF scheme outperforms the AF and DF schemes when noise is considered on the relays.

2.5 Conclusion

In this chapter, we considered the rotate-and-forward protocol in the two-hop relay networks. We studied the performance of this protocol in terms of outage gain. We derived closed form outage gain expressions for the RF and for other protocols having the same diversity. We verified these expression through simulation results at high signal to noise ratio. The numerical results show the accuracy of this criterion at moderate signal to noise ratio as well.

Moreover, we proposed to improve the performance of the RF scheme using a limited feedback channel between the destination and the relays. We required the destination to calculate the optimal rotations and to feed them back to the relays. In this scope, we gave an iterative algorithm with low complexity. Through numerical simulations, we showed that this algorithm has the same performance in terms of outage probability as that of an optimal global algorithm.

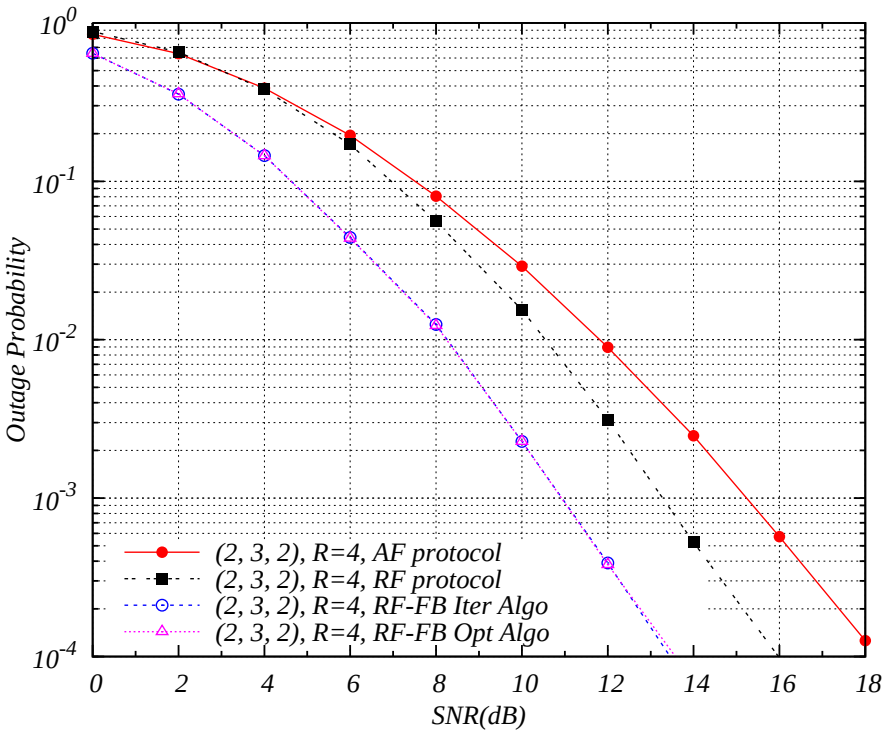


Figure 2.8: Outage probability of the (2, 3, 2) channel under AF, RF, and RF with Feedback schemes.

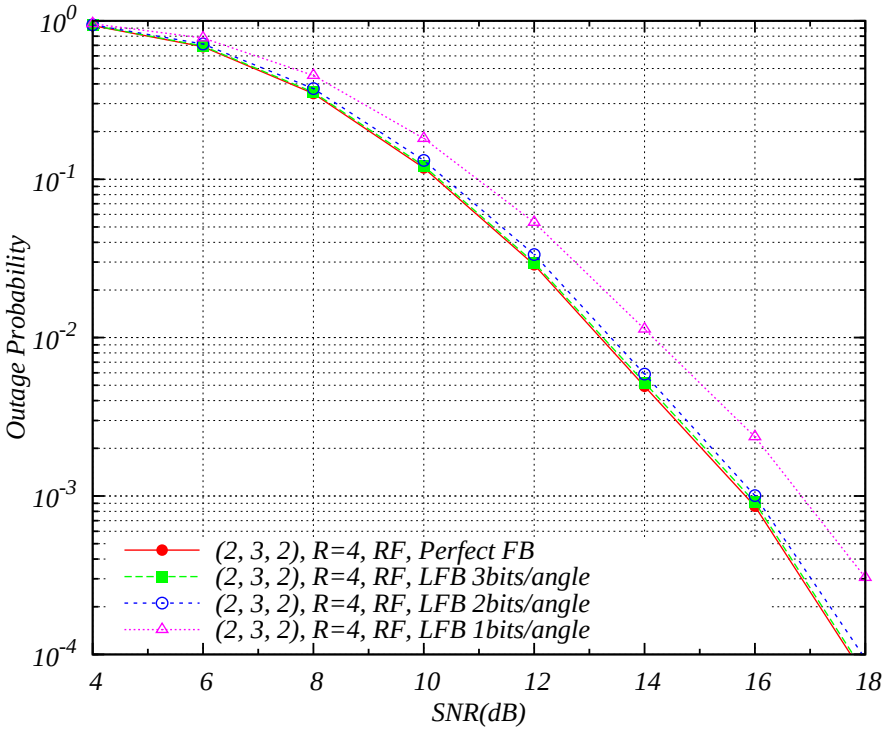


Figure 2.9: Outage probability of the (2, 3, 2) channel under limited Feedback.

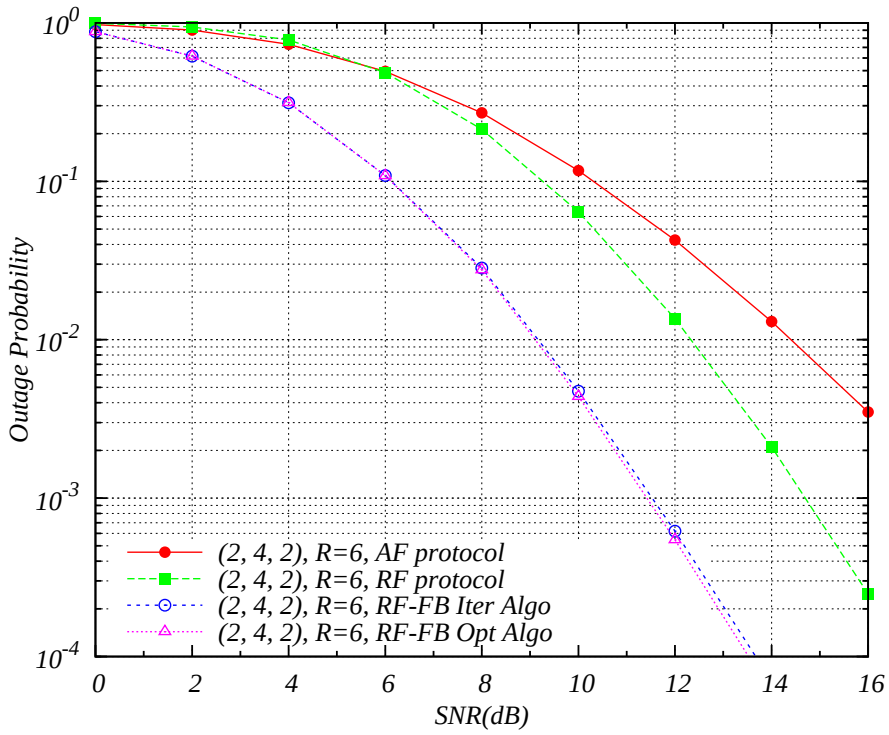


Figure 2.10: Outage probability of the (2, 4, 2) channel under AF, RF, and RF with Feedback schemes.

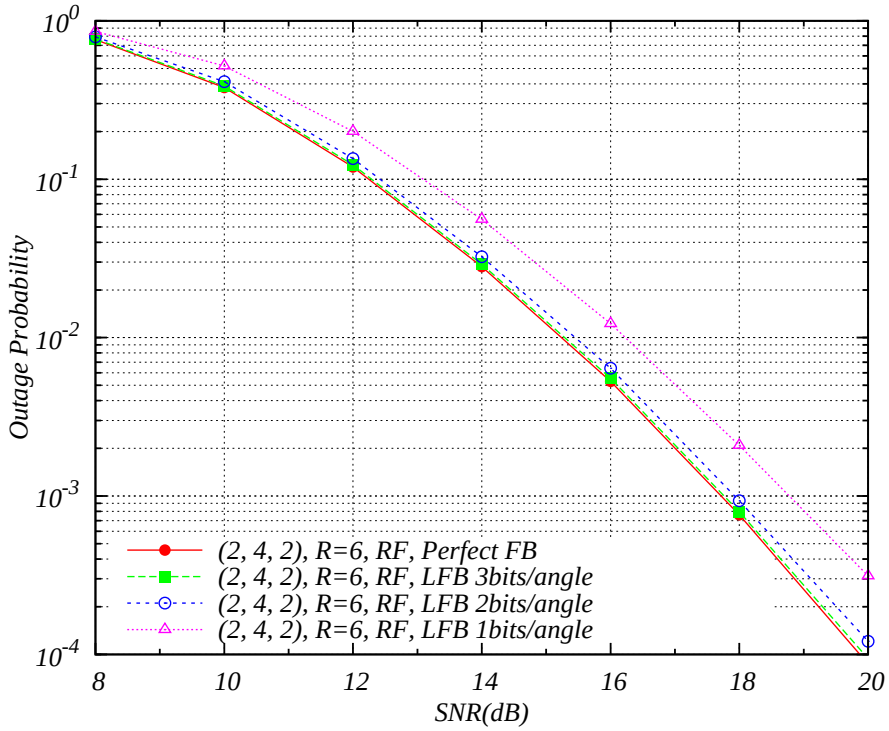


Figure 2.11: Outage probability of the (2, 4, 2) channel under limited Feedback.

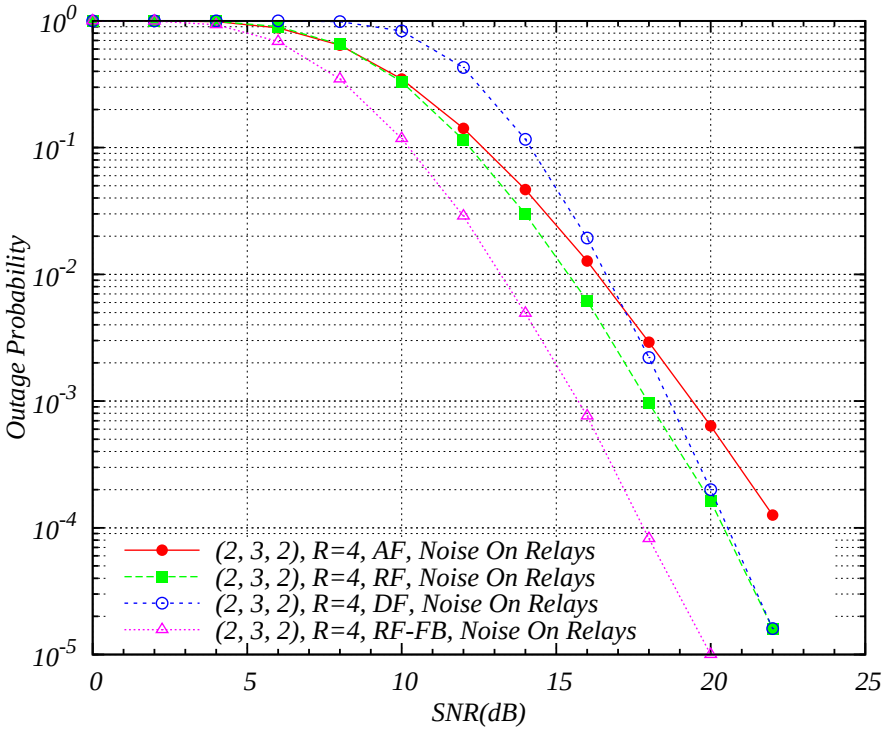


Figure 2.12: Outage probability of the (2, 3, 2) channel under AF, DF, RF, and RF with Feedback schemes with noise on relays.

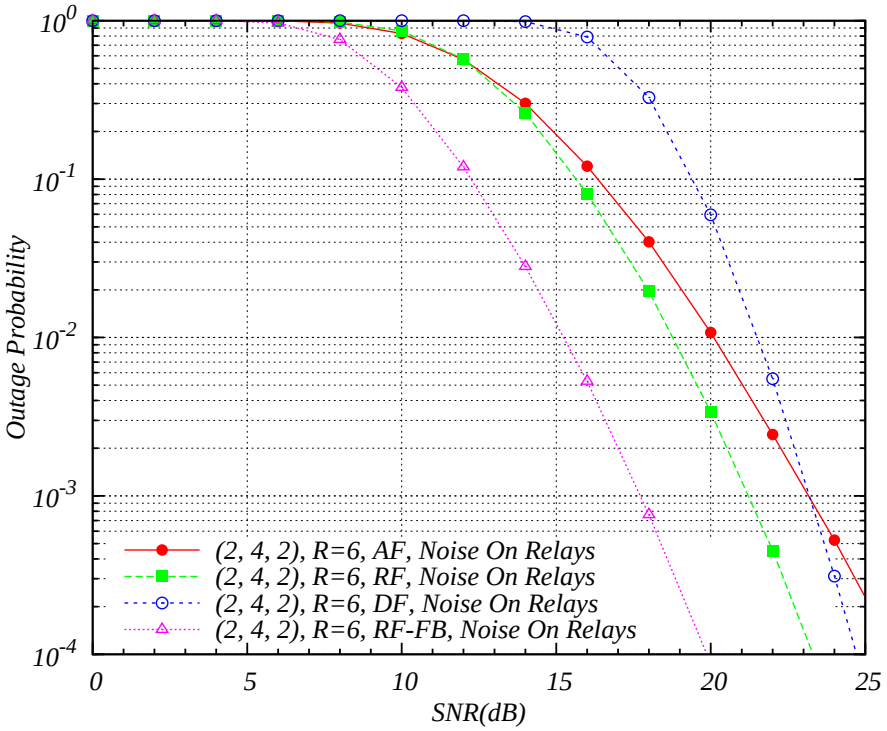


Figure 2.13: Outage probability of the (2, 4, 2) channel under AF, DF, RF, and RF with Feedback schemes with noise on relays.

2.A Proofs

2.A.1 Distribution of the product of two central independent chi-square variates in Eq.2.25

Let $x_1 = \sum_{i=1}^{k_1} x_{1i}^2$ and $x_2 = \sum_{i=1}^{k_2} x_{2i}^2$ be two central independent chi-square variates of k_1 and k_2 degrees of freedom respectively. x_{1i} and x_{2i} are independent normal variates with zero means and deviations $\sigma_1^2/2$ and $\sigma_2^2/2$ respectively.

Theorem 2.5 *[32] Consider the product of two independent variates $w = x_1 x_2$, where x_1 is a central chi-square variate with k_1 degrees of freedom and x_2 is a central chi-square variate with k_2 degrees of freedom, then the density function of w is*

$$f_W(w) = \frac{4}{\sigma_1^2\sigma_2^2} \frac{\left(\frac{4w}{\sigma_1^2\sigma_2^2}\right)^{\frac{1}{4}k_1+\frac{1}{4}k_2-1} K_{\frac{1}{2}k_1-\frac{1}{2}k_2}\left(\sqrt{\frac{4w}{\sigma_1^2\sigma_2^2}}\right)}{2^{\frac{1}{2}k_1+\frac{1}{2}k_2-1}\Gamma\left(\frac{1}{2}k_1\right)\Gamma\left(\frac{1}{2}k_2\right)} \tag{2.42}$$

$K_\nu(w)$ is the modified Bessel function of the second kind, and Γ is the Gamma function.

Using the pdf in Eq.2.42 in the integral form of Eq.2.25 and making the development in Taylor series as SNR $\to \infty$, we get the Eq.2.25 of the outage probability of the (M, 1, M) network operating under the RF protocol.

2.A.2 The value of c_k in Eq.2.9

g_k is the product of two independent central chi-square variates of two degrees of freedom each with respective variances σ_{1k}^2 and σ_{2k}^2. Using Eq.2.42 with $k_1 = k_2 = 2$, the density function of g_k is

$$f_{G_k}(g_k) = \frac{2}{\sigma_{1k}^2\sigma_{2k}^2} K_0\left(\sqrt{\frac{4g_k}{\sigma_{1k}^2\sigma_{2k}^2}}\right)$$

K_0 is the zeroth order Bessel function of the second kind. Using the development of the function K_0 in [[33], page 909], we obtain the value of Eq.2.A.2 as SNR $\to \infty$:

$$f_{G_k}\left(g_k \propto \frac{1}{\text{SNR}}\right) = \frac{1}{\sigma_{1k}^2\sigma_{2k}^2} \ln \text{SNR} \tag{2.43}$$

2.A.3 Proof of the equation Eq.2.28

We detail here how we extract the equation (2.28). We define, $\boldsymbol{H}_\theta$, $\boldsymbol{W}_\theta$, $\boldsymbol{W}_1$, and $\boldsymbol{W}_2$ as,

$$\boldsymbol{H}_\theta \triangleq \boldsymbol{H}_2 \boldsymbol{F} \boldsymbol{H}_1 = \boldsymbol{H}_2 \begin{bmatrix} \boldsymbol{I}_{N-1} & 0 \\ 0 & e^{j\theta} \end{bmatrix} \boldsymbol{H}_1$$

$$\boldsymbol{W}_\theta \triangleq \boldsymbol{H}_\theta \boldsymbol{H}_\theta^\dagger, \quad \boldsymbol{W}_1 \triangleq \boldsymbol{H}_1 \boldsymbol{H}_1^\dagger, \quad \boldsymbol{W}_2 \triangleq \boldsymbol{H}_2^\dagger \boldsymbol{H}_2$$

And we decompose $\boldsymbol{W}_1$ as

$$\boldsymbol{W}_1 \triangleq \boldsymbol{D} + \boldsymbol{A} = \begin{bmatrix} \boldsymbol{W}_{11} & 0 \\ 0 & w_{12} \end{bmatrix} + \begin{bmatrix} 0 & \boldsymbol{w}_{1,c} \\ \boldsymbol{w}_{1,c}^{\dagger} & 0 \end{bmatrix}$$

Then, we can write

$$\begin{aligned} \boldsymbol{W}_\theta &= \boldsymbol{H}_2\boldsymbol{D}\boldsymbol{H}_2^{\dagger} + \boldsymbol{H}_2\boldsymbol{F}\boldsymbol{A}\boldsymbol{F}^{\dagger}\boldsymbol{H}_2^{\dagger} \\ &= \boldsymbol{H}_2\boldsymbol{D}\boldsymbol{H}_2^{\dagger} + \boldsymbol{H}_2\boldsymbol{\Delta}\boldsymbol{R}_\theta\boldsymbol{\Delta}^{\dagger}\boldsymbol{H}_2^{\dagger} \end{aligned}$$

where

$$\boldsymbol{\Delta} \triangleq \begin{bmatrix} \boldsymbol{w}_{1,c} & 0 \\ 0 & 1 \end{bmatrix}, \quad \boldsymbol{R}_\theta \triangleq \begin{bmatrix} 0 & e^{-j\theta} \\ e^{j\theta} & 0 \end{bmatrix}$$

Let

$$\begin{aligned} \mathcal{D} &\triangleq \det(\boldsymbol{I}_2 + \mathrm{SNR}\boldsymbol{H}_2\boldsymbol{\Delta}\boldsymbol{R}_\theta\boldsymbol{\Delta}^{\dagger}\boldsymbol{H}_2^{\dagger}(\boldsymbol{I} + \mathrm{SNR}\boldsymbol{H}_2\boldsymbol{D}\boldsymbol{H}_2^{\dagger})^{-1}) \\ &= \det(\boldsymbol{I}_2 + \mathrm{SNR}\boldsymbol{R}_\theta\boldsymbol{\Delta}^{\dagger}\boldsymbol{H}_2^{\dagger}(\boldsymbol{I} + \mathrm{SNR}\boldsymbol{H}_2\boldsymbol{D}\boldsymbol{H}_2^{\dagger})^{-1}\boldsymbol{H}_2\boldsymbol{\Delta}) \\ &= \det(\boldsymbol{I}_2 + \mathrm{SNR}\boldsymbol{R}_\theta\boldsymbol{\Delta}^{\dagger}\boldsymbol{W}_2\left(\boldsymbol{I} + \mathrm{SNR}\boldsymbol{D}\boldsymbol{W}_2\right)^{-1}\boldsymbol{\Delta}) \\ &= 1 + \mathrm{SNR}^2\det\left(\boldsymbol{R}_\theta\right)\det(\boldsymbol{\Delta}^{\dagger}\boldsymbol{Q}\boldsymbol{\Delta}) + \mathrm{SNR}\mathrm{Tr}(\boldsymbol{R}_\theta\boldsymbol{\Delta}^{\dagger}\boldsymbol{Q}\boldsymbol{\Delta}) \\ &= 1 - \mathrm{SNR}^2\det\left(\boldsymbol{P}\right) + \mathrm{SNR}\mathrm{Tr}\left(\boldsymbol{R}_\theta\boldsymbol{P}\right) \\ &= 1 - \mathrm{SNR}^2\det\left(\boldsymbol{P}\right) + 2\mathrm{SNR}\mathcal{R}\left\{P_{12}e^{j\theta}\right\} \\ &= 1 - \mathrm{SNR}^2\det\left(\boldsymbol{P}\right) + 2\mathrm{SNR}|P_{12}|\cos\left(\theta + \angle P_{12}\right), \end{aligned} \tag{2.44}$$

where

$$\boldsymbol{Q} \triangleq \boldsymbol{W}_2\left(\boldsymbol{I} + \mathrm{SNR}\boldsymbol{D}\boldsymbol{W}_2\right)^{-1} \text{ and } \boldsymbol{P} \triangleq \boldsymbol{\Delta}^{\dagger}\boldsymbol{Q}\boldsymbol{\Delta} \in \mathbb{C}^{2\times 2}.$$

Considering one rotation, the expression of $\mathcal{D}$ is periodic in θ over $[0, 2\pi)$. The destination feeds back to the relay the value of θ that maximizes the mutual information of the channel, $\theta_{opt} = -\angle P_{1,2}$.

Chapter 3

Introduction to Network Coding Theory

NETWORKS are taking a central place in our daily life. The network systems arise in various communication contexts such as phone networks, sensor networks, wireless ad-hoc networks and the world wide web. The emersion of network use in the last decade appeals to significant efforts devoted to the operation and management of these networks. The traditional way of information transportation on these networks is to keep independent information streams separate. In existing network systems, information is transmitted from the source node to each destination node through a chain of intermediate nodes by a method known as *store-and-forward*. In this method, data packets received from an input link of an intermediate node are stored and a copy is forwarded to the next node via an output link. In case of multiple destinations, the intermediate node sends a copy of the data packets onto each output link that leads to at least one of the destinations. Therefore, the only data processing on intermediate nodes is *replication*.

In case of one source-destination pair, the store-and-forward strategy is sufficient to achieve the capacity of the network. However, in case of multiple source-destination pairs, applying this approach on the common intermediate nodes results in forwarding only one source information packet at a time, and then more power consumption at the intermediate node, and more latency and smaller bit rate in the network. Recently, an important observation was made that in communication networks, we can allow intermediate nodes to not only forward but also process the incoming independent information flows. At the network layer, for example, intermediate nodes can perform binary operations on independent bit streams, whereas, at the physical layer, intermediate nodes can perform linear and non linear

operations. In other words, it is not necessary to keep separate independent bit streams and there exist several ways to combine them and later extract independent information.

Combining independent data streams is the fundamental concept of *network coding* developed in [34]. Due to its generality and its wide application potential, network coding has generated much interest in information and coding theory, networking, switching, wireless communications, complexity theory, cryptography, operations research, and matrix theory. The network coding have changed our way of manage and organize networks and is expected to have a deep impact on wide range of areas such as reliable delivery, ressource sharing, efficient flow control, network monitoring, and security.

Section 3.1 introduces this chapter with simple examples to illustrate the basic concepts in network coding and to give a general idea about the benefits and challenges. In Section 3.2, we give the main theorem of the network coding based on the Graph Theory. This theorem gives the sufficient conditions to allow each destination to receive information at a certain rate as if it uses the hole network alone. We give also an equivalent algebraic statement of the theorem. In Section 3.3, we introduce the physical-layer network coding (PLNC) which is the electromagnetic-wave-based network coding, and we give an overview of the literature in this field.

3.1 Network Coding: Benefits and Challenges

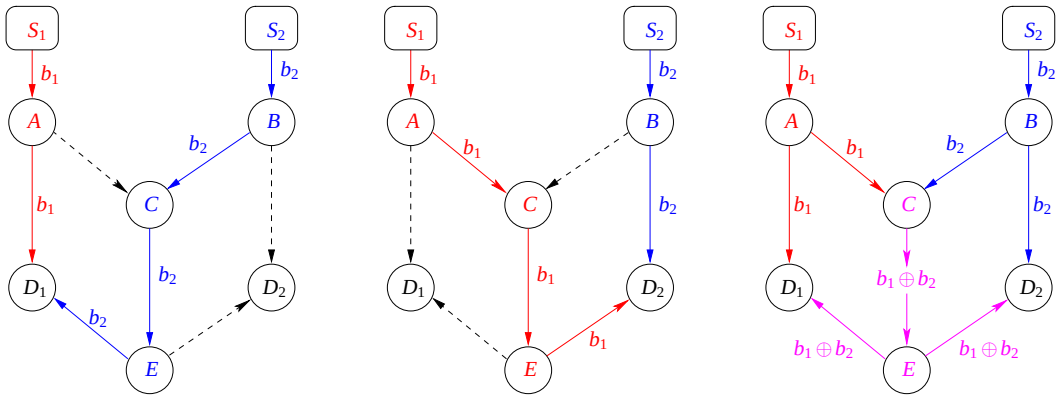
Network coding offers benefits in numerous aspects of communication networks. We highlight, through examples, the added value of this technique in throughput, wireless ressources sharing, and security. On the other hand, the deployment of network coding faces a number of challenges as complexity, security, and integration in existing infrastructures. We give the definition of multicast for convenience.

Definition 3.1 *In networking, multicast is the delivery of a message or information to a group of destinations simultaneously in a single transmission from the source creating copies automatically in other network elements, such as routers (relays), only when the topology of the network requires it.*

3.1.1 Throughput

The first benefits of network coding are in terms of throughput when we are interested in multicast. We show this using the butterfly network, a well-known network in the network coding literature.

Figure Fig.3.1 depicts the butterfly communication network in which vertices correspond to nodes and edges correspond to channels. The directed edges indicate the propagation of information between nodes. Assume that the time is slotted, and that through each channel



(a) Routing to D_1 (b) Routing to D_2 (c) Network coding

Figure 3.1: The Butterfly Network. Sources S_1 and S_2 multicast their information to receiver D_1 and D_2.

we can send one bit per time slot. In addition, we suppose that each source sends one bit by time slot. The network is composed of two sources S_1 and S_2, and two destinations D_1 and D_2. The sources information bits are denoted by b_1 and b_2 respectively.

If destination D_1 uses all the network ressources alone, it could receive both sources bits. Indeed, D_1 can receive b_1 through the path $\{S_1AD_1\}$, and b_2 through the path $\{S_2BCED_1\}$ as presented in Fig.3.1(a). Similarly if destination D_2 uses all the network ressources alone, it could receive b_1 through the path $\{S_1ACED_2\}$, and b_2 through the path $\{S_2BD_2\}$ as presented in Fig.3.1(b).

Now, we are interested in multicast. Suppose that we want to send b_1 and b_2 simultaneously to both destinations. Using the traditional way of transportation over networks which is keeping independent flows separate, we have to make a decision on the channel $\{CE\}$ to transmit either b_1 or b_2; each channel is able to transmit one bit at a time slot. In this case, destination D_1 receives both b_1 and b_2, and destination D_2 receives only b_2, or vice versa. Alternating the use of the channel $\{CE\}$ to transmit the bits of S_1 and S_2 acheives a multicast rate of 1.5 bits per unit time, which is the maximum possible rate when the intermediate nodes perform just bits replication.

Another way of multicast is to allow the intermediate nodes to process independent data streams, and not only forward them toward the destination. In this scope, node C can take the two bits b_1 and b_2, xor them (binary addition operation) to create the exclusive-OR bit $b_1 \oplus b_2$, and then send $b_1 \oplus b_2$ on the channel $\{CE\}$ as shown in Fig.3.1(c). Then, node E forwards $b_1 \oplus b_2$ to D_1 and D_2. Having b_1 and $b_1 \oplus b_2$, the destination D_1 can solve the system to obtain b_2. Similarly, D_2 can solve the system to obtain b_1 and b_2. In this way, we can achieve a multicast rate of 2 bits per unit time.

The derivation of the exclusive-OR bit is a simple form of coding. The coding mechanism enhances the bit rate. The previous example shows a fundamental fact in information theory: when there are multiple sources transmitting information over a communication network, we can increase the throughput by allowing joint coding of information at intermediate nodes.

3.1.2 Wireless Ressources

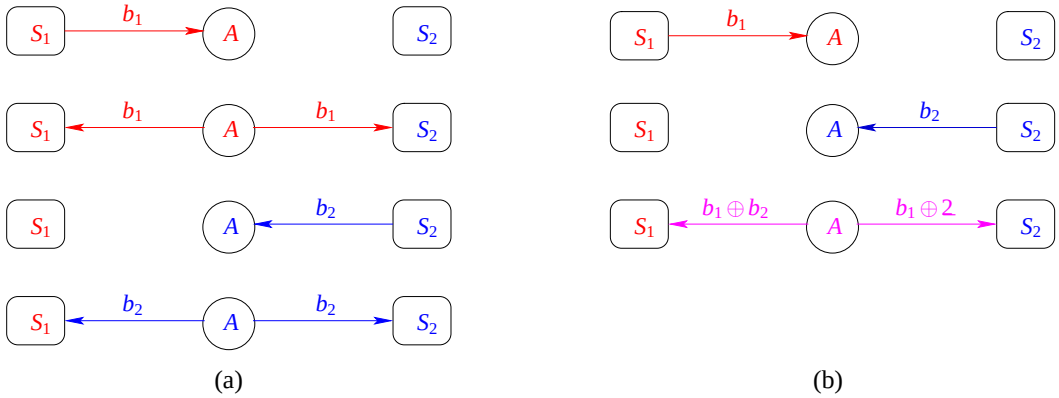


Figure 3.2: The sources S_1 and S_2 exchange bits via relay node A.

Consider that the sources S_1 and S_2 would like to exchange their bits b_1 and b_2 via the relay node A. The Fig.3.2(a) shows the bits exchange using the traditional way: S_1 and S_2 send their bits to relay A, who in turn forwards each bit to the corresponding destination.

Using the network coding approach, we allow relay A to produce an exclusive-OR bit $b_1 \oplus b_2$ and to broadcast this bit to S_1 and S_2. Then, S_1 has b_1, and can decode b_2. Similarly, S_2 has b_2, and can decode b_1. This is shown in the Fig.3.2(b).

This approach offers benefits in terms of energy efficiency (relay A transmits once instead of twice); the battery lifetime is enhanced, delay (three time slots instead of four to exchange the bits), wireless bandwidth (the wireless channel is occupied for a smaller amount of time), and interference (if there are other wireless nodes attempting to communicate in the neighborhood).

3.1.3 Security

Consider a source S sending information to a destination D via two paths $\{SAD\}$ and $\{SBD\}$. Assume that there exists an eavesdropper that can wiretap a single path. If the bits b_1 and b_2 are sent without coding as in Fig.3.3(a), the eavesdropper can intercept one of them. However, if we send a linear combination of bits as in Fig.3.3(b), the eavesdropper can not decode any of them. Thus, sending linear combination of bits or packets instead of uncoded data offers a natural way of protection against wiretapping attacks.

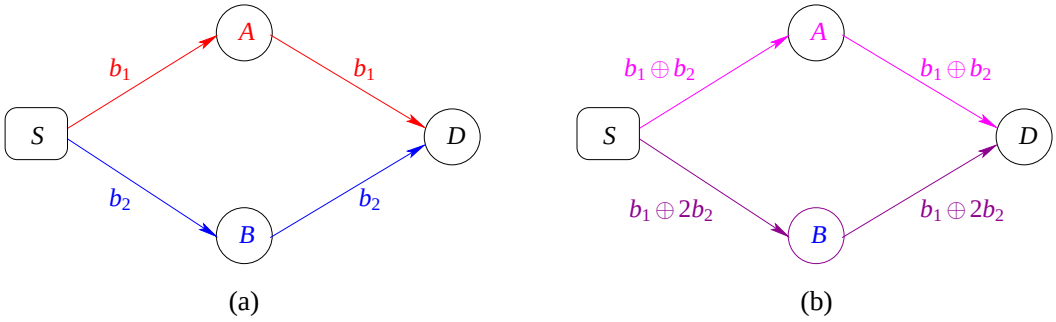


Figure 3.3: Mixing information offers a natural protection against eavesdroppers.

3.1.4 Complexity

The nodes in a network are required additional functionalities if network coding is deployed. For example, in Fig.3.2, the relay node A needs additional memory to store the bits b_1 and b_2, and additional computation ability to perform the exclusive-OR operations. Moreover, the nodes S and D need to store their own information and resolve a linear system to extract the each others bits.

An essential question in network coding research today is to investigate the complexity requirements of network coding and the tradeoff that offers between complexity and performance.

3.1.5 Security

Network coding requires intermediate nodes to perform operations on data. This could be problematic for some applications traffic such as banking transactions. In these types of applications, the destination is the only entity eligible to treat the data. Therefore, the deployment of network coding requires to put in place some mechanisms that allow to make operations without affecting the authenticity of the data.

3.1.6 Integration with Existing Infrastructure

A challenging task is to integrate network coding into existing network architectures. We would like to take benefits from the added value of network coding without dramaticly changing the existing equipments and softwares.

3.2 The Main Network Coding Theorem

3.2.1 The Min-Cut Max-Flow Theorem

Let $G = (V, E)$ be a graph (network) with a set of vertices (nodes) V and a set of edges (channels) $E \subset V \times V$. Consider a source $S \in V$ transmitting information to a destination

$D \in V$. We assume that each edge has a unit capacity and allow multiple edges between two vertices. For convenience, we give the following definitions.

Definition 3.2 *A communication network is a finite directed graph, where multiple edges from one node to another are allowed.*

Definition 3.3 *A communication network is said to be acyclic if it contains no directed cycles.*

Definition 3.4 *A cut between S and D is a set of graph edges whose removal disconnects S from D. The value of a cut is the sum of the capacities of the edges in the cut. A min-cut is a cut with the smallest value.*

The min-cut value represents the maximum amount of information that can be sent from the source to the destination in a given network. This result is stated in the following theorem.

Theorem 3.1 *Consider a graph $G = (V, E)$ with unit capacity edges, a source vertex S, and a destination vertex D. If the min-cut value between S and D equals R, then the information can be sent between S and D over G at a maximum rate R. Equivalently, there exist exactly R edge-disjoint paths between S and D.*

The min-cut max-flow theorem was proven in 1927 by Menger [35]. It was also proven in 1956 by Fulkerson [36] and independently the same year by Elias *et al.* [37].

3.2.2 The Main Network Coding Theorem

Consider a multicast scenario over a network $G = (V, E)$, in which the rate R source S is seen as R unit rate sources $S_1, \ldots, S_R$ located at the same network vertex. The R sources are simultaneously transmitting information to N destinations. G is acyclic with unit capacity edges. The value of the min-cut between the source node and each of the destinations is R. We also assume *zero delay*, which means that during each time slot, all nodes simultaneously receive all their inputs and send their outputs.

Each unit source S_i emits an element of the finite field $\mathbb{F}_q$ of size q. Using an alphabet of size $q = 2^m$ simply means that the bits are sent form the sources in packets of m bits. Suppose that each edge can reliably carry one bit and each source can produce one bit in each time unit, the m time-units corresponding to sending a symbol are defined as one time slot. The m bits are seen as one symbol of $\mathbb{F}_q$ and are processed using operations over $\mathbb{F}_q$ by the nodes in the network. The main theorem in network coding is stated as follows.

Theorem 3.2 *Consider a directed acyclic graph $G = (V, E)$ with unit capacity edges, R unit rate sources located on the same vertex of the graph and N destinations. Assume that the value of the min-cut to each destination is R. Then there exists a multicast transmission scheme over a large enough finite field $\mathbb{F}_q$, in which intermediate network nodes linearly*

combine their incoming information symbols over $\mathbb{F}_q$, that delivers the information from the sources simultaneously to each receiver at a rate equal to R.

The min-cut value to each destination is equal to R. So, if each destination uses the network ressources by itself, the information can be routed to that destination at rate R through a set of R edge-disjoint paths. However, when multiple destinations use the network, their set of paths may overlap. Traditionally, the network ressources are shared between destinations, and then, the rate transmission is reduced. The main network coding theorem states that if we allow intermediate nodes to not only forward but to combine their received information flows, then each destination will have his information at rate R as if it had sole access to network ressources.

The theorem additionally claims that it is sufficient for intermediate nodes to perform linear operations, namely, additions and multiplications over a finite field $\mathbb{F}_q$. Thus the theorem establishes the existence of linear network codes over some large enough finite field $\mathbb{F}_q$.

3.2.3 An Equivalent Algebraic Statement of the Theorem

In linear network coding [38], we can transmit through each edge e, a linear combination of the incoming source symbols $\sigma_1, \ldots, \sigma_R$, $\sigma_i \in \mathbb{F}_q$. The coefficient used to form the linear combination constitute a vector $c(e) = [c_1(e) \ \ldots \ c_R(e)]$, associated with edge e. Then, the symbol flowing through an edge e of a graph network G is given by

$$c_1(e)\sigma_1 + c_2(e)\sigma_2 + \ldots + c_R(e)\sigma_R = \begin{bmatrix} c_1(e) & c_2(e) & \ldots & c_R(e) \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_R \end{bmatrix}$$

$c(e) \in \mathbb{F}_q^{1\times R}$ is the *coding vector*.

The coding vectors associated with the input edges of a destination node define a system of linear equations that the destination can solve to determin the source symbols. Consider for example a receiver D_j and let r_i^j be the symbol received at the last edge of the path (S_j, D_j), and $\boldsymbol{A}_j$ the matrix whose ith row is the coding vector of the last edge on the path (S_j, D_j). Then, the destination D_j has to solve the following system of linear equations:

$$\begin{bmatrix} r_1^j \\ r_2^j \\ \vdots \\ r_R^j \end{bmatrix} = \boldsymbol{A}_j \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_R \end{bmatrix}$$

to extract the symbol information $\sigma_1, \ldots, \sigma_R$. Therefore, choosing the coding vectors such

that all $\boldsymbol{A}_j$, $1 \leq j \leq N$, are full rank, enables all destinations to extract source information symbols from the linear combinations that they have received. One more condition that these vectors have to satisfy: the global coding vector of an output edge of a node has to lie in the linear span of the coding vectors of the node's input edges.

As example, we take the network in Fig.3.4, the three destinations D_1, D_2, and D_3 observe the linear combinations defined by the matrices $\boldsymbol{A}_1$, $\boldsymbol{A}_2$, and $\boldsymbol{A}_3$ as

$$\boldsymbol{A}_1 = \begin{bmatrix} 1 & 0 \\ \alpha_3 + \alpha_1\alpha_4 & \alpha_2\alpha_4 \end{bmatrix}, \quad \boldsymbol{A}_2 = \begin{bmatrix} 0 & 1 \\ \alpha_1 & \alpha_2 \end{bmatrix}$$
$$\boldsymbol{A}_3 = \begin{bmatrix} \alpha_1 & \alpha_2 \\ \alpha_3 + \alpha_1\alpha_4 & \alpha_2\alpha_4 \end{bmatrix}$$

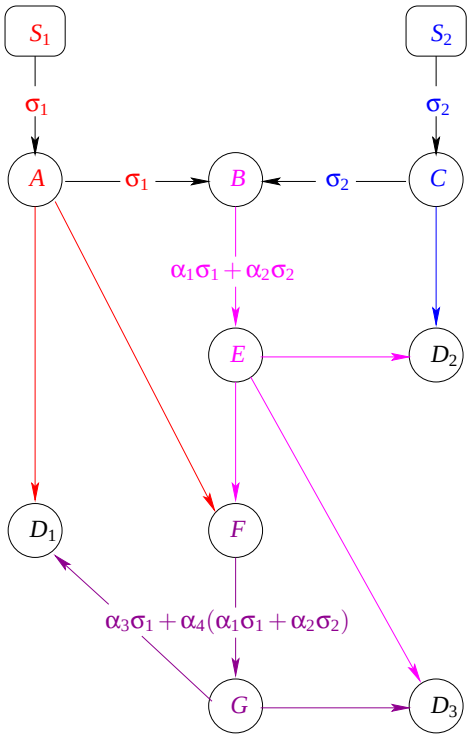


Figure 3.4: Example of a linear network coding solution.

The network code design problem consists of finding coefficients α_k, $1 \leq k \leq 4$, such that the matrices $\boldsymbol{A}_j$, $1 \leq j \leq 3$, are full rank. The main multicast theorem can be expressed as follows,

Theorem 3.3 *In linear network coding, there exist values in some large enough finite field $\mathbb{F}_q$ for the components $\{\alpha_k\}$ of the coding vectors, such that all matrices $\boldsymbol{A}_j$, $1 \leq j \leq N$, defining information that the receivers observe, are full rank.*

The main theorem in network coding was proven by Ahlswede *et al.* [34] in 2000. It claims the existence of network codes for multicast. Many questions arise from this theorem. Can we construct network codes efficiently? How large does the operating field $\mathbb{F}_q$ need to be? What are the complexity requirements of network coding? Does network coding give benefits in other network types, such as networks with noisy links, or wireless networks, or traffic patterns other than multicast? What is the possible impact on applications.

We refer the reader to more discussions about these issues in [39], and [40], and to the *Network Coding Homepage* [41].

3.3 Physical Layer Network Coding

At the physical layer of wireless networks, the data is transmitted through electromagnetic (EM) waves. At this level, wireless networks are characterized by two principle features; broadcast and interference. Under the broadcast feature, the EM wave transmitted by a node is received not only by the intendant receiver, but also by all the nodes connected to the transmitter. Under the interference feature, the EM wave received at a receiver node is the sum of all EM waves transmitted, at the same time, by different transmitters in the network.

Traditionally, the interference nature of a wireless network has long been considered as a source of nuisance. It has particularly, negative effects on multi-hop ad-hoc networks. Therefore, most communication system designs try to either reduce or avoid interference. However, instead of avoiding interference, we can actuallay embrace interference to improve systems performance. To do so in a multi-hop network, two goals must be met [42]:

1. A relay must be able to convert simultaneously received signals to interpretable output signal to be relayed to the final destination.
2. A destination must be able to extract the information addressed to it from the relayed signals.

Network coding as we have presented in previous sections, applies on bits that have already been detected. In [42], Zhang *et al.* have proposed the Physical-Layer Network Coding (PLNC) to emulate the *straightforward* network coding, but at the lower physical layer that deals with EM signals, and to make use of the additive nature of simultaneously arriving EM waves. The authors have proven that PLNC can yield higher capacity than straightforward network coding when applied to wireless networks.

3.3.1 Illustrating Example

The authors in [42] have proven the potential of PLNC schemes in boosting the capacity of wireless networks. As an illustration, we reconsider here the network of Fig.3.2 where two nodes S_1 and S_2 exchange information via a relay A. As seen before, the traditional way of

transmission using a scheduling scheme takes four time slots to do the information exchange, Fig.3.2(a), while it took three time slots using the straightforward network coding scheme, Fig.3.2(b).

In order to introduce PLNC, the authors assume the use of QPSK modulation at all nodes. They further assume symbol-level and carrier-phase synchronization, and the use of power control, so that the frames form S_1 and S_2 arrive at A with the same phase and amplitude. The combined bandpass signal at A during one symbol period is,

$$\begin{aligned} s_A(t) &= s_1(t) + s_2(t) \\ &= [a_1 \cos(wt) + b_1 \sin(wt)] + [a_2 \cos(wt) + b_2 \sin(wt)] \\ &= (a_1 + a_2)\cos(wt) + (b_1 + b_2)\sin(wt). \end{aligned} \tag{3.1}$$

where $s_i(t)$, $i = 1, 2$, is the bandpass signal transmitted by S_i and $s_A(t)$ is the bandpass signal received at A during one symbol period. a_i and b_i are the QPSK modulated information bits of S_i, and w is the carrier frequency.

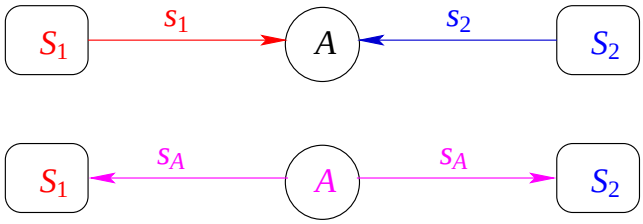


Figure 3.5: Physical Layer Network Coding.

The relay A can not extract the individual information of the sources S_1 and S_2. However, A just relays information to S_1 and S_2 that help them to extract a_1, a_2, b_1 and b_2. For this end, the authors have proposed a special modulation/demodulation mapping scheme to obtain the equivalence of $\mathbb{F}_2$ summation of bits from S_1 and S_2 at the physical layer. We refer the reader to the paper [42] for more details about the PLNC mapping of the in-phase and quadrature-phase bits $s_A^{(I)}$ and $s_A^{(Q)}$ of A and the corresponding BPSK modulated bits a_A and b_A. Based on this, the relay A obtains the information bits:

$$s_A^{(I)} = s_1^{(I)} \oplus s_2^{(I)}. \tag{3.2}$$

$$s_A^{(Q)} = s_1^{(Q)} \oplus s_2^{(Q)}. \tag{3.3}$$

$s_j^{(I)} \in \{0, 1\}$ is the in-phase data bit of S_j and $s_j^{(Q)} \in \{0, 1\}$ is the quadrature bit of S_j. The relay transmits

$$s_A(t) = a_A \cos(wt) + b_A \sin(wt). \tag{3.4}$$

Upon receiving $s_A(t)$, S_1 and S_2 can derive $s_A^{(I)}$ and $s_A^{(Q)}$ by ordinary QPSK demodulation. The derived bits are used to form the frame S_A.

As illustrated in Fig.3.5, PLNC requires only two time slots for the exchange of one frame as opposed to three time slots in straightforward network coding and four time slots in traditional scheduling. The authors have shown that PLNC has the same BER performance as the straightforward network coding scheme, and that PLNC can achieve the theoretical upper-bound capacity of the linear networks. They established the general PLNC modulation/demodulation mapping principle required to ensure the equivalence of network coding arithmetic and EM wave interference arithmetic.

3.3.2 A Quick Overview on the State of the Art

Physical layer network coding moves the principle of network coding closer to the channel. Instead of avoiding interference and decoding individually received packets, the intermediate nodes are allowed to send a noiseless linear combinations of these packets such that any destination node in the network is able to recover the original packets.

The idea of physical network coding (PLNC) appears to be proposed independently by several research groups in 2006; Zhang, Liew, and Lam in [42] [43], and Popovski and Yomo [44]. The authors showed that the we can significantly improve the throughput of the two-way relay channel by allowing the relay to forward a combination of the received information [42] [44]. Due to its potential, PLNC has received particular research attention over the last few years, with a particular focus on the two-way relay channel, *e. g.*, Popovski and Koike-Akino [45], Wilson, Narayanan, Pfister and Sprintson [46], Koike-Akino, Popovski and Tarokh [47], and Hern and Narayanan [48].

R. Koetter and M. Medard in [49] have extended the network coding framework to arbitrary networks. For networks which are restricted to using linear network codes, they have found necessary and sufficient conditions for the feasibility of any given set of connections over a given network. For the multicast setup, they have proven that there exist coding strategies that provide maximally robust networks and that do not require adaptation of the network interior to the failure pattern in question. The results are derived for both delay-free networks and networks with delays.

The authors Katti, Gollakota, and Katabi in [50] have reconsidered the two-way relay network and have implemented a design using software radios and have shown that it achieves significantly higher throughput than both traditional wireless routing. In this paper, PLNC is called *analog network coding* because the relays mix signals not bits.

Lim, Kim, El Gamal, and Chung in [51] have proposed a noisy network coding scheme over a general noisy network between multiple sources and destinations. Their scheme is a generalization of the network coding over wireless networks (Ahlswede *et al.* [34]), the compress-forward coding for the relay channel (Cover *et al.* [13]), and the deterministic networks (Avestimehr *et al.* [28]). They key features of their scheme are: first, a source node

sends the same message over multiple blocks, second, the relays do not use Wyner-Ziv coding (no binning indices to decode), and third, simultaneous nonunique decoding over all blocks is used without requiring the compression indices to be decoded uniquely. They have used their scheme to establish inner bounds on the capacity region of general multi-message noisy networks. They have proven that for the Gaussian multicast network, noisy network coding improves the previously established gap to the cut-set bound, and that noisy network coding can outperform conventional compress-forward, amplify-forward, and hash-forward coding schemes.

In a recent work [3], Nazer and Gastpar have proposed a new physical-layer network coding scheme. Their strategy, called compute-and-forward (CF), exploits interference to obtain higher end-to-end transmission rates between users in a network. The relays are required to decode noiseless linear equations of the transmitted messages using the noisy linear combination provided by the channel. The destination, given enough linear combinations, can solve the linear system for its desired messages. This strategy is based on the use of structured codes, particularly nested lattice codes to ensure that integer combinations of codewords are themselves codewords. The authors have demonstrated its asymptotic gain using information-theoretic tools.

The authors Feng, Silva, and Kschischang in [52] have followed the framework of Nazer and Gastpar and have shown the potential of the compute-and-forward protocol using an algebraic approach. They have related the Nazer-Gastaper's approach to the theorem of finitely generated modules over a principle ideal domain (PID). They have given sufficient conditions for lattice partitions to have a vector space structure which is a desirable property to make them well suited for physical-layer network coding. Then, they have generalized the code construction and have developed encoding and decoding methods. In their work [53], based on the algebraic approach, they have derived the design criteria for the compute-and-forward codes driven from finite-dimensional lattice partitions.

In [5], Niesen and Whiting have proven that the lattice implementation of compute-and-forward as proposed by Nazer and Gastpar suffers from a loss in number of achieved degrees of freedom. They have proposed a different implementation consisting of a modulation scheme and an outer code and have shown that it achieves full degrees of freedom as if full cooperation among transmitters and among relays was permitted.

3.4 Conclusion

This chapter served to introduce the principle of network coding for multicasting in multiple-source multiple-destination networks. First, we gave a general idea about the benefits and challenges of network coding. Second, we developed the main network coding theorem in both network and algebraic forms. And third, we presented the physical-layer network cod-

ing, which is the equivalent of the classical network coding at the physical layer.

In the next chapter, we are particularly interested in the compute-and-forward (CF) protocol. This relaying strategy is an application of the physical-layer network coding. In the last two years, the CF has become an attractive research field. In the sequel of this thesis, we study the practical issues and the implementation of the CF protocol. We propose a new decoding technique and give criteria to design lattice codes.

Chapter 4

Physical Layer Network Coding: The Compute-and-Forward Protocol

INTERFERENCE is commonly seen as nuisance in wireless communication systems. The physical layer network coding (PLNC) principle takes advantage of the intrinsic noisy-interfered nature of the wireless medium to increase the transmission rates between users in a network. More precisely, the users help to relay each other's messages by exploiting the broadcast and multiple-access properties of the wireless medium.

In this scope, Bobak Nazer and Michael Gastpar have proposed a new PLNC scheme, the compute-and-forward (CF) protocol [3]. Briefly, the relays decode linear functions of all of the transmitted messages rather than decoding some of them and considering the others as interference. After decoding these linear functions, the relays send them to the other relays or to the destination. The destination, given enough equations, can recover the original messages. The CF strategy is based on the use of structured codes, particularly nested lattice codes. This ensures that integer functions of codewords are themselves codewords.

In this chapter, we are interested in the practical aspects of the compute-and-forward scheme. We take the protocol as presented by Nazer and Gastpar and implement the scheme for real Gaussian channels and one dimensional lattices. We begin by presenting the protocol as described in the original work [3] in Section 4.1. In Section 4.2, we define the rate outage probability for the CF scheme and show that it is less than the channel outage probability of a multiple-access channel (MAC). In Section 4.4.1, we give the system model of our interest. In Section 4.3, we explain how to find the linear function that maximizes the computation rate

of the CF scheme, and relate this to the lattice shortest vector problem. In Sections 4.4.2, 4.4.3, and 4.4.4, we derive a decoding technique based on the Maximum Likelihood (ML) criterion. We show that it can be implemented by using an Inhomogeneous Diophantine Approximation algorithm. Finally, we give some numerical examples showing the performance of our decoding strategy.

4.1 The Compute-and-Forward Protocol: The Original Work

As a starting point, we provide a description of the compute-and-forward protocol as presetend in [3]. In this section, we present the framework on how to deliver equations to a set of relays, and show how a destination, given sufficiently many equations, can recover the intendant messages. Then, we describe the achievable rate region for any AWGN network.

4.1.1 Decoding Equations

Consider a finite field of size p denoted by $\mathbb{F}_p$, with p prime. $\mathbb{C}$ is the complex field. Consider N transmitters indexed by n, $n = 1, \ldots, N$. Each transmitter has two vectors of length k over the finite field, $\boldsymbol{w}_n^R$, $\boldsymbol{w}_n^I \in \mathbb{F}_p^k$. The superscripts R and I designate the real and imaginary parts of the channel. $\boldsymbol{w}_n = (\boldsymbol{w}_n^R, \boldsymbol{w}_n^I)$ is the message of transmitter n. Each transmitter is equipped with an encoder, $\mathcal{E}_n$, that maps messages $\boldsymbol{w}_n$ of length k each over the finite field to messages $\boldsymbol{x}_n$ of length K each over the complex field, *i. e.* $\boldsymbol{x}_n = \mathcal{E}(\boldsymbol{w}_n)$,

$$\mathcal{E}_n : \mathbb{F}_p^k \times \mathbb{F}_p^k \to \mathbb{C}^K.$$

The message rate r of each transmitter is

$$r = \frac{2k}{K} \log p,$$

and each transmitter is subject to the power constraint:

$$\frac{1}{K} \|\boldsymbol{x}_n\|^2 \leq \text{SNR}.$$

Consider M relays. Each relay sees a noisy linear combination of the transmitted signals x_n through the channel. The input-output relation at a relay m, $m = 1, \ldots, M$, is:

$$\boldsymbol{y}_m = \sum_{n=1}^{N} h_{mn} x_n + \boldsymbol{z}_m, \tag{4.1}$$

where $h_{mn} \in \mathbb{C}$ is the channel coefficients from transmitter n to receiver m. $\boldsymbol{h}_m = [h_{m1} \ldots h_{mN}]^T$ denotes the vector of channel coefficients to relay m. $\boldsymbol{z}$ is i.i.d. circularly symmetric Gaussian noise, $\boldsymbol{z} \sim \mathcal{CN}(\boldsymbol{0}, \boldsymbol{I}^{K \times K})$.

Each relay is equipped with a decoder, $\mathcal{D}_m$, that maps the observed channel output from the complex field back to two equations of messages over the finite field:

$$\mathcal{D}_m : \mathbb{C}^K \to \mathbb{F}_p^k \times \mathbb{F}_p^k.$$

Each relay aims to decode a linear equation of the transmitted messages. Relay m selects coefficients q_{mn}^R, $q_{mn}^I \in \mathbb{F}_p$ for $n = 1, \ldots, N$ and decodes the two equations:

$$\boldsymbol{u}_m^R = \sum_{n=1}^{N} q_{mn}^R \boldsymbol{w}_n^R \oplus (-q_{mn}^I)\boldsymbol{w}_n^I \tag{4.2}$$

$$\boldsymbol{u}_m^I = \sum_{n=1}^{N} q_{mn}^I \boldsymbol{w}_n^R \oplus q_{mn}^R \boldsymbol{w}_n^I. \tag{4.3}$$

$\oplus$ is the addition over the finite field $\mathbb{F}_p$. The coefficient vector $\boldsymbol{a}_m = [a_{m1} \ldots a_{mN}]^T \in \mathbb{Z}[i]^N$ is the equivalent in the complex field of the coefficient vector $\boldsymbol{q}_m = (\boldsymbol{q}_m^R, \boldsymbol{q}_m^I)$, where $\boldsymbol{q}_m^R$ and $\boldsymbol{q}_m^I \in \mathbb{F}_p^N$.

A set of equations with coefficient vectors $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_M \in \mathbb{Z}[i]^N$ are decoded with an average probability of error ϵ if [3]:

$$\begin{aligned} &(\hat{\boldsymbol{u}}_m^R, \hat{\boldsymbol{u}}_m^I) \triangleq \mathcal{D}(\boldsymbol{y}_m) \\ &\mathrm{P}_e\left(\bigcup_{m=1}^{M} \left\{(\hat{\boldsymbol{u}}_m^R, \hat{\boldsymbol{u}}_m^I) \neq (\boldsymbol{u}_m^R, \boldsymbol{u}_m^I)\right\}\right) < \epsilon. \end{aligned} \tag{4.4}$$

A computational rate $R(\boldsymbol{h}, \boldsymbol{a})$ is achievable if for any $\epsilon > 0$ and n large enough, there exist encoders and decoders, $\mathcal{E}_1, \ldots, \mathcal{E}_N, \mathcal{D}_1, \ldots, \mathcal{D}_M$, such that for any set of channels, $\boldsymbol{h}_1, \ldots, \boldsymbol{h}_M \in \mathbb{C}^N$, and coefficient vectors, $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_M \in \mathbb{Z}[i]^N$, all relays can recover their desired equations with average probability of error ϵ so long as the underlying message rates $r_1, \ldots, r_N$ satisfy:

$$r_n < \min_{m:a_{mn}\neq 0} R(\boldsymbol{h}_m, \boldsymbol{a}_m). \tag{4.5}$$

4.1.2 Recovering Messages

The relays forward the equation of messages to the appropriate destinations. The messages may arrive at destination via several relays. The destination can recover a message $\boldsymbol{w}_n \in \mathbb{F}_p^{kn}$ at rate r_n from the equations with coefficient vectors $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_M \in \mathbb{Z}[i]^N$ if for any $\epsilon > 0$ and K large enough, there exists a decoder $\mathcal{D} : \left\{\mathbb{F}_p^k \times \mathbb{F}_p^k\right\}^M \to \mathbb{F}^k \times \mathbb{F}^k$ such that [3]:

$$\begin{aligned} &\hat{\boldsymbol{w}}_n = \mathcal{D}\left((\boldsymbol{u}_1^R, \boldsymbol{u}_1^I), \ldots, (\boldsymbol{u}_M^R, \boldsymbol{u}_M^I)\right) \\ &\mathrm{P}_e(\hat{\boldsymbol{w}}_n \neq \boldsymbol{w}_n) < \epsilon \end{aligned} \tag{4.6}$$

where $(\boldsymbol{u}_m^R, \boldsymbol{u}_m^I)$ represents the equation from relay m.

4.1.3 Nested Lattice Codes

In order to allow relays to decode linear and integer combinations of codewords, the authors, Bobak and Gastpar, proposed to use lattice codes that have good statistical and algebraic properties. These lattice codes are well-suited for mapping operations over a finite field to the complex field. We give some necessary definitions on lattices and nested lattice codes in Appendix 4.A.

The structured codes with specific algebraic structure are becoming attractive for proving capacity theorems. In a previous work by Bobak and Gastpar, they showed that structured coding arguments, such as random linear or lattice codes, attain higher rates than random coding arguments [54]. In another work, the authors showed that structured computation codes offer large gains for linear computation over multiple-access channels [55].

The construction of dense lattices and nested lattices is well known in all dimensions up to 29. The Construction A is the most effective in up to 15 dimensions. Construction B is effective in dimensions 8 to 24. Construction C, which generalizes A and B; is especially effective in dimensions that are powers of 2 [56]. Several generalizations of these three constructions exist in the literature [56].

4.1.4 Achievable Computation Rate

The channel output is a linear function of the channel inputs plus independent noise (Eq.4.1). The goal is to reconstruct a linear function with integer coefficients of the source symbols, $x_R = \sum_{n=1}^{N} a_n x_n$ at the relay with the lowest possible distortion. The distortion is given by the mean-squared error measure, $D = \frac{1}{N}\sum_{n=1}^{N} \mathbb{E}\left[x^R - \hat{x}^R\right]^2$.

The authors used a joint source-channel lattice scheme based on a joint Wyner-Ziv/dirty-paper coding scheme developed in [55]. The received signal y is scaled by a coefficient α. The following distorsion is achievable

$$D = \sigma_x^2 \left(\frac{|\alpha|^2 + \mathrm{SNR}\sum_{n=1}^{N}(\alpha h_n - a_n)}{\mathrm{SNR}} \right)$$

By evaluating $\log\left(\frac{\sigma_x^2}{D}\right)$, Nazer and Gastpar showed that a relay can recover any set of linear equations with coefficient vector $\boldsymbol{a}$ as long as the message rates are less than the computation rate defined as,

$$R_{\mathrm{comp}}(\boldsymbol{h}, \boldsymbol{a}) = \log\left(\frac{\mathrm{SNR}}{|\alpha|^2 + \mathrm{SNR}\|\alpha\boldsymbol{h} - \boldsymbol{a}\|^2} \right) \tag{4.7}$$

where $\boldsymbol{h} \in \mathbb{C}^N$ is the channel vector, $\boldsymbol{a} \in \mathbb{Z}[i]^N$ is the integer coefficient vector, and SNR is the signal-to-noise ratio at the relay. This computation rate is uniquely achievable by scaling

the received signal by the MMSE coefficient [3],

$$\alpha_{MMSE} = \frac{\mathrm{SNR}\boldsymbol{h}^{\dagger}\boldsymbol{a}}{1+\mathrm{SNR}\|\boldsymbol{h}\|^2}. \tag{4.8}$$

which results in a computation rate

$$R_{\mathrm{comp}}(\boldsymbol{h},\boldsymbol{a}) = \log\left(\left(\|\boldsymbol{a}\|^2 - \frac{\mathsf{SNR}|\boldsymbol{h}^{\dagger}\boldsymbol{a}|^2}{1+\mathsf{SNR}\|\boldsymbol{h}\|^2}\right)^{-1}\right), \tag{4.9}$$

Each relay is free to decode any linear equation, and is free to decode more than one equation as long as the appropriate computation rate is satisfied. However, it will often be interesting to find the coefficient vector $\boldsymbol{a}$ that maximizes the computation rate. Note that, if the nested lattice codes operate over the reals $\mathbb{R}^N$, the rate in Eq.4.9 is multiplied by a factor of $\frac{1}{2}$.

4.2 Rate Outage Probability

4.2.1 Definition

We consider a system operating with a computation rate R^0_{comp}. We define the rate outage probability as,

Definition 4.1 *The rate outage event occurs when the maximum achievable rate R_{comp} is lower than a fixed computational rate R^0_{comp}. The rate outage probability is defined as*

$$\mathsf{P}_{\mathsf{out}} = \mathsf{Prob}\left\{R_{\mathrm{comp}}(\boldsymbol{h},\boldsymbol{a}) < R^0_{\mathrm{comp}}\right\} \tag{4.10}$$

4.2.2 Upper Bound

We want to find an upper bound on the rate outage probability of the CF scheme.

We search for the coefficient vector $\boldsymbol{a}$ that maximizes the computation rate R_{comp} in Eq.4.9. This maximization is equivalent to the minimization of

$$R_{\mathrm{comp}}(\boldsymbol{h},\boldsymbol{a}) = \log\left(\left(\min_{\boldsymbol{a}}\left\{\boldsymbol{a}^{\dagger}\left(\boldsymbol{I} - c_h\boldsymbol{e}_h\boldsymbol{e}_h^{\dagger}\right)\boldsymbol{a}\right\}\right)^{-1}\right) \tag{4.11}$$

where $\boldsymbol{e}_h \triangleq \boldsymbol{h}/\|\boldsymbol{h}\|$ and $c_{\boldsymbol{h}} \triangleq 1-(1+\mathsf{SNR}\|\boldsymbol{h}\|^2)^{-1}$. The hermitian matrix $\left(\boldsymbol{I} - c_h\boldsymbol{e}_h\boldsymbol{e}_h^{\dagger}\right) \triangleq \boldsymbol{M}\boldsymbol{M}^{\dagger}$ defines a lattice Λ with generator matrix $\boldsymbol{M}$.

The minimum distance of a lattice can be equivalently defined as the shortest non zero lattice vector,

$$\boldsymbol{v}_{\min}(\Lambda) = \inf\left\{\|\boldsymbol{v}\| : \boldsymbol{v}\in\Lambda - \{\boldsymbol{0}\}\right\}. \tag{4.12}$$

Then, the problem is to solve for the minimal distance of the lattice Λ,

$$R_{\text{comp}} = \log\left\{d_{min}^{-2}(\Lambda)\right\}. \tag{4.13}$$

The theorem of Minkowski provides an upper bound on the minimal distance given by,

$$d_{min} \leq 2\left(\frac{vol(\Lambda)}{V_N}\right)^{\frac{1}{N}}, \tag{4.14}$$

where $vol(\Lambda)$ is the volume of the fundamental region given by $vol(\Lambda) = |\det(M)| = \sqrt{1 - c_{\boldsymbol{h}}}$, and V_N is the volume of the sphere of radius 1 given in Def.4.5 and Eq.4.30, respectively (see Appendix 4.A).

The rate outage probability of the compute-and-forward scheme, defined as the probability of the computation rate falling down under a certain given rate R^0_{comp}, is then

$$\begin{aligned}
\mathsf{P}_{\text{out}} = \mathsf{Prob}\left\{R_{\text{comp}} < R^0_{\text{comp}}\right\} &= \mathsf{Prob}\left\{d_{min} > 2^{-R^0_{\text{comp}}/2}\right\} \\
&\leq \mathsf{Prob}\left\{(1 - c_{\boldsymbol{h}})^{1/2N} > \frac{V_N^{1/N}}{2}.2^{-R^0_{\text{comp}}/2}\right\} \\
&= \mathsf{Prob}\left\{1 + \mathsf{SNR}\|\boldsymbol{h}\|^2 < 2^{N(R^0_{\text{comp}}+2)}V_N^{-2}\right\} \\
&= \mathsf{Prob}\left\{1 + \mathsf{SNR}\|\boldsymbol{h}\|^2 < 2^{N(R^0_{\text{comp}}+c)}\right\}.
\end{aligned} \tag{4.15}$$

where $c = \frac{1}{N}\log\left(\frac{2^N}{V_N}\right)^2 < 0$ independent of R^0_{comp}. Eq.4.15 is similar to the channel outage probability of a multiple-access channel (MAC) where the target rate is $N(R^0_{\text{comp}} + c)$.

Let I_{MAC} designate the mutual information of a two-user MAC channel, and I_{CF} be the mutual information in the compute-and-forward sense, *i.e.*, the maximum computation rate that can be used over the channel with asymptotically small *decoding* error. Using Eq.4.15, we can write

$$\begin{aligned}
\mathsf{Prob}\left\{I_{CF} < R^0_{\text{comp}}\right\} &\leq \mathsf{Prob}\left\{\log(1 + \mathsf{SNR}\|\boldsymbol{h}\|^2) < N(R^0_{\text{comp}} + c)\right\} \\
&= \mathsf{Prob}\left\{I_{MAC} < N(R^0_{\text{comp}} + c)\right\} \\
&= \mathsf{Prob}\left\{I_{MAC}/N - c < R^0_{\text{comp}}\right\},
\end{aligned}$$

and then, we conclude the following inequality:

$$I_{CF} > I_{MAC}/N - c. \tag{4.16}$$

The relay goal is to make a linear combination with integer coefficients of the transmitted messages. This will always be possible as long as the channel is not in outage. Therefore, the outage event of the compute-and-forward occurs when the following two conditions are

verified: the channel is in outage and the maximum computation rate that can be achieved falls below the target computation rate,

$$\begin{aligned} \mathsf{P}_{\mathsf{out}}(R^0_{\text{comp}}) &= \mathsf{Pout}\left\{\left\{I_{MAC} \leq NR^0_{\text{comp}}\right\} \cap \left\{I_{CF} \leq R^0_{\text{comp}}\right\}\right\} \quad (4.17) \\ &= \mathsf{Pout}\left\{I_{MAC} \leq NR^0_{\text{comp}}\right\}.\mathsf{Pout}\left\{I_{CF} \leq R^0_{\text{comp}} | I_{MAC} \leq NR^0_{\text{comp}}\right\} \\ &\leq \mathsf{Pout}\left\{I_{MAC} \leq NR^0_{\text{comp}}\right\}. \quad (4.18) \end{aligned}$$

4.2.3 Numerical Results For The Rate Outage Probability

In Fig.4.1 and Fig.4.2, we show using simulations that the rate outage probability is less or equal to the channel outage probability in the two cases of $N = 2$ and $N = 3$ sources, and for different values of target computation rate $R^0_{\text{comp}} = R$.

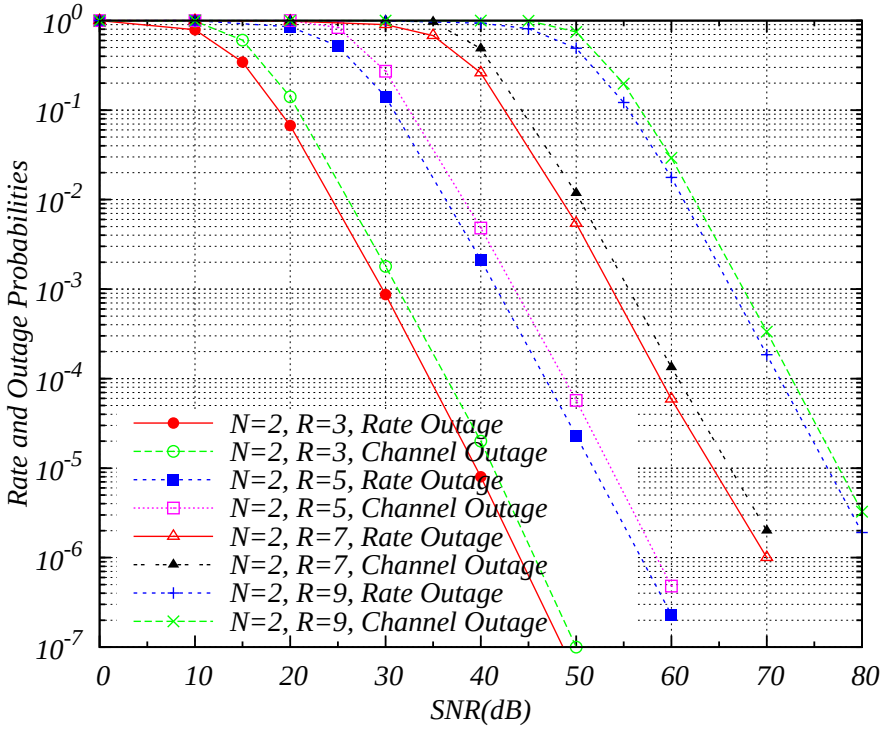


Figure 4.1: Rate outage probability and channel outage probability for 2 sources and one relay, and for $R^0_{\text{comp}} = R = 3,\ 5,\ 7,\ 9$.

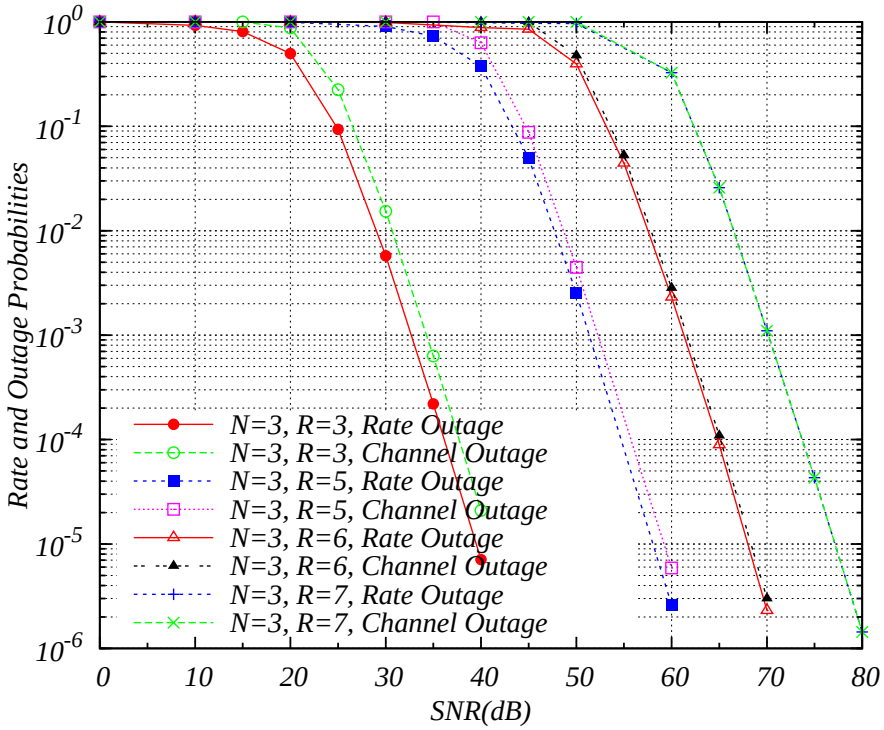


Figure 4.2: Rate outage probability and channel outage probability for 3 sources and one relay, and for $R^0_{\text{comp}} = R = 3,\ 5,\ 6,\ 7$.

4.3 Maximizing The Achievable Computation Rate

Consider the expression of the computation rate R_{comp} in Eq.4.9, and we want to find the vector $\boldsymbol{a}$ that maximizes R_{comp}. Hereafter, we show that the maximization of R_{comp} is equivalent to the search of a shortest vector in a lattice.

The primary goal of the decode-and-forward is to enable higher achievable rates across the network. Nazer and Gastpar showed that the relays can recover any set of linear equations with coefficient vector $\boldsymbol{a}$ as long as the message rates are less than the computation rate. We are interested in finding the coefficient vector with the highest computation rate. We state the result in the following theorem. This result is obtained in general settings, for a relay combining N symbols and for complex-valued channels.

Theorem 4.1 *For a given $\boldsymbol{h} \in \mathbb{C}^N$ (resp. $\mathbb{R}^N$), $R_{\text{comp}}(\boldsymbol{h}, \boldsymbol{a})$ is maximized by choosing $\boldsymbol{a} \in \mathbb{Z}[i]^N$ (resp. $\mathbb{Z}^N$) as*

$$\boldsymbol{a} = \arg\min_{\boldsymbol{a} \neq \boldsymbol{0}} \left(\boldsymbol{a}^\dagger \boldsymbol{G} \boldsymbol{a} \right) \tag{4.19}$$

where

$$\boldsymbol{G} = \boldsymbol{I} - \frac{\mathsf{SNR}}{1 + \mathsf{SNR}\|\boldsymbol{h}\|^2} \boldsymbol{H}. \tag{4.20}$$

$\boldsymbol{H} = [H_{ij}]$, $H_{ij} = h_i h_j^\star$, $1 \leq i, j \leq N$ and $\dagger$ is for the Hermitian transpose (resp. the regular

transpose).

Proof: Maximizing $R_{\text{comp}}(\boldsymbol{h}, \boldsymbol{a})$ is equivalent to the following minimization

$$\min_{\boldsymbol{a}\neq\boldsymbol{0}} \left\{ \|\boldsymbol{a}\|^2 + \mathsf{SNR}\|\boldsymbol{h}\|^2\|\boldsymbol{a}\|^2 - \mathsf{SNR}|\boldsymbol{h}^\dagger\boldsymbol{a}|^2 \right\}. \tag{4.21}$$

We can write

$$|\boldsymbol{h}^\dagger\boldsymbol{a}|^2 = |<\boldsymbol{a}, \boldsymbol{h}>|^2 = \sum_{i,j} h_i h_j^\star a_i^\star a_j,$$

$<\boldsymbol{a}, \boldsymbol{h}>$ is the inner Hermitian product of vectors $\boldsymbol{a}$ and $\boldsymbol{h}$.

Define the matrix $\boldsymbol{H} = [H_{ij}]$, where $H_{ij} = h_i h_j^\star$, for $1 \leq i, j \leq N$, it follows that $\sum_{i,j} h_i h_j^\star a_i^\star a_j = \boldsymbol{a}^\dagger \boldsymbol{H} \boldsymbol{a}$. Using these notations, we can write (4.21) as

$$(1 + \mathsf{SNR}\|\boldsymbol{h}\|^2) \min_{\boldsymbol{a}\neq\boldsymbol{0}} \boldsymbol{a}^\dagger \left[\boldsymbol{I} - \frac{\mathsf{SNR}}{1 + \mathsf{SNR}\|\boldsymbol{h}\|^2} \boldsymbol{H} \right] \boldsymbol{a}.$$

$\boldsymbol{H}$ admits one non-zero eigenvalue equal to $\sum_{i=1}^{N} h_i^2$. The other eigenvalues are zeros. Then, $\boldsymbol{I} - \frac{\mathsf{SNR}}{1 + \mathsf{SNR}\|\boldsymbol{h}\|^2} \boldsymbol{H}$ has N strictly positive eigenvalues; $\lambda_1 = 1 - \mathrm{SNR}\|\boldsymbol{h}\|^2/(1 + \mathrm{SNR}\|\boldsymbol{h}\|^2)$, and $\lambda_i = 1$, for $i = 2, \ldots, N$. It is then positive definite. Now, the problem is reduced to the minimization of $\boldsymbol{a}^\dagger \boldsymbol{G} \boldsymbol{a}$.

Proposition 4.2 *Searching for the vector $\boldsymbol{a}$ that minimizes Equation (4.19) of theorem 4.1 is equivalent to a "Shortest Vector" problem for the lattice Λ_a whose Gram matrix is $\boldsymbol{G}$.*

Proof: As $\boldsymbol{G}$ is a definite positive Hermitian (resp. symmetric) matrix, it is the Gram matrix of a lattice Λ. This lattice is either a $\mathbb{Z}[i]-$ lattice in the complex case, or a $\mathbb{Z}-$ lattice in the real case. Then, the minimization problem in Theorem 4.1 is equivalent to find a non zero vector in $\Lambda_{\boldsymbol{a}}$ with shortest length (See Appendix 4.B.1).

Algorithms for solving this problem are given in [57]. The best known one is the Fincke-Pohst algorithm [58].

4.4 The Compute-and-Forward In Real One-Dimensional Lattices

In their joint source-channel scheme, Bobak and Gastpar obtained the computation rate R_{comp} as the highest number of functions per channel use that can be conveyed to the decoder with average distortion D [55]. We will be interested in minimizing the error probability

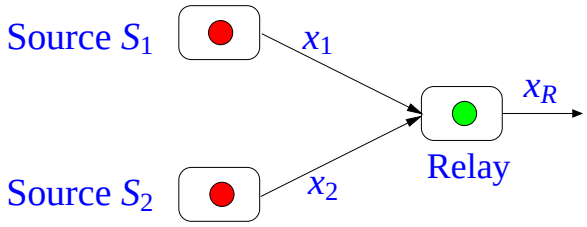


Figure 4.3: System model: 2 sources and one relay.

instead of the distrotion. We have

$$\log\left(\frac{\text{SNR}}{|\alpha|^2+\text{SNR}\|\alpha\boldsymbol{h}-\boldsymbol{a}\|^2}\right) \leq \log\left(1+\frac{\text{SNR}}{|\alpha|^2+\text{SNR}\|\alpha\boldsymbol{h}-\boldsymbol{a}\|^2}\right)$$

The rate at the RHS of the above inequality which is higher than R_{comp}, can be obtained by minimum Euclidian distance decoding if we consider that all noise terms are white Gaussian and independent which is a quite strong requirement. In our work, we will use the maximum likelihood (ML) criterion to propose a decoding technique that can be seen as an inhomogeneous Diophantine approximation.

4.4.1 System Model and Assumptions

As a starting point, we consider two sources sending two independent messages and one relay. Moreover, we consider the real one-dimensional lattices to get insights on how to do the ML decoding. The relay observes a noisy linear combination of the two transmitted messages from the sources S_1 and S_2, and decodes a noiseless linear combination of these two messages, as described in Figure 4.3. The received signal at the relay is expressed as,

$$y = h_1x_1 + h_2x_2 + z. \tag{4.22}$$

The relay searches for the integer coefficient vector $\boldsymbol{a} = [a_1 \;\; a_2]^T$ that maximizes the transmission rate of Eq.4.9. Then, without decoding the individual messages x_1 and x_2, the relay decodes the following noiseless linear equation,

$$x_R = a_1x_1 + a_2x_2, \tag{4.23}$$

and retransmits it to the destination or to another relay. We consider a real-valued channel model with real inputs and outputs. The channel coefficients h_1 and h_2 are real, i.i.d. Gaussian, $h_i \sim \mathcal{N}(0,1)$. z is Gaussian, zero mean, with variance $\sigma^2 = 1$ ($z \sim \mathcal{N}(0,1)$). Let $\boldsymbol{h} = [h_1 \;\; h_2]^T$ denotes the vector of channel coefficients. Source symbols x_i belong to a PAM constellation, they are integers and verify $|x_i| \leq s_m$, i.e., $x_i \in \mathcal{S} = \{-s_m, -s_m+1, \ldots, s_m\}$. S_1 and S_2 transmit x_1 and x_2 respectively. Both sources have no channel state information (CSI). CSI is only available at the relay.

4.4.2 Recovering Linear Equations

After calculating the vector $\boldsymbol{a}$ as in (4.19), the relay recovers a linear combination of the transmitted signal x_1 and x_2. We rewrite the received signal at the relay in the following form

$$y = \lambda + \xi_1 x_1 + \xi_2 x_2 + z \tag{4.24}$$

where λ is an integer, $\xi_i = h_i - a_i$ and z is the additive white noise.

The recovered linear equation $x_R = a_1 x_1 + a_2 x_2 := \lambda$ is a linear Diophantine equation. The coefficients λ, a_1 and a_2 are known integers, and the coefficients x_1 and x_2 are unknown integers. This equation admits the following solutions.

4.4.3 Linear Diophantine Equation Solution

If λ is a multiple of the greatest common divisor (gcd) of a_1 and a_2, then the Diophantine equation has an infinite number of solutions. The *Extended Euclid Algorithm* allows to exhibit a particular solution (u_1, u_2) to $a_1 x_1 + a_2 x_2 = g$ [59]. The set of all solutions is obtained as follows

$$\begin{cases} x_1 = \frac{u_1}{g}\lambda + \frac{a_2}{g}k \\ x_2 = \frac{u_2}{g}\lambda - \frac{a_1}{g}k \end{cases} \tag{4.25}$$

where $g = a_1 \wedge a_2$ is the greatest common divisor (gcd) of a_1 and a_2, $k \in \mathbb{Z}$.

It λ is not a multiple of the greatest common divisor of a_1 and a_2, then the Diophantine equation $\lambda = a_1 x_1 + a_2 x_2$ has no solution. In our settings, as $\boldsymbol{a}$ is of shortest length, a_1 and a_2 are coprime and then $g = 1$. This simplifies the Eq.4.25, and the Diophantine Equation has always an infinite number of solutions. Note also that this applies to any number of transmitters.

Besides finding the greatest common divisor of integers a_1 and a_2, as the Euclidean algorithm does, the Extended Euclidean algorithm also finds integers x and y (one of which is typically negative) that satisfy Bezout's identity $a_1 x_1 + a_2 x_2 = gcd(a_1, a_2)$.

4.4.4 Decoding Metric

The Maximum Likelihood decoder maximizes $p(y|\lambda)$ over all possible values of λ. The conditional probability $p(y|\lambda)$ can be expressed as,

$$p(y|\lambda) = \sum_{\substack{(x_1,x_2) \\ a_1 x_1 + a_2 x_2 = \lambda}} p(y|x_1, x_2) p(x_1, x_2), \tag{4.26}$$

where

$$p(y|x_1,x_2) \propto \exp\left[-\frac{(y-h_1x_1-h_2x_2)^2}{2\sigma^2}\right],$$

and x_1, x_2 are (*a priori*) equiprobable and given by (4.25). The decoding rule is now to find,

$$\hat{\lambda} = \arg\max_{\lambda} \varrho(\lambda) := \sum_{k=-\infty}^{+\infty} \exp\left[-\frac{(y-\beta\lambda+k\alpha)^2}{2\sigma^2}\right], \tag{4.27}$$

where $\beta = \frac{1}{g}(h_1u_1+h_2u_2)$, $\alpha = \frac{1}{g}(h_2a_1-h_1a_2)$.

In [60], it has been proven that, for $\lambda \in \mathbb{R}$, $\varrho(\lambda)$ achieves its maximum for

$$\lambda \in \frac{\alpha}{\beta}\mathbb{Z} + \frac{y}{\beta},$$

i.e., for all values of λ such that $y-\beta\lambda+k\alpha = 0$. Since we want to maximize $\varrho(\lambda)$ for $\lambda \in \mathbb{Z}$, the solution is given by the integer-valued couple (λ,k) minimizing $|y-\beta\lambda+k\alpha|$. Thus, since $x_1,x_2 \in \mathcal{S}$ which is a finite subset of $\mathbb{Z}$ and verify Equation (4.25), we state a new minimization problem which is equivalent to (4.27),

$$\hat{\lambda} = \arg_{\lambda} \min_{\substack{(\lambda,k) \\ x_1,x_2\in\mathcal{S}}} |y-\beta\lambda+k\alpha|\,. \tag{4.28}$$

The problem is therefore equivalent to the minimization of

$$F(k,\lambda) = \left|k\alpha'-\lambda+y'\right| \tag{4.29}$$

with $\alpha' = \alpha/\beta$ and $y' = y/\beta$.

The minimization is called *Inhomogeneous Diophantine Approximation* (IDA) in the absolute sense. It consists of finding the best approximation of a real number α' by a rational number λ/k, $k \in \mathbb{N}$, given an additional real shift y', while keeping the denominator k as small as possible. In the general settings for such problems, an error approximation function $F(k,\lambda)$ is set and it is stated that a rational number λ/k is the Best Diophantine Approximation if, for all other rational numbers λ'/k'

$$k' \leq k \Rightarrow F(k',\lambda') \geq F(k,\lambda).$$

and

$$F(k',\lambda') \leq F(k,\lambda) \Rightarrow k' \geq k$$

In our settings, in addition to the error approximation function, limits are imposed by the finite constellation $\mathcal{C}$ to which the transmitted symbols belong. The algorithms used to find the best Diophantine approximations of real numbers are in general simple and easy to implement. The best known one is the Cassel's algorithm [61]. In [62], the authors develop

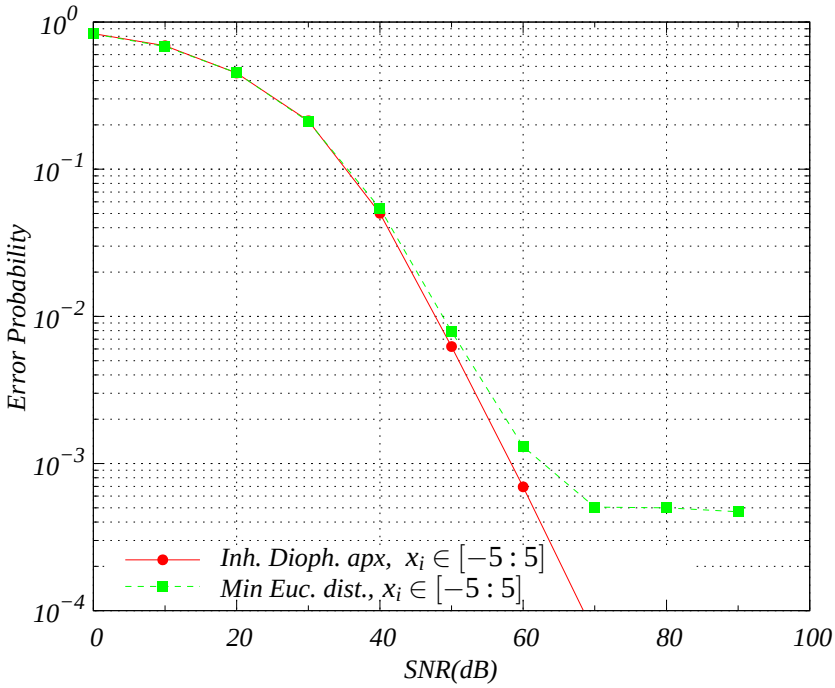


Figure 4.4: Error Probability on decoding λ using the Inhomogeneous Diophantine Approximation and the minimum Euclidian distance decoding.

and compare several ones. The algorithm used in our settings is given in Appendix 4.B.2.

4.4.5 Numerical Results

In the simulations, the set of symbols is of the form $\mathcal{S} = \{-s_m, \ldots, s_m\}$. We consider two sources transmitting x_1 and x_2, and one relay recovering a linear equation of x_1 and x_2 with integer coefficients.

At first, based on its CSI, the relay finds the vector $\boldsymbol{a}$ as the shortest vector described in theorem 4.1. Then, the relay finds a particular solution of the linear Diophantine equation $a_1x_1 + a_2x_2 = g$ using the *Extended Euclid* algorithm. Finally, the relay searches for the couple (k, λ) which gives the best inhomogeneous Diophantine approximation by minimizing the function F defined in (4.29).

In Figure 4.4, we compare the IDA decoding and the minimum Euclidian distance decoding. We plot the error probability on decoding λ for a PAM constellation with $s_m = 5$ in function of the signal to noise ratio SNR. We can see that the error probability using the minimum Euclidian distance decoding has a floor while it continues to decrease with SNRusing the IDA decoding. This floor is due to the quantization error $\|\alpha\boldsymbol{h} - \boldsymbol{a}\|^2$ which has an absolute value bounded away from zero.

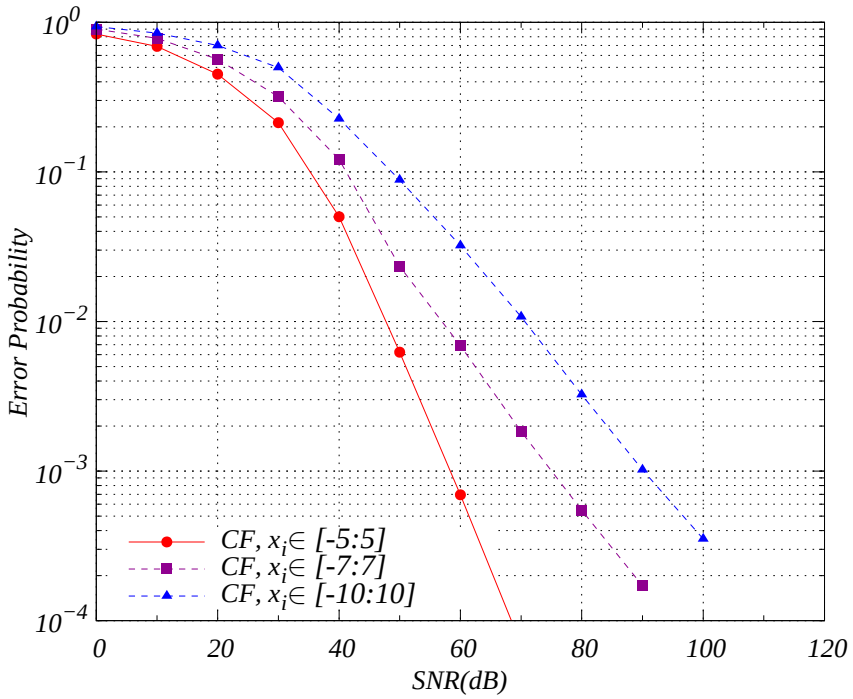


Figure 4.5: Error Probability on decoding λ using the Inhomogeneous Diophantine Approximation.

In Figure 4.5, we show the error probability of the proposed decoding strategy for three different constellations $\mathcal{S}$, defined by $s_m = 5, 7, 10$, respectively. For $s_m = 5$ or less, the diversity order of the system is 1 for real entries (which would correspond to a diversity order equal to 2 with complex symbols). For $s_m > 6$, the diversity order collapses to $1/2$. This is due to the fact that $p(y/\lambda)$ is constant, as a function of λ, on a bigger interval giving rise to ambiguities. We give an esample in Figure 4.6. For $s_m = 5$, $p(y|\lambda)$ is maximized for one integer value of λ, and then no ambiguity. However, for $s_m = 10$, $p(y|\lambda)$ is maximized for several integer values which gives rise to ambiguities.

In one-dimensional lattices, the only existing integer lattice is the ring of integers $\mathbb{Z}$. Therefore,thee loss of degrees of freedom seems inevitable in one dimension. In multi-dimensional lattices, the problem is treated differently.

4.5 Conclusion

In this chapter, we considered the Compute-and-Forward scheme with real-valued channels and one-dimensional lattices. We showed that the coefficient vector that maximizes the transmission rate is the shortest vector in a given lattice. We proposed a quasi-ML decoding technique based on the inhomogeneous Diophantine approximation that performs better than

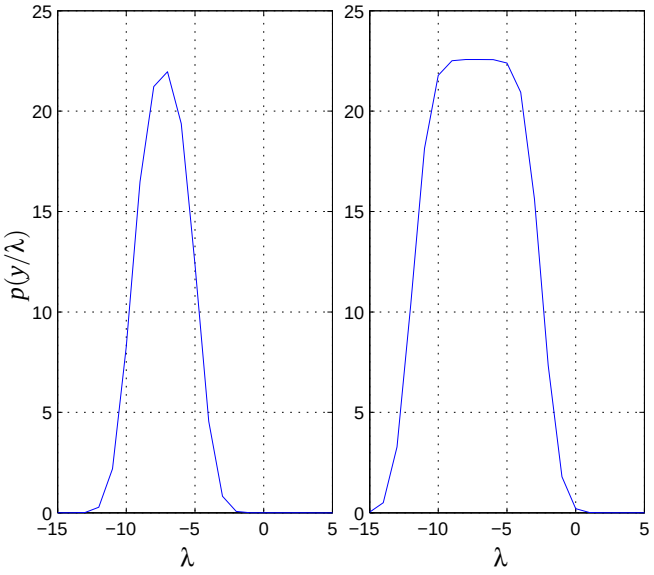


Figure 4.6: $p(y/\lambda)$ for $\boldsymbol{h} = [-1.274\ 0.602]^T$, $\boldsymbol{a} = [2\ -1]^T$, $\mathsf{SNR} = 40dB$, $x_1 = -2$ and $x_2 = 3$. $p(y/\lambda)$ is maximized for one value, $\lambda = -7$ in the left subfigure while it is maximized for several values of λ in the right one.

the minimum Euclidian distance decoding. For large lattices, we observed a loss in degrees of freedom. This is due to the fact that the ML function which is a sum of Gaussian measures, becomes flat and gives rise to ambiguities. Numerical results showed the performance of our decoding method.

In the next chapter, we generalize the results to the multi-dimensional case, and complex-valued channels and symbols. We introduce the flatness factor to obtain criterion design for the lattices in order to avoid the flatness of the ML function.

4.A Lattice definitions

In this Appendix, we give some basic definitions for lattices, nested lattices, and nested lattice codes. All of these definitions are given over $\mathbb{R}^n$. The definitions are mainly from [56].

Definition 4.2 *Lattice: An n-dimensional lattice, Λ, is a set of points in $\mathbb{R}^n$ such that if $x, y \in \Lambda$, then $x + y \in \Lambda$, and if $x \in \Lambda$, then $-x \in \Lambda$. A lattice has basis vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$, and the generic lattice vector $\boldsymbol{x} = (x_1, \ldots, x_n) \in \Lambda$ may be written as*

$$\boldsymbol{x} = \xi_1 \boldsymbol{v}_1 + \ldots + \xi_n \boldsymbol{v}_n = \boldsymbol{\xi} \boldsymbol{M}$$

$\boldsymbol{M} \in \mathbb{R}^{n \times n}$ is the lattice generator matrix, and $\boldsymbol{\xi} = (\xi_1, \ldots, \xi_n) \in \mathbb{Z}^n$. $\boldsymbol{x} = \boldsymbol{0}$ is a lattice point.

Definition 4.3 *Nested Lattice: A lattice Λ is said to be nested in lattice Λ_1 if $\Lambda \subseteq \Lambda_1$. Λ is the coarse lattice and Λ_1 is the fine lattice.*
A sequence of lattices $\Lambda, \Lambda_1, \ldots, \Lambda_L$ is nested if $\Lambda \subseteq \Lambda_1 \subseteq \ldots \subseteq \Lambda_L$.

Definition 4.4 *Generator Matrix: The matrix $\boldsymbol{M}$ built by the lattice basis vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ is the generator matrix of the lattice. The basis vector $\boldsymbol{v}_i$ constitutes the matrix line i.*
The matrix

$$G = \boldsymbol{M}\boldsymbol{M}^T$$

where T denotes transpose, is called the Gram matrix of the lattice.

Definition 4.5 *Fundamental Volume: The parallelotope consisting of the points*

$$\theta_1 \boldsymbol{v}_1 + \ldots + \theta_n \boldsymbol{v}_n, \quad 0 \leq \theta_i < 1$$

is a fundamental parallelotope or a fundamental region for Λ. The fundamental volume of a lattice, $vol(\Lambda)$, is the volume of the fundamental parallelotope. The fundamental volume is equal to: $vol(\Lambda) = |\det(\boldsymbol{M})|$.

There are many ways of choosing the basis and the fundamental region of a lattice Λ. But the volume of the fundamental region is independent of that choice, and is uniquely determined by Λ. The square of this volume is called the *determinant* or *discriminant* of the lattice. If $\boldsymbol{M}$ is a square matrix, we have

$$\det \Lambda = \det \boldsymbol{G} = (\det \boldsymbol{M})^2 .$$

Definition 4.6 *Voronoi Region: Let $\boldsymbol{u} \in \Lambda$. The Voronoi region associated with $\boldsymbol{u}$, $\mathcal{V}(\boldsymbol{u})$, is the set of all points in $\mathbb{R}^n$ that are the closest to $\boldsymbol{u}$:*

$$\mathcal{V}(\boldsymbol{u}) = \{\boldsymbol{w} \in \mathbb{R}^n : \|\boldsymbol{w} - \boldsymbol{u}\| \leq \|\boldsymbol{x} - \boldsymbol{y}\|, \forall \boldsymbol{y} \in \Lambda\}$$

The fundamental Voronoi region is associated with zero, $\mathcal{V}(\mathbf{0})$. All voronoi cells in a lattice are identical to $\mathcal{V}(\mathbf{0})$, and we have $vol(\mathcal{V}(\mathbf{0})) = vol(\Lambda)$.

Definition 4.7 *Nested Lattice Codes: A nested lattice code $\mathcal{L}$ is the set of all points of a fine lattice Λ_1 that are within the fundamental Voronoi region $\mathcal{V}$ of a coarse matrix Λ:*

$$\mathcal{L} = \Lambda_1 \cap \mathcal{V} = \{\boldsymbol{x} : \|\boldsymbol{x} - \mathbf{0}\| \leq \|\boldsymbol{x} - \boldsymbol{y}\|, \boldsymbol{x} \in \Lambda_1, \boldsymbol{y} \in \Lambda, \mathbf{0} \in \Lambda\}.$$

The rate of a nested lattice code is:

$$R = \frac{1}{n}\log|\mathcal{L}| = \frac{1}{n}\log\frac{vol(\mathcal{V})}{vol(\mathcal{V}_1)}.$$

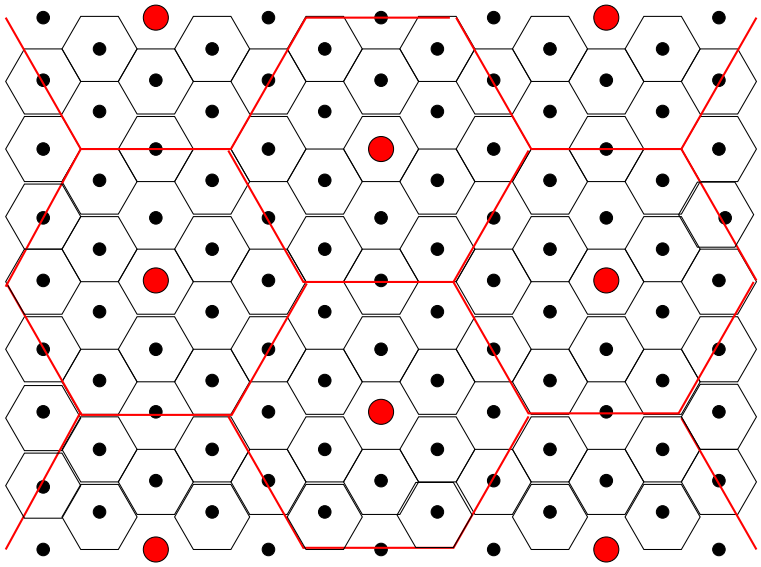


Figure 4.7: Black points are elements of fine lattice Λ_1 and red points are element of the coarse lattice point Λ. A nested lattice code is the set of all fine lattice points within the Voronoi region of the coarse lattice centered on zero.

Definition 4.8 *Covering Radius: The covering radius R of a lattice Λ is the radius of the smallest circumscribed circle of the Voronoi region of Λ.*

Definition 4.9 *Packing Radius: The packing radius ρ of a lattice Λ is the radius of the biggest inscribed circle of the Voronoi region of Λ.*

Definition 4.10 *Density of a lattice: The density Δ of a lattice is the proportion of the space that is occupied by the sphere of radius ρ over the fundamental volume:*

$$\Delta = \frac{volume\ of\ one\ sphere}{volume\ of\ fundamental\ region} = \frac{V_n\rho^n}{(\det\Lambda)^{1/2}}.$$

where V_n is the volume of a sphere of radius 1.

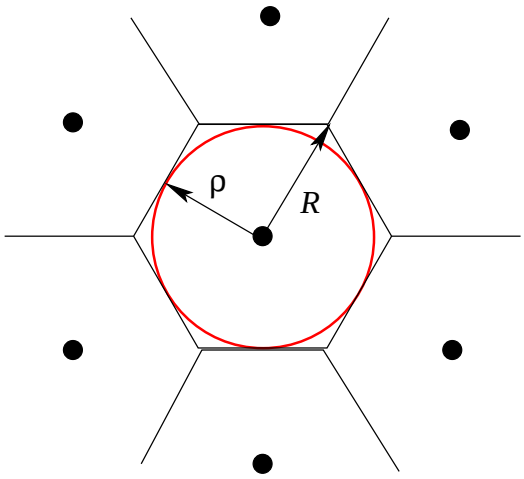


Figure 4.8: Covering radius R and packing radius ρ.

The volume of a sphere of radius $\rho \in \mathbb{R}^n$ is proportional to ρ^n. The coefficient of proportionality is the volume of a sphere of radius 1, given by

$$V_n = \frac{\pi^{n/2}}{\Gamma\left(n/2+1\right)} = \begin{cases} \frac{\pi^{n/2}}{(n/2)!}, & \text{N is even} \\ \frac{2^n \pi^{(n-1)/2}((n-1)/2)!}{n!}, & \text{N is odd} \end{cases} \tag{4.30}$$

Definition 4.11 *Kissing number: The kissing number of a lattice Λ is the number of tangent spheres to a given sphere.*

Example 4.1 *The two-dimensional hexagonal lattice A_2 represented in Fig.4.7. This is the densest lattice in $\mathbb{R}^2$ (dimension 2). A generator matrix of A_2 may be defined as:*

$$\boldsymbol{M} = \begin{pmatrix} 1 & 0 \\ 1/2 & \sqrt{3}/2 \end{pmatrix}$$

The fundamental volume of A_2 is $vol(A_2) = |\det(\boldsymbol{M})| = \sqrt{3}/2$. In Fig.4.7, the Voronoi region are presented in hexagonal form. The kissing number for lattice A_2 is 6. Each lattice point is at equal distance from 6 other lattice points. This distance is called the minimal distance of a lattice and is denoted by d_{min}.

4.B Extras

4.B.1 The Shortest Vector in Proposition 4.2

The problem is to find $\boldsymbol{a} \in \mathbb{Z}[i]$ that reduces $\boldsymbol{a}^\dagger \boldsymbol{G}\boldsymbol{a}$. For real (or complex) minimization, *i.e.* $\boldsymbol{a} \in \mathbb{R}^N (\text{or} \mathbb{C}^N)$, the problem is treated in a different way.

Let $\lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_N$ the ordered eigenvalues of $\boldsymbol{G}$. We have,

$$\lambda_1 \boldsymbol{x}^\dagger \boldsymbol{x} \leq \boldsymbol{x}^\dagger \boldsymbol{G} \boldsymbol{x} \leq \lambda_N \boldsymbol{x}^\dagger \boldsymbol{x}, \quad \boldsymbol{x} \in \mathbb{C}^N$$

Then, $\min \boldsymbol{x}^\dagger \boldsymbol{G} \boldsymbol{x} = \lambda_1 \|\boldsymbol{x}\|^2 = \lambda_1$, $\boldsymbol{x}$ being the eigenvector which corresponds to λ_1; $\|\boldsymbol{x}\|^2 = 1$.

4.B.2 Algorithm to find λ in Section 4.4.4

The algorithm for finging λ requires these integer entries: the coefficient vector $\boldsymbol{a}$, the great common divisor $g := \gcd(a_1, a_2)$, the particular solution of the linear Diophantine equation (u_1, u_2), the maximum absolute value of the constellation symbols s_m. Moreover, the algorithm needs the real values α' and y'. In addition, we impose an upper limit on searching for λ, $maxP$, drawn from the constellation size. We define the transition matrix $\boldsymbol{T}$ such that $[x_1 \;\; x_2]^T = \boldsymbol{T}[\lambda \;\; k]^T$. The algorithm is as follows:

1. **begin**
2. $q := 0$;
3. $P := round(qa - b)$;
4. $\boldsymbol{M} := \boldsymbol{T} \times [P \;\; q]^T$;
5. $x1 := \boldsymbol{M}(1)$; $x2 := \boldsymbol{M}(2)$;
6. **if** $(x_1 \in \mathcal{S})$ & $(x_2 \in \mathcal{S})$ **then**
7. $out1 := P$; $out2 := q$;
8. $\eta^\star := qa - P - b$; **else** $\eta^\star := 1$;
9. **fi**;
10.
11. $sgn := +1$;
12. **while** $|\eta^\star| \neq 0$ & $|P| \leq maxP$ **do**
13.
14. $q := q + sgn$;
15. $P := round(qa - b)$;
16. $\boldsymbol{M} := \boldsymbol{T} \times [P \;\; q]^T$;
17. $x1 := \boldsymbol{M}(1)$; $x2 := \boldsymbol{M}(2)$;
18. **if** $(x_1 \in \mathcal{S})$ & $(x_2 \in \mathcal{S})$ **then**
19. $\eta := qa - P - b$;
20. **if** $|\eta| < |\eta^\star|$ **then**
21. $\eta^\star := \eta$; $out1 := P$; $out2 := q$; **fi**;
22. **fi**;
23. **od**;
24. $P := 1$;
25. $q := 0$;
26. $sgn := -1$;
27. **while** $|\eta^\star| \neq 0$ & $|P| \leq maxP$ **do**

28.
29. $q := q + sgn$;
30. $P := round(qa - b)$;
31. $\boldsymbol{M} := \boldsymbol{T} \times [P \;\; q]^T$;
32. $x1 := \boldsymbol{M}(1); \;\; x2 := \boldsymbol{M}(2)$;
33. **if** $(x_1 \in \mathcal{S})$ & $(x_2 \in \mathcal{S})$ **then**
34. $\eta := qa - P - b$;
35. **if** $|\eta| < |\eta^\star|$ **then**
36. $\eta^\star := \eta$; $out1 := P$; $out2 := q$; **fi**;
37. **fi**;
38. **od**;
39.
40. $output(out1, out2)$;
41. **end**.

Chapter 5

Compute-and-Forward Protocol: Multi-Dimensional Case

STARTING with real one-dimensional lattices in the previous chapter, we developed a decoding strategy for the compute-and-forward protocol based on the Maximum Likelihood (ML) criterion. In this chapter, we go forward to generalize the previous results in the general settings of complex-valued channels and multi-dimensional lattices.

Section 5.1 gives the system model. In Section 5.2, we follow the same steps as before to extract the Maximum Likelihood decoding function in which intervene a system of linear Diophantine equations. In Section 5.3, we introduce the flatness factor of a sum of Gaussian measures as a tool to design lattices for the compute-and-forward scheme. In Section 5.4, we give a brief analysis of the lattices involved in the ML decoding function. In Section 5.5, we reconsider the computation rate maximization, and in Section 5.6, we state an open problem on finding a decoding algorithm based on simultaneous Diophantine approximation.

5.1 Compute-and-Forward Protocol

Consider k sources, $S_1, \ldots, S_k$, and a relay. The source j transmits the message x_j. Based on the compute-and-forward scheme described by Nazer and Gastpar [3], the relay wants to reliably recover an integer combination of the transmitted signals:

$$\boldsymbol{\lambda} = \sum_{j=1}^{k} a_j \boldsymbol{x}_j, \tag{5.1}$$

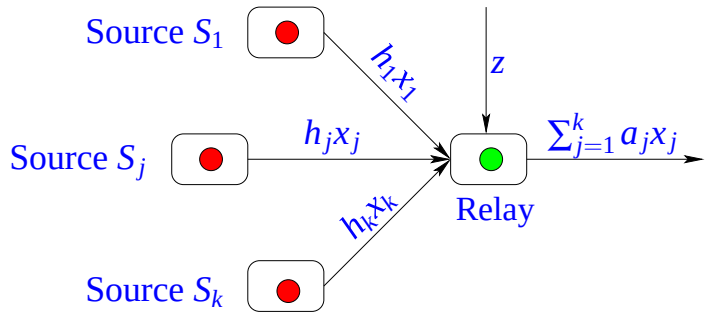


Figure 5.1: System model: k sources and one relay.

where $a_j \in \mathbb{Z}[i]$ are the elements of the coefficient vector $\boldsymbol{a} \in \mathbb{Z}[i]^k$. The Figure 5.1 illustrates the system model.

The received signal at the relay is

$$\boldsymbol{y} = \sum_{j=1}^{k} h_j \boldsymbol{x}_j + \boldsymbol{z}. \tag{5.2}$$

where $\boldsymbol{x}_j \in \Lambda_j \subset \mathbb{Z}[i]^n$ are $\mathbb{Z}[i]$-lattice points. $h_j \in \mathbb{C}$ are the channel coefficients and $\boldsymbol{z}$ is the i.i.d. additive Gaussian noise. Our goal in this study is to propose a design criterion for lattice coding when using an ML decoding.

5.2 Maximum Likelihood Decoding

5.2.1 Received Signal

The relay scales the received signal in Eq.5.2 by the MMSE factor given in Eq.4.8. Then, we can rewrite the received signal as,

$$\boldsymbol{y} = \boldsymbol{\lambda} + \sum_{j=1}^{k} \epsilon_j \boldsymbol{x}_j + \boldsymbol{z}, \tag{5.3}$$

where $\boldsymbol{\lambda} = \sum_{j=1}^{k} a_j \boldsymbol{x}_j$ is the integer combination that the relay wants to recover. $\epsilon_j = h_j - a_j$ and $\boldsymbol{z}$ is the i.i.d. additive Gaussian noise. $\boldsymbol{\lambda}$ lives in the lattice Λ defined as,

$$\Lambda = \sum_{j=1}^{k} a_j \Lambda_j. \tag{5.4}$$

5.2.2 Decoding Metric

The Maximum Likelihood (ML) decoder maximizes $p(\boldsymbol{y}|\boldsymbol{\lambda})$ over all of the possible values of $\boldsymbol{\lambda}$. The conditional probability $p(\boldsymbol{y}|\boldsymbol{\lambda})$ can be expressed as,

$$p(\boldsymbol{y}|\boldsymbol{\lambda}) = \sum_{\substack{\{\boldsymbol{x}_j \in \Lambda_j\}_{1\leq j\leq k} \\ \boldsymbol{\lambda}=\sum_{j=1}^{k} a_j \boldsymbol{x}_j}} p\left(\boldsymbol{y}|\left\{\boldsymbol{x}_j\right\}_{1\leq j\leq k}\right) p\left(\left\{\boldsymbol{x}_j\right\}_{1\leq j\leq k}\right), \tag{5.5}$$

where the conditional probability is similar to

$$p\left(\boldsymbol{y}|\left\{\boldsymbol{x}_j\right\}_{1\leq j\leq k}\right) \propto \exp\left[-\frac{\|\boldsymbol{y}-\sum_{j=1}^{k} h_j \boldsymbol{x}_j\|^2}{2\sigma_z^2}\right],$$

and $\{\boldsymbol{x}_j\}$ are (*a priori*) equiprobable. The decoding rule is now to find,

$$\hat{\boldsymbol{\lambda}} = \arg \max_{\boldsymbol{\lambda}|\boldsymbol{\lambda}=\sum_{j=1}^{k} a_j \boldsymbol{x}_j} p(\boldsymbol{y}|\boldsymbol{\lambda}) = \arg \max_{\boldsymbol{\lambda}\in\Lambda} \sum_{\{\boldsymbol{x}_j\}|\sum_{j=1}^{k} a_j \boldsymbol{x}_j=\boldsymbol{\lambda}} \exp\left[-\frac{\|\boldsymbol{y}-\sum_{j=1}^{k} h_j \boldsymbol{x}_j\|^2}{2\sigma_z^2}\right]. \tag{5.6}$$

Now, we need to explicit the expression of $\boldsymbol{x}_j$ in function of $\boldsymbol{\lambda}$ as in Eq.4.25. In this scope, we have to solve a linear system of Diophantine equations $\boldsymbol{\lambda} = \sum_{j=1}^{k} a_j \boldsymbol{x}_j$, since the components of $\boldsymbol{x}_j$ are in $\mathbb{Z}[i]$ as well as a_j. To do this, we need to use the Hermite Normal Form (HNF) of integral matrices. In the following, $\boldsymbol{M}_j$ is the generator matrix of the lattice Λ_j.

5.2.3 Diophantine Equations: Hermite Normal Form

Let we define the matrix $\boldsymbol{M}$ in the following form,

$$\boldsymbol{M} = [a_1\boldsymbol{M}_1|\ldots|a_k\boldsymbol{M}_k].$$

where $\boldsymbol{M}_j \in \mathbb{Z}[i]^{n\times n}$ are full rank matrices and $\boldsymbol{M} \in \mathbb{Z}^{n\times nk}$. The elements of $\boldsymbol{M}$ are integers, we are then able to write the matrix $\boldsymbol{M}$ in the Hermite Normal Form (HNF). This condition on the elements of $\boldsymbol{M}$ is necessary (see definition of HNF in Appendix 5.A.2). We right-multiply $\boldsymbol{M}$ by $\boldsymbol{U}$ as,

$$\boldsymbol{M}.\boldsymbol{U} = [\boldsymbol{0}|\boldsymbol{B}].$$

$[\boldsymbol{0}|\boldsymbol{B}]$ is the HNF of $\boldsymbol{M}$ where $\boldsymbol{B} \in \mathbb{Z}^{n\times n}$ is an invertible matrix, and $\boldsymbol{U} \in \mathbb{Z}^{kn\times kn}$ is an invertible unimodular matrix with $\det(\boldsymbol{U}) = \pm 1$. We put $\boldsymbol{U}$ in the form,

$$\boldsymbol{U} = \begin{bmatrix} \boldsymbol{U}_1 & \boldsymbol{V}_1 \\ \boldsymbol{U}_2 & \boldsymbol{V}_2 \\ \vdots & \vdots \\ \boldsymbol{U}_k & \boldsymbol{V}_k \end{bmatrix},$$

$\boldsymbol{V}_j \in \mathbb{Z}^{n\times n}$ and $\boldsymbol{U}_k \in \mathbb{Z}^{n\times n(k-1)}$. Using the HNF of $\boldsymbol{M}$, the system of Diophantine equations has the following solutions:

$$\boldsymbol{x}_j = \boldsymbol{M}_j \boldsymbol{V}_j \boldsymbol{B}^{-1}\boldsymbol{\lambda} + \boldsymbol{s}_j, \tag{5.7}$$

where $\boldsymbol{s}_j$ is any point of the lattice L_j generated by $\boldsymbol{M}_j\boldsymbol{U}_j$ (see Appendix 5.A.3 for details). Note that the HNF form implies that $\sum_{j=1}^{k} a_j \boldsymbol{M}_j \boldsymbol{U}_j = 0$.

5.2.4 Likelihood Decoding Function

Combining the Diophantine solutions in Eq.5.7 and the ML decoding metric in Eq.5.6, we obtain the ML decision

$$\hat{\boldsymbol{\lambda}} = \arg\max_{\boldsymbol{\lambda}\in\Lambda} \sum_{u\in\mathcal{L}} \exp\left[-\frac{\|w(\boldsymbol{\lambda}) - \boldsymbol{u}\|^2}{2\sigma_z^2}\right], \tag{5.8}$$

where $w(\boldsymbol{\lambda}) = \boldsymbol{y} - \left[\sum_{j=1}^{k} h_j \boldsymbol{M}_j \boldsymbol{V}_j\right] \boldsymbol{B}^{-1}\boldsymbol{\lambda}$ and $\mathcal{L}$ is a lattice with generator matrix $\sum_{j=1}^{k} h_j \boldsymbol{M}_j \boldsymbol{U}_j$.

We want to find λ that maximizes the likelihood function $\varrho(\boldsymbol{\lambda})$,

$$\varrho(\boldsymbol{\lambda}) = \sum_{u\in\mathcal{L}} \exp\left[-\frac{\|w(\boldsymbol{\lambda}) - \boldsymbol{u}\|^2}{2\sigma_z^2}\right]. \tag{5.9}$$

Then, the error probability is small if $\varrho(\hat{\boldsymbol{\lambda}})$ is as different of $\varrho(\boldsymbol{\lambda})$ as possible, and that for $\boldsymbol{\lambda} \neq \hat{\boldsymbol{\lambda}}$. However, $\varrho(\boldsymbol{\lambda})$ which is a sum of Gaussian measures, can be flat what prevents us to maximize it.

5.3 The Flatness Factor

5.3.1 Definition

We introduce the flatness factor as a tool to study the flatness of a function. We consider the study of the function $\phi(\boldsymbol{y})$ which is an infinite sum of Gaussian measures,

$$\begin{cases} \phi : \mathbb{R}^n \to \mathbb{R} \\ \phi : \boldsymbol{y} \mapsto \sum\limits_{\boldsymbol{x}\in\Lambda} e^{-\frac{\|\boldsymbol{y}-\boldsymbol{x}\|^2}{2\sigma^2}} \end{cases} \tag{5.10}$$

where Λ is an Euclidian lattice of order n.

We begin by giving an example showing the flatness of the function $\phi(\boldsymbol{y})$ in Fig.5.2. We consider the $2\mathbb{Z}^2$ lattice and plot the function $\phi(\boldsymbol{y}) = \sum\limits_{\boldsymbol{x}\in 2\mathbb{Z}^2} e^{-\frac{\|\boldsymbol{y}-\boldsymbol{x}\|^2}{2\sigma^2}}$ for $\sigma^2 = 0.3$ and $\sigma^2 = 1$. As σ^2 increases, the difference between the maximum value and the mean value of $\phi(\boldsymbol{y})$

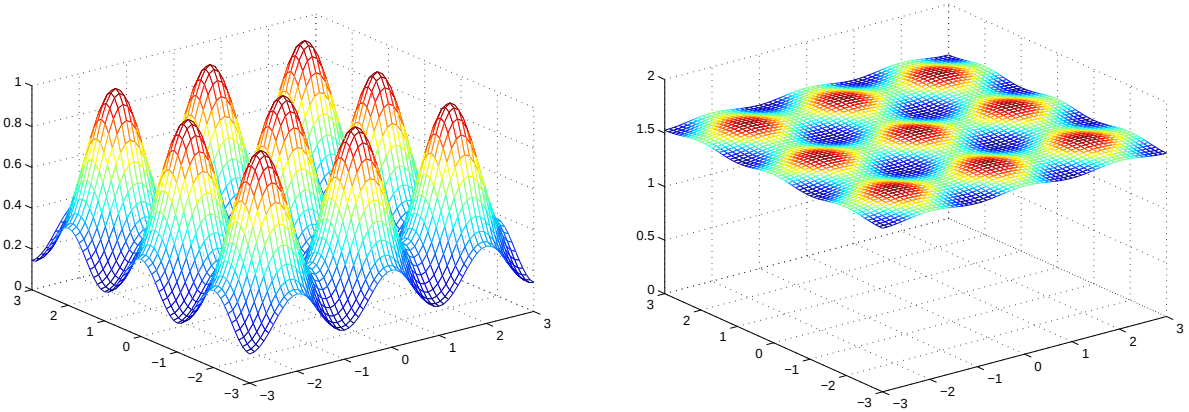


Figure 5.2: Sum of Gaussian Measures on the $2\mathbb{Z}^2$ lattice with $\sigma^2 = 0.3$ and $\sigma^2 = 1$.

becomes smaller, and hence, the function becomes flatter. We define then the flatness factor of a function as the ratio between the mean value and the maximum value of $\phi(\boldsymbol{y})$.

Definition 5.1 *Flatness factor: Let Λ be a n-dimensional full rank lattice and define the periodic function*

$$\phi_\Lambda(\boldsymbol{y}, \mu) = \sum_{\boldsymbol{x}\in\Lambda} \exp\left[-\frac{\|\boldsymbol{y}-\boldsymbol{x}\|^2}{2\sigma^2}\right] = \sum_{\boldsymbol{x}\in\Lambda} \exp\left[-\frac{\mu\|\boldsymbol{y}-\boldsymbol{x}\|^2}{2} vol(\Lambda)^{-\frac{2}{n}}\right],$$

where $vol(\Lambda)$ is the fundamental volume of Λ and $\mu = \frac{vol(\Lambda)^{\frac{2}{n}}}{\sigma^2}$ is the generalized signal-to-noise ratio (GSNR) *[63]. The flatness factor of the lattice Λ is the function*

$$\epsilon_\Lambda(\mu) \triangleq \frac{\mathbb{E}_{\boldsymbol{y}}\left(\phi_\Lambda(\boldsymbol{y}, \mu)\right)}{\max\limits_{\boldsymbol{y}\in\mathbb{R}^n}\left\{\phi_\Lambda(\boldsymbol{y}, \mu)\right\}}, \tag{5.11}$$

where $\mathbb{E}_{\boldsymbol{y}}\left(\phi_\Lambda(\boldsymbol{y}, \mu)\right)$ is understood as,

$$\mathbb{E}_{\boldsymbol{y}}\left(\phi_\Lambda(\boldsymbol{y}, \mu)\right) = \frac{1}{vol(\Lambda)} \int_{\mathcal{V}(\Lambda)} \phi_\Lambda(\boldsymbol{y}, \mu) d\boldsymbol{y}.$$

$\mathcal{V}(\Lambda)$ is the Voronoi region of Λ.

The GSNR is introduced in the work of Poltyrev [63] to replace the traditional signal-to-noise ratio SNR when infinite constellations are considered. This consideration is essentially taken in order to be free from the shaping problem. $\epsilon_\Lambda(\mu)$ measures the flatness of the function $\phi_\Lambda(\boldsymbol{y}, \mu)$ in $\mathbb{R}^n$. Obviously,

$$0 \leq \epsilon_\Lambda(\mu) \leq 1. \tag{5.12}$$

In the compute-and-forward context, we are interested in minimizing the flatness factor of the lattice $\mathcal{L}$ in order to avoid ambiguities.

5.3.2 The Average Value

By definition of the periodic function ϕ_Λ, we have

$$\begin{aligned}
\mathbb{E}_{\boldsymbol{y}}(\phi_\Lambda(\boldsymbol{y})) &= \frac{1}{vol(\Lambda)}\int_{\mathcal{V}(\Lambda)}\phi_\Lambda(\boldsymbol{y})d\boldsymbol{y} \\
&= \frac{1}{vol(\Lambda)}\int_{\mathcal{V}(\Lambda)}\sum_{\boldsymbol{x}\in\Lambda} e^{-\frac{\|\boldsymbol{y}-\boldsymbol{x}\|^2}{2\sigma^2}}d\boldsymbol{y} \\
&= \frac{(\sqrt{2\pi}\sigma)^n}{vol(\Lambda)}\sum_{\boldsymbol{x}\in\Lambda}\int_{\mathcal{V}(\Lambda)}\frac{1}{(\sqrt{2\pi}\sigma)^n}e^{-\frac{\|\boldsymbol{y}-\boldsymbol{x}\|^2}{2\sigma^2}}d\boldsymbol{y} \\
&= \frac{(\sqrt{2\pi}\sigma)^n}{vol(\Lambda)}\sum_{\boldsymbol{x}\in\Lambda}\int_{\mathcal{V}(\Lambda)+\boldsymbol{x}}\frac{1}{(\sqrt{2\pi}\sigma)^n}e^{-\frac{\|\boldsymbol{t}\|^2}{2\sigma^2}}d\boldsymbol{t} \\
&= \frac{(\sqrt{2\pi}\sigma)^n}{vol(\Lambda)}\int_{\mathbb{R}^n}\frac{1}{(\sqrt{2\pi}\sigma)^n}e^{-\frac{\|\boldsymbol{t}\|^2}{2\sigma^2}}d\boldsymbol{t}
\end{aligned}$$

which eventually gives

$$\mathbb{E}_{\boldsymbol{y}}(\phi_\Lambda(\boldsymbol{y})) = \frac{(\sqrt{2\pi}\sigma)^n}{vol(\Lambda)} \tag{5.13}$$

since $\frac{1}{(\sqrt{2\pi}\sigma)^n}e^{-\frac{\|\boldsymbol{t}\|^2}{2\sigma^2}}$ is a probability density function. Using the GSNR, we obtain

$$\mathbb{E}_{\boldsymbol{y}}\left(\phi_\Lambda(\boldsymbol{y},\mu)\right) = \left(\frac{2\pi}{\mu}\right)^{\frac{n}{2}}. \tag{5.14}$$

5.3.3 The Maximum Value

Lemma 5.1 *[60] The maximum of $\phi_\Lambda(\boldsymbol{y},\mu)$ is given by the theta series of Λ and is achieved for $\boldsymbol{y}\in\Lambda$, more precisely*

$$\max_{\boldsymbol{y}\in\mathbb{R}^n}\{\phi_\Lambda(\boldsymbol{y},\mu)\} = \Theta_\Lambda\left(e^{-\frac{1}{2\sigma^2}}\right) = \Theta_\Lambda\left(e^{-\frac{\mu}{2}vol(\Lambda)^{-\frac{2}{n}}}\right) \tag{5.15}$$

where $\Theta_\Lambda(q)=\sum_{\boldsymbol{x}\in\Lambda}q^{\|x\|^2}$ is the theta series of the lattice Λ.

Proof: We use the result from [60] that the maximum value is achieved for $\boldsymbol{y}\in\Lambda$. We prove that the maximum is given by the theta series of Λ. We have,

$$\begin{aligned}
\max_{\boldsymbol{y}\in\mathbb{R}^n}\{\phi_\Lambda(\boldsymbol{y},\mu)\} &= \sum_{\boldsymbol{x}\in\Lambda}\exp\left[-\frac{\mu\|\boldsymbol{y}-\boldsymbol{x}\|^2}{2}vol(\Lambda)^{-\frac{2}{n}}\right]\Bigg|_{\boldsymbol{y}\in\Lambda} \\
&= \sum_{\boldsymbol{t}\in\Lambda}\exp\left[-\frac{\mu\|\boldsymbol{t}\|^2}{2}vol(\Lambda)^{-\frac{2}{n}}\right] \\
&= \Theta_\Lambda\left(e^{-\frac{\mu}{2}vol(\Lambda)^{-\frac{2}{n}}}\right),
\end{aligned}$$

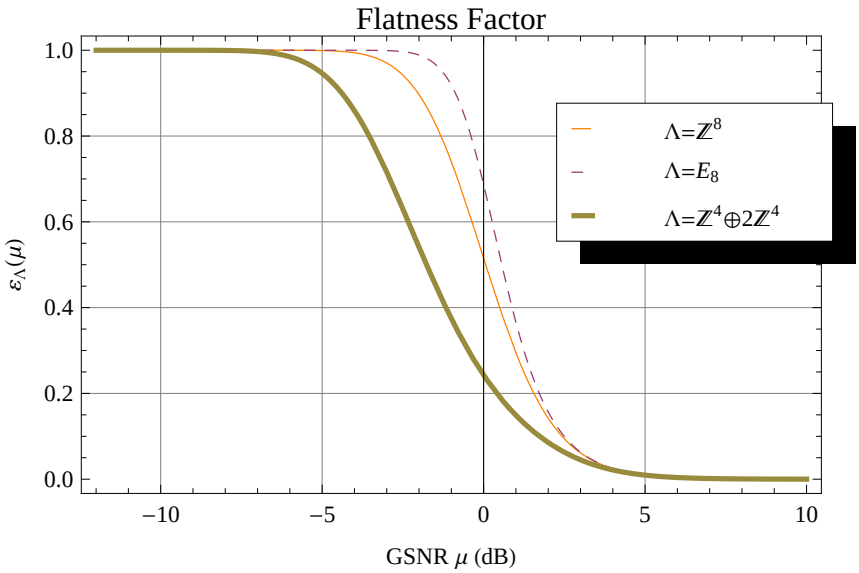


Figure 5.3: Some flatness factors in dimension 8.

where

$$\Theta_\Lambda(q) = \sum_{\boldsymbol{x}\in\Lambda} q^{\|x\|^2}$$

is the theta series of the lattice Λ.

Eq.5.14 and Eq.5.15 brought together, the flatness factor of the n-dimensional full rank lattice Λ is

$$\epsilon_\Lambda(\mu) = \frac{(2\pi)^{\frac{n}{2}}}{\mu^{\frac{n}{2}}\Theta_\Lambda\left(e^{-\frac{\mu}{2}vol(\Lambda)^{-\frac{2}{n}}}\right)}. \tag{5.16}$$

Example 5.1 *Consider the normalized lattice $\Lambda = \mathbb{Z}^n$. The fundamental volume $vol(\Lambda)$ is equal to 1. The flatness factor of $\mathbb{Z}^n$ is*

$$\epsilon_{\mathbb{Z}^n}(\mu) = (2\pi)^{\frac{n}{2}}\left[\sqrt{\mu}.\vartheta_3\left(e^{-\frac{\mu}{2}}\right)\right]^{-n},$$

where $\vartheta_3(q) = 1 + \sum_{k=1}^{\infty} 2q^{k^2}$ is the theta function of $\mathbb{Z}$. Consider also the lattice $\Lambda = E_8$ which is the densiest in dimension 8. The flatness factor of E_8 is

$$\epsilon_{E_8}(\mu) = 8.\left(\frac{\pi}{\mu}\right)^4.\left(\vartheta_2^8\left(e^{-\frac{\mu}{2}}\right) + \vartheta_3^8\left(e^{-\frac{\mu}{2}}\right) + \vartheta_4^8\left(e^{-\frac{\mu}{2}}\right)\right)^{-1}$$

We illustrate in Fig.5.3 some flatness factors in dimension 8 in function of the GSNR. *The Gosset lattice E_8 which is the densest lattice in dimension 8, has the highest flatness factor. However, the lattice $\mathbb{Z}^4 \oplus 2\mathbb{Z}^4$ which is a sparse lattice, has the smallest flatness factor. Therefore, in our scope of interest on minimizing the flatness factor, $\mathbb{Z}^4 \oplus 2\mathbb{Z}^4$ is the more convenient lattice.*

5.4 Good Lattice, Bad Lattice

In the ML decoding metric Eq.5.8, two lattices, Λ and $\mathcal{L}$, are intervening. We aim to give lattice design criteria for the ML decoding. The lattice Λ in which lives the decoded codeword $\boldsymbol{\lambda} = \sum_{j=1}^{k} a_j \boldsymbol{x}_j$, is defined as

$$\Lambda = \sum_{j=1}^{k} a_j \Lambda_j.$$

We have to choose this lattice Λ to be a dense lattice, a "Good" lattice. A detailed analysis of the error probability is necessary to extract the design criterion of such lattice. If $\Lambda_j = \Lambda_0$, for $j = 1, \dots k$, then

$$\Lambda = \left(\bigwedge_{j=1}^{k} a_j \right) \Lambda_0. \tag{5.17}$$

$\left(\bigwedge_{j=1}^{k} a_j \right)$ is the great common divisor (gcd) of a_j. If not, Λ will depend on the choice of a_j.

The lattice $\mathcal{L}$ on which is performed the sum of Gaussian measures, has the generator matrix

$$\boldsymbol{M}_{\mathcal{L}} = \sum_{k=1}^{j} h_j \boldsymbol{M}_j \boldsymbol{U}_j,$$

given that $\sum_{k=1}^{j} a_j \boldsymbol{M}_j \boldsymbol{U}_j = 0$ (HNF decomposition). In order to be able to decode $\boldsymbol{\lambda}$ with a small error probability, we should minimize the flatness factor of the lattice $\mathcal{L}$. Thus, the generator matrix $\boldsymbol{M}_{\mathcal{L}}$ is almost rank deficient, and $\mathcal{L}$ is a "Bad" lattice. Therefore, this could be done by aligning $\boldsymbol{a}$ with $\boldsymbol{h}$ as much as possible.

5.5 Maximizing The Computation Rate

Nazer and Gastpar showed in [3] that relays can recover any set of linear equations with coefficient vector $\boldsymbol{a}$, as long as the message rates are less than the computation rate. The computation rate is given by

$$R_{\text{comp}}(\boldsymbol{h}, \boldsymbol{a}) = \log \left(\left(\|\boldsymbol{a}\|^2 - \frac{\mathsf{SNR}|\boldsymbol{h}^\dagger \boldsymbol{a}|^2}{1 + \mathsf{SNR}\|\boldsymbol{h}\|^2} \right)^{-1} \right), \tag{5.18}$$

where $\boldsymbol{h} \in \mathbb{C}^N$ is the channel vector, $\boldsymbol{a} \in \mathbb{Z}[i]^k$ is the coefficient vector, and SNR is the signal-to-noise ratio at the relay. This computation rate is uniquely achievable by scaling the received signal by the MMSE coefficient [3],

$$\alpha_{MMSE} = \frac{\text{SNR}\boldsymbol{h}^\dagger \boldsymbol{a}}{1 + \text{SNR}\|\boldsymbol{h}\|^2}. \tag{5.19}$$

Maximizing R_{comp} requires to choose the optimal $\boldsymbol{a}_{\text{opt}} \in \mathbb{Z}[i]^k$ as explained in Theorem 4.1, *i.e.*,

$$\boldsymbol{a}_{\text{opt}} = \arg\min_{\boldsymbol{a}\neq\boldsymbol{0}} \boldsymbol{a}^{\dagger}\left(\boldsymbol{I} - \frac{\mathsf{SNR}}{1+\mathsf{SNR}\|\boldsymbol{h}\|^2}\boldsymbol{H}\right)\boldsymbol{a} \tag{5.20}$$

where $\boldsymbol{H} = [h_i h_j^{\star}]$. Searching for the vector $\boldsymbol{a}_{\text{opt}}$ is equivalent to search for the shortest vector problem in the lattice $\Lambda_{\boldsymbol{a}}$ whose Gram matrix is $\left(\boldsymbol{I} - \frac{\mathsf{SNR}}{1+\mathsf{SNR}\|\boldsymbol{h}\|^2}\boldsymbol{H}\right)$. When SNR grows up, it is equivalent to align $\boldsymbol{a}$ with $\boldsymbol{h}$ as much as possible.

5.6 Decoding Algorithm: Diophantine Approximation

The ML decision is to choose $\boldsymbol{\lambda}$ to maximize

$$\hat{\boldsymbol{\lambda}} = \arg\max_{\boldsymbol{\lambda}\in\Lambda} \sum_{u\in\mathcal{L}} \exp\left[-\frac{\|w(\boldsymbol{\lambda}) - \boldsymbol{u}\|^2}{2\sigma_z^2}\right], \tag{5.21}$$

where $w(\boldsymbol{\lambda})$ lives in the lattice generated by $\left[\sum_{j=1}^{k} h_j \boldsymbol{M}_j \boldsymbol{V}_j\right]\boldsymbol{B}^{-1}$ and shifted by the received vector $\boldsymbol{y}$.

We know that [60]

$$\hat{w} = \arg\max_{w(\boldsymbol{\lambda})\in\mathbb{C}^n} \sum_{\boldsymbol{u}\in\mathcal{L}} \exp\left[-\frac{\|w(\boldsymbol{\lambda}) - \boldsymbol{u}\|^2}{2\sigma_z^2}\right] \Leftrightarrow \hat{w} \in \mathcal{L}$$

We can deduce that an approximated solution to Eq.5.21 is

$$\boldsymbol{\lambda}_{\text{approx}} = \arg\min_{\boldsymbol{\lambda}\in\Lambda_f, \boldsymbol{u}\in\mathcal{L}_f} \|w(\boldsymbol{\lambda}) - \boldsymbol{u}\|^2, \tag{5.22}$$

where Λ_f and $\mathcal{L}_f$ are the finite subsets of Λ and $\mathcal{L}$ determined by the boundaries of the constellations $\{\boldsymbol{x}_j\}$.

Solving Eq.5.22 requires to be able to find an efficient algorithm of simultaneous Diophantine approximation.

5.7 Conclusion

In this chapter, we made a forward step on generalizing the results obtained in real one-dimensional lattices in the previous chapter. In particular, we show the importance of the sum of Gaussian measures in the Maximum Likelihood expression. We introduced the flatness factor as a tool to study the sum of Gaussian measures, and to design the multi-dimensional lattices. In ML function two lattices intervene. The first should be a "Good" dense lattice, and the second a "Bad" lattice with generator matrix almost rank deficient. A more careful analysis of the probability of error should be made to design more precisely the involved

lattices. More research should be done in order to find efficient algorithms to perform simultaneous Diophantine approximation. We believe that this constitutes a step towards a rich and fruitful research area.

5.A Appendix

We give in this appendix some definitions, lemmas and theorems without including the proofs.

5.A.1 Unimodular Matrix

Definition 5.2 *An integral square matrix $\boldsymbol{U}$ is called unimodular if* $|\det(\boldsymbol{U})| = 1$.

Lemma 5.2 *Let $\boldsymbol{U}$ be a unimodular matrix. Then*

1. *the inverse $\boldsymbol{U}^{-1}$ is also unimodular;*
2. *$\boldsymbol{x}$ is an integral vector if and only if $\boldsymbol{U}\boldsymbol{x}$ is an integral vector.*

Lemma 5.3 *Let $\boldsymbol{B}$ and $\boldsymbol{B}'$ be 2 matrices. If $\boldsymbol{B} = \boldsymbol{B}'\boldsymbol{U}$ for some unimodular matrix $\boldsymbol{U}$, then $\Lambda(\boldsymbol{B}) = \Lambda(\boldsymbol{B}')$, $\Lambda(\boldsymbol{B})$ is the lattice generated by $\boldsymbol{B}$ (see definition in Appendix 4.A). Moreover, if $\boldsymbol{B}$ and $\boldsymbol{B}'$ have full row rank and $\Lambda(\boldsymbol{B}) = \Lambda(\boldsymbol{B}')$, then $\boldsymbol{B} = \boldsymbol{B}'\boldsymbol{U}$ for some unimodular matrix $\boldsymbol{U}$.*

Example 5.2 *The following elementary row (resp. column) operations are particular unimodular transformation of a matrix $\boldsymbol{B} = [\boldsymbol{b}_1 \dots \boldsymbol{b}_n]^T$.*

1. *swap two row (resp. column) in $\boldsymbol{B}$: $\boldsymbol{b}_i \leftrightarrow \boldsymbol{b}_j$, $i \neq j$;*
2. *multiply a row (resp. column) by -1: $\boldsymbol{b}_i \leftrightarrow -\boldsymbol{b}_j$;*
3. *add an integer multiple of a row (reps. column) to another row (resp. column): $\boldsymbol{b}_i \leftrightarrow \boldsymbol{b}_i + \alpha\boldsymbol{b}_j$, $i \neq j$, $\alpha \in \mathbb{Z}$.*

5.A.2 Hermite Normal Form

Definition 5.3 *[57] We say that an $m \times n$ matrix $\boldsymbol{B}$ of full column rank with integer coefficients is in **Hermite Normal Form** (HNF), if it has the form $\boldsymbol{B} = [\boldsymbol{0}|\boldsymbol{H}]$, where $\boldsymbol{H} = [h_{ij}]$ is an $m \times m$ square matrix satisfying the following conditions*

1. *$h_{ij} = 0$ for $i > j$, (i.e. $\boldsymbol{H}$ is upper-triangular);*
2. *$0 \leq h_{ij} \leq h_{ii}$ for $i < j$ (i.e., $\boldsymbol{H}$ is non-negative and each row has a unique maximum entry, which is on the main diagonal).*

A matrix $\boldsymbol{M}$ in HNF has the following shape

$$\begin{pmatrix} 0 & 0 & \dots & 0 & * & * & \dots & * \\ 0 & 0 & \dots & 0 & 0 & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 & * \end{pmatrix}.$$

Theorem 5.1 *[57] Let $\boldsymbol{A}$ be a $m \times n$ matrix with coefficients in $\mathbb{Z}$. Then, there exists a unique $m \times n$ matrix $\boldsymbol{B} = [b_{ij}]$ in HNF of the form $\boldsymbol{B} = \boldsymbol{A}\boldsymbol{U}$ with $\boldsymbol{U} \in \mathrm{GL}_n(\mathbb{Z})$, where $\mathrm{GL}_n(\mathbb{Z})$ is the group of matrices with integer coefficients which are invertible,* i.e., *whose determinant is equal to ± 1.*

Although $\boldsymbol{B}$ is unique, the matrix $\boldsymbol{U}$ will not be unique.

5.A.3 Solution of the System of Diophantine Equations

Using the HNF of matrix $\boldsymbol{M}$, we can write,

$$\begin{aligned}\sum_{j=1}^{k} a_j \boldsymbol{M}_j \boldsymbol{V}_j &= \boldsymbol{B} \\ \sum_{j=1}^{k} a_j \boldsymbol{M}_j \boldsymbol{V}_j \boldsymbol{B}^{-1} &= \boldsymbol{I} \\ \sum_{j=1}^{k} a_j \boldsymbol{M}_j \boldsymbol{V}_j \boldsymbol{B}^{-1} \boldsymbol{\lambda} &= \boldsymbol{\lambda}.\end{aligned}$$

Identifying the last equality to $\sum_{j=1}^{k} a_j \boldsymbol{x}_j = \boldsymbol{\lambda}$ we obtain,

$$\boldsymbol{x}_j = \boldsymbol{M}_j \boldsymbol{V}_j \boldsymbol{B}^{-1} \boldsymbol{\lambda}.$$

This gives us a particular solution of the system of Diophantine equations. The set of all solution is given by (Eq.5.7)

$$\boldsymbol{x}_j = \boldsymbol{M}_j \boldsymbol{V}_j \boldsymbol{B}^{-1} \boldsymbol{\lambda} + \boldsymbol{s}_j,$$

where $\boldsymbol{s}_j$ is any point of the lattice L_j generated by $\boldsymbol{M}_j \boldsymbol{U}_j$, *i.e.*, $\boldsymbol{s}_j = \boldsymbol{M}_j \boldsymbol{U}_j \boldsymbol{\xi}$ verifying

$$\sum_{j=1}^{k} a_j \boldsymbol{M}_j \boldsymbol{U}_j \boldsymbol{\xi} = \boldsymbol{0}.$$

Conclusion and Perspectives

MOTIVATED by the huge interest for the wireless multi-hop relaying channels, two major issues are addressed in this dissertation: the cooperative relaying protocols in the two-hop wireless networks, and the physical layer network coding for networks with multiple source-destination pairs.

The linear rotate-and-forward (RF) protocol based on AF, is considered in this work for the two-hop relay networks. In this protocol, the relays rotate randomly their received signals before retransmitting them. We used the outage gain metric to study the behavior of the channel outage probability at high signal-to-noise (SNR) ratio. We considered some network configurations, and we extracted outage gain values for the RF protocol and for other protocols having the same diversity order. The outage gain allows us to exactly characterize the outage probability at moderate and high SNR values and to compare the performance of different protocols. We verified numerically the obtained outage gain values. Moreover, we assumed that a limited feedback channel exits between the destination and the relays. We prosposed a low complexity algorithm to find the optimal rotations. The destiantion calculates these optimal rotations and send them back to the relays via the limited feedback channel. We studied the effect on the channel outage probability performance of the limitation in the feedback channel through numerical results.

In multicast networks where several source-destination pairs communicate, network coding is necessary to achieve the cut-set bound on the capacity. In this scope, the compute-and-forward (CF) protocol is a recent relaying scheme that captures much of interest in the literature. In our work, we treated the implementation and practical issues of the CF scheme. We proposed a technique to maximize the computation rate by relating this problem to the shortest vector problem in a lattice. First, we considered the real one-dimensional lattices. Then, based on the maximum-likelihood (ML) function, we proposed a quasi-ML decoding technique and showed that it could be seen as an inhomogeneous Diophantine approximation. Secondly, we generalized our work to the complex multi-dimensional lattices. In this case, we rewrote the maximum-likelihood function which is a sum of Gaussian measures. A system of linear Diophantine equations appears in the ML function for which we give the solution. We then introduced the flateness factor of the sum of Gaussian measures and proposed to use it as a criterion for designing the lattices intervening in the ML function. Moreover, we showed

that the decoding technique involves a system of simultaneous inhomogeneous Diophantine approximations.

As perspectives for future works, we point out the following directions:

- *Degrees of freedom of the CF scheme:* In [5], the authors showed that the lattice scheme of the compute-and-forward has an asymptotic behavior that is not significantly better than time sharing. For large networks with k users, the lattice coding of the CF achieves at most 2 degrees of freedom, far off $k/2$ achieved by interference alignment and the MIMO upper bound of k degrees of freedom. It is of interest to find the degrees of freedom allowed by our scheme based on inhomogeneous Diophantine approximations.

- *Lattice alignment for the interference channel:* In the compute-and-forward framework, the relays decode linear functions of transmitted codewords rather than treating interference as noise. There is a possible coupling of the compute-and-forward and interference alignment. We give the following case to illustrate the idea. For example, we assume that 3 transmitter-receiver couples share the same medium. The transmitted symbol $\boldsymbol{x}_i \in \Lambda_i \subset \mathbb{Z}[i]^n$ is a $\mathbb{Z}[i]$-lattice point. The receiver R_1 sees a linear combination of the transmitted symbols plus independent noise,

  $$\boldsymbol{y}_1 = h_{11}\boldsymbol{x}_1 + h_{21}\boldsymbol{x}_2 + h_{31}\boldsymbol{x}_3 + \boldsymbol{z}.$$

  Instead of considering $h_{21}\boldsymbol{x}_2 + h_{31}\boldsymbol{x}_3$ as an additive noise, the receiver R_1 can approximate this term by an integer combination $a_{21}\boldsymbol{x}_2 + a_{31}\boldsymbol{x}_3$, which is a point in a lattice $\Lambda_1 \subset \mathbb{Z}[i]^n$. The receiver R_1 quantizes the received signal with respect to Λ_1, and then recover its intendant message $\boldsymbol{x}_1$. A possible study of this scheme can be carried out.

- *Decoding several linear functions:* In the CF scheme, each relay is free to decode more than one integer function, and particularly as functions as there is unknown symbols in the received signal. We showed that the coefficient vector is the shortest length vector in a lattice. Decoding successive shortest vectors in a way to obtain independent linear functions, allows us to decode the sources symbols. A fine analysis can be carried out to investigate this possible decoding strategy.

Bibliography

[1] S. Yang and J.-C. Belfiore, "Distributed rotation recovers spatial diversity," in *International Symposium on Information Theory, Austin, Texas, June 2010.*

[2] W. Hachem, P. Bianchi, and P. Ciblat, "Outage probability based power and time optimization for relay networks," *IEEE Transactions on Signal Processing*, vol. 57, no. 2, pp. 764 – 782, February 2009.

[3] B. Nazer and M. Gastpar, "Compute-and-forward: Harnessing interference through structured codes," iEEE Transaction on Information Theory available on arxiv http://arxiv.org/abs/0908.2119, Aug. 2009.

[4] O. L. R. Pedarsani and S. Yang, "On the dmt optimality of the rotate-and-forward scheme in a two-hop mimo relay channel," in *Annuel Allerton Conference on Communications Control an Computing, Allerton, Texas, February 2011.*

[5] U. Niesen and P. Whiting, "The degrees of freedom of compute-and-forward," available on arxiv http://arxiv.org/abs/1101.2182, January 2011.

[6] A. Sendonaris, E. Erkip, and B. Aazhang, "User Cooperation diversity - Part I: System description," *IEEE Transactions on Communications*, vol. 51, no. 11, pp. 1927 – 1938, November 2003.

[7] ——, "User cooperation diversity - Part II: Implementation aspects and performance analysis," *IEEE Transactions on Communications*, vol. 51, no. 11, pp. 1939 – 1948, November 2003.

[8] J. N. Laneman, D. Tse, and G. W. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Transactions on information theory*, vol. 50, no. 12, pp. 3062 – 3080, December 2004.

[9] J. N. Laneman and G. W. Wornell, "Distributed space-time-coded protocols for exploiting cooperative diveristy in wireless networks," *IEEE Transactions on Communications*, vol. 49, no. 10, pp. 2415 – 2425, Octobre 2003.

[10] K. Azarian, H. E. Gamal, and P. Schniter, "On the achievable diversity-multiplexing tradeoff in half-duplex cooperative channels," *IEEE Transactions on Information Theory*, vol. 51, no. 12, pp. 4152 – 4172, Decembre 2005.

[11] R. U. Nabar, H. Bolcskei, and F. W. Kneubuhler, "Fading relay channels: performance limits and space-time signal design," *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 6, pp. 1099 – 1109, August 2004.

[12] S. Yang and J.-C. Belfiore, "Towards the optimal amplify-and-forward cooperative diversity scheme," *IEEE Transactions on Information Theory*, vol. 53, no. 9, pp. 3114 – 3126, Septembre 2007.

[13] T. M. Cover and A. A. E. Gamal, "Capacity theorems for the relay channel," *IEEE Transactions on Information Theory*, vol. 25, no. 5, pp. 572 – 584, Septembre 1979.

[14] M. Yukusel and E. Erkip, "Multiple-antenna cooperative wireless systems: A diversity-multiplexing tradeoff perspective," *IEEE Transactions on Information Theory*, vol. 5, no. 12, pp. 3371 – 3393, Octobre 2007.

[15] K. Sreeram, s. Birenjith, and P. V. Kumar, "Dmt of multi-hop cooperative networks - Part I: Basic results, note = available on arxiv http://arxiv.org/abs/0808.0234,."

[16] ——, "Dmt of multi-hop cooperative networks - Part II:Half-duplex networks with full-duplex performance," available on arxiv http://arxiv.org/abs/0808.0235.

[17] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, pp. 379 – 423 and 623 – 656, 1948.

[18] G. J. Foschini, "Layered Space-Time architecture for wireless communication in a fading environment when using multi-element antennas," *Bell Labs Tech. J.*, vol. 1, pp. 41–59, 1996.

[19] L. Zheng and D. Tse, "Diversity and multiplexing : A fundamental tradeoff in multiple antenna channels," *IEEE Transactions on Information Theory*, vol. 49, no. 5, pp. 1073 – 1096, May 2003.

[20] E. Lawler, *Combinatorial Optimization: Networks and Matroids*. Dover Publications, 2001.

[21] S. Yang and J.-C. Belfiore, "Diversity of MIMO multihop relay channels," available http://arxiv.org/abs/0708.0386.

[22] Y. Jing and B. Hassibi, "Distrinuted space-time coding in wireless relay networks," *IEEE Transactions on Wireless Communications*, vol. 5, no. 12, pp. 3524 – 3536, December 2006.

[23] ——, "Cooperative diversity in wireless relay networks with multiple-antenna nodes," October 2005, pp. 815 – 819.

[24] C. Rao and B. Hassibi, "Diversity-multiplexing gain trade-off of a MIMO system with relays," in *Information Theory Workshop, Norway, July 2007*.

[25] S. Borade, L. Zheng, and R. Gallager, "Amplify and Forward in wireless relay networks: Rate, diversity and network size," *IEEE Transactions on Information Theory*, vol. 53, no. 10, pp. 3302 – 33 018, October 2007.

[26] S. O. Gharan, A. Bayesteh, and A. K. Khandani, "Diversity multiplexing tradeoff in multi-antenna multi-relay networks: Improvements and some optimality results," available http://arxiv.org/abs/0708.0386.

[27] ——, "On the diversitymultiplexing tradeoff in multiple relay networks," *IEEE Transactions on Information Theory*, vol. 55, no. 12, pp. 5423 – 5444, December 2009.

[28] A. S. Avestimehr, S. N. Diggavi, and D. Tse, "Wireless network information flow: a deterministic approach," available http://arxiv.org/abs/0906.5394.

[29] S. Yang, "Cooperative diversity of MIMO channels with Amplify-and-Forward," Ph.D. dissertation, Telecom ParisTech, 2007.

[30] W. Zeng, M. Wang, C. Xiao, and J. Lu, "On the power allocation for relay networks with finite-alphabet constraints," in *Globcom 2010, Miami, FL, december 2010*.

[31] J. M. Paredes and A. B. Gershman, "Relay network beamforming and power control using maximization of mutual information," in *Globcom 2010, Miami, FL, december 2010*.

[32] W. T. Wells, R. L. Anderson, and J. W. Cell, "The distribution of the product of two central or non-central chi-square variates," *Annals of Mathematical Statistics*, vol. 33, no. 3, pp. 1016 – 1020, January 1962.

[33] L. S. Gradshteyn and I. M. Ryzbik, *Tables of Integrals. Series and Products.* 6th ed. Allen Jeffrey and Daniel Zwillinger, July 2000.

[34] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204 – 1216, July 2000.

[35] K. Menger, "Zur allgemeinen kurventheorie," *Fundamenta Mathematicae*, vol. 10, pp. 95 – 115, 1927.

[36] L. R. F. Jr. and D. R. Fulkerson, "Maximal flow through a network," *Canadian Journal of Mathematics*, vol. 8, pp. 399 – 404, 1956.

[37] P. Elias, A. Feinstein, and C. E. Shannon, "Note on maximum flow through a network," *IEEE Transaction on Information Theory*, vol. 2, pp. 117 – 119, 1956.

[38] S.-Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," *IEEE Transactions on Information Theory*, vol. 49, pp. 371 – 381, February 2003.

[39] R. W. Yeung, S.-Y. R. Li, N. Cai, and Z. Zhang, *Foudations and Trends in Communications and Information Theory: Network Coding Theory.* Now Publishers, 2005.

[40] C. Fragouli and E. Soljanin, *Foudations and Trends on Networking: Network Coding Fundamentals*. Now Publishers, 2007.

[41] "Network coding homepage," http://www.networkcoding.info.

[42] S.Zhang, S.-C. Liew, and P. P. Lam, "Physical-layer network coding," available on arxiv http://arxiv.org/abs/0704.2475.

[43] ——, "Hoc topic: Physical layer network coding," in *ACM International Conference on Mobile Computing and Networking (Mobicom 2006), Los Angeles, CA, USA, Sep.24-29 2006*.

[44] P. Popovski and H. Yomo, "The anti-packets can increase the achievable throughput of a wireless multihop network," in *IEEE Intenrational Conference on Communications (ICC 2006), Istanbul, Turkey, 11-15 June 2006*.

[45] P. Popovski and T. Koike-Akino, "Coded bidirectional relaying in wireless networks," *New Directions in Wireless Communications Research, V. Tarokh, Ed. Springer*, pp. 291 – 316, 2009.

[46] M. P. Wilson, K. Narayanan, H. Pfister, and A. Sprintson, "Joint physical layer coding and network coding for bi-directional relaying," *IEEE Transactions on Information Theory*, vol. 56, pp. 5641 – 5654, 2010.

[47] T. Koike-Akino, P. Popovski, and V. Tarokh, "Optimized constellations for two-way wireless relaying wih physical network coding," *IEEE Journal on Selected Areas in Communications*, vol. 27, pp. 773 – 787, June 2009.

[48] B. Hern and K. Narayanan, "Multilevel coding schemes for computeand-forward," available on arxiv http://arxiv.org/abs/1010.1016, Oct 2010.

[49] R. Koetter and M. Medard, "An algebraic approach to network coding," *IEEE ACM Transaction on Networking*, vol. 11, no. 5, pp. 782 – 795, October 2003.

[50] S. Katti, S. Gollakota, and D. Katabi, "Embracing wireless interference: Analog network coding," in *ACM SIGCOMM, October 2007*.

[51] S. H. Lim, Y.-H. Kim, A. E. Gamal, and S.-Y. Chung, "Noisy network coding," *IEEE Transactions on Information Theory*, vol. 57, no. 5, pp. 3132 – 3152, May 2011.

[52] C. Feng, D. Silva, and F. R. .Kschischang, "An algebraic approach to Physical-Layer Network Coding," in *ISIT 2010, May 2010*, available on arxiv http://arxiv.org/abs/1005.2646.

[53] ——, "Design criteria for Lattice Network Coding," in *45th Annual Conference on Information Sciences and Systems (CISS), Baltimore, MD, March 2011*.

[54] B. Nazer and M. Gastpar, "The case for structured random codes in network capacity theorems," available on arxiv http://arxiv.org/abs/0802.0342, February 2008.

[55] ——, "Computation over multiple-access channels," *IEEE Transactions on Information Theory*, vol. 53, no. 5, pp. 3498 – 3516, October 2007.

[56] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups.* 2th ed. Springer-Verlag New York, Ink., 1998.

[57] H. Cohen, *A Course in Computational Algebraic Number Theory.* Springer-Verlag. Pages 103-105. Section 2.7.3: Finding Small Vectors in Lattices., 1993.

[58] U. Fincke and M. Pohst, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis," math. Comp. 44 (1985), 463-471.

[59] R. L. R. T. H. Cormen, C. E. Leiserson and C. Stein, *Introduction to Algorithms.* Third Edition. The MIT Press. Pages 933-939. Section 31.2: Greatest Common Divisor., 2009.

[60] D. Micciancio and O. Regev, "Worst-case to average-case reductions based on gaussian measure," sIAM J. on Computing, 37(1):267-302 (May 2007).

[61] J. W. S. Cassels, *Introduction to Algorithms.* An Introduction to Diophantine Approximation. Cambridge University Press., 1957.

[62] S. V. L. Clarkson, "Approximation of linear forms by lattice points with applications to signal processing," Ph.D. dissertation, January 1997.

[63] G. Poltyrev, "On coding without restructions for the AWGN channel," *IEEE Transactions on Information Theory*, vol. 40, no. 2, pp. 409 – 417, March 1994.

About the author

ALi Osmane was born in Lebanon, on February 3, 1985. He received his engineering diploma from Telecom ParisTech former Ecole Nationale Supérieure des Télécommunications de Paris in 2008 and his master degree from Université Pierre et Marie Curie, France in the same year. Since October 2008, he is pursuing his PhD in the group of Professor Jean-Claude Belfiore at Telecom ParisTech.

Publications

The content of this thesis was submitted to the following conferences and journal papers.

Journal papers

- A. Osmane and J.-C Belfiore, "The Compute-and-Forward Protocol: Implementation and Practical Aspects," available on http://arxiv.org/abs/1107.0300.

- A. Osmane and J.-C Belfiore, "Practical Constraints on Lattice Codes for the Compute-and-Forward Protocol: The Flatness Factor," *in preparation to be submitted to* IEEE Transactions on Wireless Communications.

- A. Osmane, S. Yang and J.-C Belfiore, "Performance of the Rotate-and- Forward Protocol in the Two-Hop Relay Channels," *submitted to* IEEE Transactions on Wireless Communications.

Conference papers

- A. Osmane, S. Yang and J.-C Belfiore, "On the Performance of the Rotate-and-Forward Protocol in the Two-Hop Relay Channels", ICC, San Francisco, CA USA, June 2011.

- A. Osmane, S. Yang and J.-C Belfiore, "Two-Hop Relay Channels with Limited Feed-Back ", PIMRC, Istanbul Turkey, September 2010.

Réseaux Spontanés et Auto-Organisants : du Codage Spatio-Temporel au Codage de Réseaux

RESUME : Nous étudions un protocole de coopération dans les réseaux MIMO à deux sauts : le rotate-and-forward (RF). Dans ces réseaux, la source et la destination ne communiquent qu'à travers une couche de relais. Nous étudions la performance du protocole RF à partir d'une nouvelle métrique appelée gain de coupure. Ce gain nous permet de décrire le comportement de la probabilité de coupure à des valeurs du rapport signal à bruit moyennes et élevées. En utilisant le gain de coupure, nous comparons la performance du RF aux performances d'autres protocoles ayant le même ordre de diversité que le RF. Nous supposons aussi qu'une voie de retour existe entre la destination et les relais et nous donnons un algorithme qui permet d'améliorer les performances du RF en termes de probabilité de coupure en se basant sur la connaissance des gains du canal.

Nous considérons un protocole de codage de réseaux au niveau physique : le compute-and-forward (CF). Nous nous intéressons à la maximisation du débit de calcul et nous montrons que c'est équivalent à la recherche du vecteur le plus court dans un réseau de points donné. Tout d'abord, nous implémentons le protocole utilisant des réseaux de points uni-dimensionnels et des gains de canal réels. Nous nous basons sur la fonction de maximum de vraisemblance (ML) pour proposer une technique de décodage quasi-ML et nous montrons que le décodage s'effectue par une approximation Diophantienne inhomogène. Ensuite, nous généralisons certains de ces résultats au cas des réseaux de points multi-dimensionnels et des gains de canal complexes, et nous proposons un critère de construction des codes en réseaux de points qu'on appelle le facteur de platitude.

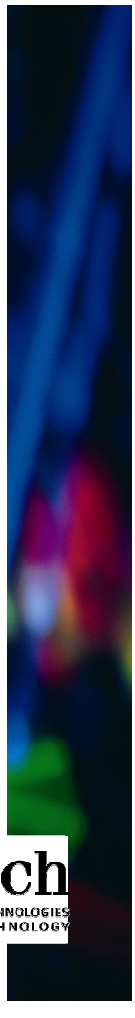
Mots clés : Protocole de Coopération, rotate-and-forward, gain de coupure, codage de réseaux au niveau physique, compute-and-forward, facteur de platitude, réseaux de points.

Spontaneous and Self-Organizing Networks: from Space-Time Coding to Network Coding

ABSTRACT : We study the rotate-and-forward (RF) cooperative protocol in the two-hop MIMO relay networks. In these networks, the source communicates with the destination via a layer of relays. We consider different network configurations and we study the performance of the RF scheme using a new metric called outage gain. This gain gives us an exact characterization of the outage probability's behavior at moderate and high signal-to-noise ratio. Using this metric, we compare the performance of the RF scheme to the performance of other schemes having the same diversity order. Moreover, we assume that a feedback channel exists between the destination and the relays, and we use the channel knowledge to improve the performance of the RF scheme in terms of outage probability.

We consider the physical layer network coding protocol; the compute-and-forward. We consider the transmission rate maximization problem and we relate it to the lattice shortest vector problem. We first implement this protocol for real Gaussian channels and one-dimensional lattices. We derive the maximum likelihood (ML) criterion and we propose a quasi-ML decoding technique and show that it can be implemented by using an Inhomogeneous Diophantine Approximation algorithm. Secondly, we generalize some of these results to the complex Gaussian multi-dimensional lattices, and introduce the flatness factor as a design criterion for lattice codes.

Keywords : Cooperation protocol, rotate-and-forward, outage gain, physical layer network coding, compute-and-forward, flatness factor, lattice codes.



TELECOM ParisTech

EDITE

ParisTech
INSTITUT DES SCIENCES ET TECHNOLOGIES
PARIS INSTITUTE OF TECHNOLOGY