Amélioration de la sécurité et de la fiabilité des systèmes de communication sans fil

Mémoire

Ahmadreza Amirzadeh

Maîtrise en génie électrique
Maître ès sciences (M. Sc.)

Québec, Canada

Amélioration de la sécurité et de la fiabilité des systèmes de communication sans fil

Mémoire

Ahmadreza Amirzadeh

Sous la direction de :

Jean-Yves Chouinard, directeur de recherche

Résumé

Dans ce mémoire, de nouvelles approches ont été introduites pour concevoir les systèmes de communication fiables, **Section 1**, et sécurisées, **Section 2**, où les codes LDPC ont été choisis comme schéma de codage principal. Ce mémoire comprend deux sections :

Section 1 : Les codes LDPC réguliers et irréguliers sont définis et différents décodeurs basés sur l'échange de message de décisions fermes et souples sont introduits. Par la suite, quelques définitions, comme le seuil des codes LDPC utilisant l'évolution de la densité de probabilité (ou la propagation de croyance), l'écart multiplicatif et les distributions de degrés de nœuds de parité et de nœuds de variable, sont énoncées. Par après, ces concepts préliminaires sont utilisés pour concevoir des ensembles de code LDPC irréguliers approchant la capacité du canal à l'aide de programmation linéaire et d'un algorithme génétique.

Section 2 : Une méthode est introduite pour l'amélioration du secret dans ce genre de système. Cette méthode fonctionne sur la base de demande de retransmission de paquets d'information. Selon cette approche, lorsque le récepteur ne peut pas converger vers le bon message, une demande de retransmission est envoyée. Au lieu d'envoyer le paquet entier dans le cas d'une défaillance à la sortie du décodeur du destinataire, la retransmission des sous-paquets est explorée. Le système proposé dans cette phase est appelé protocole HARQ-Granulaire Adaptatif (AG-HARQ). Il essaie de réduire au minimum le taux requis pour un décodage réussi par les parties légitimes tout en augmentant la sécurité en minimisant les fuites d'information vers un espion éventuel. En outre, pour améliorer encore le niveau de sécurité dans la méthode AG-HARQ proposée, le schéma de contamination d'erreur intra-trame (IntraEC) et le schéma de contamination d'erreur inter-trame (InterEC) sont utilisés en conjonction avec cette méthode. Cette combinaison permet un haut niveau de sécurité dans le système de communication sans fil.

Abstract

In this memoir, new approaches have been introduced for designing reliable, **Section 1**, and secure, **Section 2**, communication systems where the LDPC codes have been chosen as the principal coding scheme. This memoir comprises two sections:

Section 1: Regular and irregular LDPC codes are defined and different message passing decoders based on hard and soft decisions are introduced. Afterward, some definitions like the threshold of LDPC codes using Density Evolution (or Belief Propagation), the Multiplicative Gap, and the check node and variable node degree distributions are explained in detail. Later, these preliminary concepts are used to design the channel capacity approaching Irregular LDPC codes combining Genetic Algorithm and Linear Programming.

Section 2: A new scheme is introduced for secrecy enhancement for these systems. This method is based on feedback retransmission requests. With this approach, when the intended recipient cannot converge to the right message, a retransmission request is sent back to the transmitter. The retransmission of the sub-packets, instead of sending the whole packet in the case of failure at the intended recipient's decoder output, is explored in detail. Our proposed scheme is called Adaptive Granular Hybrid Automatic Repeat reQuest (AG-HARQ) protocol, which tries to minimize the required rate for successful decoding of the legitimate parties while amplifying the privacy by minimizing the information leakage to a wiretapper. In addition, to further improve the security level of the proposed AG-HARQ method, Intra-frame error contamination (IntraEC) and Inter-frame error contamination (InterEC) schemes are used in conjunction with this method. This combination can provide a high level of security in wireless communication systems.

Table des matières

Liste des tableaux

Liste des figures

Liste des symboles

c	mot de code
C	capacité du canal
$C_{BEC}(\varepsilon)$	capacité du canal binaire à effacement
$\hat{C}_j$	indice de niveau de confiance
$\mathbb{E}$	espérance mathématique
g	granularité
$\mathbf{G}$	matrice génératrice
$\mathbf{H}$	matrice de contrôle de parité
$\mathbf{H}(\mathbf{x})$	entropie
l	nombre d'itérations
$\hat{l}_{max}$	degré maximal des noeuds de variable
$\hat{l}_{avg}$	valeur moyenne des degrés de noeuds de variables
$L(x)$	distribution de degré de variable normalisée à partir d'une perspective de noeud
$LLR(x)$	rapport de vraisemblance logarithmique
$\mathbf{m}$	message
$\hat{m}$	nombre d'équations de contrôle de parité
$\tilde{\mathbf{m}}$	estimation du message original
n	nombre de bits dans le mot de code
$\hat{n}_{avg}$	valeur moyenne des degrés de noeuds de parité
$\hat{n}_{LP}$	taille de l'espace de recherche de la Programmation Linéaire
$\hat{n}_{max}$	degré maximal des noeuds de parité
$\hat{n}_{pop}$	nombre maximum de la population
p^{BP}	probabilité d'effacement obtenu par l'algorithme de propagation des croyances

$P(x)$	distribution des degrés de parité à partir d'une perspective de noeud
$r(\lambda(x),\rho(x))$	taux de conception
$R(x)$	distribution de degrés de parité normalisée à partir d'une perspective de noeud
$\mathbf{S}$	matrice d'embrouillage
$\mathbf{S^{-1}}$	matrice de désembrouillage
$v_{\varepsilon}^{-1}(x)$	taux de conception
w_c	poids de colonne
w_r	poids de rangée
$\mathbf{x^n}$	message codé
$\mathbf{y^n}$	observation du récepteur légitime
$\mathbf{z^n}$	observation de l'espion
ε	probabilité d'effacement
ε^{BP}	probabilité d'effacement obtenu par l'algorithme de propagation des croyances
$\lambda(x)$	distribution des degrés de noeuds de variable
$\Lambda(x)$	distribution des degrés de variable à partir d'une perspective de noeud
$\rho(x)$	distribution des degrés de noeuds de parité
δ	écart multiplicatif

Abréviations

LDPC	Code à faible densité de parité / Low Density Parity Check Code
DE	Évolution de densité de probabilité / Density Evolution
HARQ	Requête automatique de répétition hybride / Hybrid Automatic Repeat reQuest
G-HARQ	Requête automatique de répétition hybride-granulaire / Granular Hybrid Automatic Repeat reQuest
AG-HARQ	Requête automatique de répétition hybride granulaire adaptative / Adaptive Granular Hybrid Automatic Repeat reQuest
AD	Analogique-numérique / Analog-Digital
DA	Numérique-analogique / Digital-Analog
BEC	Canal binaire à effacement / Binary Erasure Channel
BSC	Canal symétrique binaire / Binary Symmetric Channel
AWGN	Canal à bruit blanc gaussien additif / Additive White Gaussian Noise
GA	Algorithme génétique / Genetic Algorithm
LP	Programmation linéaire / Linear Programming
LLR	Rapport de vraisemblance logarithmique / Logarithmic Likelihood Ratio
FER	Taux d'erreur par trame / Frame Error Rate
BER	Taux d'erreur par bit / Bit Error Rate
SG	Écart de sécurité / Security Gap
SPA	Algorithme somme-produit / Sum-Product Algorithm
BF	Basculement de bit / Bit Flipping
SPA-Log	Algorithme somme-produit dans le domaine logarithmique / Sum-Product Algorithm in the Logarithmic Domain
SNR	Rapport signal sur bruit / Signal to Noise Ratio
MAP	Maximum A Posteriori
IntraEC	Contamination d'erreur intra-trame / Intra-frame error contamination
InterEC	Contamination d'erreur inter-trame / Inter-frame error contamination

Remerciements

Je tiens tout d'abord à remercier vivement mon directeur de recherche, le professeur Jean-Yves Chouinard, pour sa méthodologie de travail et sa disponibilité malgré un emploi de temps fort chargé. Le déroulement de mon projet de recherche a été sagement guidé par des réunions régulières aux cours desquelles il a su combiner sympathie et sérieux afin de me faire profiter de son expertise pour évaluer mes travaux de recherche et de ses conseils enrichissants pour diriger l'évolution de mon cursus académique ainsi celle de mon projet de recherche.

Je remercie aussi mes amis, les Dr. Mohammed Hadj Taieb et M. Mohammad Amin Haji Bagheri Fard. Je les consultais fréquemment au sujet de certains points : ils n'ont jamais hésité à consacrer leur temps pour se pencher pleinement avec moi sur ces questions et à me faire part de toute leur expertise.

J'adresse ensuite mes remerciements à tous les étudiants et amis du laboratoire de radiocommunication et de traitement de signal (LRTS) et tout le corps enseignant et administratif qui ont fait en sorte que le cadre de travail soit instructif, propice et agréable.

Finalement, je remercie spécialement tous les membres de ma famille pour la patience qu'ils m'ont accordée et les énormes sacrifices qu'ils ont faits pour que je sois là où je n'aurais jamais pu être sans eux.

Chapitre 1

Introduction

1.1 Motivations de la recherche

Au cours des dernières années, on a observé une énorme demande pour la transmission de données fiable, sécurisée et efficace. L'importance de ce sujet peut être comprise par l'émergence de réseaux de communication avancés pour le stockage et le traitement des informations dans des applications industrielles. La combinaison des théories de la communication et de l'information est nécessaire pour la conception de ces systèmes.

En 1948, Shannon [1] a montré que lorsque le taux d'information est inférieur à la capacité du canal, en utilisant le codage de l'information approprié, les erreurs introduites par un canal bruité peuvent corrigées. Depuis l'article de Shannon, de grands efforts ont été déployés pour la conception de codeurs et décodeurs efficaces pour le contrôle des erreurs produites par l'environnement bruité.

Les réalisations récentes en technologie de transmission sont l'épine dorsale pour obtenir la fiabilité requise pour les systèmes numériques à grande vitesse d'aujourd'hui. Les techniques de codage de contrôle d'erreurs sont utilisées comme partie importante à la conception de ces systèmes.

Selon la théorie de l'information, la capacité d'un canal de communication est la limite supérieure du taux de l'information pour laquelle les données peuvent être transmises de manière fiable par un émetteur vers un récepteur. En d'autres termes, malgré toutes les techniques de modulation et de codage possibles, le théorème de Shannon indique que la capacité C du canal constitue la limite théorique, c'est-à-dire le taux de données pour lequel nous pouvons avoir une communication avec un taux d'erreurs arbitrairement faible. La notion de la capacité du canal est au cœur du développement des systèmes de communication sans fil modernes. Avec l'avènement des nouvelles méthodes de codage de correction d'erreurs, des performances très proches des limites promises par la capacité de canal ont été atteintes. Par conséquent, il est souhaitable de concevoir des codes appropriés et de les mettre en œuvre dans des systèmes de communication réels. Dans ce travail, nous nous concentrons sur les codes à faible densité de parité (LDPC) et la conception des codes LDPC irréguliers est aussi étudiée.

Un autre problème important dans les systèmes de communication sans fil est le problème de la sécurité. Les systèmes de communication sans fil sont vulnérables à l'espionnage en raison de leur nature de radiodiffusion. Par conséquent, avec l'avancement des systèmes de transmission modernes, il y a un besoin croissant pour des modèles de communication sécurisés. Les protocoles de sécurité font partie des intérêts majeurs au cours des dernières années avec le développement d'un vaste éventail de réseaux sans fil. La cryptographie est une façon populaire de fournir des protocoles sécurisés à la couche d'application. Avec l'avènement des ères numérique et mobile, la cryptographie non seulement permet la confidentialité, mais contribue aussi aux autres questions telles que la signature numérique, l'authentification, l'échange et la gestion de clés, etc.

Contrairement aux approches cryptographiques, l'objectif de sécurité au niveau de la couche physique est d'introduire des stratégies efficaces de communication sécurisée en utilisant les propriétés de la couche physique. Ces stratégies peuvent améliorer la sécurité des systèmes disponibles en ajoutant un niveau de sécurité à l'information théorique. Il convient de mentionner que la sécurité de la couche physique peut être combinée avec les méthodes de sécurité existantes afin d'améliorer le niveau général de la sécurité des systèmes de communication.

Pour illustrer le concept de sécurité de la couche physique, la Fig. 1.1 montre un réseau sans fil. Le terminal E espionne la communication entre l'émetteur A et le récepteur légitime B. Le canal de communication entre les terminaux A et B est appelé le canal principal, tandis que le canal de communication entre les terminaux A et E est connu comme le canal de l'espion.

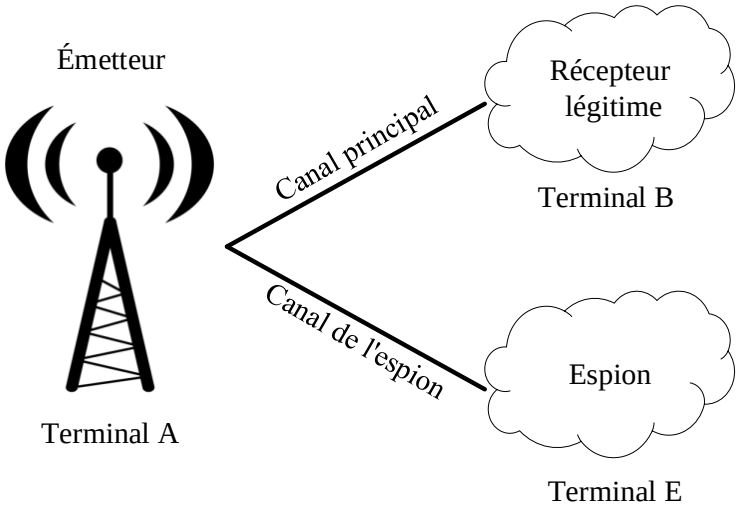


FIGURE 1.1 – L'espionnage dans les réseaux de communication sans fil.

Par conséquent, il est nécessaire de concevoir une méthode permettant de sécuriser les informations pouvant être espionnées. Dans ce mémoire, une nouvelle approche basée sur le protocole de la requête automatique de répétition hybride (HARQ) et la contamination d'erreur est proposée. Son objectif est de réduire au minimum le taux requis pour le décodage réussi des parties légitimes tout en amplifiant

la sécurité afin de réduire les fuites d'informations vers l'espion.

1.2 Contributions

Ce mémoire comprend deux contributions principales :

Au chapitre 3, nous cherchons à trouver une approche efficace pour minimiser l'écart δ entre la capacite d'un canal et le taux de transmission maximum atteignable en pratique. Cette méthode itérative optimise la distribution des degrés de nœuds de variables à l'aide d'un algorithme génétique (GA) et la distribution des degrés des nœuds de parité en utilisant la programmation linéaire (LP). L'alternance entre ces deux problèmes d'optimisation est beaucoup moins complexe en raison du modèle simple que nous avons pris en considération pour la distribution des degrés de nœuds de parité. Il convient de mentionner qu'il existe différents canaux qui peuvent être choisis de telle sorte que les codes LDPC irréguliers puissent être optimisés. Ici, le canal binaire à effacement (BEC), largement utilisé comme modèle des systèmes de communication, est choisi. Il est l'un des canaux les plus simples à analyser en raison de la simplicité des contraintes d'évolution de la densité de probabilité (DE) [2].

Au chapitre 4, pour améliorer davantage le mécanisme de rétroaction utilisé dans les procédés précédents [3], une méthode adaptative G-HARQ (AG-HARQ) est introduite pour envoyer les sous-paquets appropriés lorsque la retransmission est demandée. Dans ce procédé, après le décodage LDPC, l'indice de niveau de confiance, $\hat{C}_j$, pour un décodage correct est calculé pour chaque sous-paquet. Cet indice indique la moyenne de la valeur absolue du rapport de vraisemblance logarithmique (LLR) correspondant aux valeurs de vraisemblance à la sortie du décodeur. En d'autres termes, pour un mot de code LDPC reçu de la longueur désirée, divisé en plusieurs sous-paquets, la fiabilité de décodage de chaque sous-paquet peut être estimée à l'aide de cet indice. Contrairement au G-HARQ qui retransmet les sous-paquets au hasard, le destinataire, Bob, demande la retransmission de sous-paquets spécifiques avec les valeurs $\hat{C}_j$ les plus basses dans un ordre croissant s'il ne peut pas faire converger le message correctement. Ce schéma permet d'éviter la retransmission de l'information plus redondante qui n'est pas nécessaire à Bob, mais qui peut être utile pour l'espion. En outre, l'AG-HARQ nécessite un moins grand nombre de demandes de retransmission comparativement au G-HARQ. L'efficacité de la méthode AG-HARQ proposée est évaluée en utilisant le taux d'erreurs de trame (FER). Le cas de la valeur négative de l'écart de sécurité (SG), où la qualité du canal de l'espion est meilleure que celle du canal principal, est aussi considéré. En outre, la méthode AG-HARQ est combiné avec la contamination d'erreur intra-trame (IntraEC) et la contamination d'erreur inter-trame (InterEC) pour diminuer encore les fuites d'information vers un éventuel espion. La méthode IntraEC utilise une matrice d'embrouillage $\mathbf{S}$ pour propager une erreur dans la trame entière. D'autre part, la méthode InterEC propage non seulement une erreur dans la trame courante, mais aussi aux autres trames en utilisant l'entrelacement et le désentrelacement. L'efficacité de la méthode AG-HARQ proposée avec IntraEC et InterEC est évaluée en utilisant le taux d'erreur par bit (BER).

1.3 Organisation de mémoire

L'organisation de ce mémoire peut être résumée comme suit.

Le chapitre 2 présente les définitions et le contexte des systèmes de communication ainsi que l'importance des codes de correction d'erreurs. Les codes LDPC sont introduits comme une classe importante de codes correcteurs d'erreurs et le processus de décodage et la notion de seuil de codage sont présentés. Les méthodes proposées précédemment dans la conception de codes LDPC sont discutées en bref. Une nouvelle approche pour la conception de l'approche capacitive des codes LDPC irréguliers sur le canal binaire à effacement est développée sur la base du concept de l'écart multiplicatif. Le reste du chapitre 2 décrit la notion de sécurité dans les systèmes de communication sans fil où la sécurité de la couche physique est notre principale préoccupation. Le modèle de canal à écoute est dépeint comme un modèle de diagramme fonctionnel pour les systèmes de communication sans fil. La capacité secrète et une nouvelle approche pour améliorer la sécurité sont aussi discutées.

Au chapitre 3, l'optimisation de codes LDPC irréguliers sur BEC est formulée et les mesures utiles pour choisir les meilleurs ensembles de distribution de degrés sont données. La méthode GA-LP proposée est ensuite discutée en détail et enfin, les résultats de simulation sont présentés.

Au chapitre 4, le processus de décodage des codes LDPC est discuté et une vue d'ensemble du décodage souple LDPC en utilisant la valeur LLR est donnée. Les méthodes HARQ et G-HARQ et l'AG-HARG précédemment proposées, qui travaillent en fonction des requêtes de la rétroaction de retransmission, sont ensuite discutées en détail. Enfin, les résultats de simulation, qui montrent l'efficacité de notre méthode AG-HARQ proposée dans l'amélioration de la sécurité dans les systèmes de communication, sont présentés. En outre, les concepts de IntraEC et InterEC sont expliqués et les résultats de simulation montrent que l'AG-AHRQ en conjonction avec IntraEC et InterEC peut produire un haut niveau de sécurité.

Le chapitre 5 présente le sommaire des travaux réalisés dans ce mémoire ainsi que les articles publiés. En outre, ce chapitre donne quelques suggestions de travaux futurs.

Chapitre 2

Revue de la littérature

2.1 Systèmes de transmission typiques

En télécommunication, un système de transmission est un système qui transmet un signal d'un endroit à un autre. Le signal peut être un signal électrique, optique ou radio. Le système de transmission est un médium par lequel les données sont transmises d'un point à un autre. Des exemples de systèmes de transmission communs couramment utilisés sont les suivants : internet, réseau mobile, câbles sans fil, etc. La Fig. 2.1 montre un système de transmission typique.

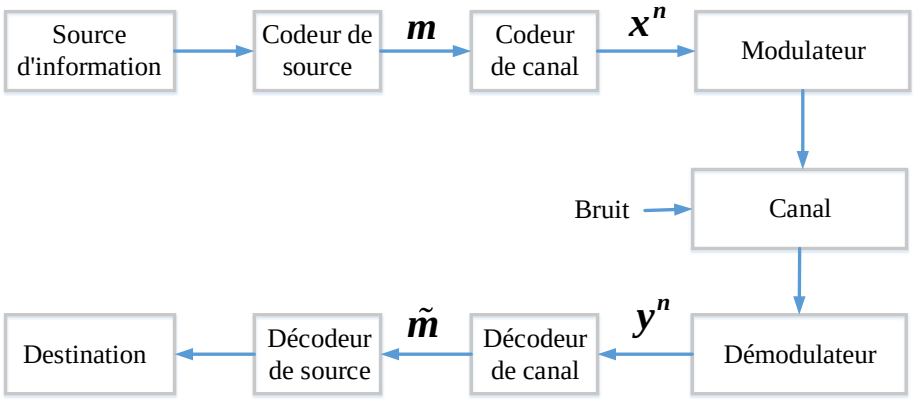


FIGURE 2.1 – Système de transmission typique.

Selon cette figure, la source d'information peut être considérée comme une personne ou une machine. La sortie de la source est un signal continu ou discret. Le codeur de source numérise la sortie de la source en une séquence de bits connue comme la séquence d'informations **m**. Dans cette étape, la conversion analogique numérique (A/D) est utilisée lorsque nous avons une source continue. Le premier objectif de la conception du codeur de source est de minimiser le rapport (bits/temps) nécessaire pour produire la sortie de la source, tandis que le deuxième objectif est que la sortie de la source puisse être précisément régénérée à partir des informations de séquence **m**.

La séquence $\mathbf{m}$ est convertie en une séquence discrète $\mathbf{x^n}$ connue comme un mot de code en utilisant le codeur de canal. La conception et la mise en œuvre de codeurs et décodeurs efficaces pour surmonter le bruit introduit par le canal ont été parmi les sujets de recherche les plus importants au cours des dernières décennies. Afin de rendre les symboles discrets $\mathbf{x^n}$ appropriés pour la transmission sur un canal bruité, chaque sortie du codeur de canal est convertie par le modulateur en une forme d'onde dont la durée est exprimée en T secondes.

Les séquences reçues $\mathbf{y^n}$ sont converties par le décodeur de canal en une séquence $\tilde{\mathbf{m}}$ c'est-à-dire la séquence de l'information estimée. La technique de codage appliquée et les caractéristiques de bruit du canal sont deux paramètres majeurs qui affecteront le choix de la stratégie de décodage. Le bruit introduit par le canal peut provoquer des erreurs de décodage, mais la séquence $\tilde{\mathbf{m}}$ sera idéalement une réplique de $\mathbf{m}$.

Les principales préoccupations dans la conception des codeurs et décodeurs peuvent être résumées en trois points clés : l'information peut être transmise rapidement dans l'environnement bruité, la reproduction de l'information peut être réalisée de manière fiable à la sortie du décodeur de canal et le coût de mise en œuvre de la conception du décodeur et du codeur est dans une plage acceptable.

Nous pouvons simplifier le diagramme fonctionnel représenté sur la Fig. 2.1 en combinant la source d'information et le codeur de source, en fusionnant le modulateur, le canal, et le démodulateur en un seul bloc nommé «canal» (avec entrée $\mathbf{x^n}$ et sortie $\mathbf{y^n}$), et en combinant le décodeur de source et de destination dans le récepteur à l'entrée $\tilde{\mathbf{m}}$. La Fig. 2.2 montre le modèle simplifié.

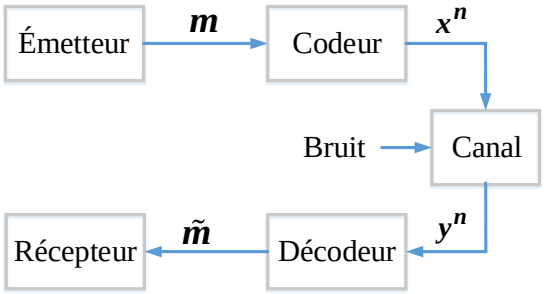


FIGURE 2.2 – Modèle simplifié du système de communication.

L'émetteur transmet le message $\mathbf{m}$ à travers le canal par le codage de $\mathbf{x^n}$ de longueur n. Ensuite, le canal introduit du bruit au message codé $\mathbf{x^n}$ et un nouveau signal $\mathbf{y^n}$ est produit par conséquent. Enfin, le décodeur estime le $\tilde{\mathbf{m}}$ du signal original $\mathbf{m}$ en corrigeant les erreurs du signal reçu.

Maintenant, nous avons un canal de communication bruité à travers lequel nous voulons envoyer l'information de manière fiable. Shannon [4] a montré que la transmission fiable est possible par ce canal si le taux d'information est inférieur à la capacité du canal. Afin d'approcher la limite de Shannon, nous avons cependant besoin d'utiliser la technique de correction d'erreurs de codage. La détection et la correction d'erreurs sont des techniques qui permettent une transmission fiable des

données numériques sur des canaux de communication peu fiables. Les canaux de communication sont soumis au bruit, et donc des erreurs peuvent être introduites lors de la transmission de la source vers le récepteur. Les techniques de détection d'erreurs permettent la détection de telles erreurs, tandis que la correction d'erreurs permet la reconstruction des données d'origine. En d'autres termes, le schéma de correction d'erreurs de codage [5] aide à ce que le récepteur soit capable de corriger les erreurs. Cette méthode ajoute deux éléments importants pour les systèmes de communication. Un codeur de canal, qui introduit de la redondance aux données transmises ; et un décodeur de canal, qui exploite cette redondance pour trouver et corriger les erreurs produites par le bruit du canal.

2.2 Codes correcteurs d'erreurs

L'idée originale des codes correcteurs d'erreurs est d'abord née de l'article publié par Shannon "A Mathematical Theory of Communication" [1]. À peu près au même moment, Hamming construit la première classe de codes correcteurs d'erreurs [6] chez Bell Labs alors qu'il travaille sur une machine à calculs constituée de nombreux relais. En 1949, Golay [7] a publié un article intitulé "Notes sur le codage numérique" dans lequel le code de (23,12)-Golay a été décrit. En 1954, les codes de Reed-Muller ont été décrits par Irving S. Reed et David E. Muller [8, 9]. En 1957 et 1958, le Dr. Prange a inventé les codes cycliques et les codes à résidus quadratiques. En 1959 et 1960, les codes de Bose-Chaudhuri-Hocquenghem (BCH) ont été découverts [10, 11, 12]. En 1960, les codes Reed-Solomon [13] ont été inventés par Irving S. Reed et Gustave Solomon et sont des cas spéciaux des codes de Reed-Muller. Enfin, les codes convolutifs sont des codes correcteurs d'erreurs qui génèrent les symboles de parité via la "convolution" du codeur sur les données [14].

Les codes Turbo [15] sont une classe de correction d'erreurs introduite en 1993. Ils ont été les premiers codes pratiques à approcher la capacité du canal (un maximum théorique du taux de code pour lequel une communication fiable est encore possible étant donné un niveau spécifique de bruit). Cependant, l'avènement des codes à faible densité de parité (LDPC) avec décodage souple a surpassé les codes Turbo en ce qui concerne les erreurs plancher et les performances dans la plage de taux de codes plus élevés [16].

2.3 Codes LDPC et capacité dans les canaux binaires à effacement

2.3.1 Codes LDPC

Impossibles à mettre en œuvre lors de la première mise au point par Gallager [17] en 1963, les codes LDPC ont été oubliés jusqu'à ce qu'ils soient "redécouverts" en 1996. Le terme «faible densité» signifie que le nombre de 1 dans chaque rangée et chaque colonne de la matrice de contrôle de parité est faible par rapport à la longueur du bloc. La matrice suivante montre un exemple la matrice de contrôle de parité de code LDPC :

Exemple 1 :

$$\mathbf{H_1} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}_{4\times 6} \tag{2.1}$$

où $\hat{m} = 4$ et $n = 6$ représentent le nombre d'équations de contrôle de parité et le nombre de bits dans le mot de code. En arrangeant la matrice de contrôle de parité en forme systématique en utilisant des opérations de rangées et de colonnes, nous pouvons obtenir la matrice génératrice $\mathbf{G} = \left[\mathbf{P}^T_{(n-\hat{m})\times\hat{m}} \middle| \mathbf{I}_{(n-\hat{m})}\right]$. Maintenant, le mot de code peut être généré en multipliant le message $\mathbf{m}$ par la matrice génératrice $\mathbf{G}$.

$$\mathbf{c} = \mathbf{mG} \tag{2.2}$$

À la sortie de décodage, le mot de code est dit valide si nous avons l'équation suivante (équation de syndrome) :

$$\mathbf{cH_1^T} = \mathbf{0} \tag{2.3}$$

Les codes LDPC sont des codes binaires construits sur la base des transformations linéaires définies par les matrices de contrôle de parité clairsemées. Connus comme étant quelques-uns des meilleurs codes correcteurs d'erreurs de nos jours, ces codes peuvent fournir un compromis raisonnable entre la simplicité et l'efficacité. Ces codes ont été proposés par Gallager, tandis que leurs performances et leurs capacités ont été analysées récemment par Richardson et Urbanke [18]. En raison de la longueur des blocs et des calculs nécessaires pour le décodeur de codes LDPC, il était trop difficile pour les ordinateurs de l'époque d'explorer pleinement les performances de ces algorithmes. Enfin, il a été démontré par MacKay et Neal [18] que les codes LDPC sont des codes qui fonctionnent près de la limite de Shannon. La matrice de contrôle de parité du code LDPC est appelée (w_c,w_r) régulière si chaque bit de code comprend un nombre fixe de bits de parité (w_c) et chaque équation de contrôle de parité contient un nombre fixe de bits de code (w_r). Les codes LDPC réguliers correspondent en fait à la variante étudiée à l'origine par Gallager [17], que l'on retrouve également dans les travaux de Mackay et Neal [19, 20] et Sipser et Spielman [21, 22]. La matrice $\mathbf{H_1}$ précédente montre un exemple de matrice de contrôle de parité régulière pour le code LDPC avec $w_c = 2, w_r = 3$.

Plus tard, les généralisations des codes LDPC de Gallager produisirent les codes LDPC irréguliers qui offrent certains avantages pratiques. Si les valeurs de w_r et w_c sont différentes entre les rangées et les colonnes de la matrice de contrôle de parité, respectivement, le code LDPC est dit irrégulier. La matrice $\mathbf{H_2}$ suivante montre une matrice de contrôle de parité irrégulière pour le code LDPC :

Exemple 2 :

$$\mathbf{H_2} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}_{4\times 6} \tag{2.4}$$

Dans les codes LDPC irréguliers, les poids des rangées ou des colonnes de la matrice de parité sont identifiés par la distribution des degrés de noeuds de variable et des noeuds de parité. L'étude des graphes irréguliers par Luby et al. [23, 24] a constitué l'une des grandes avancées conceptuelles. En particulier, les auteurs ont introduit la notion d'ensembles irréguliers en termes de ces distributions de degrés. L'avantage des codes LDPC irréguliers sur les codes Turbo est que la terminaison précoce du processus de décodage des codes LDPC peut être vérifiée à la sortie du décodeur. Cela signifie que si un mot de code valide est obtenu soit à la terminaison précoce du processus de décodage, soit à l'échec du décodage du code, il peut être connu.

2.3.2 Graphe de Tanner et définition de la distribution de degré du code LDPC

La première personne qui a analysé les codes LDPC en utilisant une représentation graphique par graphe bipartite était Tanner [25]. Ce graphique bipartite est utile pour visualiser le décodage itératif des codes comme l'algorithme de passage de messages [26, 27, 28]. Un graphe de Tanner est composé de nœuds de variables et de nœuds de parité. Les messages sont transmis entre les arêtes avec la propriété que le message sortant envoyé par un nœud sur une arête particulière dépend du message entrant sur toutes les autres arêtes (adjacentes à ce nœud) et de l'observation du canal. La Fig. 2.3 représente un exemple de graphe de Tanner de codes LDPC correspondant à la matrice $\mathbf{H_1}$ (avec les lignes pointillés) et $\mathbf{H_2}$ (sans les lignes pointillés) des exemples 1 et 2.

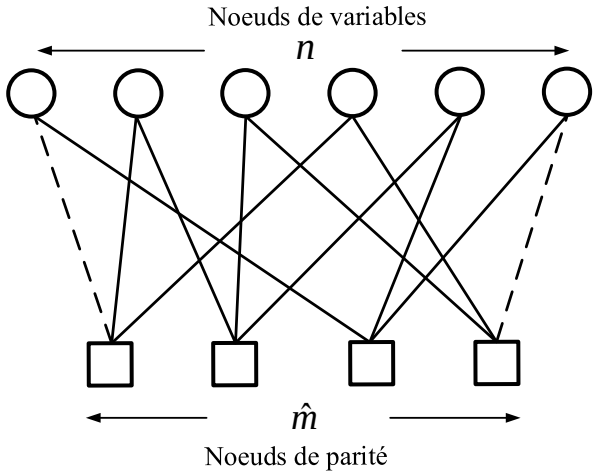


FIGURE 2.3 – Exemple de graphe de Tanner de codes LDPC.

Dans ce graphe, il existe n nœuds de variables (un pour chaque bit de mot de code) et $\hat{m}$ nœuds de parité (un pour chaque contrôle de parité). Les algorithmes de passage de messages pour le décodage des codes LDPC utilisant ce schéma sont connus sous plusieurs noms différents, tels que : le décodage itératif, la propagation de croyance (BP), le décodage probabiliste, etc. [29].

Supposons que le code LDPC a une longueur n et que le nombre de nœuds de variables de degré i soit Λ_i de sorte que $\sum_i \Lambda_i = n$. De la même manière, nous déterminons le nombre de noeuds de parité de degré i par P_i de sorte que $\sum_i P_i = n\bar{r}$ et $\bar{r} = 1 - r$, où r est le taux de conception du code LDPC. En plus, nous avons $\sum_i i\Lambda_i = \sum_i iP_i$ qui indique le nombre d'arêtes dans le graphe de Tanner. Maintenant, la notation suivante peut être introduite :

$$\Lambda(x) = \sum_{i=1}^{\hat{l}_{\max}} \Lambda_i x^i, \quad P(x) = \sum_{i=1}^{\hat{n}_{\max}} P_i x^i \tag{2.5}$$

et

$$\Lambda'(x) = \frac{d}{dx}\Lambda(x),\ P'(x) = \frac{d}{dx}P(x) \tag{2.6}$$

où $\Lambda(x)$ et $P(x)$ sont des polynômes avec des coefficients égaux aux noeuds de différents degrés. Basé sur l'équation (2.5), on peut voir que :

$$\Lambda(1) = n, \quad P(1) = n\bar{r}, \quad r(\Lambda, P) = 1 - \frac{P(1)}{\Lambda(1)}, \quad \Lambda'(1) = P'(1) \tag{2.7}$$

où Λ et P sont appelées les distributions des degrés de parité et de variables à partir d'une perspective de noeud. Parfois, il convient d'utiliser la distribution de degrés normalisée comme suit :

$$L(x) = \frac{\Lambda(x)}{\Lambda(1)}, \qquad R(x) = \frac{P(x)}{P(1)} \tag{2.8}$$

Pour l'analyse asymptotique des codes LDPC, il est commode du formuler la distribution du graphe de Tanner du point de vue de perspective d'arêtes.

$$\lambda(x) = \sum_i \lambda_i x^{i-1} = \frac{\Lambda'(x)}{\Lambda'(1)} = \frac{L'(x)}{L'(1)},\ \rho(x) = \sum_i \rho_i x^{i-1} = \frac{P'(x)}{P'(1)} = \frac{R'(x)}{R'(1)} \tag{2.9}$$

Notez que λ et ρ sont des polynômes, où les coefficients λ_i et ρ_i montrent la fraction des arêtes qui a été connectée aux noeuds de variables de degré i et aux noeuds de parité de degré i, respectivement.

La moyenne du degré de variable ($\hat{l}_{avg}$) et la moyenne du degré de parité ($\hat{n}_{avg}$) peuvent être représentés comme :

$$\hat{l}_{avg} = L'(1) = \frac{1}{\int_0^1 \lambda(x)dx}, \quad \hat{n}_{avg} = R'(1) = \frac{1}{\int_0^1 \rho(x)dx} \tag{2.10}$$

et le taux de conception peut être décrit par :

$$r(\lambda,\rho) = 1 - \frac{\hat{l}_{avg}}{\hat{n}_{avg}} = 1 - \frac{L'(1)}{R'(1)} = 1 - \frac{L'(1)}{R'(1)} = 1 - \frac{\int_0^1 \rho(x)dx}{\int_0^1 \lambda(x)dx} \tag{2.11}$$

Pour le code LDPC régulier de l'**exemple 1** dans la Fig. 2.3, nous avons :

$$\begin{gathered}\Lambda(x) = 6x^2, P(x) = 4x^3, L(x) = x^2, R(x) = x^3, \lambda(x) = x, \rho(x) = x^2, \\ \hat{l}_{avg} = 2, \hat{n}_{avg} = 3, r(\lambda(x) = x, \rho(x) = x^2) = \tfrac{1}{3}\end{gathered} \tag{2.12}$$

Et aussi, pour le code LDPC irrégulier de l'**exemple 2** dans la Fig. 2.3, nous avons :

$$\begin{gathered}\Lambda(x) = 2x + 4x^2, P(x) = 2x^2 + 2x^3, L(x) = \tfrac{2}{6}x^1 + \tfrac{4}{6}x^2, R(x) = \tfrac{2}{4}x^2 + \tfrac{2}{4}x^3, \lambda(x) = \tfrac{2}{10} + \tfrac{8}{10}x, \\ \rho(x) = \tfrac{4}{10}x + \tfrac{6}{10}x^2, \hat{l}_{avg} = \tfrac{10}{6}, \hat{n}_{avg} = \tfrac{10}{4}, r(\lambda(x) = \tfrac{2}{10} + \tfrac{8}{10}x, \rho(x) = \tfrac{4}{10}x + \tfrac{6}{10}x^2) = \tfrac{1}{3}\end{gathered} \tag{2.13}$$

2.3.3 Algorithmes de passage de messages pour décodage des codes LDPC

L'un des plus importants développements de Gallager dans le domaine de l'analyse de passage de messages a été décrit dans la série d'articles [30, 31, 24, 32]. Ces travaux ont porté sur l'algorithme de passage de messages itératifs pour le décodage des codes LDPC. Ce sujet était un vaste domaine de recherche avec de nombreux résultats significatifs. Pour une analyse détaillée de ce domaine, le livre de Richardson et Urbanke [29] est une excellente ressource. Le volume 47 de «IEEE Transactions on Information Theory» de 2001 [23, 24, 26, 31, 33, 34] est une autre ressource importante. Ce numéro a été spécialement dédié au décodage itératif et contient une série d'articles sur les développements les plus importants dans l'analyse de décodage itératif qui sont les fondements d'une grande partie des progrès récents dans ce domaine.

Algorithme par basculement de bit (BF)

L'un des premiers algorithmes de passage de messages pour le décodage des codes LDPC est basé sur les décisions fermes et le décodeur par basculement de bit (BF) [35]. Dans cet algorithme, pour chaque bit reçu, une décision ferme est utilisée par le décodeur afin de prendre une décision sur le bit reçu. Les messages qui passent dans les arêtes de graphe de Tanner sont binaires : un nœud de variable transmet un message indiquant s'il est à un ou zéro, de même que chaque nœud de parité transmet un message à chaque nœud de variable connecté, indiquant la valeur du bit à l'aide des informations disponibles dans le nœud de parité. L'équation de contrôle de parité est satisfaite si la somme modulo 2 des valeurs de bits entrants est égale à zéro (c.-à-d. parité paire). Ce processus est répété jusqu'à ce que, soit les équations de parité soient respectées, soit le nombre maximum d'itérations de décodage soit atteint. Si toutes les équations de parité sont respectées, un mot de code valide peut être trouvé et le processus de décodage de BF peut être terminé.

Algorithme Somme-Produit (SPA)

Un autre type d'algorithme BP permettant de passer des messages à travers un graphe de Tanner est l'algorithme somme-produit (SPA) [36]. Les algorithmes de décodage Turbo et BCJR sont des instances de l'algorithme SPA. Ceux-ci utilisent un algorithme de passage de messages basé sur les décisions souples. Le SPA est comparable à l'algorithme de BF introduit précédemment à la différence essentielle que chaque message représente des décisions avec des probabilités de valeurs souples. Alors que le décodage BF accepte une décision ferme initiale des bits reçus comme son entrée, le SPA est un algorithme de décision souple qui accepte la probabilité de bits reçus pour ses entrées. Les probabilités de bits d'entrée sont appelées les probabilités a priori des bits reçus, avant d'exécuter le décodage LDPC.

Les probabilités de bits calculées par le décodeur sont connues comme les probabilités a posteriori. Le rapport de probabilité peut être exprimé par le rapport de vraisemblance logarithmique (LLR). Pour une variable binaire x, $p(x=1) = 1 - p(x=0)$, et donc nous avons seulement besoin de stocker une valeur de probabilité pour la variable x. Les valeurs LLR sont utilisées comme une métrique :

$$LLR(x) = \ln \frac{p(x=0)}{p(x=1)} \tag{2.14}$$

Si $p(x=0) > p(x=1)$, $LLR(x)$ sera positif et si la différence entre $p(x=0)$ et $p(x=1)$ augmente, nous pourrons par conséquent dire que nous sommes plus confiants que $p(x) = 0$. Au contraire, si $p(x=1) > p(x=0)$, alors $LLR(x)$ est négatif et si la différence entre $p(x=0)$ et $p(x=1)$ augmente, on peut dire que nous serons plus confiants que le $p(x) = 1$. Le signe de $LLR(x)$ donne une décision ferme pour x et la valeur absolue $|LLR(x)|$ démontre la fiabilité de cette décision. La représentation LLR a l'avantage de ne nécessiter d'être ajoutée que lorsque les probabilités sont multipliées, ce qui diminue la complexité de mise en œuvre.

Nous pouvons mettre fin à l'algorithme si l'on obtient un mot de code valide. Dans le cas contraire, l'algorithme se poursuit jusqu'à ce qu'un mot de code valide soit obtenu ou jusqu'à ce que le nombre maximal d'itérations soit effectué.

L'algorithme SPA dans le domaine des probabilités comporte des lacunes dont notamment une grande plage dynamique requise pour les calculs, pouvant entraîner une instabilité numérique potentielle. Le problème de la mise en œuvre est une autre lacune de cet algorithme en raison de la complexité de calcul requise par celui-ci. De plus, cet algorithme est sensible aux effets de la quantification et il a besoin de plusieurs niveaux de quantification [37]. Cependant, l'algorithme SPA dans le domaine logarithmique (Log-SPA) [38] n'a pas besoin de l'étape de normalisation.

2.3.4 Seuil des codes LDPC sur un canal BEC

Seuil des codes LDPC sur un canal binaire à effacement

Le seuil de bruit définit une limite supérieure pour le bruit du canal, jusqu'à laquelle la probabilité de perte d'information peut être réduite à la valeur désirée. Les codes LDPC montrent un phénomène de seuil pour lequel un taux d'erreur par bit (BER) arbitrairement petit peut être réalisé lorsque la longueur du bloc tend vers l'infini et que le bruit du canal est inférieur à une certaine valeur. En revanche, le BER ne sera pas une petite valeur si le niveau de bruit est au-dessus de ce seuil [39]. Ce phénomène de seuil indiqué par Luby [30] existe aussi pour le cas des codes LDPC irréguliers.

Par la suite, Richardson et Urbanke [33] généralisèrent cette observation pour différents canaux, y compris le canal binaire à effacement (BEC), le canal symétrique binaire (BSC), et le canal à bruit blanc gaussien additif (AWGN), pour différents algorithmes de décodage, y compris SPA. Richardson et al. généralisèrent les résultats de Luby et al. [30] et ont démontré que la performance du décodeur sur les graphes aléatoires converge vers sa "valeur d'équilibre" lorsque la longueur du code augmente. Comme il est difficile de déterminer la performance attendue à un ensemble de dimension finie, ils ont utilisé le comportement attendu à la limite des codes infiniment longs qui peuvent être déterminés à partir d'un graphe de Tanner sans cycle. Ils ont défini le seuil pour un ensemble aléatoire de codes irréguliers spécifiés par des distributions de degrés et mis au point l'algorithme d'évolution de densité (DE) pour le calcul itératif des densités de messages, ce qui permet la détermination des seuils. En utilisant ce résultat, ils ont construit des codes LDPC qui présentent clairement de meilleures performances que les codes Turbo sur les canaux AWGN. En ce qui concerne la matrice $\mathbf{H_1}$ et son graphe de Tanner correspondant, on peut trouver le cycle qui a été déterminé par les flèches dans la matrice $\mathbf{H_1}$ et par les lignes pointillés dans le graphe de Tanner.

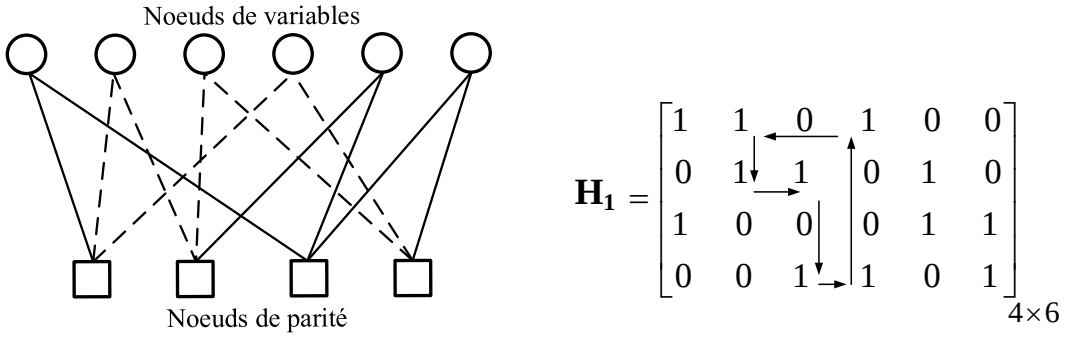


FIGURE 2.4 – Exemple de cycle dans le graphe de Tanner de code LDPC et la matrice de contrôle de parité correspondant.

Un outil approprié introduit dans [40] pour déterminer le seuil des codes LDPC est l'algorithme d'évaluation de densité de probabilité DE qui permet de suivre l'évolution des fonctions de densité [33, 16, 41]. Cette méthode suppose des codes de blocs longs et un grand nombre d'itérations pour analyser numériquement le processus de décodage. Cet algorithme fournit la valeur maximale du bruit

du canal de telle sorte que l'algorithme de décodage peut converger vers le bon mot de code. Mis à part les canaux BEC, le calcul des seuils à l'aide de la DE est numériquement intensif pour la plupart des autres canaux. Parce que l'algorithme DE pour le BEC est un problème unidimensionnel, il est difficile d'analyser et même de concevoir des ensembles de code approchant la capacité du canal [32].

Quatre méthodes d'approximation ont été proposées par Ryan et Lin [41] et par Chung, Richardson et Urbanke [34] pour estimer le seuil des codes LDPC sur différents canaux sans mémoire avec l'algorithme SPA. Ces méthodes d'approximation sont basées sur le suivi du comportement de l'algorithme DE en utilisant une représentation unidimensionnelle de la densité du message.

La première méthode, appelée l'approximation de canal d'effacement [41, 34], est basée sur le fait que les valeurs de seuil pour un canal peuvent être mises en correspondance avec les valeurs de seuil des autres canaux avec une bonne précision en utilisant un certain "mapping". Cette méthode fonctionne très bien pour prédire les seuils du canal AWGN et du canal de Laplace. Cependant, pour utiliser cette méthode afin d'optimiser la distribution de degrés, nous devons modifier la condition de stabilité du BEC.

La deuxième méthode [41, 34], nommée approximation gaussienne, est basée sur l'approximation de densité de messages (pour les codes LDPC réguliers) ou des messages gaussiens mélangés (pour les codes LDPC irréguliers). L'idée derrière cette approche est de ne conserver que la moyenne et la variance de densité de probabilité des messages pour avoir les spécifications requises de l'algorithme DE. Par conséquent, le problème complexe de suivi des densité de probabilité de messages à chaque itération pour trouver le seuil exact est réduit au problème unidimensionnel de calcul des moyennes des densités gaussiennes.

Une troisième méthode [41, 34], appelée l'approximation capacités-gaussiennes (en anglais : "gaussian-capacity approximation"), est équivalente à la normalisation itérative du canal. Il a été montré que cette méthode donne de meilleurs résultats que l'approximation gaussienne. Cependant, en général, ils sont moins bons que ceux obtenus avec l'approximation d'un canal réciproque.

La quatrième méthode [41, 34], intitulée l'approximation-réciproque du canal (en anglais : "reciprocal-channel approximation"), est basée sur les codes LDPC duals et fournit un modèle très précis de l'algorithme DE pour les canaux AWGN. Ceci est une approximation unidimensionnelle de l'algorithme DE en utilisant le "mapping" réciproque de canal (" en anglais : reciprocal-channel mapping"), où tous les messages approximatifs sont des nombres réels.

Ces quatre méthodes sont relativement faciles à analyser et sont numériquement plus rapides que le DE, où elles peuvent être utilisées comme un outil pour pour étudier le comportement du décodeur pour optimiser les codes irréguliers.

Conception des codes LDPC irréguliers

Un code LDPC irrégulier est caractérisé par une distribution de degrés de nœuds de variables, $\lambda(x)$, et une distribution de degrés de nœuds de parité, $\rho(x)$, appelées paire ou ensemble de distributions de degrés [29]. Pour chaque paire/ensemble utilisé comme constituant des codes LDPC, il y a une différence entre la capacité du canal C et le taux de conception (en anglais : "design rate") du code LDPC obtenu par l'optimisation de la distribution des degrés de nœuds de parité et de nœuds des variable. En d'autres termes, la distribution de degrés de conception approche une fraction $(1-\delta)$ de la capacité du canal, où δ est appelé l'écart multiplicatif (MG) [29].

Par conséquent, l'un des problèmes majeurs dans la conception des codes LDPC irréguliers est de trouver une distribution des degrés de nœuds de variable appropriée, $\lambda(x)$, et une distribution des degrés de nœuds de parité, $\rho(x)$, conduisant à un meilleur seuil pour un taux donné, ou le taux le plus élevé pour un paramètre de canal donné [2]. Cette procédure est appelée la conception de code et elle a été divisée en deux catégories principales dans la littérature [42] :

- Pour un canal BEC donné avec la probabilité d'effacement ε ou un niveau de bruit σ, concevoir un code qui maximise le taux $r(\lambda(x), \rho(x))$.
- Pour un taux donné $r(\lambda(x), \rho(x))$, le code devrait fournir une transmission fiable pour le pire canal BEC avec probabilité d'effacement ε ou un niveau de bruit σ.

Selon les catégories ci-dessus, l'ensemble optimal est un ensemble de distributions de degrés de nœuds de parité et de nœuds de variables, $\lambda(x)$ et $\rho(x)$, qui donne le seuil d'effacement ε le plus élevé ou le taux de transmission fiable r le plus élevé, respectivement.

Trouver une méthode efficace pour approcher la capacité du canal est encore un problème ouvert. L'approche de la capacité du canal est basée sur la structure du code, bien que certaines expériences pour atteindre la capacité du canal avec une distribution de degrés infinis aient été rapportées dans [43, 44, 45]. En particulier, pour le BEC, dans les articles [23, 45, 43, 44] on atteint la capacité du canal asymptotiquement. Dans [23], [46], [47] une analyse mathématique complète de la performance des codes LDPC sur le BEC, à la fois asymptotiquement et pour des longueurs de blocs finis, a été développée.

Pour les autres types de canaux, tels que le canal BSC et le canal AWGN, l'analyse est disponible dans [33]. La référence [48] donne les expressions analytiques pour trouver selon l'approche capacitive, des ensembles de codes de LDPC avec décodage itératif et sur les canaux binaires symétriques sans mémoire.

Certaines tentatives pour trouver les distributions de degrés appropriées sur BEC sont présentées dans les références [31, 49, 42]. Dans [31], une classe de codes correcteurs d'erreurs basées sur un graphe bipartite en cascade a été introduit.

Dans [49], une nouvelle séquence d'ensembles de codes LDPC pouvant atteindre la capacité du BEC a été introduite. Contrairement aux séquences proposées par Shokrollahi et al. [33], qui ont des coefficients non nuls pour chaque degré de nœuds de variable constituant $i \in [2, \hat{l}_{\max}]$, où $\hat{l}_{\max}$ est le degré de nœud de variable maximum, les nouvelles séquences ont seulement des coefficients non nuls pour $i \in [2, f(\hat{l}_{\max})]$ et $i = \hat{l}_{\max}$ où $f(.)$ est une fonction linéaire de $\hat{l}_{\max}$. Une nouvelle méthode pour concevoir des ensembles de codes LDPC irréguliers pour BEC a été introduite dans [42]. L'idée principale est de maximiser la fraction des arêtes qui sont connectées aux nœuds avec un degré inférieur en utilisant les algorithmes gloutons ('greedy algorithms' en anglais). En considérant un degré fini pour les nœuds de variable et les nœuds de parité, les ensembles conçus sont presque optimaux : ils sont légèrement inférieurs aux ensembles conçus par recherche exhaustive. Cependant, ces méthodes ne sont pas efficaces pour approcher la capacité du canal.

Les méthodes typiques pour la conception des ensembles optimaux peuvent être divisées en quatre catégories principales [2, 16, 23]. Selon la première méthode, le code optimal est conçu sur la base d'optimisation évolutive telle que l'algorithme génétique (GA). Selon la seconde méthode, des algorithmes tels que l'évolution différentielle sont utilisés. Pour la troisième méthode, la programmation linéaire (LP) est utilisée pour trouver des paires de distributions pour lesquelles le taux se rapproche de la capacité du canal. La quatrième méthode est basée sur utilisation de la programmation semi-définie (SDP). L'assouplissement de certaines des restrictions dans les problèmes d'optimisation précédents conduit à une solution sous optimale, alors que pour cette méthode, une contrainte exacte sans relaxation est considérée et la solution devient optimale.

Bien que les méthodes mentionnées ci-dessus conduisent à des codes approchant la capacité, le principal problème est que la plupart d'entre elles gardent la distribution des degrés de nœuds de parité fixe tandis que la distribution de degrés de nœuds de variable est optimisée.

Idéalement, on voudrait optimiser à la fois les distributions des degrés des nœuds de parité et des nœuds de variable conjointement, mais cela est très complexe et difficile à mettre en œuvre [2, 50]. Pour faire face à cette difficulté, nous proposons de définir la distribution de degrés de nœuds de parité à des degrés de un (c.-à-d. nœuds de parité régulier) ou de deux, car celui-ci a très peu d'effets sur la fonction de coût, puis d'optimiser la distribution des nœuds de variables. Les ensembles de codes LDPC irréguliers sur BEC sont ensuite conçus en utilisant une procédure combinée GA et LP. Dans ce mémoire, le BEC a été choisi parce que le DE pour ce canal est vraiment relativement simple et facile à mettre en œuvre. La méthode proposée cherche à minimiser l'écart multiplicatif δ par itération entre l'optimisation de la distribution de degrés de nœuds de variables à l'aide de GA et l'optimisation de la distribution de degrés de nœuds de parité en utilisant LP. À la première étape, la distribution de degrés de nœuds de variables est optimisée et l'algorithme proposé recherche la meilleure distribution de degrés de nœud de parité, jusqu'à ce qu'un ensemble ou des ensembles optimaux qui minimisent δ soient trouvés. Comme l'itération entre ces deux problèmes d'optimisation est beaucoup moins complexe en raison du modèle simple, nous l'avons considérée pour la distribution de degrés de nœud de parité. Ce sujet est examiné dans le chapitre suivant.

2.4 Sécurité dans les systèmes de communication sans fil

L'utilisation des réseaux sans fil a augmenté de manière significative au cours du temps et continue de se développer. La nature même des communications sans fil les rend cependant particulièrement vulnérables à l'espionnage. Avec l'avancée des systèmes d'infrastructures modernes, il y a un besoin croissant pour des solutions de communications sécurisées. Par conséquent, les protocoles de sécurité sont les éléments les plus critiques pour permettre la croissance de la grande variété de réseaux sans fil. La cryptographie est une méthode traditionnelle qui fournit des protocoles sécurisés à la couche d'application. Contrairement aux approches cryptographiques, la sécurité de la couche physique vise à développer des systèmes de communication sécurisés efficaces exploitant les propriétés de la couche physique. Ce nouveau paradigme peut augmenter la sécurité des systèmes existants en introduisant un niveau de sécurité de l'information théorique sur les systèmes. Notez que la sécurité de la couche physique a un rôle complémentaire et peut être intégrée aux solutions de sécurité existantes pour améliorer le niveau total de la sécurité pour les systèmes de communication. Contrairement aux solutions traditionnelles, qui traitent généralement la sécurité à la couche d'application, la première préoccupation de ce mémoire est d'analyser et de développer des solutions sur la couche physique. La Fig. 2.5 montre les différentes couches d'un protocole de communication sans fil typique avec leurs objectifs spécifiques.

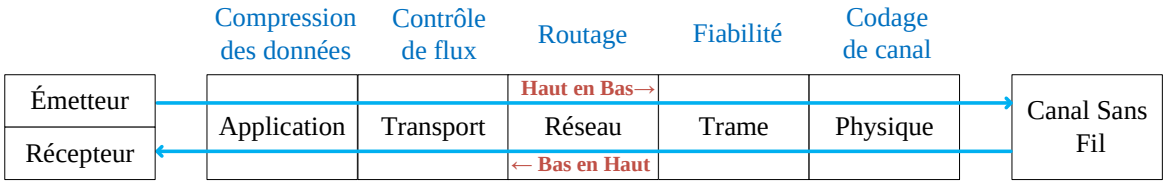


FIGURE 2.5 – Architecture de protocole en couches.

Les problèmes de sécurité qui apparaissent dans les systèmes de communication peuvent être divisés en quatre domaines fondamentaux comprenant la confidentialité, l'intégrité, l'authentification et la non-répudiation. La confidentialité confirme que les parties légitimes reçoivent avec succès l'information attendue alors que les informations sont sécurisées contre les espions. L'intégrité confirme aux parties qui communiquent qu'un message n'a pas changé au cours de la transmission. L'authentification garantit que le récepteur légitime de l'information est en mesure d'identifier l'émetteur. La non-répudiation empêche la répudiation des entités de participer à la communication.

En outre, il existe d'autres problèmes de sécurité qui peuvent ajouter de nouvelles vulnérabilités de sécurité pour les systèmes sans fil. Tout d'abord, en brouillant les canaux de communication physiques, l'attaquant peut simplement bloquer l'accès des utilisateurs au réseau. Le brouilleur perturbe le trafic de communication afin de prévenir la transmission de l'information. Le deuxième problème de sécurité est le choix des mécanismes d'authentification appropriés. Sans avoir un mécanisme puissant, l'attaquant peut illégitimement accéder aux ressources du réseau en désactivant les infrastructures de sécurité. Pour faire face à ces problèmes de sécurité, les fournisseurs de services sans fil essaient

d'utiliser une approche de protocoles en couches qui est typique pour simplifier les procédures de conception de réseau. Cette approche divise le réseau en différentes couches où chaque couche exécute différentes tâches en utilisant leurs propres protocoles affectés.

2.4.1 Communication sécurisée au niveau de la couche physique

Dans ce mémoire, nous nous concentrons sur la couche physique (couche 1) dont l'objectif est de transmettre le flux de l'information sur un canal de communication en convertissant les bits en signaux électriques ou optiques. La mise en œuvre du codage de canal au niveau de la couche physique consiste à fournir un milieu exempt d'erreurs pour les couches supérieures. Nous remarquons que la conception des protocoles de communication modernes ne se limite pas à l'approche en couches mentionnée ci-dessus, mais elle donne un aperçu général de la procédure de conception.

Les solutions de sécurité peuvent être utilisées dans différentes couches. Par exemple, afin d'atténuer le brouillage de canal, les techniques de modulation à spectre étalé [51] peuvent être utilisées sur la couche physique. Sur la couche réseau, les mécanismes d'authentification peuvent être mis en œuvre pour empêcher l'accès non autorisé. Par conséquent, le brouillage de canal et l'accès non autorisé, qui sont vulnérables à la couche physique et à la couche de liaison, respectivement, sont manipulés par des solutions de sécurité sur leurs couches respectives. En outre, l'espionnage qui est une vulnérabilité de la couche physique peut être traditionnellement traité en exploitant les propriétés de la couche physique.

L'objectif d'une communication sécurisée est que le récepteur légitime devrait récupérer le message sans erreurs alors que personne d'autre ne devrait acquérir l'information. Historiquement, Shannon [1] a été le premier à introduire la notion de secret sous l'aspect de la théorie de l'information dans les systèmes de communication. La Fig. 2.6 montre le modèle de communication sécurisée proposé par Shannon.

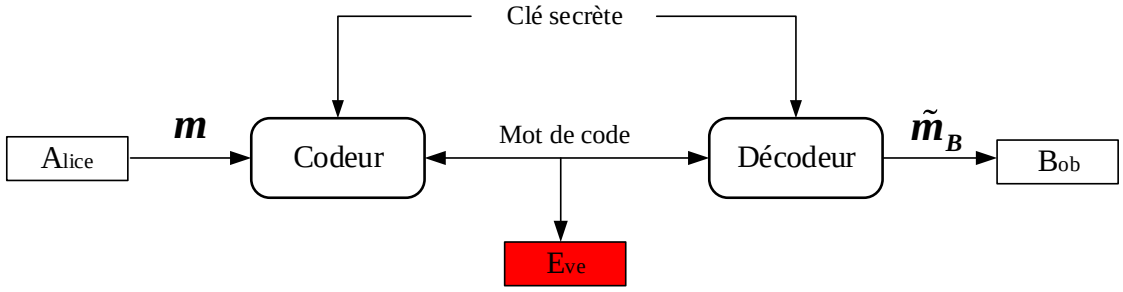


FIGURE 2.6 – Modèle de communication sécurisée proposé par Shannon.

Les messages interceptés par un éventuel espion ne devraient pas fournir des informations sur les messages originaux. La théorie de l'information démontre que des systèmes de communications sécurisées parfaits sont réalisables si l'émetteur et le récepteur légitime partagent une clé secrète pour

le cryptage et le décryptage du message original. Cette clé secrète est seulement connue de l'émetteur et du récepteur légitime, mais reste inconnue de l'espion. Shannon a montré que pour l'obtention du secret parfait, l'entropie de la clé secrète partagée doit être supérieure ou égale à l'entropie du message transmis. Bien que le masque jetable ('one-time pad' en anglais) puisse atteindre le secret parfait avec une faible complexité, son applicabilité est limitée par les exigences suivantes : les partenaires légitimes doivent générer et stocker de longues clés composées de bits aléatoires, chaque clé ne peut être utilisée qu'une seule fois (sinon il y a une bonne chance d'obtenir la clé par cryptanalyse), et la clé doit être partagée sur un canal sécurisé.

2.4.2 Modèle de canal à écoute de Wyner

Les travaux de recherche pour obtenir la sécurité sans clé ont été lancés par Wyner [52] qui considérait le caractère aléatoire de canal pour enlever la contrainte de clé secrète du travail de Shannon. Wyner a démontré que l'avantage d'un meilleur canal principal par rapport à un canal à écoute peut être utilisé pour la transmission des bits secrets en utilisant un des codes aléatoires. En d'autres termes, un émetteur peut envoyer des messages sécurisés au récepteur en cachant le flux d'information dans le bruit supplémentaire subi par le canal de l'espion [53]. La principale différence entre cette approche et celle de Shannon est que l'émetteur légitime encode un message $\mathbf{x^n}$ de longueur n, qui est envoyé sur un canal bruité pour le récepteur légitime, et l'espion observe une version bruité, notée $\mathbf{z^n}$, du signal $\mathbf{y^n}$ disponible pour le récepteur.

Les hypothèses implicites qui ont été utilisées dans le modèle de canal à écoute et les autres modèles peuvent être résumées comme suit [54] :

- **L'information sur l'état du canal** : dans le modèle de canal à écoute, il est supposé que les informations sur l'état du canal (CSI) sur le canal principal et le canal de l'espion sont complètement accessibles par l'émetteur. On peut supposer que l'état du canal principal est parfaitement connu de l'espion.
- **Authentification** : dans le modèle du canal à écoute, il est supposé que le canal principal est authentifié. Dans les couches supérieures de la pile de protocoles, ces mécanismes d'authentification peuvent être mis en œuvre facilement.
- **L'espion passif** : dans le modèle de canal à écoute, l'adversaire est limité aux stratégies d'espionnage passif. Dans l'espionnage passif, l'espion surveille la communication et n'interfère pas sur le canal de communication. Les espions passifs sont difficiles à détecter, car leur présence ne produit pas d'effets observables.
- **Disponibilité du générateur aléatoire** : contrairement aux codeurs traditionnels qui possèdent des fonctions déterministes, les codeurs de canal pour canaux sous écoute ("wiretap codes" en anglais) sont stochastiques et comptent sur la disponibilité des générateurs aléatoires parfaits. Dans la pratique, des générateurs pseudo-aléatoires puissants peuvent être utilisés. Le mécanisme d'initialisation de ces générateurs doit être soigneusement examiné.

Aussi, Wyner a proposé une nouvelle définition de la condition du secret. Au lieu d'exiger que l'équivoque de l'espion soit exactement égale à l'entropie du message, il a suggéré que l'entropie conditionnelle $\mathbf{H}(\mathbf{x^n}\,|\mathbf{z^n})$ soit arbitrairement proche de l'entropie $\mathbf{H}(\mathbf{x^n})$ du message pour un mot de code n suffisamment long. Avec cette condition, il existe des codes à écoute qui garantissent asymptotiquement une faible probabilité d'erreurs par le récepteur légitime ainsi qu'une faible fuite d'informations. Le taux de transmission maximale qui est réalisable dans cette condition est appelé capacité secrète et peut se montrer strictement positif chaque fois que l'observation de l'espion, $\mathbf{z^n}$, est plus bruyante que le $\mathbf{y^n}$.

Au début des années 1970 et 1980, l'impact du travail de Wyner a été limité en raison de certaines restrictions :

- La construction de codes pratiques pour le canal à écoute n'était pas disponible. Mais, deux codes pour les canaux à écoute [51] utilisant des codes polaires [55] et extracteurs [56] ont été introduits récemment dans la littérature.
- Le modèle de canal à écoute restreint l'espion en supposant qu'il souffre de plus de bruit que le récepteur légitime.

De plus, le travail de Diffie et Hellman [57, 58] sur l'échange de clés cryptographiques a montré d'autres limitations pour la sécurité des transmissions. Traditionnellement, la communication cryptée sécurisée entre deux parties exige l'échange de clés par un canal sécurisé. La méthode d'échange de clé Diffie-Hellman permet à deux parties qui n'ont aucune connaissance préalable de l'autre d'établir conjointement une clé secrète partagée sur un canal non sécurisé. Cette clé peut ensuite être utilisée pour chiffrer les communications ultérieures en utilisant un algorithme de chiffrement à clé symétrique.

2.4.3 Capacité secrète

Le premier travail de cryptage de Wyner dans les années 1970 a posé le problème de transmission entre un émetteur (Alice), un récepteur legitime (Bob) et un observateur ou espion (Eve), (Alice-Bob-Eve), dans lequel Alice veut envoyer un message à Bob, sans qu'il soit décodé par Eve. Il a été montré que si le canal d'Alice à Bob est statistiquement meilleur que le canal d'Alice à Eve, la communication sécurisée est possible [52]. Ceci est intuitif, mais Wyner a mesuré le secret en termes d'informations théoriques définissant la capacité secrète, qui est essentiellement le taux auquel Alice peut transmettre des informations secrètes à Bob sans fuite d'informations vers Eve.

Peu de temps après le travail de Wyner, la notation de la capacité secrète pour les canaux symétriques a été établie par Leung Yan-Cheong [59], et une preuve simplifiée du résultat de Wyner a été proposée par Massey [60]. L'extension du travail de Wyner au canal de diffusion avec des messages confidentiels est due à Csiszar et Korner [61].

Le calcul de la capacité secrète, quand le canal principal est moins bruyant que le canal à écoute, en utilisant l'algorithme Blahut-Arimoto-Like a été montré dans [62]. La capacité secrète du canal à

écoute gaussien physiquement dégradé a été créée en [63] et sa généralisation au canal de diffusion générale gaussienne est due à [64].

La capacité secrète est la restriction fondamentale des communications sécurisées sur des canaux bruyants [65, 66]. La capacité secrète est positive lorsque le canal principal est moins bruyant que le canal de l'espion. Une façon d'augmenter la capacité secrète dans un système de communication est d'utiliser un canal de rétroaction [66]. Le canal à écoute avec lien de retour sécurisé a été étudié par [67, 68, 69, 70, 3]. Il est connu que lorsque les canaux d'Eve et de Bob ont la même qualité, ou que le canal d'Eve est meilleur que celui de Bob, un mécanisme de rétroaction est nécessaire pour atteindre la sécurité de la couche physique [63, 66].

Dans [69, 68], afin de transmettre les messages en toute sécurité, dans les cas défavorables (lorsque le canal de l'espion est moins bruyant que le canal principal), on considère un canal à écoute avec de la rétroaction. il a été démontré que l'on peut tirer parti de la rétroaction pour atteindre un taux de secret parfait positif, même lorsque la capacité secrète est égale à zéro. Dans ce modèle, il existe un canal public sans bruit séparé, par lequel le transmetteur et le récepteur peuvent échanger des informations. L'espion est censé obtenir une copie parfaite des messages transmis sur ce canal public. Les limites supérieures et inférieures ont été établies pour la capacité secrète.

2.4.4 Amélioration de la sécurité physique dans les canaux à écoute

Une façon d'augmenter la capacité secrète dans un système de communication est d'utiliser un canal de rétroaction [66]. Il a été démontré que l'utilisation de ce canal supplémentaire peut augmenter la capacité secrète. Dans [70], Baldi et al. ont mis en place un canal de rétroaction sur la base de protocole requête automatique de répétition hybride (HARQ), où une demande de retransmission est renvoyée par Bob à Alice quand le décodeur de Bob ne peut converger vers la valeur réelle. La Fig. 2.7 montre la structure de la méthode HARQ. Dans ce procédé, le paquet entier est renvoyé quand une retransmission est demandée lorsque la granularité est considérée comme égale à un $(g = 1)$. Cependant, l'envoi du paquet entier (en particulier avec de grandes tailles) au cours de la phase de retransmission peut aussi donner des informations supplémentaires au canal de l'espion. Pour résoudre ce problème, un schéma HARQ avec une granularité plus fine, connu sous le nom HARQ-granulaire (G-HARQ), a été introduit par Haj Taieb dans [3] pour réduire cette fuite d'informations. Cette méthode consiste à diviser le paquet demandé en g sous-paquets, et lorsque la retransmission est demandée, seuls ces sous-paquets sont envoyés à Bob, un par un, jusqu'à ce que le décodeur converge vers la valeur souhaitable. Dans cette méthode, les sous-paquets sont envoyés au hasard et il n'y a pas de mécanisme impliquant le choix des sous-paquets les plus importants dans le cas de la demande par Bob.

Dans ce mémoire, pour améliorer davantage la sécurité dans les méthodes précédentes, une méthode HARQ-granulaire adaptative (AG-HARQ) est introduite pour le choix et l'envoi de sous-paquets appropriés lorsque la retransmission est demandée. Par cette méthode, après décodage LDPC, l'indice de niveau de confiance, $\hat{C}_j$, pour un décodage correct est calculé pour chaque sous-paquet. Cet indice

indique la moyenne de la valeur absolue du rapport de vraisemblance logarithmique (LLR), correspondant aux valeurs de vraisemblance à la sortie du décodeur. Contrairement à la méthode G-HARQ pour la méthode proposée AG-HARQ, Bob demande seulement la retransmission de sous-paquets spécifiques avec les valeurs $\hat{C}_j$ les plus basses dans un ordre croissant (le plus bas LLR, le deuxième plus bas LLR, ...) s'il ne peut pas faire converger le message correctement. Ce schéma permet d'éviter la retransmission de l'information plus redondante qui n'est pas nécessaire pour Bob, mais qui pourrait être utile à l'espion. En outre, l'AG-HARQ nécessite un moins grand nombre de demandes de retransmission comparativement au G-HARQ. L'efficacité de la méthode AG-HARQ proposée est évaluée en utilisant le taux de trame d'erreurs (FER). Le cas de la valeur négative de l'écart de sécurité (SG), où la qualité du canal de l'espion est meilleure que celle du canal principal, est aussi considéré.

En outre, le schéma G-HARQ est utilisé conjointement avec la méthode contamination d'erreur proposée par Haj Taieb [3] pour augmenter encore la sécurité. L'objectif de la contamination d'erreur intra-frame (IntraEC) est de propager le bit (ou les bits) d'erreur à une trame entière en utilisant une matrice d'embrouillage (**S**) et une matrice de désembrouillage ($\mathbf{S^{-1}}$), tandis que l'objectif de contamination d'erreur inter-trame (InterEC) est non seulement de propager un seul bit d'erreur à la trame courante, mais aussi aux autres trames en utilisant un entrelaceur et un désentrelaceur sur un ensemble de trames.

Dans ce mémoire, pour augmenter encore la sécurité donnée par la méthode AG-HARQ proposé, nous combinons l'AG-HARQ avec les méthodes IntraEC et InterEC. La combinaison de AG-HARQ avec les IntraEC et InterEC peut conduire à des systèmes de communication hautement sécurisés.

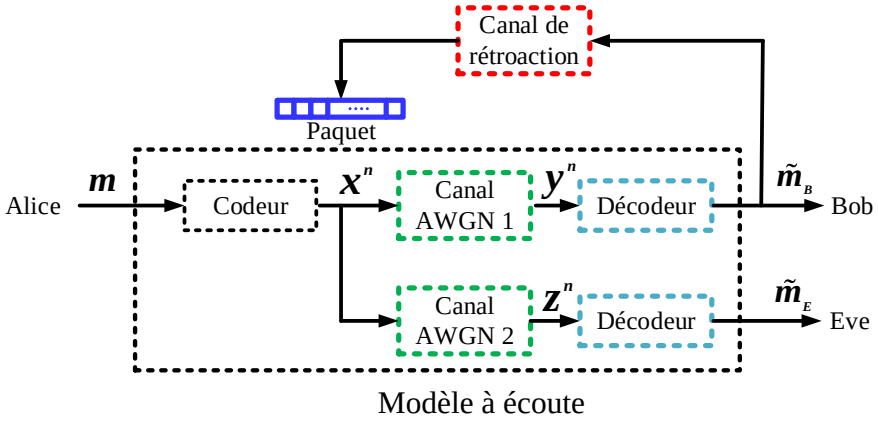


FIGURE 2.7 – Structure du système HARQ du canal à écoute avec rétroaction parfaite.

2.5 Conclusion

Dans ce chapitre, les systèmes de transmission typiques ont été introduits et l'importance des codes correcteurs d'erreur dans les systèmes de communication sans fil ont été expliqués. Les codes LDPC

constituent l'un des principaux schéma du codes correcteurs d'erreur en ce qu'il fournit un bon compromis entre la complexité et la performance. Certaines spécifications importantes de ce code comme le seuil, le taux, et le processus de décodage ont été introduit. Une nouvelle approche pour la conception de codes LDPC qui minimise l'écart multiplicatif δ a été introduit. La procédure d'optimisation itérative GA-LP dans cette approche est un outil puissant pour obtenir des valeurs inférieures de δ. Cette approche nous aide à améliorer la fiabilité de la transmission dans les systèmes de communication sans fil.

En outre, la sécurité des systèmes de communication sans fil a été introduite et les différents problèmes de sécurité qui apparaissent dans les systèmes de communication ont été présentés. L'architecture de protocole en couches a été donnée et l'importance de la sécurité physique qui ajoute un niveau de sécurité à l'information théorique du système a été discutée. Le modèle de canal à écoute de Wyner comme l'un des modèles importants lors de la conception des systèmes de communication sécurisés a été expliqué et la notion de capacité secrète a été présentée. Il a été discuté de la façon dont la combinaison du canal de rétroaction supplémentaire et le concept de granularité dans le modèle Wyner peuvent augmenter la capacité secrète. Un nouveau système AG-HARQ pour améliorer le secret dans les systèmes de communication sans fil est introduit. Enfin, la méthode AG-HARQ proposée est combinée avec l'IntraEC et l'InterEC et l'efficacité de cette combinaison pour fournir le système sécurisé est également introduit.

Chapitre 3

Minimisation de l'écart multiplicatif de la capacité pour un canal binaire à effacement

Il existe une différence entre la capacité d'un canal telle que définie par Shannon et le taux de transmission maximal et fiable qui peut être obtenu par l'optimisation de la distribution de degrés d'un code LDPC. Un code correcteur peut atteindre une fraction $(1-\delta)$ de la capacité, où δ est appelé écart multiplicatif. Afin de minimiser cet écart, on désire optimiser les distributions des degrés des nœuds de parité et des nœuds de variables conjointement. Malheureusement, cette optimisation est particulièrement complexe. Pour résoudre ce problème, dans ce mémoire, nous avons réduit la distribution de degrés de nœuds de parité à un ou deux degrés et nous essayons de concevoir des ensembles de codes à faible densité de parité irréguliers pour un canal binaire à effacement (BEC). Nous minimisons δ par itération dans l'optimisation de la distribution de degrés de nœuds de variables en utilisant un algorithme génétique (GA) et par l'optimisation de la distribution de degrés des nœuds de parité en utilisant la programmation linéaire (LP). Nos résultats montrent l'amélioration de la minimisation de l'écart δ comparativement aux méthodes précédentes.

3.1 Taux de conception et écart multiplicatif

Dans ce chapitre, nous nous concentrons sur les codes LDPC. Comme indiqué dans le chapitre 2, une représentation graphique bipartite des codes LDPC a été présentée par Tanner [25] pour analyser le mécanisme de passage de messages de décision souple entre les nœuds de parité et les nœuds de variables.

Chaque matrice de parité $\mathbf{H}$ d'un code LDPC est caractérisé par une distribution de degrés de nœuds de variables, $\lambda(x)$, et une distribution de degrés de nœuds de parité, $\rho(x)$, lesquels sont liés à la distribution de degrés [29] :

$$\begin{aligned}\rho(x) &= \sum_{i=2}^{\hat{n}_{\max}} \rho_i x^{i-1} \\ \lambda(x) &= \sum_{i=2}^{\hat{l}_{\max}} \lambda_i x^{i-1}\end{aligned} \tag{3.1}$$

avec les contraintes $\sum_{i=2}^{\hat{n}_{\max}} \rho_i = 1$ et $\sum_{i=2}^{\hat{l}_{\max}} \lambda_i = 1$. Les coefficients ρ_i et λ_i représentent les fractions d'arêtes connectées aux nœuds du degré $i+1$. $\hat{l}_{\max}$ et $\hat{n}_{\max}$ représentent le degré maximal des noeuds de variable et des noeuds de parité du code LDPC, respectivement. Le taux de conception $r(\lambda,\rho)$ pour un ensemble de codes LDPC (ou graphes bipartites) est défini comme [29] :

$$r(\lambda,\rho) = 1 - \frac{\int_0^1 \rho(x)dx}{\int_0^1 \lambda(x)dx} = 1 - \frac{\sum_{i=2}^{\hat{n}_{\max}} \rho_i x^{i-1}}{\sum_{i=2}^{\hat{l}_{\max}} \lambda_i x^{i-1}} \tag{3.2}$$

Le taux de conception $r(\lambda,\rho)$ de tout ensemble LDPC pour un décodage réussi sur $BEC(\varepsilon)$ ne peut pas dépasser la capacité du canal C. Par conséquent, pour un canal à effacement BEC, le taux de conception est limité à $C_{BEC}(\varepsilon) = 1-\varepsilon$ [71] :

$$r = r(\lambda,\rho) \leq C_{BEC}(\varepsilon) \tag{3.3}$$

Soit (λ,ρ) un ensemble de distributions de degrés avec le seuil de probabilité d'effacement $\varepsilon^{BP} = \varepsilon^{BP}(\lambda,\rho)$, obtenu en utilisant la propagation des croyances (BP) [29]. Le taux de conception du code LDPC peut alors être exprimé comme suit :

$$r(\lambda,\rho) = (1-\delta)(1-\varepsilon^{BP}) \tag{3.4}$$

δ étant donc fonction des distributions de degrés de noeuds de parité et de noeuds de variables (λ,ρ) :

$$\delta(\lambda,\rho) = \frac{(1 - r(\lambda,\rho) - \varepsilon^{BP}(\lambda,\rho))}{(1-\varepsilon^{BP}(\lambda,\rho))} \tag{3.5}$$

Malheureusement, il n'y a pas de distributions de degrés qui donnent un écart nul $\delta = 0$. La première limite inférieure de l'écart $\delta(\lambda,\rho)$ provenant de l'algorithme de l'évolution de la densité (DE) est due à Shokrollahi [44]. Le théorème de Shokrollahi peut être utilisé comme une mesure pour montrer à quel point le graphique de Tanner devrait être clairsemé pour atteindre une fraction $(1-\delta)$ de la capacité. Cette limite [29] est déterminée par l'équation suivante avec le degré moyen de noeuds de parité $\hat{n}_{avg}$:

$$\delta(\lambda,\rho) \geq \frac{r^{r_{avg}-1}(1-r)}{1+r^{r_{avg}-1}(1-r)} \tag{3.6}$$

Exemple 1 :
La Fig. 3.1 montre un exemple de graphe de Tanner de code LDPC régulier qui comprend quatre noeuds de variables (V_1, V_2, V_3, V_4) et trois noeuds de parité (C_1, C_2, C_3) :

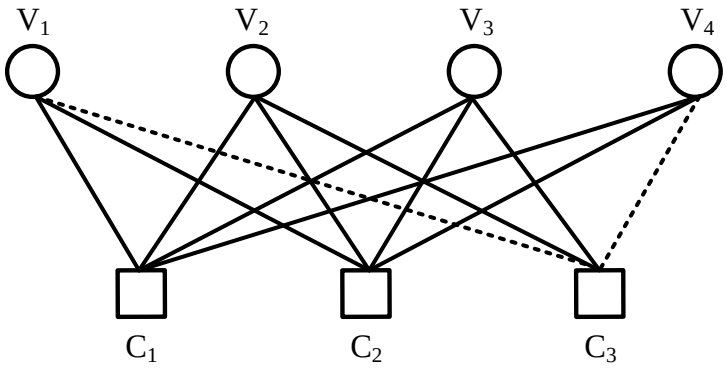


FIGURE 3.1 – Exemple de graphe de Tanner de code LDPC.

où

$$\begin{aligned} &\lambda(x) = x^2, \rho(x) = x^3, r(\lambda,\rho) = \tfrac{1}{4}, \\ &\varepsilon^{BP}(\lambda,\rho) = 0.6474, \delta(\lambda,\rho) = 0.2910 \end{aligned} \tag{3.7}$$

Exemple 2 :
En outre, en supprimant les lignes pointillées de la Fig. 3.1 on obtient le code LDPC irrégulier :

$$\begin{aligned} &\lambda(x) = 0.4x + 0.6x^2, \rho(x) = 0.2x + 0.8x^3, r(\lambda,\rho) = \tfrac{1}{4}, \\ &\varepsilon^{BP}(\lambda,\rho) = 0.6807, \delta(\lambda,\rho) = 0.2170 \end{aligned} \tag{3.8}$$

Les exemples 1 et 2 montrent que par modification de la structure du graphe de Tanner du code LDPC, on peut obtenir les meilleures valeurs de $\varepsilon^{BP}(\lambda,\rho)$ et $\delta(\lambda,\rho)$ (équation 3.5). Par conséquent, si nous concevons convenablement la distribution des degrés, une valeur faible de l'écart $\delta(\lambda,\rho)$ peut être atteinte qui approche de la limite inférieure de l'équation (3.6).

3.2 Optimisation de la distribution des degrés

Dans [29], Richarson et Urbanke décrivent une méthode pour trouver la distribution de degrés optimale pour minimiser l'écart δ. En considérant une paire de distributions de degrés $(\lambda(x), \rho(x))$, le comportement asymptotique de cette paire peut être caractérisé par une fonction $f(\varepsilon, x)$, qui montre l'évolution de la fraction des bits effacés par les noeuds de variables. Si nous fixons le degré maximal

de $\lambda(x)$ à $\hat{l}_{\max}$, pour obtenir un seuil d'au moins ε pour les distributions de degrés de (λ,ρ), nous devrions avoir :

$$f(\varepsilon,x) = \varepsilon\lambda(1-\rho(1-x)) < x, \text{pour} x \in [0,1] \tag{3.9}$$

En remplaçant ρ par l'équation (3.1) dans l'équation (3.9), celle-ci devient :

$$f_1(x,\lambda_1,...,\lambda_{\hat{l}_{\max}}) = \varepsilon \sum_{i\geq 2} \lambda_i (1-\rho(1-x))^{i-1} - x \tag{3.10}$$

où f_1 est une fonction linéaire des variables λ_i, $i = 1,\ldots,\hat{l}_{\max}$. Considérant l'équation (3.1), le taux associé à la valeur fixe de ρ est une fonction croissante de la somme $\sum_{i\geq 2}\{\frac{\lambda_i}{i}\}$. Comme dans [29], on peut utiliser la formulation du problème suivant pour trouver la distribution des noeuds de variables $\lambda(x)$ pour les valeurs spécifiées de seuil ε qui maximise le taux $r(\lambda,\rho)$. Pour une valeur fixe de la distribution des noeuds de parité $\rho(x)$, le problème de maximisation (appelé problème $P1$) peut être exprimé comme suit :

$$\max_\lambda \left\{ \sum_{i\geq 2} \frac{\lambda_i}{i} \,\middle|\, \lambda_i \geq 0; \sum_{i\geq 2} \lambda_i = 1; f_1 \leq 0; x \in [0,1] \right\} \tag{3.11}$$

La même procédure peut être utilisée pour trouver le polynôme $\rho(x)$ approprié pour la valeur fixe de $\lambda(x)$. Dans ce cas, nous avons le problème de minimisation suivant (problème $P2$) [2] :

$$\min_\rho \left\{ \sum_{i\geq 2} \frac{\rho_i}{i} \,\middle|\, \rho_i \geq 0; \sum_{i\geq 2} \rho_i = 1; f_2 \leq 0; x \in [0,1] \right\} \tag{3.12}$$

où,

$$f_2(x,\rho_1,....,\rho_{\hat{n}_{\max}}) = \sum_{i\geq 2} \varepsilon\rho_i(1-\varepsilon\lambda(1-x))^{i-1} - x \tag{3.13}$$

Afin de trouver une bonne distribution de degrés, nous pouvons itérer entre ces deux problèmes d'optimisation, $P1$ et $P2$. Malheureusement, ceci est une procédure complexe. Dans la pratique, la distribution de degrés optimaux ne peut être atteinte que si l'on considère que la distribution des noeuds de parité est de degré deux [29] au lieu du modèle complexe utilisé dans $P2$:

$$\rho(x) = \frac{j(j+1-\hat{n}_{avg})}{\hat{n}_{avg}} x^{j-1} + (1 - \frac{j(j+1-\hat{n}_{avg})}{\hat{n}_{avg}}) x^j \tag{3.14}$$

où $j = \lfloor \hat{n}_{avg} \rfloor$.

Pour obtenir une solution optimale, le problème $P1$ est d'abord résolu pour l'optimisation de la distribution des degrés des nœuds de variables. Le problème $P2$ est ensuite utilisé pour la détermination de la distribution des degrés des nœuds de parité en changeant la valeur de $\hat{n}_{avg}$, jusqu'à ce qu'une paire de distributions de degrés optimaux qui minimise l'écart δ soit atteinte. Lors de la conception d'un code LDPC avec un ensemble de distributions de degrés, on doit considérer différente spécifications. Ces critères sont énumérés comme suit dans [29] :

1. **Valeur inférieure du degré maximum** $(\hat{l}_{\max}, \hat{n}_{\max})$ **(complexité de l'ensemble)**

   En d'autres termes, nous essayons de choisir une valeur souhaitable pour le nombre d'arêtes dans le graphe de sorte que nous ayons de bonnes performances ainsi qu'une complexité raisonnable. Notre objectif est donc de minimiser les coefficients des polynômes λ_i et ρ_i pour des valeurs plus élevées de i, c'est-à-dire en choisissant les valeurs inférieures de $\hat{l}_{\max}$ et $\hat{n}_{\max}$.

2. **Taux supérieur** $r(\lambda(x), \rho(x))$ **(fiabilité de transmission)**

   En télécommunications, la vitesse de transmission ou le taux de transmission efficace est le taux auquel l'information est traitée par système de transmission. Par conséquent, il convient de concevoir un code qui maximise le taux $r(\lambda(x), \rho(x))$.

3. **Seuil supérieur** ε^{BP} **(probabilité d'effacement maximale pour laquelle une transmission fiable est encore possible)**

   Il est nécessaire que le code conçu a la valeur maximale du seuil. C'est-à-dire que dans le cas du BEC, le décodeur peut encore corriger l'erreur. La Fig. 3.2 montre que si $\varepsilon > \varepsilon^{BP}$, la courbe de taux d'erreur BER peut ne pas converger et tendre vers 0. D'autre part, si nous avons $\varepsilon < \varepsilon^{BP}$, alors la courbe de BER peut converger et tendre vers 0.

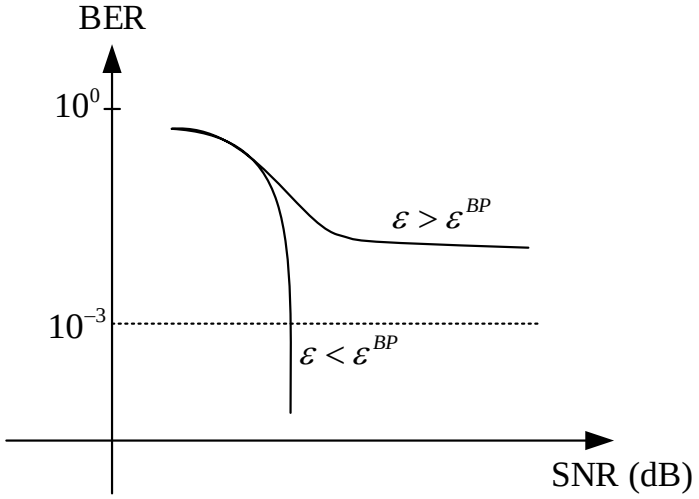


FIGURE 3.2 – Courbe typique de performance d'un code LDPC pour $\varepsilon < \varepsilon^{BP}$ et $\varepsilon > \varepsilon^{BP}$.

En outre, lorsque le code présente un seuil plus élevé, la courbe BER en fonction du SNR démontre une meilleure performance dans la région de la zone en cascade "en anglais : waterfall region". Par conséquent, lors de la conception du code LDPC, il est souhaitable de maximiser le seuil ε^{BP}.

Un diagramme EXIT [72] est un outil utile pour la démonstration de la performance dans la sortie du décodeur sous le décodage de l'algorithme BP. En considérant l'équation 3.9, on peut imaginer que $f(\varepsilon, x)$ est la combinaison de deux fonctions : $v_\varepsilon(x) = \varepsilon\lambda(x)$ qui montre l'action

des noeuds de variables, et $c(x) = 1 - \rho(1-x)$ qui montre l'action du nœuds de parité, telle que $f(\varepsilon, x) = v_\varepsilon(c(x))$.

Rappelons que la condition de convergence est $f(\varepsilon, x) - x < 0, x \in [0,1]$, ce qui signifie

$$c(x) < v_\varepsilon^{-1}(x), x \in [0,1] \tag{3.15}$$

L'interprétation graphique de cette équation est que $c(x)$ doit être strictement inférieur à $v_\varepsilon^{-1}(x)$ pour $x \in [0,1]$, et ε^{BP} est le suprême de toutes les valeurs possibles de ε qui satisfont l'équation (3.15).

En d'autres termes, les $c(x)$ et $v_\varepsilon^{-1}(x)$ peuvent être considérés comme la capacité du canal et le taux de conception du code, qui sont proches des autres, si nous avons la valeur maximale de ε^{BP}.

Exemple 3 :

En considérant l'exemple 1 ($\lambda(x) = x^2, \rho(x) = x^3$), nous avons $c(x) = 1 - (1-x)^3$ et $v_\varepsilon^{-1}(x) = (\frac{x}{\varepsilon})^{\frac{1}{2}}$. La courbe de la fonction $c(x)$ est montrée à la Fig. 3.3 et $v_\varepsilon^{-1}(x)$ est également montré pour $\varepsilon = 0.5$, 0.6, 0.6474, et 0.7. Comme on le voit, pour $\varepsilon = 0.6474$, $v_\varepsilon^{-1}(x)$ touche la courbe $c(x)$ qui signifie $\varepsilon^{BP} = 0.6474$.

Exemple 4 :

En considérant l'exemple 2 ($\lambda(x) = 0.4x + 0.6x^2, \rho(x) = 0.2x + 0.8x^3$), nous avons $c(x) = 1 - (0.2(1-x) + 0.8(1-x)^3)$ et $v_\varepsilon^{-1}(x) = -\frac{1}{3} + \frac{1}{12}\sqrt{16 + \frac{240x}{\varepsilon}}$. Le diagramme EXIT est montré à la Fig. 3.4. Comme on le voit, pour $\varepsilon = 0.6807$, $v_\varepsilon^{-1}(x)$ touche la courbe $c(x)$ qui signifie $\varepsilon^{BP} = 0.6807$.

La courbe en escalier entre la $c(x)$ et $v_\varepsilon^{-1}(x)$ montre le comportement de convergence du processus de décodage en utilisant l'algorithme BP. En d'autres termes, cette courbe en escalier montre l'évolution de la fraction des messages effacés émis par le noeuds de variables. Pour $\varepsilon < \varepsilon^{BP}$, cette fraction converge vers zéro et pour $\varepsilon > \varepsilon^{BP}$ cette fraction ne converge pas, ce qui est conforme aux résultats de la Fig. 3.2.

4. **Fraction inférieure de degrés deux λ_2 (stabilité du code et minimisation de plancher d'erreur)**

   La Fig. 3.5 illustre le BER en fonction du SNR. Pour les codes LDPC et les codes Turbo, il arrive un point après lequel la courbe ne tombe plus aussi rapidement et où la performance s'aplanit. Cette région est appelée la "zone du plancher d'erreur".

   Il est difficile de concevoir un code LDPC qui a de bonnes performances à la fois dans la zone de cascade et la zone de plancher d'erreur [73]. La performance dans la zone de cascade peut être améliorée en optimisant le seuil du code basé sur l'algorithme DE. Cela équivaut à décaler la courbe de performance d'erreur vers la gauche, à proximité de la limite de capacité. Par conséquent, en autant que nous ayons un seuil plus élevé, la région de la cascade présente de meilleures performances.

   La performance du plancher d'erreur a été difficile à caractériser de manière explicite. En général, la performance dans cette région dépend de la structure du graphe de Tanner du code LDPC

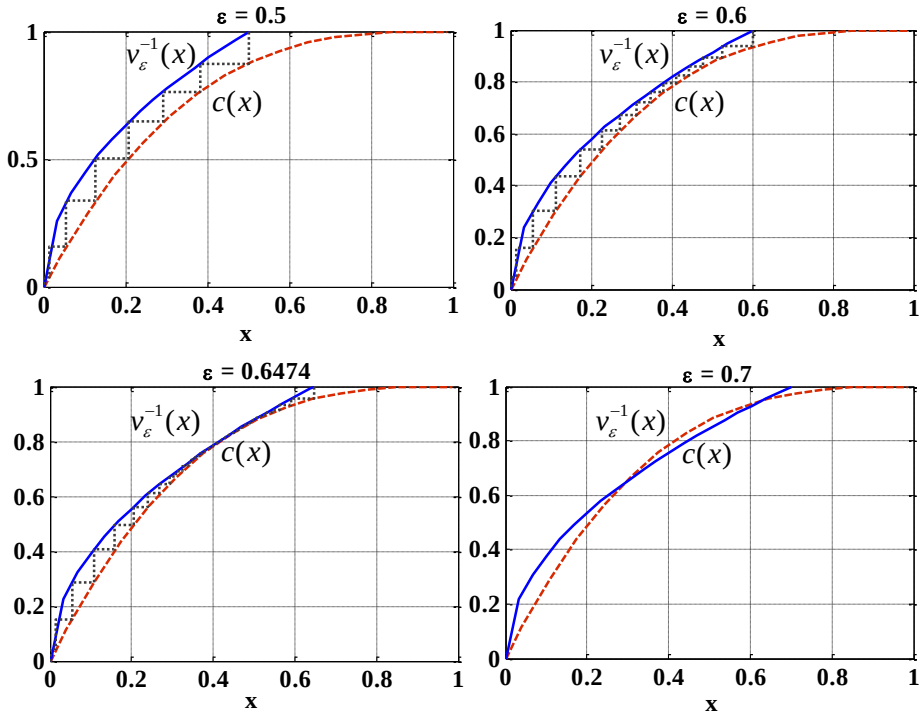


FIGURE 3.3 – Diagramme EXIT de l'exemple 1 pour différentes valeurs de ε.

tel que la maille (en anglais : "girth"), les ensembles d'arrêts (en anglais : "stopping sets"), l'algorithme de décodage, etc. La maille est le plus petit nombre de cycles dans le graphe de Tanner associé à une matrice de contrôle de parité LDPC. Une petite maille limite l'indépendance des messages transmis dans le processus de décodage et se traduit par un échec de la convergence vers un mot de code valide. Il a été observé que les codes à petite maille ont tendance à présenter des planchers d'erreur élevés.

Un ensemble de nœuds de variables est appelé un ensemble d'arrêts si tous ses voisins sont connectés à cet ensemble au moins à deux reprises. Dans le contexte du décodage de code LDPC, un ensemble d'arrêts est défini comme n'importe quel sous-ensemble de nœuds de variables tel que si un nœud de parité y est connecté, il y est connecté au moins deux fois. Un exemple d'ensemble d'arrêts est montré dans la Fig. 3.6.

En général, le plancher d'erreur des codes LDPC est dominé par les mauvaises sous-structures dans le graphe de Tanner [73]. Améliorer la performance du plancher d'erreur de codes LDPC est critique. Toutefois, il arrive que le plancher d'erreur n'est pas observé parce qu'il est hors de portée des simulations [73]. Afin de réduire le plancher d'erreur, nous devons concevoir des codes LDPC avec une meilleure structure. Ceci implique que la structure du code évite les imperfections du graphe de cycles courts qui forment des ensembles d'arrêts.

En concevant des codes LDPC, la valeur du deuxième coefficient λ_2, associé au polynôme $\lambda(x)$ indique que pour une valeur de λ_2 faible, nous aurons des ensembles d'arrêts avec une plus

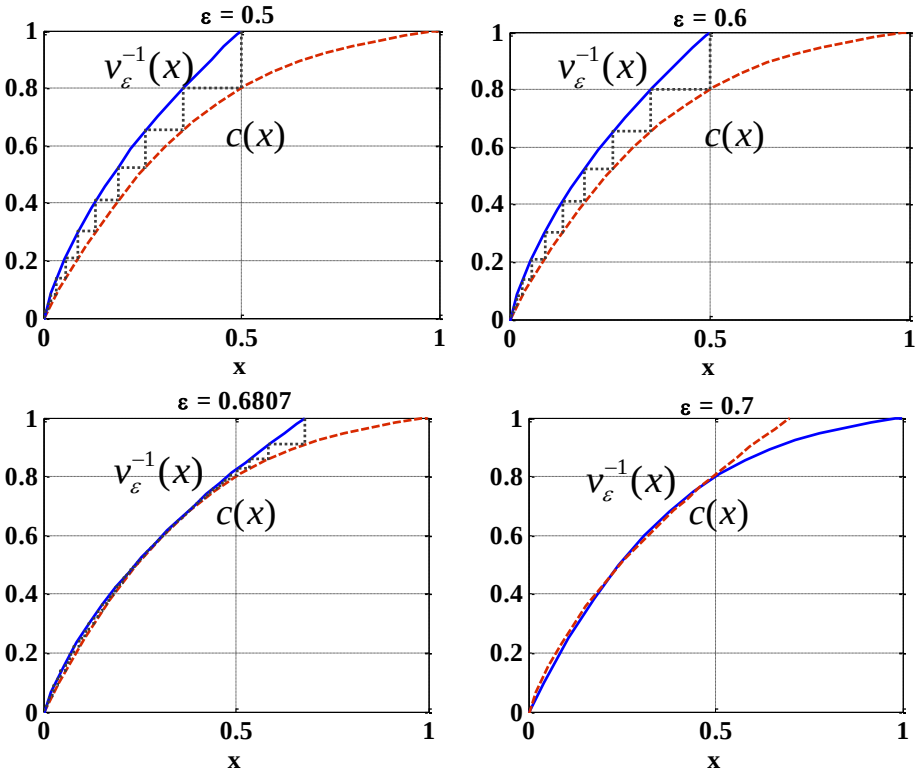


FIGURE 3.4 – Diagramme EXIT de l'exemple 2 pour différentes valeurs de ε.

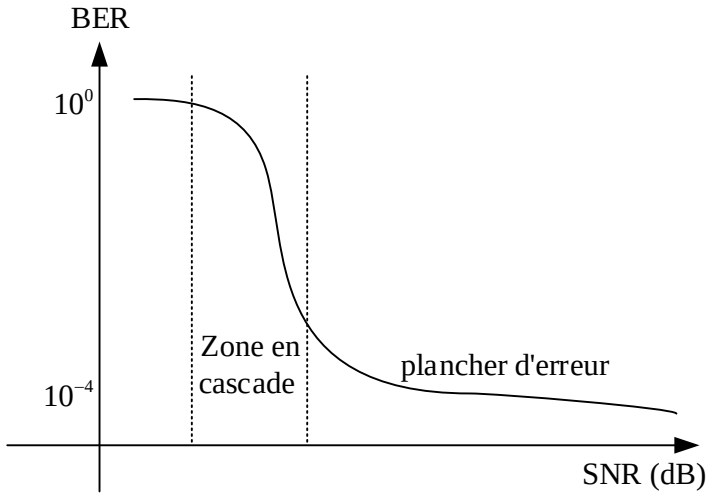


FIGURE 3.5 – Courbe BER en fonction du SNR

faible probabilité [74]. Cela suggère que si un graphe a une fraction considérable de nœuds de variables de degrés deux, il est probable que de petits ensembles d'arrêts puissent exister.

L'autre problème est la stabilité du code. Quand un message est passé à travers le graphe de Tanner du code LDPC, la probabilité moyenne d'effacement au niveau des nœuds de variables

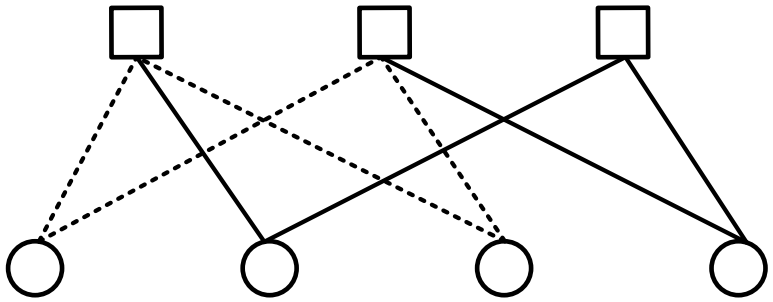


FIGURE 3.6 – Exemple d'ensemble d'arrêts et une maille de longueur 4 (ligne pointillée).

est définie par l'équation suivante [29] :

$$x_l = \varepsilon\lambda(1-\rho(1-x_{l-1})) \tag{3.16}$$

En décomposant en série de Taylor autour de zéro le côté droit de (3.16), nous obtenons [29] :

$$x_l = \varepsilon\lambda'(0)\rho'(1)x_{l-1} + O(x_{l-1}^2) \tag{3.17}$$

où $\lambda' = \frac{\partial\lambda(x)}{\partial x}$ et $\rho' = \frac{\partial\rho(x)}{\partial x}$.

Pour un x_l suffisamment petit, le comportement de convergence est déterminé par le terme linéaire en x_l et $O(x^2)$ converge vers zéro. Plus précisément, la convergence de l'équation (3.17) dépend de la valeur de $\varepsilon\lambda'(0)\rho'(1)$.

La conséquence la plus importante de la condition de stabilité est liée à la limite supérieure sur le seuil comme :

$$\varepsilon^{BP}(\lambda,\rho) \leq \frac{1}{\lambda'(0)\rho'(1)} \tag{3.18}$$

ce qui implique que lorsque λ_2 est faible, nous avons une meilleure condition de stabilité. En effet, le $\lambda_2 = \lambda'(0)$ (équation 3.1) et nous attendons d'avoir une grande valeur de ε^{BP} lorsque nous concevons les codes LDPC. Par conséquent, en considérant l'équation (3.18), la valeur de λ_2 doit être faible.

5. **Minimum de l'écart δ (distance de la capacité du canal).** Pour avoir un bon code, le code conçu $v_\varepsilon^{-1}(x)$ doit être près de à la capacité du canal $c(x)$. Dans ce cas, nous aurons une petite valeur de δ. En d'autres termes, l'objectif ici est de minimiser la différence δ entre la capacité C et le taux de conception $r(\lambda(x),\rho(x))$ comme indiqué dans les sections précédentes.

3.3 Méthode de recherche de codes LDPC irrégulier GA-LP proposée

Selon [29], afin de trouver une bonne distribution de degrés $(\lambda(x),\rho(x))$ on peut procéder comme suit. On commence la procédure avec une paire de distributions de degrés donnée et on itère entre les

problèmes d'optimisation $P1$ et $P2$ comme décrit dans la section 3.2.

Pour la méthode proposée, nous exécutons à la première étape le problème d'optimisation $P1$ en utilisant un algorithme génétique (GA) et en recherchant les meilleures populations de degrés de nœuds de variables $\lambda_i, i = 1,2,\ldots,\hat{l}_{\max}$. Au même moment, en utilisant la méthode de programmation linéaire (LP), nous recherchons la meilleure distribution $\rho(x)$ de nœuds de parité, en changeant $\hat{n}_{avg}$ pour chaque population de $\lambda_i, i = 1,2,\ldots,\hat{l}_{max}$. Ces deux procédures d'optimisation nous aident à réduire notre fonction de coût, l'écart $\delta(\lambda,\rho)$ (équation 3.5), pour cette population spécifique. Après avoir répété la même procédure pour toutes les populations, nous les classons afin de sélectionner les meilleures d'entre elles et de les transmettre à l'itération suivante, jusqu'à ce que le nombre maximum d'itérations soit atteint. Enfin, nous extrayons les codes qui satisfont aux cinq critères présentés à la section précédente et obtenus par optimisation.

La Fig. 3.7 montre la structure de la méthode GA-LP proposée pour résoudre les problèmes d'optimisation $P1$ et $P2$. Sur cette figure, $\hat{n}_{pop}$, l, $\hat{n}_{LP}$ et CF indiquent respectivement le numéro de l'itération, l'indice du nombre de chromosomes à chaque itération, l'indice de $\hat{n}_{avg}$ pour chaque chromosome et la fonction de coût correspondants à chaque ensemble de distributions de degrés.
Le principal avantage de l'algorithme GA-LP proposé est que des ensembles avec des valeurs inférieures à δ peuvent être obtenus, en comparaison avec le cas d'une distribution de degrés de noeuds de parité régulier. Par ailleurs, l'algorithme d'optimisation GA-LP peut converger vers des valeurs acceptables de δ avec moins d'itérations.

La Fig. 3.8 montre l'organigramme de la méthode GA-LP proposée. Comme on peut le voir, la méthode GA-LP essaie de trouver les chromosomes pour lesquels le taux $r(\lambda,\rho)$ est dans la plage de tolérance prédéterminée autour de $C_{BEC}(\varepsilon)$. Au niveau suivant, l'algorithme proposé calcule les valeurs d'écart δ de tous les chromosomes choisis et sélectionne le meilleur ensemble de distributions de degrés satisfaisant aux cinq critères mentionnés précédemment.

3.4 Résultats des simulations

Dans cette section, les résultats de simulations sont présentés pour comparer la performance de la méthode proposée à celle des méthodes existantes. Le tableau 3.4 résume les résultats obtenus avec notre procédé et les compare à ceux obtenus avec la méthode GA, ainsi qu'avec la méthode de Tavakoli [2]. Dans [2], la recherche des ensembles de codes LDPC sur un canal BEC a été conçu en utilisant la programmation semi-définie (en anglais : "semidefinite programming"). Cette méthode considère une distributions de noeuds de parité régulière et optimise les coefficients de noeuds de variables. Les résultats indiqués dans ce tableau montrent une performance acceptable de l'approche GA-LP proposée par rapport aux cinq critères énumérés à la section 3.2. Nous remarquons que pour la méthode GA-LP

proposée, nous avons sélectionné ;

$$\begin{aligned}
\rho(x) &= 0.81231x^3 + 0.18769x^4 \quad \text{pour} \quad 4 \leq \hat{n}_{avg} < 5; \\
\rho(x) &= 0.57621x^4 + 0.42379x^5 \quad \text{pour} \quad 5 \leq \hat{n}_{avg} < 6; \\
\rho(x) &= 0.72000x^5 + 0.28000x^6 \quad \text{pour} \quad 6 \leq \hat{n}_{avg} < 7; \\
\rho(x) &= 0.11563x^7 + 0.88437x^8 \quad \text{pour} \quad 7 \leq \hat{n}_{avg} < 8.
\end{aligned}$$

En comparant les résultats de la méthode de Tavakoli [2] et ceux obtenus avec l'algorithme GA (avec des nœuds de parité réguliers), on constate qu'ils conduisent à peu près aux mêmes résultats, car la seule différence entre eux est le choix de la méthode d'optimisation. Les résultats de la méthode GA-LP proposée sont meilleurs selon la plupart des critères mentionnés dans la section 3.2, mais avec le désavantage d'une distribution plus complexe pour des nœuds de parité. Ceci est dû au fait que notre algorithme d'optimisation GA-LP peut rechercher différentes valeurs de $\hat{n}_{avg}$ pour fournir les meilleures distributions de degrés de nœud de parité.

Dans les deux exemples suivants, nous présentons quelques résultats numériques obtenus avec les algorithmes GA et GA-LP, où ils ont été comparés avec les résultats présentés à la section 3.18 de [29].

Exemple 1 :

Si nous fixons $\rho(x) = x^5$, le meilleure distribution de degrés $\lambda(x)$ avec 7 degrés de liberté $\hat{l}_{\max} = 8$ obtenue par les algorithmes GA et Richardson et Urbanke [29] (ces méthodes sont identifiées avec les indices *GA* et *R*, respectivement) est :
$\lambda_{GA}(x) = 0.39947x + 0.22981x^2 + 0.02501x^3 + 0.03076x^4 + 0.07594x^5 + 0.04205x^6 + 0.19967x^7$
et $\lambda_R(x) = 0.409x + 0.202x^2 + 0.0768x^3 + 0.1971x^6 + 0.1151x^7$.

Ceci permet d'obtenir des seuils de $\varepsilon_{GA}^{BP} = 0.48326$ et $\varepsilon_R^{BP} = 0.4810$, des taux de $r_{GA} = 0.49803$ et $r_R = 0.5004$, et des écarts $\delta_{GA} = 0.036$ et $\delta_R = 0.0359$ respectivement avec notre d'algorithme GA et celui de Richardson.

Maintenant, en utilisant l'algorithme proposé GA-LP avec $4 \leq \hat{n}_{avg} < 8$, on obtient :
$\rho_{GA-LP}(x) = 0.66412x^5 + 0.33588x^6$ et
$\lambda_{GA-LP}(x) = 0.37810x + 0.20799x^2 + 0.05363x^3 + 0.00950x^4 + 0.00233x^5 + 0.00248x^6 + 0.34597x^7$.

Ceci conduit au seuil $\varepsilon_{GA-LP}^{BP} = 0.48339$, au taux de $r_{GA-LP} = 0.50053$, et à l'écart $\delta_{GA-LP} = 0.03112$.

Exemple 2 :

Si nous fixons $\rho(x) = x^5$, la meilleure distribution de degrés $\lambda(x)$ avec 12 degrés de liberté $\hat{l}_{\max} = 13$ obtenue par les algorithmes GA et Richardson et Urbanke [29] est :
$\lambda_{GA}(x) = 00.38138x + 00.30350x^2 + 00.00201x^3 + 00.06322x^4 + 00.00201x^5 + 00.00425x^6 + 00.00275x^7 + 00.23078x^8 + 00.00417x^9 + 00.00427x^{10} + 00.00104x^{11} + 00.00060x^{12}$ et

$\lambda_R(x) = 0.416x + 0.166x^2 + 0.1x^3 + 0.07x^4 + 0.053x^5 + 0.042x^6 + 0.035x^7 + 0.03x^8 + 0.026x^9 + 0.023x^{10} + 0.02x^{11} + 0.0183x^{12}$.

On obtient des seuils $\varepsilon_{GA}^{BP} = 0.476155$ et $\varepsilon_{R}^{BP} = 0.480896$, des taux de $r_{GA} = 0.499315$ et $R_R = 0.499013$ et des écarts $\delta_{GA} = 0.04683$ et $\delta_R = 0.03853$.

Maintenant, en utilisant l'algorithme proposé GA-LP avec $4 \leq \hat{n}_{avg} < 8$, on obtient :
$\rho_{GA-LP}(x) = 0.05123x^5 + 0.94877x^6$ et
$\lambda_{GA-LP}(x) = 0.29571x + 0.27795x^2 + 0.04321x^3 + 0.00071x^4 + 0.00145x^5 + 0.00052x^6 + 0.00108x^7 + 0.00238x^8 + 0.09432x^9 + 0.00323x^{10} + 0.26989x^{11} + 0.00955x^{12}$.

Ceci conduit au seuil $\varepsilon_{GA-LP}^{BP} = 0.49277$, au taux de $r_{GA-LP} = 0.49478$, et à l'écart $\delta_{GA-LP} = 0.024553$.

En comparaison avec les résultats de l'algorithme génétique (GA) et celle proposée par Tavakoli [2], l'ensemble de distributions obtenu par l'algorithme combinée proposé GA-LP a amélioré la majorité des critères énumérés précédemment, mais au coût d'un modèle plus complexe pour la distribution de degrés des nœuds de parité (critère 1).

Enfin, il faut mentionner que lors de la recherche sur les ensembles de distributions de degrés optimaux en utilisant les algorithmes GA ou GA-LP, divers ensembles avec des spécifications différentes peuvent être obtenus en ce qui concerne les cinq critères mentionnés dans la section 3.2. Par conséquent, on doit choisir le code approprié adapté au système et à l'application prévue. Les Fig. 3.9 et Fig. 3.10 montrent les distributions et le nombre d'itérations nécessaires pour obtenir les spécifications pour la conception des codes pour les exemples 1 et 2. La méthode GA-LP pourrait converger au bon ensemble avec moins d'itérations en adaptant les distributions de degrés de noeuds de parité.

Comme on peut le voir à la Fig. 3.9, le taux obtenu avec la méthode GA-LP converge beaucoup plus rapidement qu'avec la méthode GA (voir Figs. 3.9 b) et 3.10 b). En outre, les histogrammes des écarts de capacité des codes optimisés pour les méthodes GA et GA-LP ont été présentés aux Figs. 3.9 a) et 3.10 a), ce qui montre que, en donnant la liberté du choix de $\rho(x)$, nous pouvons atteindre des valeurs plus petites de l'écart δ et améliorer les critères énumérés précédemment.

3.5 Complexité de l'algorithme GA-LP proposé

Maintenant, nous étudions le coût de mise en œuvre des algorithmes GA et GA-LP en termes de complexité et de temps d'exécution pour chaque itération. La notation Big-O est une notation mathématique qui décrit le comportement asymptotique d'une fonction quand l'argument tend vers l'infini. Soit f et g deux fonctions, on peut écrire $f(x) = O(g(x)), x \to \infty$ si et seulement s'il existe une constante positive K telle que pour toutes les valeurs suffisamment grandes de x c'est-à-dire $x \geq x_0$, l'expression suivante soit satisfaite :

$$|f(x)| \leq K\,|g(x)|\,,\ \ x \geq x_0 \tag{3.19}$$

Il convient de mentionner que la complexité de chaque méthode en termes de temps d'exécution pour chaque itération en secondes (sec) est obtenue sur la base des fonctions *tic/toc* du logiciel MATLAB sur une plate-forme Intel P4 à 2.60 GHz. Pour l'algorithme GA, nous avons utilisé les $\hat{l}_{max} = 8, \hat{n}_{pop} = 1000, l = 1000$; pour l'algorithme GA-LP, nous avons utilisé les $\hat{l}_{max} = 8, \hat{n}_{pop} = 50, l = 50, \hat{n}_{LP} = 100$, et pour méthode de Tavakoli [2] nous avons $\hat{l}_{max} = 8$. Le Tableau 3.2 indique ce résultat.

3.6 Conclusion

Dans ce chapitre, nous avons proposé une méthode pour minimiser l'écart multiplicatif δ itérativement entre l'optimisation de la distribution de degrés des nœuds de variables à l'aide de l'algorithme génétique GA et l'optimisation de la distribution des degrés de nœuds de parité en utilisant la programmation linéaire LP. Les résultats des simulations montrent l'avantage de la méthode GA-LP proposée alors que la majorité des critères de conception de codes LDPC irrégulier mentionnés à la section 3.2 ont été améliorés, mais ce, au coût d'un modèle plus complexe pour la distribution des degrés de nœud de parité (critère 1). Ce choix permet la conception de codes correcteurs LDPC ayant des meilleures distributions de degrés de nœuds de parité. En outre, en utilisant cette approche, on peut atteindre les distributions de degrés désirées avec moins d'itérations.

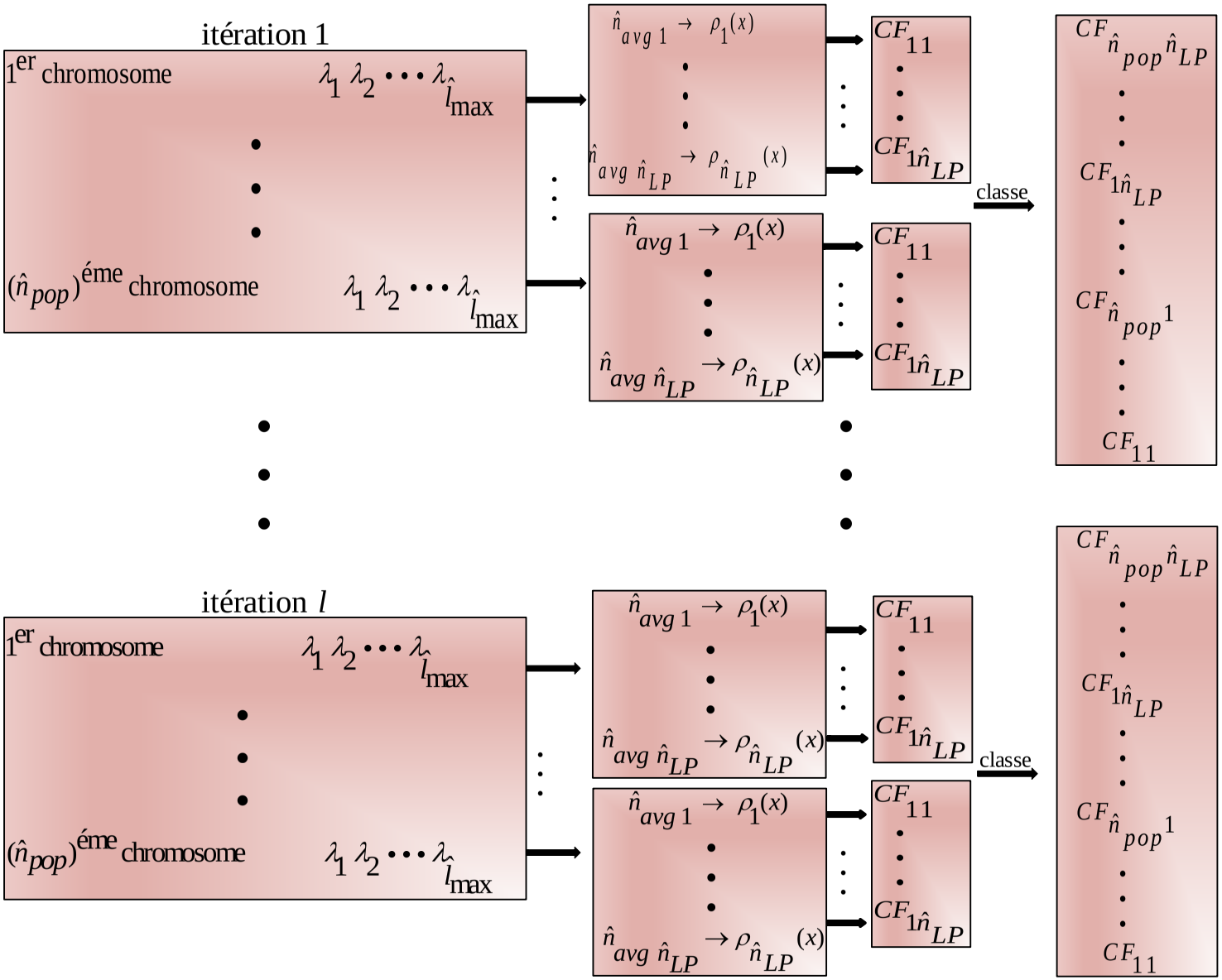


FIGURE 3.7 – Méthode GA-LP proposée pour résoudre les problèmes d'optimisation de P1 et P2.

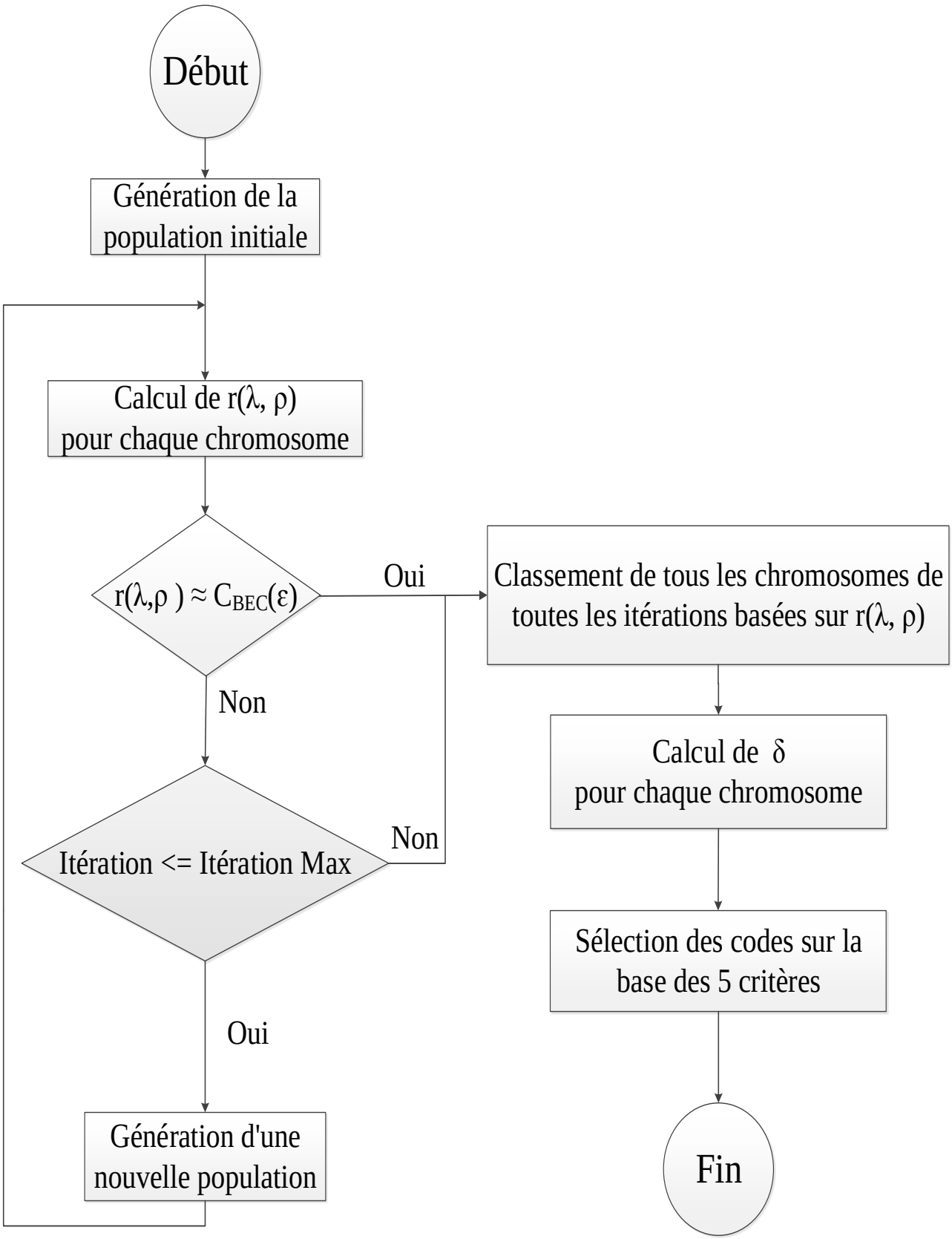


FIGURE 3.8 – Organigramme de la méthode GA-LP proposée.

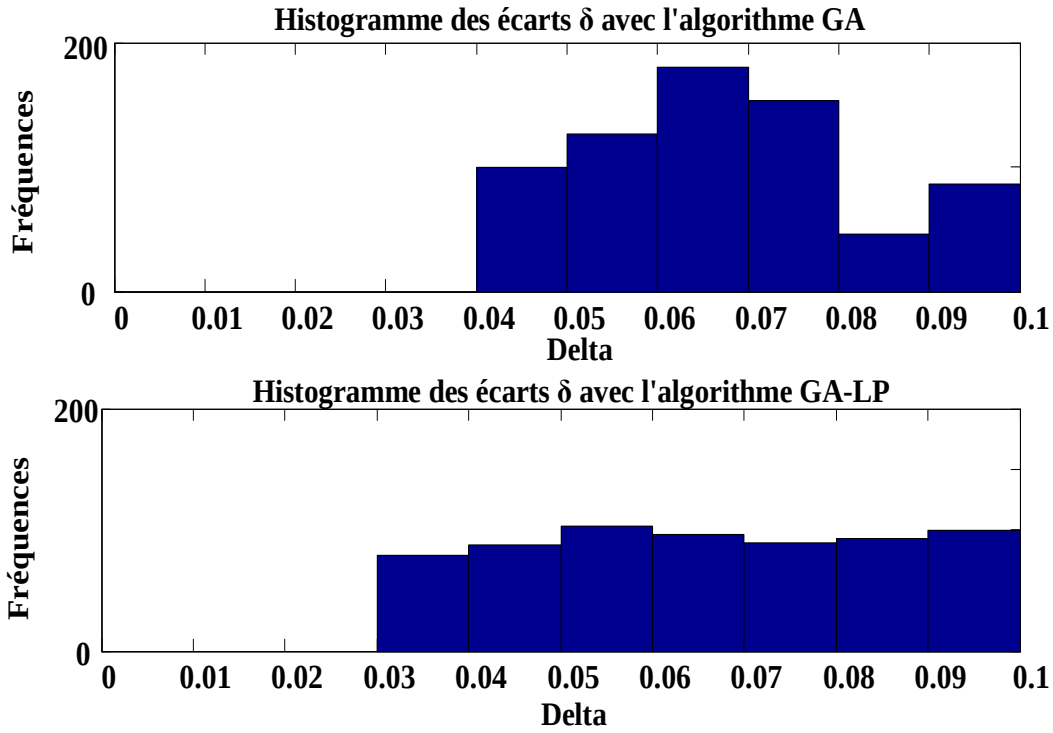
TABLE 3.1 – Codes LDPC optimaux en utilisant la méthode de Tavakoli et les algorithmes GA et GA-LP.

paramètres → / méthode d'optimisation ↓	$\lambda(x)$ / $\rho(x)$	λ_2	λ_3	λ_4	λ_5	λ_6	λ_7	ε^{Sh}	C^{Sh}	ε^{BP}	r	δ
algorithme GA	x^3	0.47085	0.22827	0.00185	0.00287	0.00083	0.29532	0.69	0.31	0.68889	0.29554	0.05005
	x^4	0.43758	0.26135	0.00192	0.00439	0.29384	0.00089	0.56	0.44	0.53502	0.43879	0.05632
	x^5	0.41618	0.21552	0.00282	0.11946	0.00290	0.24312	0.49	0.51	0.46900	0.50943	0.04060
	x^6	0.48575	0.06071	0.44165	0.00154	0.00261	0.00774	0.38	0.62	0.34580	0.61943	0.05310
méthode de Tavakoli [2]	x^3	0.4735	0.2244	0	0	0	0.3021	0.69	0.31	0.6900	0.2952	0.0479
	x^4	0.4393	0.2097	0.0536	0.2974	0	0	0.56	0.44	0.5191	0.4481	0.0680
	x^5	0.4021	0.2137	0	0	0	0.3902	0.49	0.51	0.4904	0.4919	0.0347
	x^6	0.4385	0.1456	0	0.4159	0	0	0.38	0.62	0.3801	0.5930	0.0435
algorithme GA-LP	$0.81231x^3+0.18769x^4$	0.47017	0.18284	0.00074	0.00045	0.13012	0.21566	0.69	0.31	0.67532	0.31018	0.04467
	$0.57621x^4+0.42379x^5$	0.40836	0.15692	0.05765	0.07140	0.03129	0.27438	0.56	0.44	0.54065	0.43605	0.05073
	$0.72000x^5+0.28000x^6$	0.39999	0.22027	0.00001	0.00671	0.06431	0.30865	0.49	0.51	0.46845	0.51454	0.03199
	$0.11563x^6+0.88437x^7$	0.38342	0.19693	0.07515	0.00100	0.00162	0.34185	0.38	0.62	0.37331	0.60957	0.03023

TABLE 3.2 – Coût de mise en œuvre des algorithmes GA, GA-LP, et la méthode de Tavakoli

complexité ↓	GA	GA-LP	Méthode de Tavakoli
Big-O	$O(\hat{l}_{\max}\hat{n}_{pop}l)$	$O(\hat{l}_{\max}\hat{n}_{pop}\hat{n}_{LP}l)$	$O((\hat{l}_{\max})^3)$
temps d'exécution	69.84 (sec)	239.02 (sec)	5.43 (sec)

a)



b)

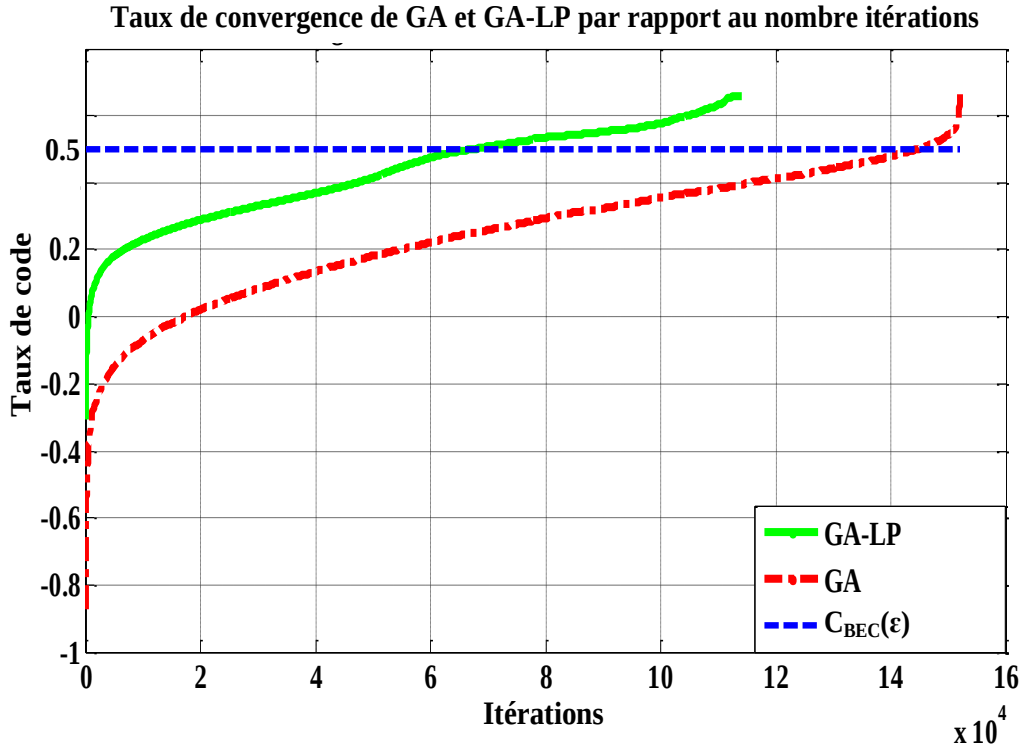


FIGURE 3.9 – Comparaison des distributions et des taux de convergence de la méthode GA-LP proposée et GA dans l'exemple 1.

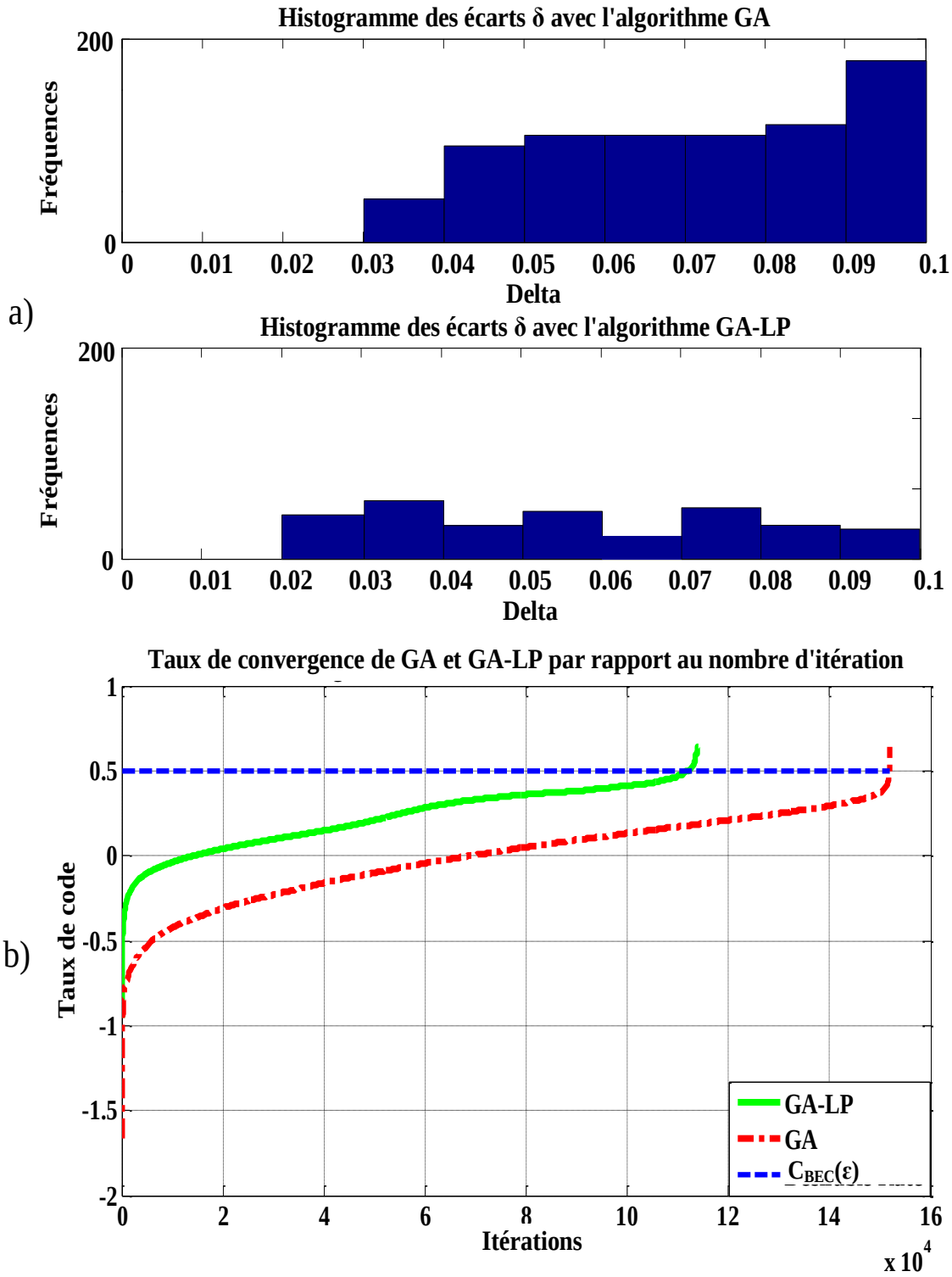


FIGURE 3.10 – Comparaison des distributions et des taux de convergence de la méthode GA-LP proposée et GA dans l'exemple 2.

Chapitre 4

Méthode de codage AG-HARQ pour l'amélioration de la sécurité dans les canaux à écoute gaussien

Dans ce chapitre, nous étudions la transmission fiable et sécurisée dans un canal à écoute gaussien. Une méthode de décodage de requête automatique de répétition hybride granulaire adaptative (AG-HARQ) est proposée. Cette méthode cherche à minimiser le taux requis pour un décodage réussi par les parties légitimes tout en augmentant la sécurité de la transmission en minimisant les fuites d'information vers un éventuel espion. Dans le cas d'un échec de décodage du protocole LDPC par le récepteur légitime (Bob), une retransmission est effectuée jusqu'à ce que le décodage soit correct ou jusqu'à ce que le nombre maximum de paquets transmis soit atteint. Dès que Bob est capable de décoder correctement le mot de code LDPC, les retransmissions sont arrêtées pour éviter toute fuite de bits supplémentaires à l'espion (Eve). Afin de minimiser les fuites, la méthode proposée ici introduit un indice de niveau de confiance en décodage correct, $\hat{C}_j$, qui est défini comme la moyenne de la valeur absolue du rapport de vraisemblance logarithmique (LLR). En cas d'échec, seuls les sous-paquets avec les plus petites valeurs $\hat{C}_j$ seront retransmis, car ils représentent les sous-paquets d'information les moins fiables. Le taux d'erreur par trame (FER) est utilisé comme un indicateur pour montrer l'efficacité de la méthode proposée.

En plus, pour augmenter encore la sécurité donnée par la méthode AG-HARQ proposé, nous combinons l'AG-HARQ avec les méthodes de contamination d'erreur intra-trame (IntraEC) et de contamination d'erreur inter-trame (InterEC). L'objectif de l'IntraEC est de propager l'effet d'un bit d'erreur à la trame entière en utilisant une matrice de brouillage ($\mathbf{S}$) et la matrice de désembrouillage ($\mathbf{S^{-1}}$), tandis que l'objectif de l'InterEC est non seulement de propager un bit en erreur à la trame courante, mais aussi aux autres trames en utilisant un entrelaceur et un désentrelaceur couvrant plusieurs trames. Le taux d'erreur par bit (BER) est utilisé comme un indicateur pour montrer l'efficacité de la méthode proposée.

4.1 Définitions de la sécurité et de la fiabilité basées sur le concept de l'écart de sécurité

La Fig. 4.1 montre le modèle de canal gaussien à écoute introduit par Wyner [52]. Alice envoie un message **m** en utilisant le codage pour produire un mot de code $\mathbf{x^n}$. Nous supposons que le mot de code $\mathbf{x^n}$ est transmis à Bob sur un canal gaussien à bruit blanc (AWGN), alors qu'Eve tente de reconstruire le message original **m** en écoutant le mot de code transmis sur son canal (canal avec écoute).

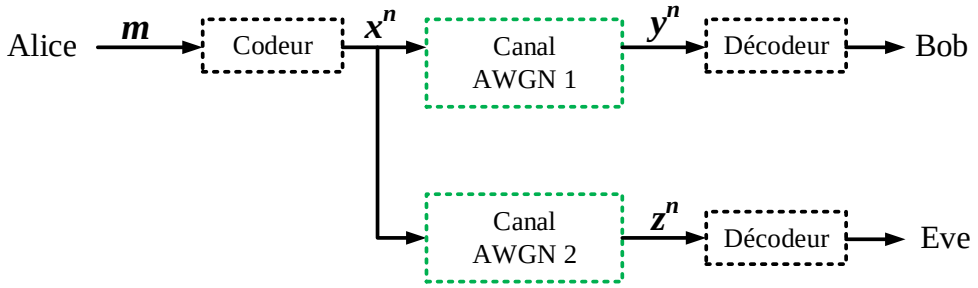


FIGURE 4.1 – Modèle de canal gaussien avec écoute.

L'objectif principal est d'assurer une transmission fiable et sécurisée des informations sur le modèle de canal avec écoute :

1. Condition de fiabilité (sur le canal principal) : $BER_{\max}^{Bob} \approx 0$. Avec ce BER à la sortie du décodeur de Bob, le récepteur légitime peut recouvrer le message original de manière fiable.

2. Conditions de sécurité (sur le canal avec écoute) : $BER_{\min}^{Eve} \approx 0.5$ (idéalement). Quand Eve subit ce BER et que les erreurs sont distribuées au hasard, elle ne devrait pas être capable d'obtenir suffisamment d'informations sur le message transmis.

Si les conditions 1 et 2 sont remplies, alors le décodeur de Bob peut extraire le message correctement après avoir observé $\mathbf{y^n}$, tandis que la séquence $\mathbf{z^n}$ reçue maintient une incertitude suffisante (pas de fuite d'information) de manière à ce que le message d'origine ne puisse pas être décodé par Eve. Pour évaluer la performance du modèle de canal avec écoute gaussien, l'écart de sécurité (SG : "Security Gap" en anglais) a été introduit dans [75]. Le paramètre SG quantifie la différence de qualité requise entre le canal du récepteur légitime et le canal de l'espion pour les communications sécurisées et fiables. L'objectif est de maintenir SG aussi petit que possible, même quand il y a une petite différence de dégradation entre le canal principal et le canal avec écoute. La Fig. 4.2 illustre les régions sécurisées et fiables en fonction du taux d'erreur par bit (BER) et du rapport signal sur bruit (SNR), selon l'écart de sécurité SG pour un modèle de canal avec écoute.

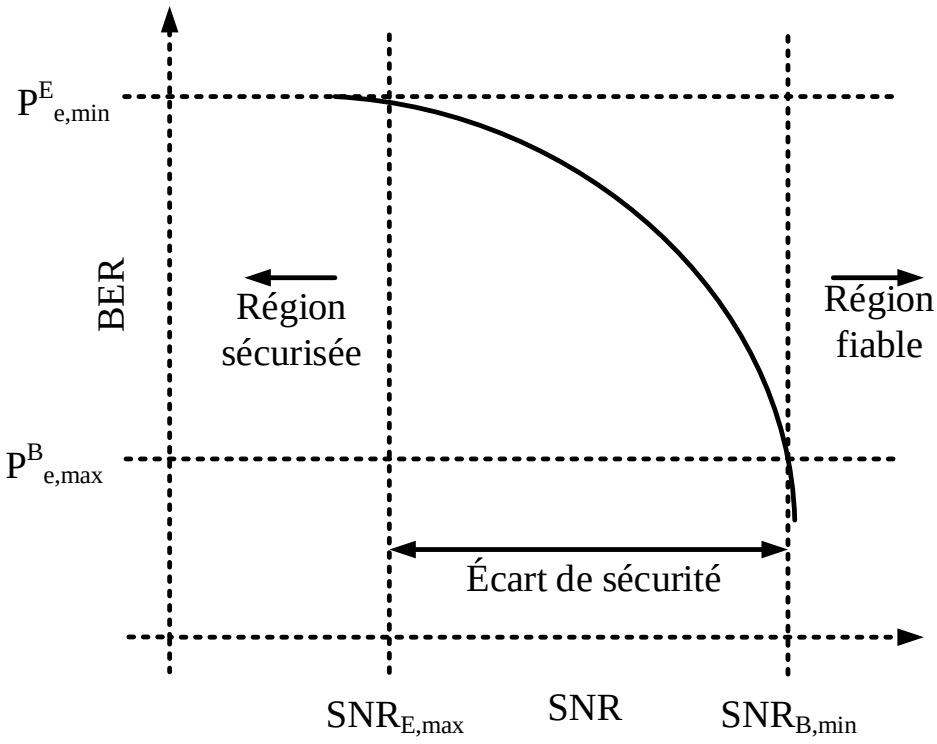


FIGURE 4.2 – Écart de sécurité (SG) : Les seuils de probabilité d'erreur canaux principal (Bob) et espion (Eve).

4.2 Méthode G-HARQ

L'objectif principal des protocoles HARQ [70] et G-HARQ [3] est de donner à Bob un avantage sur Eve. Le protocole HARQ retransmet le paquet entier au maximum q fois (par exemple $q = 3$) lorsque Bob ne peut pas décoder correctement le message. Le schéma G-HARQ divise le paquet requis pour la transmission à g sous-paquets, où g est sa granularité. Comme on le voit sur la Fig. 2.3, le premier paquet $q = 1$ est l'ensemble du mot de code de longueur n. Les sous-paquets suivants ont une longueur n/g. Contrairement à la procédure HARQ, qui envoie le paquet entier dans chaque retransmission, le schéma G-HARQ retransmet uniquement des sous-paquets aléatoires jusqu'à ce que le décodeur LDPC de Bob converge vers un message unique. Par conséquent, l'avantage principal du G-HARQ sur HARQ est que la fuite d'information à un espion diminue parce que seuls des petits sous-paquets sont retransmis dans le canal sous écoute. Nous considérons ici le même code LDPC utilisé dans [70] avec $(n = 510, n - \hat{m} = 384)$ et la distribution de degrés suivante :

$$\begin{aligned} \lambda(x) = &\quad 0.0019608 + 0.098039x + 0.0019608x^2 + 0.89804x^3 \\ \rho(x) = &\quad 0.15079x^{14} + 0.33333x^{15} + 0.51587x^{16} \end{aligned} \tag{4.1}$$

où $\lambda(x)$ représente la distribution de degré de nœud de variable et le $\rho(x)$ représente la distribution

de degré de nœud de parité. Dans [70], la granularité est fixée à $g = 1$ et chaque retransmission est constitué d'un paquet de longueur $n = 510$. Le nombre maximum de retransmissions est fixé à $q = 3$. Dans le schéma G-HARQ [3], la granularité est fixée à $g = 10$ et la taille des sous-paquets est $n/g = 51$. Dans ce cas, le nombre maximum de retransmissions est $q = 1+2g = 21$ comme indiqué à la Fig. 4.3.

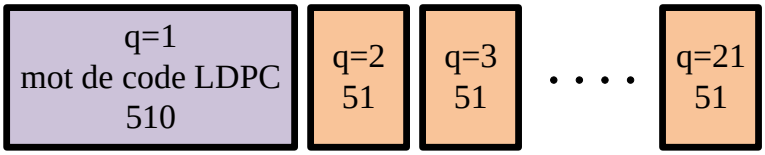


FIGURE 4.3 – Retransmission des sous-paquets en utilisant la méthode G-HARQ.

4.3 Méthode AG-HARQ proposée

Une lacune des méthodes précédentes est que pour chaque requête de retransmission de la part de Bob, le paquet entier pour la méthode HARQ [70] ou un sous-paquet choisi au hasard pour la méthode G-HARQ [3] est retransmis. Cela peut conduire à la retransmission d'informations redondantes à Bob et en conséquent, génère une fuite d'informations inutile à l'espion. Dans cette section, un protocole granulaire adaptatif de requête automatique de répétition hybride (AG-HARQ) contrôlé par le récepteur légitime est introduit pour résoudre ce problème.

4.3.1 Processus de décodage

Les probabilités de bits calculées par le décodeur LDPC sont connues comme les probabilités a posteriori, tandis que le rapport des probabilités sont exprimées en valeurs logarithmiques de vraisemblance (LLR) dans le décodeur de SPA. À chaque itération de décodage LDPC, une nouvelle valeur de vraisemblance, $LLR(x)$, peut être calculée pour les nœuds variables :

$$LLR(x) = \ln \frac{p(x=1|y)}{p(x=0|y)} \tag{4.2}$$

La valeur absolue de $LLR(x_i)$ indique la fiabilité d'une décision ferme sur un bit particulier i. Pour un mot de code LDPC reçu de longueur n, divisé en g sous-paquets, la fiabilité du décodage correct peut être estimée avec un indice de niveau de confiance $\hat{C}_j$ défini comme :

$$\hat{C}_j = \underset{i \in j^{th} \text{ sous-paquets}}{\text{moyenne}} \; [|LLR(x_i)|] \tag{4.3}$$

où $j = 1,2,\ldots,g$.

Par la méthode proposée, le récepteur légitime (Bob) demande la retransmission des sous-paquets avec les indices de confiance les plus petits, car ils peuvent être utiles pour le décodage de l'ensemble de mots de code. D'autre part, ces sous-paquets peuvent ne pas être utiles pour l'espion (Eve) en raison de l'indépendance statistique supposée entre le canal principal et le canal de l'espion.

La Fig. 4.4 montre la structure de la méthode AG-HARQ proposée. La méthode de décodage AG-HARQ proposée utilise un niveau de confiance $\hat{C}_j$ calculé à partir des valeurs de sortie souples de LLR qui aident Bob à trouver les sous-paquets avec les plus petites valeurs. En d'autres termes, l'objectif principal de l'utilisation de cet indice par AG-HARQ est d'identifier les sous-paquets avec les informations les moins fiables (petites valeurs de LLR). Lorsque le décodeur de Bob ne peut pas converger vers la valeur correcte, une demande de retransmission est renvoyée à Alice à travers un canal de rétroaction parfait. Dans le cas d'un échec à la sortie du décodeur de Bob, les sous-paquets seront retransmis à Bob avec un ordre du plus petit $\hat{C}_j$ vers le plus grand, jusque à ce que le décodage soit correct ou que le nombre maximum de paquets transmis soit atteint.

Par comparaison avec les méthodes de retransmission HARQ et G-HARQ [70, 3], la méthode AG-HARQ peut réduire le taux requis pour un décodage réussi par les parties légitimes tout en augmentant la sécurité et en minimisant les fuites d'informations à l'espion. L'AG-HARQ a besoin de moins de requêtes de retransmission en comparaison avec [3] puisque seuls les sous-paquets les moins fiables (à partir du détecteur de Bob) sont retransmis dans le cas d'échec de décodage, aidant ainsi le décodeur de Bob à converger vers la valeur correcte tout en utilisant un plus petit nombre de sous-paquets.

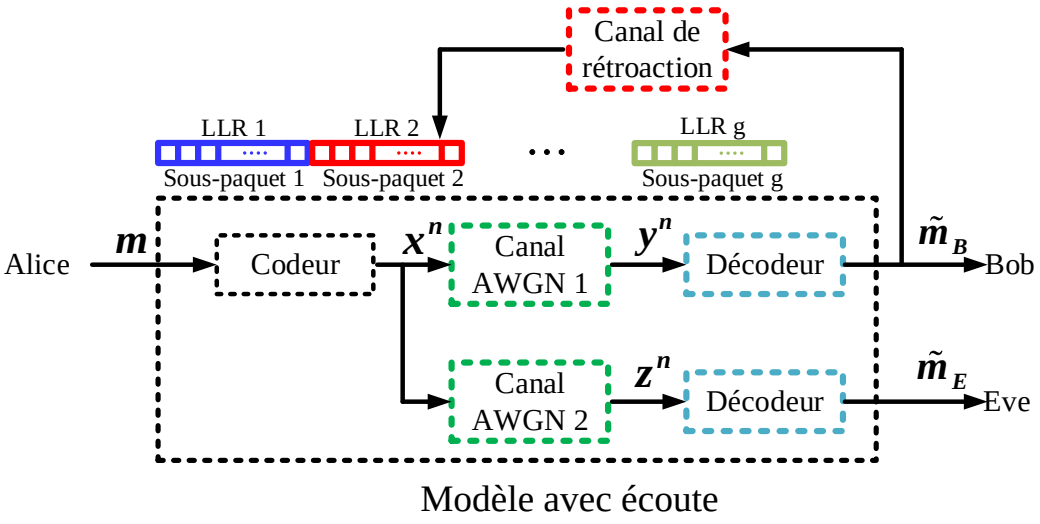


FIGURE 4.4 – Structure du système AG-HARQ du canal avec écoute avec rétroaction parfaite.

4.4 Résultats des simulations

Des simulations par ordinateur ont été effectuées pour comparer les performances de la méthode AG-HARQ proposée avec la méthode HARQ [70] et la méthode G-HARQ [3] en termes de sécurité et de fiabilité. La Fig. 4.5 montre un exemple des valeurs LLR pour chaque nœud de variable dans le processus de décodage réel du récepteur légitime (Bob), où les valeurs $\hat{C}_j$ des sous-paquets ont été représentées. Comme indiqué plus haut, en cas d'échec du décodeur de Bob, le premier sous-paquet à retransmettre est le 10^e sous-paquet de $(LLR = 1.4246)$, tandis que le dernier serait le 3^e sous-paquet (LLR = 2.0365).

L'amélioration des performances avec la méthode AG-HARQ a été étudiée en fonction du taux d'erreur par trame (FER) et en fonction du rapport signal à bruit (SNR) pour différentes valeurs des écarts de sécurité $SG = SNR_g$: 1, 0.5, 0, -0.5, -1 et -1.5 dB. Comme on le voit aux Figs. 4.6, 4.7, et 4.8, l'amélioration obtenue avec le procédé adaptatif de HARQ est due à la flexibilité du système G-HARQ en termes de granularité des paquets. Cela illustre aussi l'hypothèse de Wyner sur l'exploitation du caractère aléatoire du canal et de l'indépendance statistique entre le canal principal et le canal avec écoute, sans utilisation de clé de cryptage secrète.

Avec l'utilisation d'un canal de rétroaction contrôlé par Bob, même si Eve obtient statistiquement un meilleur canal, c'est-à-dire pour $SNR_g < 0$, une communication fiable et partiellement sécurisée est encore possible. La méthode AG-HARQ donne une meilleure amélioration par rapport à la technique G-HARQ lorsque $SNR_g < 0$. Même si le canal légitime est plus corrompu que le canal illégitime, en demandant la retransmission des sous-paquets les plus corrompus, la situation est plus profitable au processus de décodage du récepteur de Bob.

De plus, comme indiqué à la section 4.3, l'AG-HARQ a besoin de moins de requêtes de retransmission en comparaison avec le G-HARQ, car les sous-paquets les moins fiables sont demandés par Bob. Ceci aide le décodeur de Bob à converger vers la valeur correcte et avec moins de sous-paquets retransmis. Le Tableau 4.1 compare le nombre de sous-paquets nécessaires dans le cas des requêtes de retransmission à $SNR = 0$ dB pour différentes valeurs de SNR_g.

4.5 AG-HARQ avec contamination d'erreur intra-trame et inter-trame

La sécurité dans les systèmes de communication est traditionnellement assurée en utilisant des techniques cryptographiques mises en œuvre au niveau des couches de protocole. Comme nous l'avons vu précédemment, la partielle, ou totale, indépendance stochastique entre le canal principal et le canal avec écoute peut être exploitée pour améliorer le secret des informations transmises à la couche physique. Dans cette section, on démontre que les techniques G-HARQ et AG-HARQ en conjonction avec le schéma contamination d'erreur intra-trame et inter-trame peuvent assurer un niveau élevé de secret, même quand Eve obtient de meilleures conditions de canal par rapport à Bob. La Fig. 4.9 montre un système de communication utilisant la contamination d'erreur intra-trame et inter-trame.

TABLE 4.1 – Comparaison du nombre des requêtes de retransmission pour les schémas G-HARQ et AG-HARQ à $SNR = 0$ dB pour différentes valeurs de SNR_g.

$SNR_g \rightarrow$	-1.5 dB	-1 dB	-0.5 dB	0 dB	0.5 dB	1 dB
G-HARQ	10	10	8	10	10	10
AG-HARQ	8	8	7	9	8	9

4.5.1 Contamination d'erreur intra-trame

Un brouilleur peut être utilisé pour cacher les bits systématiques avant le codage de code LDPC, mais aussi on peut aussi l'utiliser pour diffuser les erreurs de bit unique sur une trame entière. Ce phénomène peut être appelé *contamination d'erreur intra-trame* (IntraEC). Alice met en oeuvre le codage comme suit :

$$\mathbf{x} = \mathbf{mSG} \tag{4.4}$$

où $\mathbf{G}$ est la matrice génératrice $(n-\hat{m}) \times n$ d'un code de bloc linéaire $(n, n-\hat{m})$ sous forme systématique et $\mathbf{S}$ est une matrice de brouillage binaire inversible $(n-\hat{m}) \times (n-\hat{m})$. En raison de sa forme systématique, $\mathbf{G}$ peut également être écrit $\mathbf{G} = [\mathbf{I} \,|\, \mathbf{P}]$, où $\mathbf{I}$ est une matrice d'identité $(n-\hat{m}) \times (n-\hat{m})$ et $\mathbf{P}$ est une matrice $(n-\hat{m}) \times \hat{m}$ représentant les contraintes de contrôle de parité.

Ainsi, le codage consiste simplement à remplacer le vecteur d'information $\mathbf{m}$ avec sa version brouillée $\mathbf{m}' = \mathbf{mS}$, et en appliquant ensuite le code de bloc linéaire donnée par $\mathbf{G}$. Selon le principe de la sécurité à la couche physique, $\mathbf{S}$ et $\mathbf{G}$ sont nécessaires pour le processus de décodage et sont connus pour Bob et Eve. La connaissance du code (par $\mathbf{G}$ ou par la matrice de contrôle de parité $\mathbf{H}$) est nécessaire pour exploiter de capacité de correction d'erreur du code, tandis que $\mathbf{S}$ (en fait, son inverse) doit être utilisé pour désembrouiller $\mathbf{m}'$ en $\mathbf{m}$.

Par conséquent, $\mathbf{G}$ et $\mathbf{S}$ sont connus pour Bob et Eve, et la sécurité du système ne repose pas sur des informations secrètes. Sur la base des hypothèses mentionnées ci-dessus, le mot de code codé peut aussi être écrit comme $\mathbf{x} = [\mathbf{mS} \,|\, \mathbf{mSP}] = [\mathbf{x_l} \,|\, \mathbf{x_r}]$, où $\mathbf{x_l}$ est le vecteur contenant les $(n-\hat{m})$ premiers bits de $\mathbf{x}$, tandis que $\mathbf{x_r}$ collecte des son dernier $r = \hat{m}$ bits.

Les deux canaux de Bob et Eve introduisent chacun des erreurs. Cependant, comme mentionné précédemment, le rapport signal-à-bruit pour Bob $\left(\frac{E_b}{N_o}\middle|_{Bob}\right)$ doit être suffisamment grand pour que le décodeur de Bob soit capable de corriger toutes les erreurs avec une probabilité élevée, récupérant ainsi le message $\mathbf{m_B} = \mathbf{m} = \mathbf{x_l S^{-1}}$. Au contraire, la rapport signal-à-bruit pour Eve $\left(\frac{E_b}{N_o}\middle|_{Eve}\right)$ devrait être assez petit pour assurer que le mot de code obtenu par Eve après décodage est toujours affectée par une vecteur d'erreur $\mathbf{e} = [\mathbf{e_l} \,|\, \mathbf{e_r}]$.

Dans ce cas, Eve obtient :

$$\mathbf{m_E} = (\mathbf{x_l} + \mathbf{e_l})\mathbf{S^{-1}} = \mathbf{m} + (\mathbf{e_l}\mathbf{S^{-1}}) \tag{4.5}$$

En raison de la multiplication du $\mathbf{e_l}$ par $\mathbf{S^{-1}}$, le désembrouillage peut propager les erreurs résiduelles.

Par conséquent, aux fins du secret, il est utile de maximiser l'incertitude en présence d'un (ou plusieurs) erreur(s) dans le message décodé. Ceci est possible en utilisant une matrice d'embrouillage **S** à haute densité, où une seule erreur dans le mot de code décodé est suffisante pour assurer un taux d'erreur proche de 50%. Cependant, une matrice d'embrouillage **S** avec une *faible densité* est moins efficace puisque les bits erronés sont moins susceptibles de conduire au BER souhaitable 0.5 après le processus de désembrouillage.

La matrice de brouillage **S** et son inverse $\mathbf{S^{-1}}$ peuvent être construites sur le $GF(2)$ sur la base de la décomposition **LU** [76]. Dans cette méthode, la matrice de brouillage **S** est considérée comme la multiplication d'une matrice triangulaire supérieure **U** et d'une matrice triangulaire inférieure **L** comme :

$$\mathbf{S} = \mathbf{LU} \tag{4.6}$$

où son inverse est

$$\mathbf{S^{-1}} = \mathbf{U^{-1}}\mathbf{L^{-1}} \tag{4.7}$$

Les matrices **L** et **U** sont construites aléatoirement. Le principal avantage de la décomposition **LU** est que l'inverse de **L** et **U** sont aussi des matrices triangulaires inférieures et supérieures qui peuvent être facilement calculées. De plus, en utilisant cette méthode, il n'est pas nécessaire de calculer directement $\mathbf{S^{-1}}$ qui peut être difficile pour les matrices de brouillage de grande taille.

Les figures 4.10 et 4.11 montrent un exemple du matrice d'embrouillage à haute densité et le taux d'erreur (BER) par rapport au nombre de bits erronés dans le paquet de longueur 384. Aussi, les figures 4.12 et 4.13 montrent un exemple de matrice d'embrouillage à faible densité et la courbe BER correspondante. Il convient de mentionner que la valeur *NN* à l'intérieur des figures 4.10 et 4.12 montre le nombre d'éléments non nuls dans la matrice correspondante.

4.5.2 Contamination d'erreur inter-trame

Pour améliorer le secret, la *contamination d'erreur inter-trame* (InterEC) est proposée. La Fig. 4.9 montre le système de codage proposé, où un seul bit d'erreur (qui est représenté par la boîte **err**) affecte non seulement la trame en cours, mais aussi d'autres trames. Le InterEC comprend deux embrouilleurs séparés par un bloc-entrelaceur. Chaque trame est envoyée à un embrouilleur, *S*, pour cacher les données systématiques et aussi pour propager l'erreur inter-trame. Ensuite, les trames sont

combinées en une méga-trame et entrelacées en bloc. Par conséquent, les nouvelles trames entrelacées de longueur 384 sont générées et brouillées.

L'objectif du deuxième embrouilleur est de propager l'erreur sur plusieurs trame. La Fig. 4.9 illustre l'effet de la propagation d'erreur d'un seul bit d'un paquet sur l'ensemble des trames. Ce bit erroné simple affecte approximativement la moitié des bits du paquet où il appartient (voir Fig. 4.11 à la valeur d'abscisse de 1). Ces bits affectés reprennent ensuite leurs positions d'origine dans les paquets désentrelacés. Si un paquet désentrelacés contient une seule erreur, le processus de débrouillage va propager cette erreur sur l'ensemble des trames.

4.6 Résultats des simulations

Les résultats de simulation démontrent l'efficacité de la méthode AG-HARQ avec contamination d'erreur intra-trame et inter-trame en termes de sécurité et de fiabilité. L'amélioration des performances avec la méthode AG-HARQ a été étudiée en fonction du taux d'erreur par bit (BER) et en fonction du rapport signal à bruit (SNR) pour différentes valeurs des écarts de sécurité SNR_g : 1, 0.5, 0, -0.5, -1 et -1.5 dB. Comme on le voit aux figures à 4.14 à 4.19, l'amélioration obtenue avec la méthode IntraEC est due à l'utilisation des matrices de brouillage et de désembrouillage. En outre, l'amélioration obtenue avec la méthode InterEC s'explique par l'utilisation de la matrice d'embrouillage (désembrouillage) et entrelaceur (désentrelaceur) conjointement.

4.7 Conclusion

L'une des principales difficultés dans les systèmes de communication sans fil est d'assurer la sécurité et la fiabilité en même temps. Dans ce chapitre, le modèle du canal à écoute gaussien a été considéré pour la conception d'un système pour transmettre des informations fiables à un récepteur légitime en cachant cette information à un espion éventuel. Dans le procédé proposé, la méthode HARQ a été modifiée. Dans le cas d'une requête de Bob, au lieu de retransmettre le paquet entier ou d'envoyer des sous-paquets de manière aléatoire comme dans la méthode G-HARQ, Bob demande la retransmission des sous-paquets spécifiques qui ont la plus basse moyenne de la valeur absolue du LLR. Le protocole AG-HARQ proposé essaie de réduire le taux de transmission requis pour les parties légitimes pour un décodage réussi tout en minimisant les fuites d'informations à un espion. En plus, la méthode AG-HARQ a besoin d'un moins grand nombre de requêtes de retransmission en comparaison avec le G-HARQ parce qu'il sélectionne de manière adaptative les sous-paquets nécessaires en cas d'échec de décodage légitime. Un autre système de communication pour la sécurisation des systèmes de transmission a été introduit avec la méthode AG-HARQ en ajoutant la contamination d'erreur intra-trame et inter-trame. Même quand la qualité du canal de l'espion est meilleure que celle du canal principal, les résultats des simulations montrent l'efficacité des deux méthodes proposées.

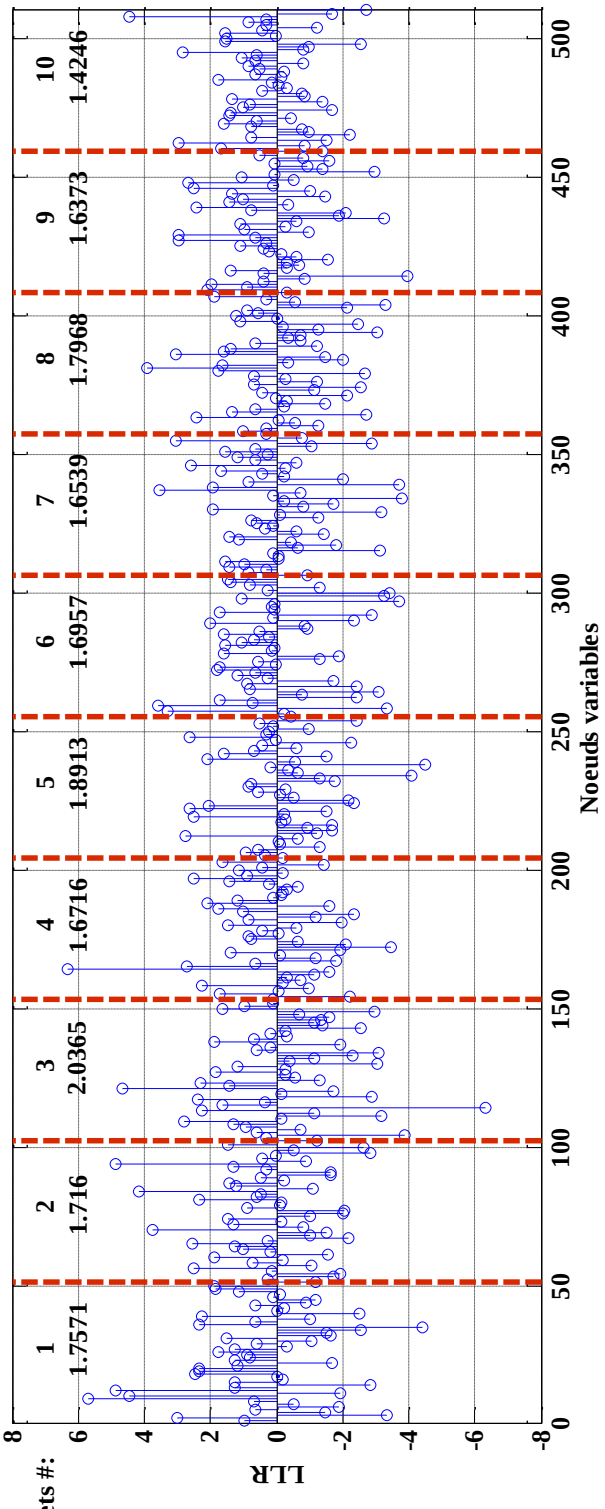
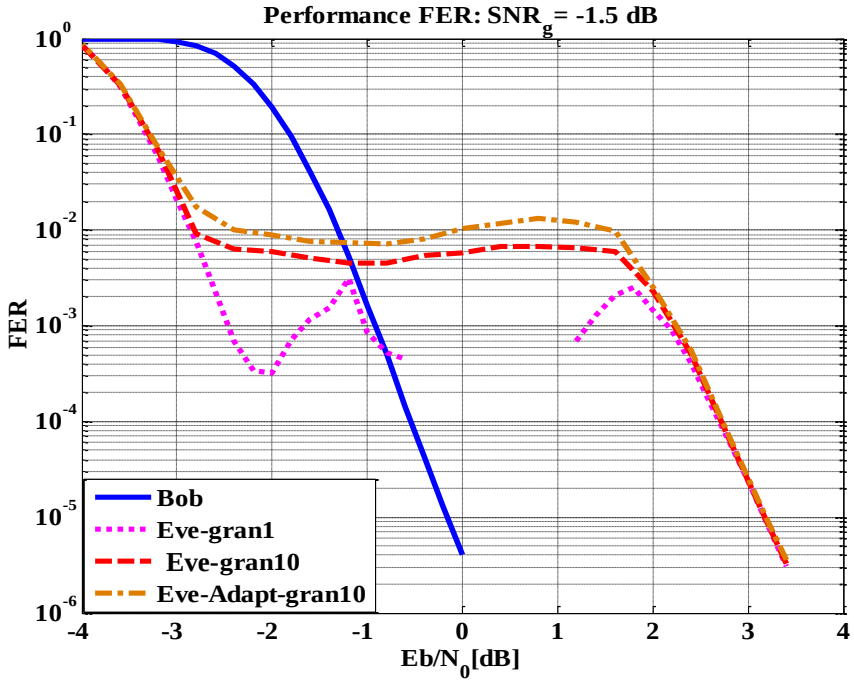
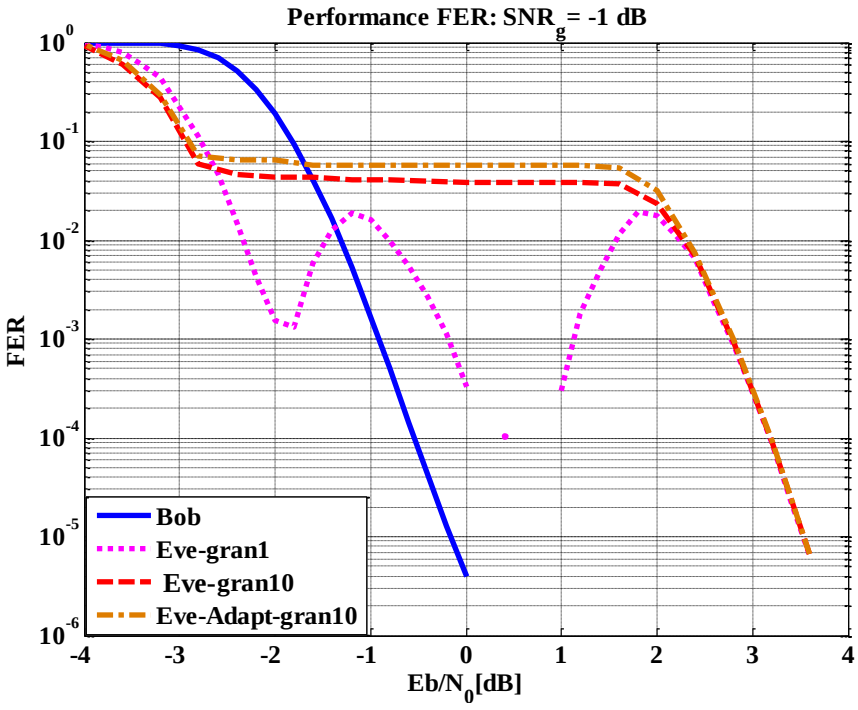


FIGURE 4.5 – Valeurs LLR pour chaque noeud de variable, le nombre de sous-paquets, et la moyenne de la valeur absolue de LLR par sous-paquets à $SNR_g = 0$ dB.

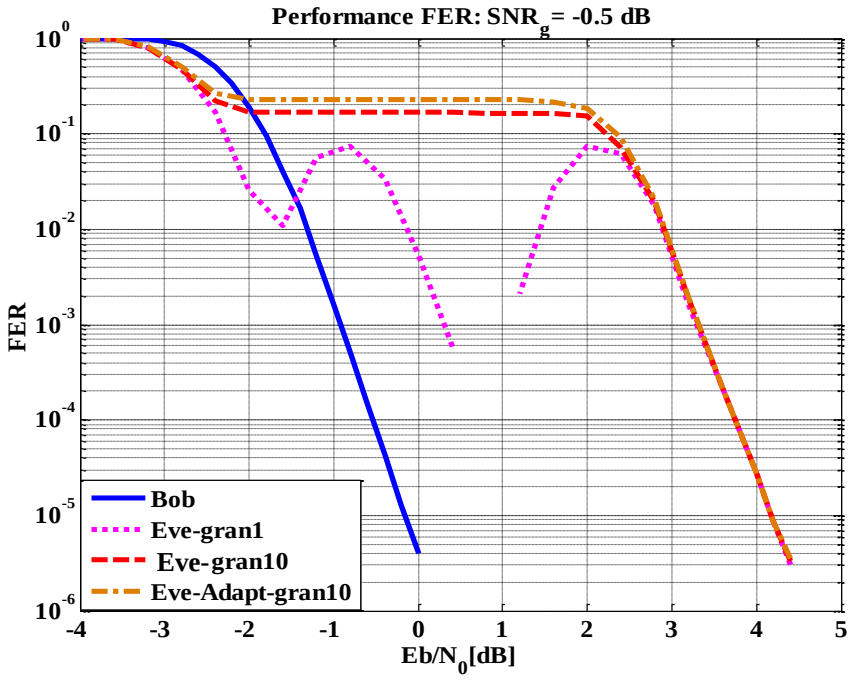


a) SNR_g= -1.5 dB

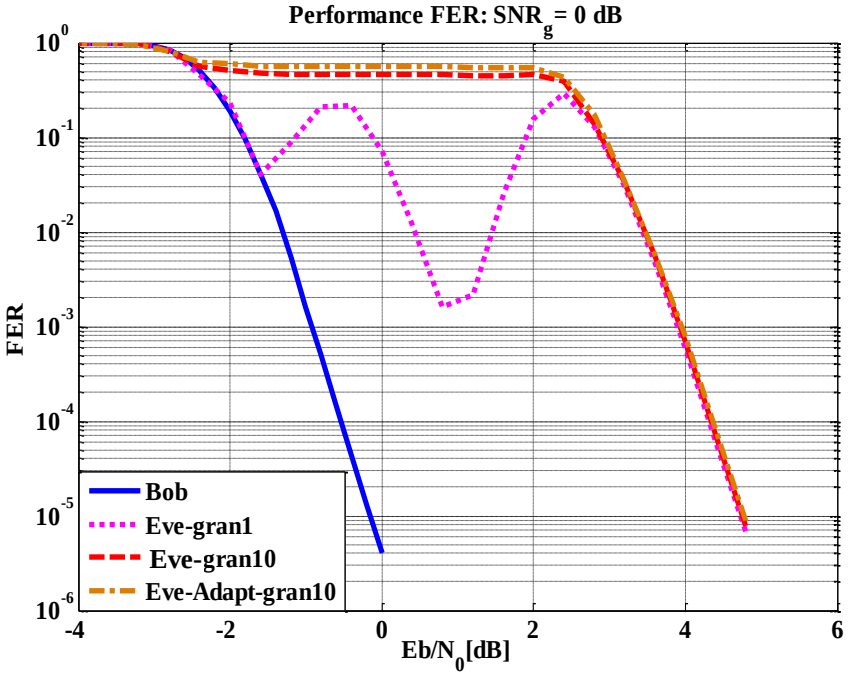


b) SNR_g= -1 dB

FIGURE 4.6 – Taux d'erreur de trame pour le canal légitime (Bob) et le canal espion (Eve) : $SNR_g = -1.5, -1$ dB.

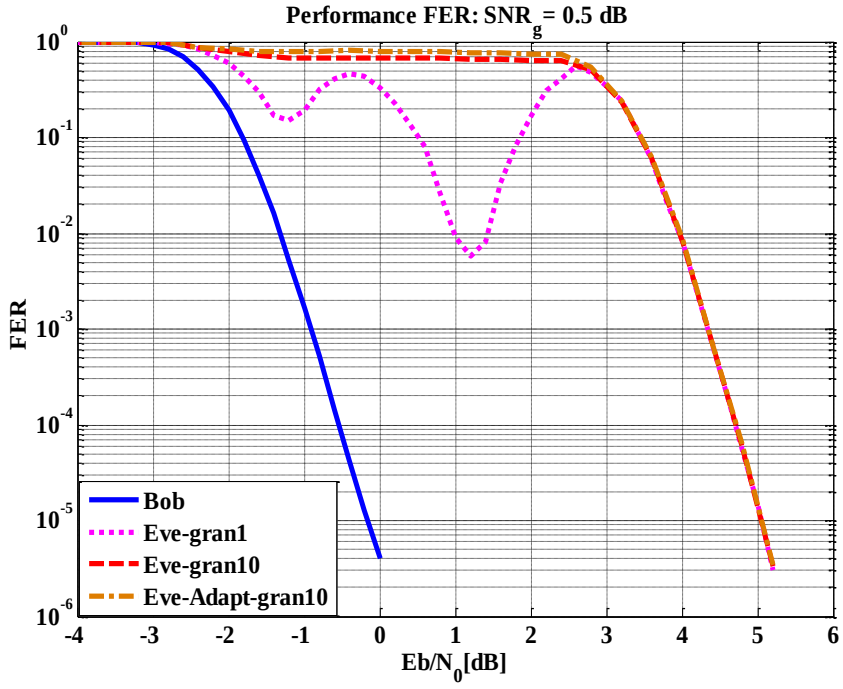


c) SNR_g= -0.5 dB

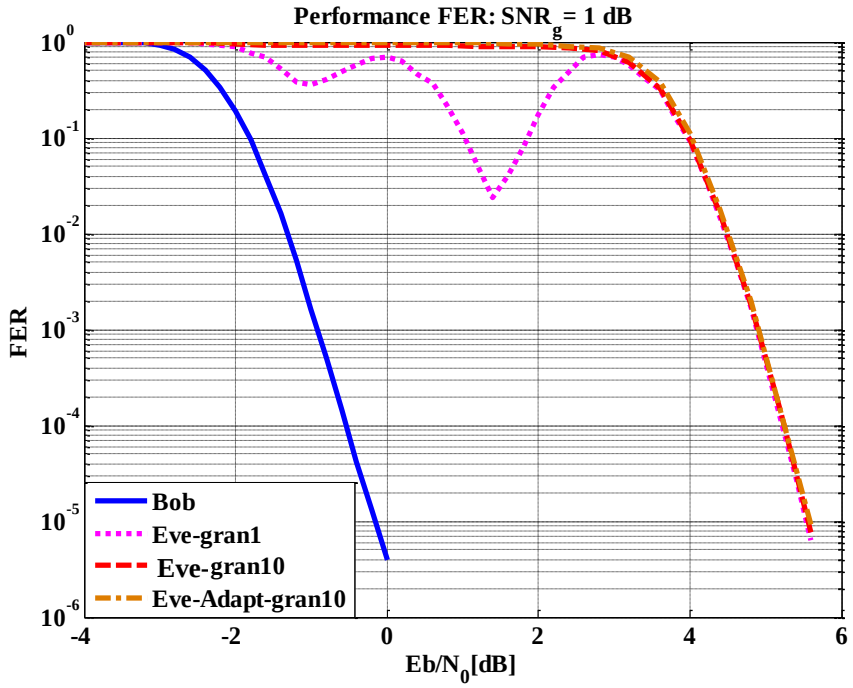


d) SNR_g= 0 dB

FIGURE 4.7 – Taux d'erreur de trame pour le canal légitime (Bob) et le canal espion (Eve) : $SNR_g = -0.5, 0$ dB.



e) SNR_g= 0.5 dB



f) SNR_g= 1 dB

FIGURE 4.8 – Taux d'erreur de trame pour le canal légitime (Bob) et le canal espion (Eve) : $SNR_g = 0.5, 1\,\text{dB}$.

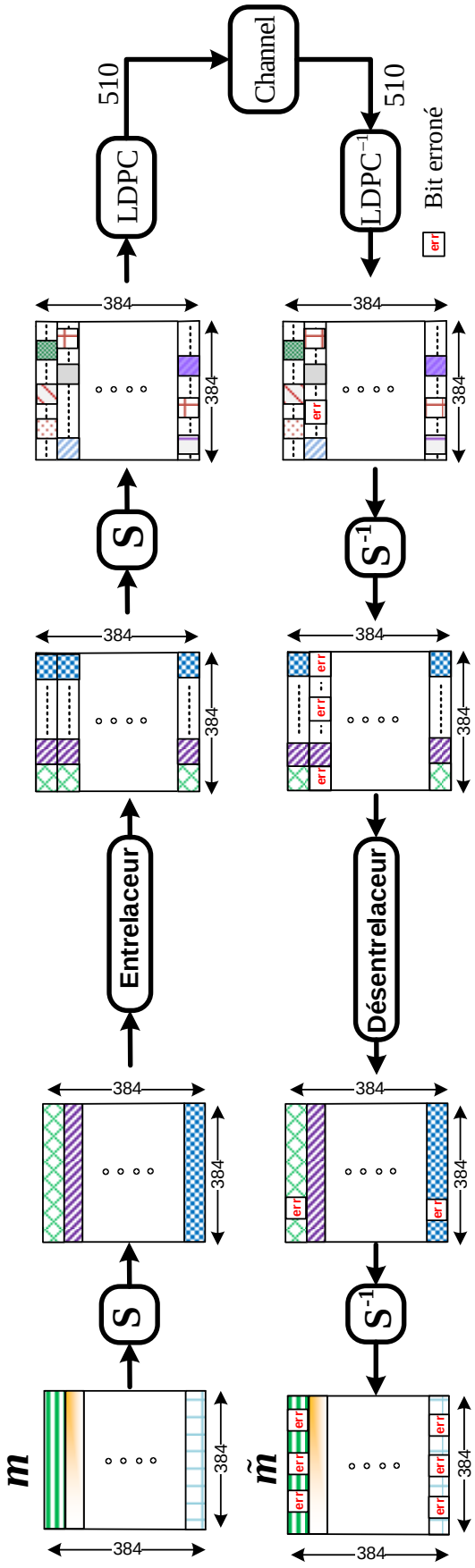


FIGURE 4.9 – Contamination d'erreur en utilisant deux matrices de embrouillage séparés par un entrelaceur.

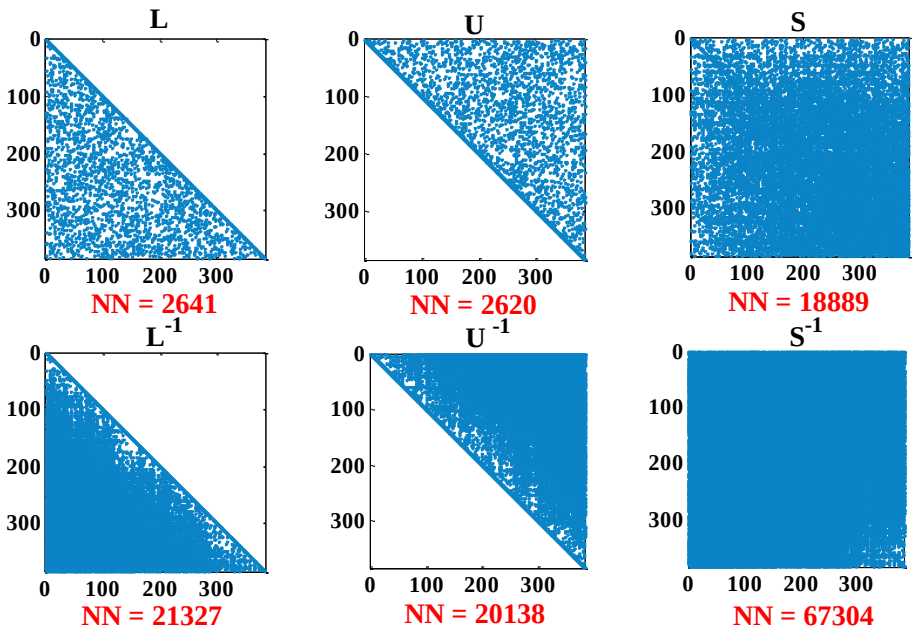


FIGURE 4.10 – Exemple du matrice de brouillage à haute densité.

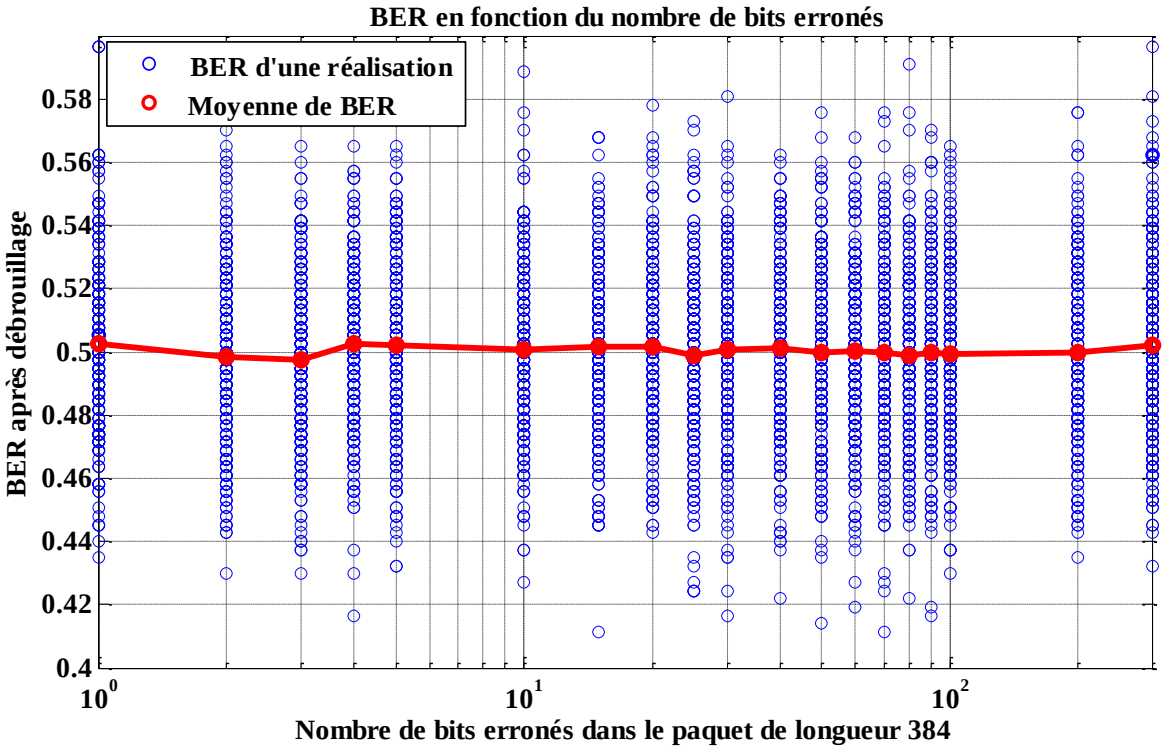


FIGURE 4.11 – Taux d'erreur (BER) par rapport au nombre de bits erronés en utilisant une matrice de brouillage à haute densité.

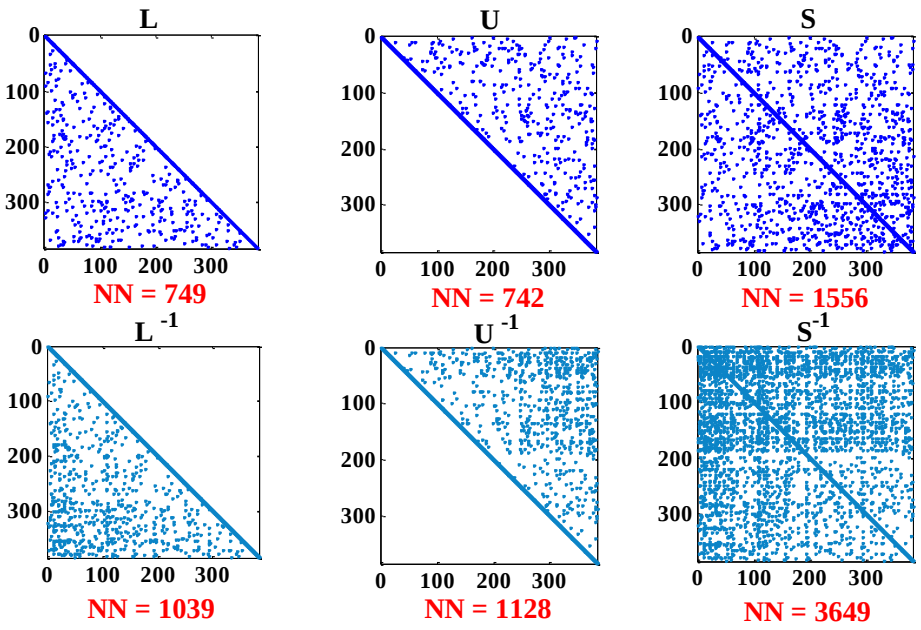


FIGURE 4.12 – Exemple du matrice de brouillage à faible densité.

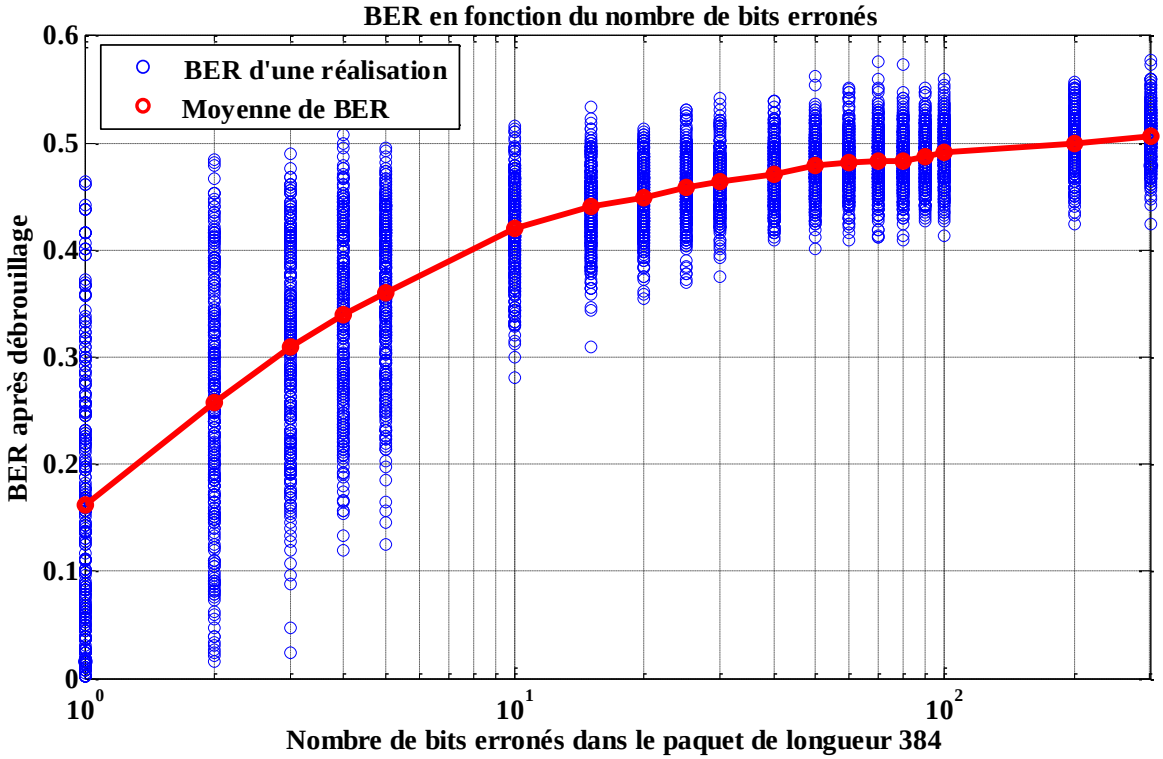


FIGURE 4.13 – Taux d'erreur (BER) par rapport au nombre de bits erronés en utilisant matrice de brouillage à faible densité.

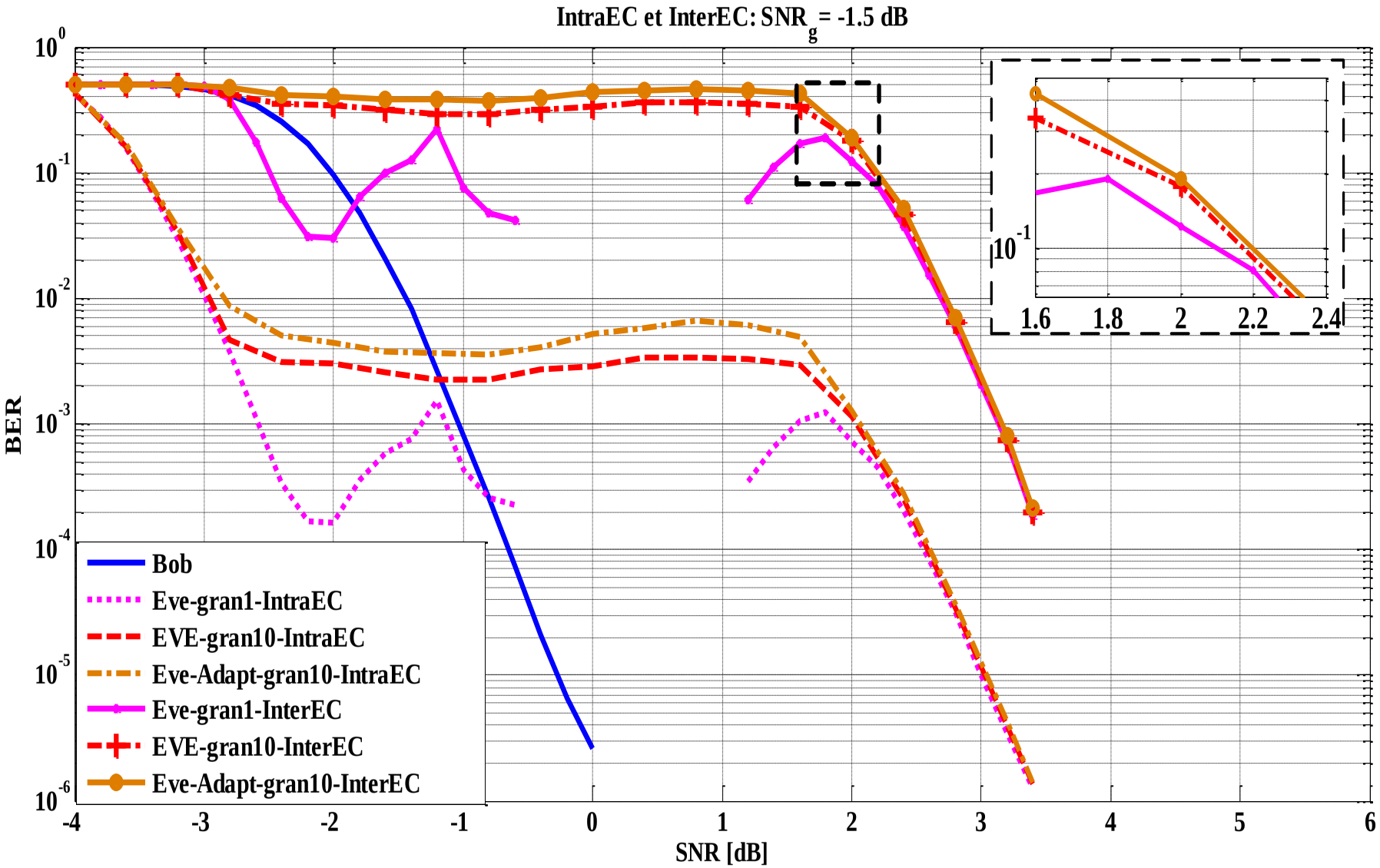


FIGURE 4.14 – Taux d'erreur de trame pour le canal légitime (Bob) et le canal espion (Eve) : $SNR_g = -1.5$ dB.

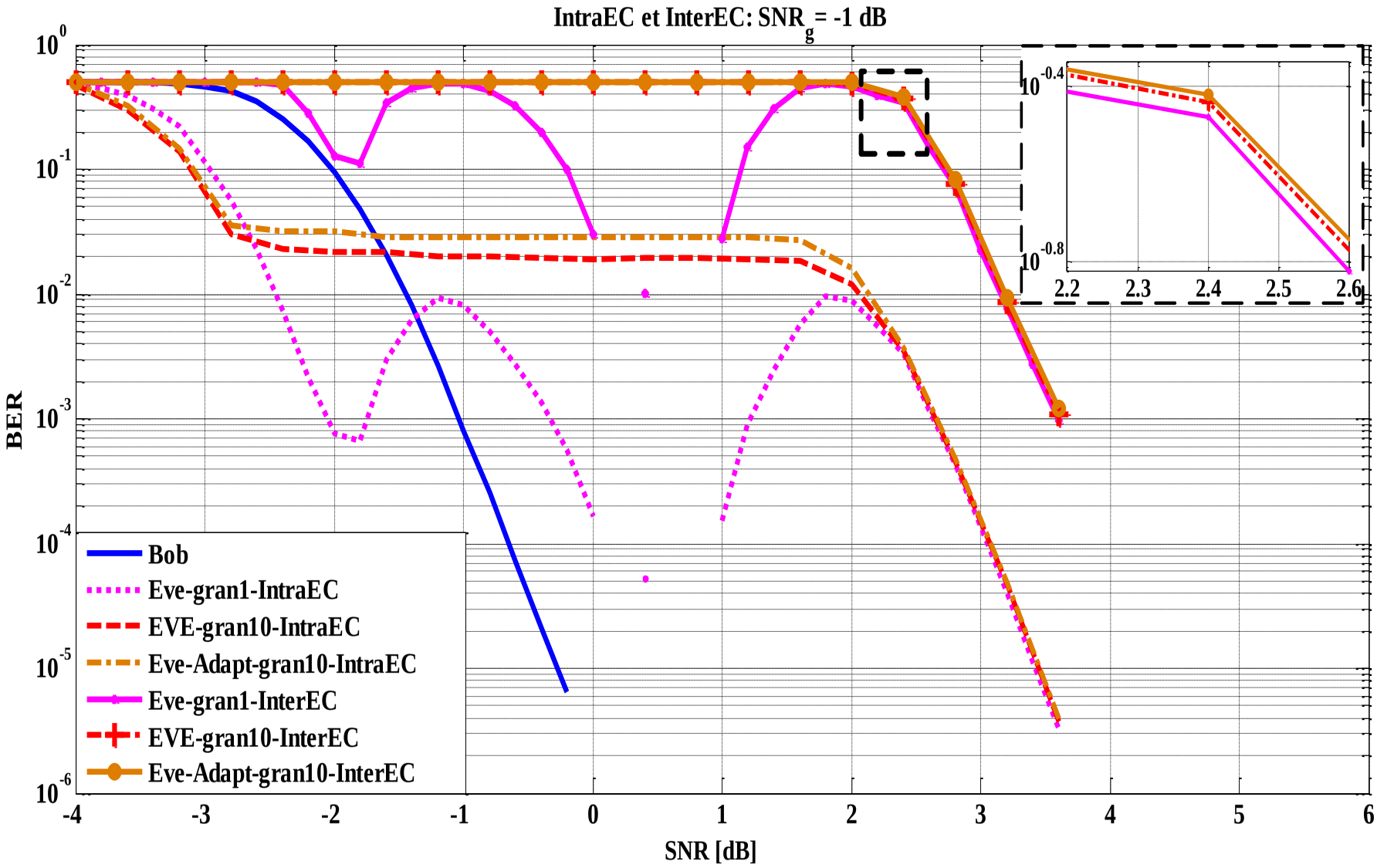


FIGURE 4.15 – Taux d'erreur de trame pour le canal légitime (Bob) et le canal espion (Eve) : $SNR_g = -1$ dB.

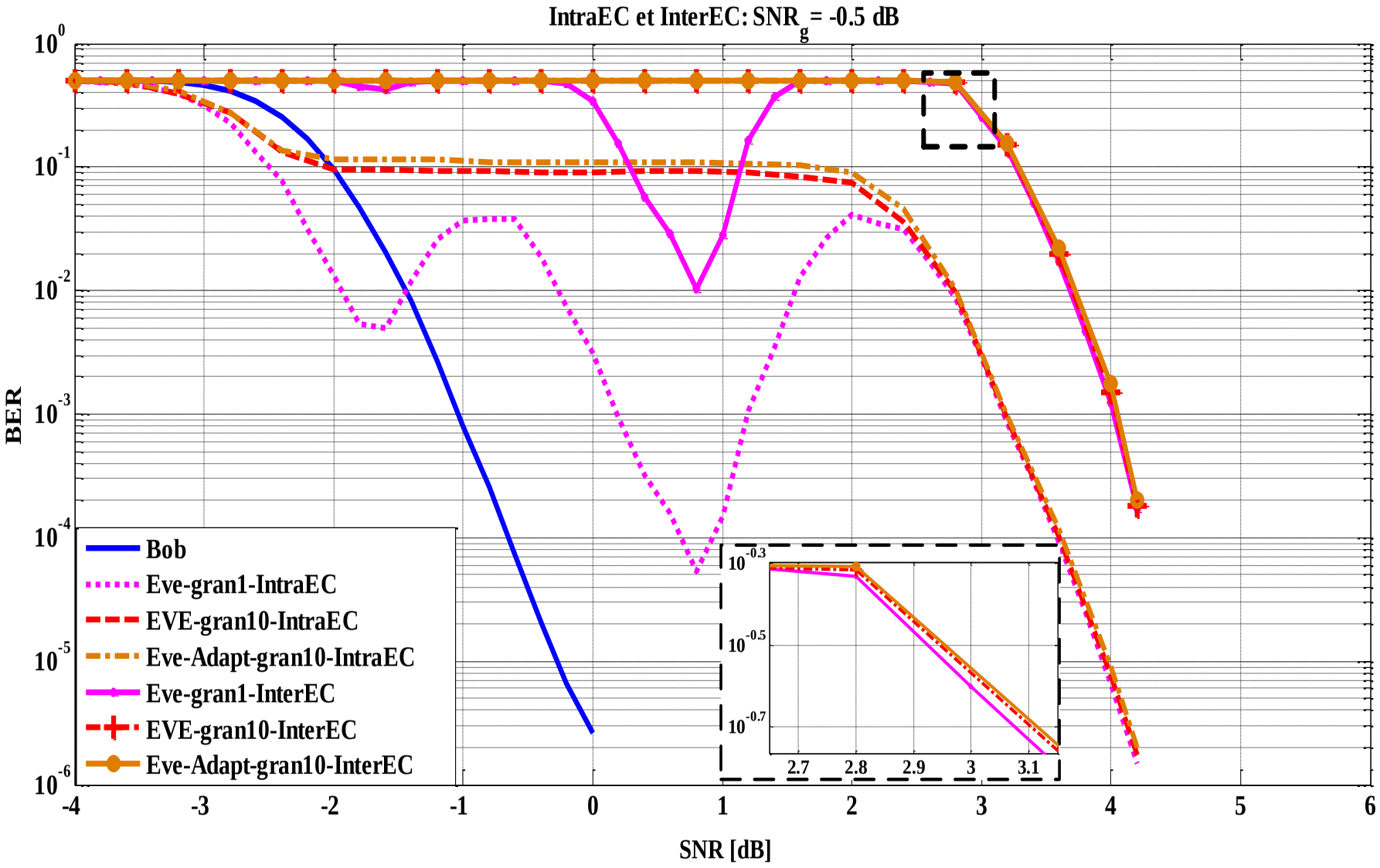


FIGURE 4.16 – Taux d'erreur de trame pour le canal légitime (Bob) et le canal espion (Eve) : $SNR_g = -0.5$ dB.

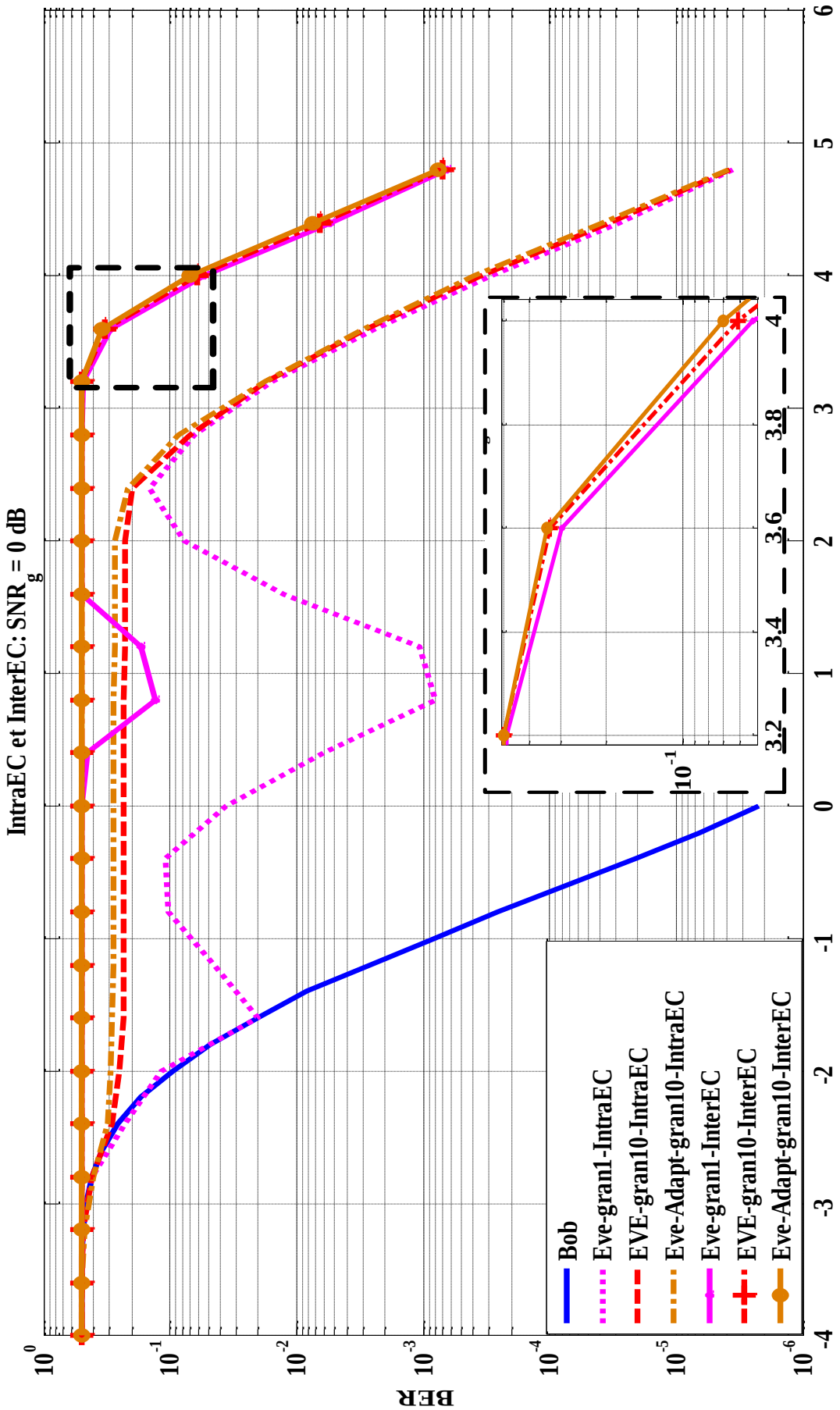


FIGURE 4.17 – Taux d'erreur de trame pour le canal légitime (Bob) et le canal espion (Eve) : $SNR_g = 0$ dB.

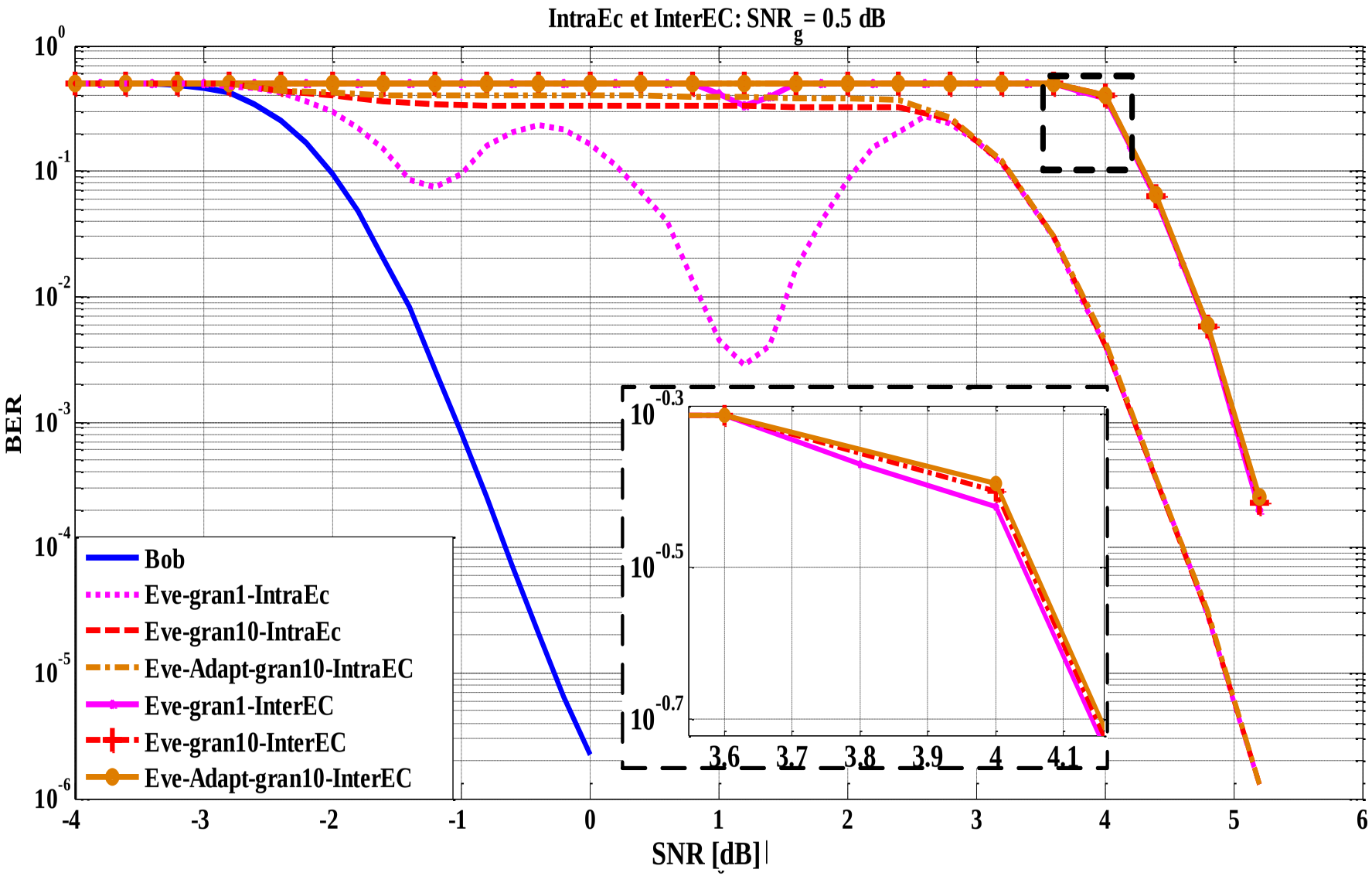


FIGURE 4.18 – Taux d'erreur de trame pour le canal légitime (Bob) et le canal espion (Eve) : $SNR_g = 0.5$ dB.

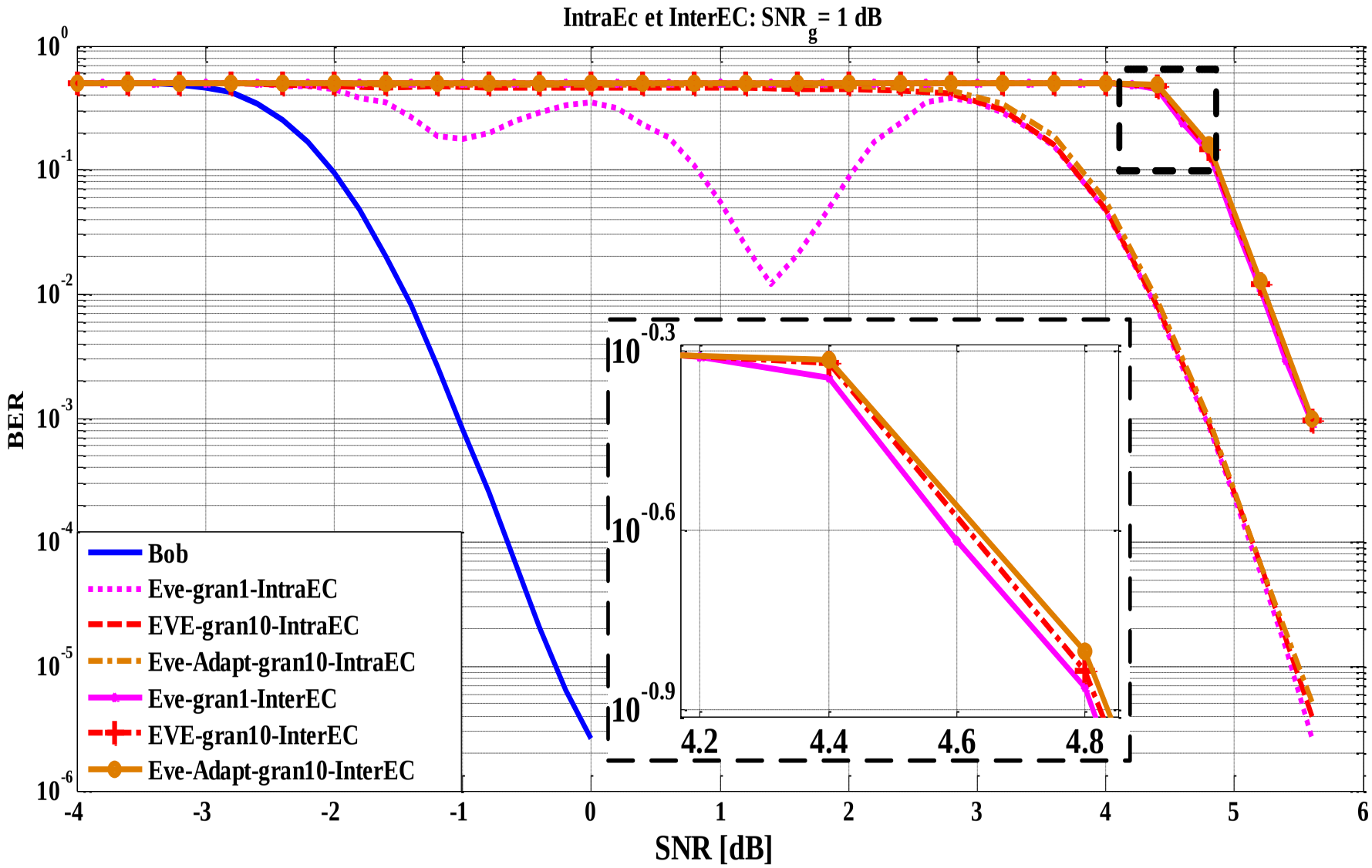


FIGURE 4.19 – Taux d'erreur de trame pour le canal légitime (Bob) et le canal espion (Eve) : $SNR_g = 1$ dB.

Chapitre 5

Conclusion

5.1 Sommaire

Pour assurer des communications sécurisées et fiable sur les canaux avec écoute gaussien à la couche physique, deux aspects doivent être pris en compte en même temps : le premier est de transmettre des informations avec une haute fiabilité au récepteur légitime, tandis que le deuxième est de cacher cette information à l'espion. Dans ce mémoire, afin de concevoir des systèmes de communication fiable, les codes LDPC ont été considérés et un nouveau mécanisme pour concevoir des ensembles de code LDPC irréguliers approchant la capacité du canal a été étudiée. En outre, afin de concevoir des systèmes de communication sécurisés, les concepts de granularité et LLR du sous-paquet ($\hat{C}_j$) sont été combinées avec la contamination d'erreur intra-trame et inter-trame.

5.2 Contributions

Au chapitre 3, nous avons introduit le taux optimal et l'approche capacitive des ensembles de codes LDPC irréguliers sur BEC en utilisant la combinaison GA et LP. La méthode proposée cherche à minimiser l'écart multiplicatif δ par itération entre l'optimisation de la distribution de degrés de nœuds de variables à l'aide de GA et l'optimisation de la distribution de degrés de nœuds de parité en utilisant LP.
Les résultats de la simulation montrent l'avantage de la méthode proposée alors que la majorité des critères de conception de codes mentionnés à la section 3.2 a été améliorée, mais au coût d'un modèle plus complexe pour la distribution des degrés de nœuds de parité (critère 1). Ce choix donne la flexibilité de rechercher les meilleures distributions de degrés de nœuds de parité. En outre, en utilisant cette approche, on peut atteindre des ensembles de degrés souhaitables en utilisant moins d'itérations. Les résultats correspondant à cette section ont été publiés dans [77].

L'une des principales difficultés dans les systèmes de communication sans fil est d'assurer la sécurité et la fiabilité en même temps. Au chapitre 4, le modèle du canal à écoute gaussien a été considéré pour la conception d'un système visant à transmettre des informations fiables au récepteur légitime en

cachant cette information à l'espion. Dans le procédé proposé, la méthode HARQ a été modifiée. Dans le cas d'une requête de Bob, au lieu de retransmettre le paquet entier ou d'envoyer des sous-paquets de manière aléatoire comme dans la méthode G-HARQ, Bob demande la retransmission de sous-paquets spécifiques qui ont la plus valeur faible absolue du LLR. Le protocole AG-HARQ proposé essaie de réduire le taux de transmission requis pour les parties légitimes pour un décodage réussi tout en minimisant les fuites d'informations à un espion. De plus, le AG-HARQ a besoin d'un moins grand nombre de requêtes de retransmission en comparaison avec le G-HARQ parce qu'il sélectionne de manière adaptative les sous-paquets nécessaires en cas d'échec. Même quand la qualité du canal de l'espion est meilleure que celle du canal principal, les résultats des simulations montrent l'efficacité de la méthode proposée. Ce travail a fait l'objet de l'article de correspondance [78].

5.3 Suggestions de travaux futurs

Les recherches futures correspondant au chapitre 3 pourraient être les suivantes : a) développer la méthodologie actuelle GA-LP pour déterminer la capacité à atteindre pour les codes LDPC irréguliers sur les autres canaux existants comme BSC, AWGN, etc ; b) mesurer à quel point les codes conçus sont valides dans la pratique en comparant les BERs par rapport SNRs d'un scénario réaliste avec d'autres méthodes de conception.

Les recherches futures correspondant au chapitre 4 pourraient être les suivantes : dans la méthode AG-HARQ proposée, il est supposé que le canal de rétroaction est idéal. On peut se demander comment la performance du système sera affectée si l'on considère un canal de rétroaction plus réaliste et qu'elle pourrait être la procédure pour traiter ce problème. Dans les méthodes G-HARQ et AG-HARQ proposées, il n'y a pas de mécanisme pour choisir précisément les valeurs de granularités (g). Ce choix dépend de la structure de graphe de Tanner des codes LDPC, ce qui pourrait être un sujet intéressant pour des travaux futurs. Les méthodes de codage securitaire G-HARQ et AG-HARQ peuvent être mis en œuvre dans la pratique sur FPGAs ou d'autres périphériques disponibles. Dans le cas de la méthode de contamination par erreur intra- et inter-trames, la construction de brouilleur (désembrouilleur) n'est pas une tâche facile ; une recherche plus approprié peut être effectuée sur la façon dont ces matrices peuvent être construites.

Bibliographie

[1] C. E. Shannon, “A mathematical theory of communication,” *Bell System Technical Journal*, vol. 27, pp. 379–423, 623–656, juillet et octobre 1948.

[2] H. Tavakoli, M. Ahmadian Attari, et M. R. Peyghami, “Optimal Rate for Irregular LDPC Codes in Binary Erasure Channel,” *IEEE Information Theory Workshop*, pp. 16–20, 2011.

[3] M. H. Taieb et J-Y. Chouinard, “Reliable and Secure Communications over Gaussian Wiretap Channel Using HARQ LDPC Codes and Error Contamination,” *IEEE Conference on Communications and Network Security, IEEE CNS*, pp. 669–674, 2015.

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

[5] C. M. Nicola, *Decoding of LDPC Codes over Channels with Binary Additive Markov Noise*. Université Queen, Kingston, Ontario, Canada, septembre 2005.

[6] R. W. Hamming, “Error detecting and error correcting codes,” *Bell System Technical Journal*, vol. 29, pp. 147–150, 1950.

[7] M. J. E. Golay, “Notes on digital coding,” *Proceedings of the IRE*, vol. 37, p. 657, 1949.

[8] I. S. Reed, “A class of multiple-error-correcting codes and the decoding scheme,” *Transactions of the IRE Professional Group on Information Theory*, vol. 4, pp. 38–49, 1954.

[9] D. E. Muller, “Application of boolean algebra to switching circuit design and to error detection,” *IRE Transactions on Electronic Computers*, vol. 3, pp. 6–12, 1954.

[10] I. S. Reed et X. Chen, *Error-Control Coding for Data Networks*. Kluwer Academic Publishers, 1999. Boston, Etats-Unis.

[11] A. Hocquenghem, “Codes correcteurs d’erreurs,” *Chiffres*, vol. 2, pp. 147–156, Septembre 1959.

[12] R. C. Bose et D. K. Ray-Chaudhuri, “On A Class of Error Correcting Binary Group Codes,” *Information and Control*, vol. 3, pp. 68–79, mars 1960.

[13] I. S. Reed et G. Solomon, “Journal of the Society for Industrial and Applied Mathematics,” *Information and Control*, vol. 8, no. 2, pp. 300–304, 1960.

[14] R. J. McEliece et W. Lin, “The trellis complexity of convolutional codes,” *IEEE Transactions on Information Theory*, vol. 42, pp. 1855–1864, 1996.

[15] C. Berrou, A. Glavieux, et P. Thitimajshima, “Near Shannon limit error correcting coding and decoding,” *In Proceedings of ICC*, pp. 1064–1070, mai 1993.

[16] T. Richardson, A. Shokrollahi, et R. Urbanke, “Design of capacity approaching irregular low-density parity-check codes,” *IEEE Transactions on Information Theory*, pp. 619–637, février 2001.

[17] R. G. Gallager, *Low-Density Parity-Check Codes*. MIT Press, 1963.

[18] D. J. C. MacKay et R. M. Neal, “Near Shannon limit performance of low density parity check codes,” *Electronics Letters*, vol. 32, pp. 1645–1646, 1996.

[19] D. MacKay, “Good error correcting codes based on very sparse matrices,” *IEEE Transactions on Information Theory*, vol. 45, pp. 399–431, mai 1999.

[20] D. MacKay et R. Neal, “Near shannon limit performance of low density parity check codes,” *Electronic Letters*, vol. 32, pp. 1645–1646, 1996.

[21] M. Sipser et D. Spielman, “Expander codes,” *IEEE Transactions on Information Theory*, vol. 42, no. 6, pp. 1710–1722, 1996.

[22] D. Spielman, “Linear-time encodable and decodable error-correcting codes,” *IEEE Transactions on Information Theory*, vol. 42, no. 6, pp. 1723–1732, 1996.

[23] M. Luby, M. Mitzenmacher, A. Shokrollahi, et D. Spielman, “Efficient erasure correcting codes,” *IEEE Transactions on Information Theory*, vol. 47, pp. 569–584, 2001.

[24] M. Luby, M. Mitzenmacher, A. Shokrollahi, et D. Spielman, “Improved low-density parity-check codes using irregular graphs,” *IEEE Transactions on Information Theory*, vol. 47, pp. 585–598, juillet et octobre 2001.

[25] R. M. Tanner, “A recursive approach to low complexity codes,” *IEEE Transactions on Information Theory*, vol. 27, pp. 533–547, septembre 1981.

[26] F. R. Kschischang, B. J. Frey, et H. A. Loeliger, “Factor graphs and the sum product algorithm,” *IEEE Transactions on Information Theory*, vol. 47, pp. 498–519, février 2001.

[27] N. Wiberg, “Codes and Decoding on General Graphs,” *Thèse de doctorat*, 1996.

[28] N. Wiberg, H. A. Loeliger, et R. Kotter, “Codes and iterative decoding on general graphs,” *European Transactions on Telecommuncations*, vol. 6, pp. 513–526, 1995.

[29] T. Richardson et R. Urbanke, *Modern Coding Theory*. Cambridge University Press, 2008.

[30] M. Luby, M. Mitzenmacher, A. Shokrollahi, et D. Spielman, “Analysis of low density codes and improved designs using irregular graphs,” *in Proceeding of 30th Annual ACM Symposium in Theory of Computing*, pp. 249–258, 1998.

[31] M. Luby, M. Mitzenmacher, A. Shokrollahi, et D. A. Spielman, "Efficient erasure correcting codes," *IEEE Transactions on Information Theory*, vol. 47, pp. 569–584, 2001.

[32] M. Luby, M. Mitzenmacher, A. Shokrollahi, et D. Spielman, "Practical loss-resilient codes," *in Proceeding of 29th Annual ACM Symposium in Theory of Computing*, pp. 150–159, 1997.

[33] T. Richardson et R. Urbanke, "The capacity of LDPC codes under message-passing decoding," *IEEE Transactions on Information Theory*, vol. 47, pp. 599–618, février 2001.

[34] S.-Y. Chung, T. J. Richardson, et R. L. Urbanke, "Analysis of Sum-Product Decoding of Low-Density Parity-Check Codes Using a Gaussian Approximation," *IEEE Transactions on Information Theory*, vol. 47, pp. 657 – 670, février 2001.

[35] T. K. Moon, *Error Correction Coding : Mathematical Methods and Algorithms*. Upper Saddle River, NJ 07458 : Prentice-Hall, Inc., 2005.

[36] J. Pearl, *Probabilistic Reasoning in Intelligent Systems : Networks of Plausible Inference*. Morgan Kaufman, 1988.

[37] A. W. Eckford, *Low-Density Parity-Check Codes for Gilbert-Elliot and Markov-Modulated Channels*. Doctorat thèse, Université de Toronto, 2004.

[38] Y. Jiang, *A Practical Guide to Error-Control Coding Using MATLAB*. Artech House, 2010.

[39] R. G. Gallager, "Low density parity check codes," *IEEE Transactions on Information Theory*, vol. 8, pp. 21–28, janvier 1962.

[40] B. M. Kurkoski, K. Yamaguchi, et K. Kobayashi, "Density Evolution for GF(q) LDPC Codes Via Simplified Message-passing Sets." Information Theory and Applications Workshop, 2007.

[41] W. E. Ryan et S. Lin, *Channel codes : classical and modern*. Cambridge ; New York : Cambridge University Press, 2009.

[42] H. Saeedi et A. H. Banihashemi, "Systematic design of Low-Density-Parity-Check code ensembles for binary erasure channels," *IEEE Transactions on Information Theory*, pp. 118–127, janvier 2010.

[43] A. Shokrollahi, "Capacity-achieving sequences," *IMA Volume in Mathematics and its Applications*, vol. 123, pp. 153–166, 2000.

[44] P. Oswald et A. Shokrollahi, "Capacity-achieving sequences for the erasure channel," *IEEE Transactions on Information Theory*, vol. 48, pp. 3017–3028, décembre 2002.

[45] A. Shokrollahi, "New sequences of linear time erasure codes approaching the channel capacity," *in Proceedings of 13th of ISAA*, no. 1719, pp. 65–76, 1999.

[46] D. Proietti, I. E. Telatar, T. J. Richardson, et R. L. Urbanke, "Finite-length analysis of low-density parity-check codes on the binary erasure channel," *IEEE Transactions on Information Theory*, vol. 48, pp. 1570–1579, juin 2002.

[47] T. Richardson, A. Shokrollahi, et R. Urbanke, “Finite-length analysis of various low-density parity check ensembles for the binary erasure channel,” *in Proceedings of IEEE International Symposium in Information Theory*, pp. 1–1, juillet 2002. Suisse, Europe.

[48] I. Sason et R. Urbanke, “Parity-check density versus performance of binary linear block codes over memoryless symmetric channels,” *IEEE Transactions on Information Theory*, vol. 49, pp. 1611–1635, juillet 2003.

[49] H. Saeedi et A. H. Banihashemi, “New sequences of capacity achieving LDPC code ensembles over the binary erasure channel,” *IEEE International Symposium on Information Theory*, juillet 2008.

[50] G. Lechner, J. Sayir, et I. Land, “Optimization of LDPC Codes for Receiver Frontends,” *IEEE International Symposium on Information Theory*, pp. 2388–2392, juillet 2006.

[51] M. Bloch et J. Barros, *Physical-Layer Security : From Information Theory to Security Engineering*. Royaume-Uni : Cambridge University Press, 2011.

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

[53] O. O. Koyluoglu et H. El Gamal, “Polar coding for secure transmission and key agreement,” *in Proc. IEEE Int. Symp. Personal Indoor and Mobile Radio Comm*, pp. 2698–2703, 2010. Istanbul, Turquie.

[54] M. Bloch, *Physical-Layer Security*. PhD thesis, School of Electrical and Computer Engineering Georgia Institute of Technology, 2008.

[55] H. Mahdavifar et A. Vardy, “Achieving the secrecy capacity of wiretap channels using polar codes,” *IEEE Transactions on Information Theory*, vol. 57, pp. 6428–6443, octobre 2011.

[56] M. Cheraghchi, F. Didier, et A. Shokrollahi, “Invertible extractors and wiretap protocols,” *IEEE Transactions on Information Theory*, vol. 58, pp. 1254–1274, février 2012.

[57] R. C. Merkle, “Secure communications over insecure channels,” *Communications of the ACM*, vol. 21, pp. 294–299, avril 1978.

[58] W. Diffie et M. E. Hellman, “New directions in crytography,” *IEEE Transactions on Information Theory*, vol. 22, pp. 644–654, novembre 1976.

[59] S. K. Leung-Yan-Cheong, “On a special class of wiretap channels,” *IEEE Transactions on Information Theory*, vol. 23, pp. 625–627, septembre 1977.

[60] J. L. Massey, “A simplified treatment of Wyner’s wiretap channel,” *Proceedings of 21st Annual Allerton Conference on Communication, Control, and Computing*, pp. 268–276, octobre 1983.

[61] I. Csiszar et J. Korner, “Broadcast channels with confidential messages,” *IEEE Transactions on Information Theory*, vol. 24, pp. 339–348, mai 1978.

[62] K. Yausi, T. Suko, et T. Matsushima, “An algorithm for computing the secrecy capacity of broadcast channels with confidential messages,” *In Proceedings of IEEE International Symposium on Information Theory*, pp. 936–940, juillet 2007.

[63] S. K. Leung-Yan-Cheong et M. E. Hellman, “The Gaussian wiretap channels,” *IEEE Transactions on Information Theory*, vol. 24, pp. 451–456, septembre 1978.

[64] Y. Liang et H. V. Poor, “Secure communication over fading channels,” *in Proceedings of the 44th Annual Allerton Conference on Communication, Control and Computing*, septembre 2006. Monticello, IL, États-Unis.

[65] M. Bloch et J. Barros, *Physical Layer Security From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[66] L. Lai, H. El Gamal, et H. V. Poor, “The Wiretap Channel With Feedback : Encryption Over the Channel,” *IEEE Transactions on Information Theory*, vol. 54, no. 11, pp. 5059–5067, 2008.

[67] S. K. Leung-Yan-Cheong, “Multi-User and Wire-Tap Channels Including Feedback,” *PhD thesis*, 1976. Stanford université, CA, Etats-Unis.

[68] U. M. Maurer, “Secret key agreement by public discussion from common information,” *IEEE Transactions on Information Theory*, vol. 39, pp. 733–742, mai 1993.

[69] R. Ahlswede et I. Csiszár, “Common randomness in information theory and cryptography, Part I : Secret sharing,” *IEEE Transactions on Information Theory*, vol. 39, pp. 1121–1132, juillet 1993.

[70] M. Baldi, M. Bianchi, et F. Chiaraluce, “Coding with Scrambling, Concatenation and HARQ for AWGN Wire-Tap Channel : A Security Gap Analysis,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 883–894, 2012.

[71] P. Elias, “Coding for two noisy channels,” *The 3rd London Symposium, Buttersworth’s Scientific Publications*, pp. 61–76, 1955.

[72] J. Hagenauer, “he EXIT chart—Introduction to extrinsic information transfer in iterative processing,” *12th European Signal Processing Conference (EUSIPCO)*, pp. 1541–1548, Sep 2004.

[73] T. V. Nguyen, *Design of capacity-approaching protograph-based LDPC coding systems*. PhD thesis, The University of Texas at Dallas, 2012.

[74] A. Orlitsky, R. Urbanke, K. Vishwanathan, et J. Zhang, “Stopping sets and the girth of Tanner graphs,” *In Proceedings of IEEE International Symposium on Information Theory*, pp. 2–2, juin et juillet 2002. Lausanne, Suisse.

[75] K. Demijan, H. Jeongseok, S. W. McLaughlin, et J. Barros, “LDPC Codes for Physical Layer Security,” *Proceedings of the 28th IEEE Conference on Global Telecommunications*, no. 6, pp. 5765–5770, 2009. Honolulu, Hawaii, États-Unis.

[76] M. H. Taieb et J-Y. Chouinard, "Reducing the Security Gap of the Gaussian Wiretap Channel using Rate Compatible LDPC Codes with Error Amplification," *14th Canadian Workshop on Information Theory*, pp. 41–45, 2015.

[77] A. Amirzadeh, M. A. Haji Bagheri Fard, M. H. Taieb, et J. -Y. Chouinard, "Multiplicative Gap Minimization Over BEC Channel Using Combined Genetic Algorithm and Linear Programming," *28th Biennial Symposium on Communications (BSC 2016)*, 5-8 juin 2016. Kelowna, British Columbia, Canada.

[78] A. Amirzadeh, M. H. Taieb, et J. -Y. Chouinard, "Adaptive Granular HARQ LDPC-Based Coding for Secrecy Enhancement in Wiretap Channels," *29th Annual IEEE Canadian Conference on Electrical and Computer Engineering(CCECE 2016)*, no. 15-18 mai, 2016. Vancouver, Canada.