Les codes à métrique de rang et leurs applications dans les réseaux Smart Grid

Abdul Karim Yazbek

UNIVERSITÉ DE LIMOGES

ÉCOLE DOCTORALE 521 :

Sciences et Ingénierie pour l'Information, Mathématiques

XLIM - Systèmes & réseaux intelligents

Année : 2017

Thèse

pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ DE LIMOGES

Discipline : Sciences et technologies de l'information et de la communication

présentée et soutenue par

Abdul Karim YAZBEK

le 05 décembre 2017

Les codes à métrique de rang et leurs applications dans les réseaux Smart Grid

Thèse dirigée par Jean-Pierre Cances et Vahid MEGHDADI

JURY :

Président :

Mme. Maryline HELARD	Professeur, INSA de Rennes

Rapporteurs :

M. Thierry CHONAVEL	Professeur, TELECOM Bretagne
Mme. Fatma ABDELKEFI	Maître de conférence - HDR, Sup'COM de Tunis

Examinateurs :

M. Yannis POUSSET	Professeur, Université de Poitiers
M. Jean-Pierre CANCES	Professeur, Université de Limoges
M. Vahid MEGDHADI	Professeur, Université de Limoges

« Quiconque aura la piété envers Dieu. Dieu donnera une issue pour lui et lui accordera ses subsistances d'où il ne s'attendait pas. Et quiconque met sa confiance en Dieu, il lui suffit. Certes, Dieu exécute ses ordres. Dieu a assigné à chaque chose un destin. »

À l'âme de mon père et à ma mère,

Remerciements

Je tiens à remercier tout d'abord mon directeur de recherches, Professeur Jean-Pierre CANCES, pour sa patience, et surtout pour sa confiance, sa disponibilité et sa bienveillance. Il m'a enseigné l'autonomie et m'a aidé au jour le jour à devenir un chercheur de qualité. Ensuite, je remercie également mon co-directeur de recherches Professeur Vahid MEGHDADI pour ses remarques, ses conseils et l'opportunité de donner des cours à l'ENSIL.

J'adresse aussi mes remerciements aux personnels de L'ENSIL et à mes collègues de Laboratoire, je nomme Imad pour ses aides scientifiques et mathématiques, et surtout les discussions qu'on a passé ensemble et l'amitié qu'il m'a apporté. Je pense aussi à Jérémy pour son aide de tous les jours.

Mes remerciements vont aussi à tous mes amis au Liban et en France, à ma famille, à mon frère et à mes sœurs en particulier Farah et Rana qui m'ont été d'un grand soutien tout au long de ma thèse.

Une pensée toute particulière à Safae qui a su trouver les mots, la patience et la passion pour me porter tout au long de la thèse et ainsi me rendre meilleur.

Table des matières

Table des figures

Liste des tableaux

Liste des acronymes :

AMM	Automated Meter Management
AMR	Automated Meter Reading
BBAG	Bruit Blanc Additif Gaussien
BSC	Binary Symmetric Channel
CENELEC	Comité Européen de Normalisation en Électronique
CPL-BE	Courant Porteur en Ligne à Bande Étroite
CPL-BUE	Courant Porteur en Ligne à Bande Ultra Étroite
CRC	Cyclic Redundancy Check
FCC	Federal Communications Commission
FEC	Forward Error Correction
FFT	Fast Fourrier Transform
HA	Home Automation
HAN	Home Area Network
LDPC	Low Parity Check Code
MAC	Medium Access Control
MAP	Maximum A Posteriori
PRIME	Powerline Related Intelligent Metering Evolution
RF	Radio Fréquence
RLNC	Random Linear Network Coding
RS	Reed-Solomon
RC	Rank Code
CC	Convolutionnal code
BER	Bit Error Rate (Taux d'Erreur Binaire)
SNR	Signal to Noise Ration (Rapport signal sur bruit)
SG	Smart Grid
LLR	Log-Likelihood Ratio (Rapport maximum à vraisemblance)
ReSyst	Réseaux et Systèmes de Télécommunications (Laboratoire XLIM)

Liste des symboles :

q	puissance d'un nombre premier.
$C(n,k)$	code en bloc de dimension k, de longueur n.
$\mathbb{F}_{q^m}$	le corps fini (corps de Galois) à q^m éléments.

Introduction générale

0.1 Contexte de l'étude

Élément incontournable dans notre vie quotidienne, les réseaux électriques offrent de l'énergie en continu provenant de sources de production diverses et variées comme les barrages hydroélectriques, les centrales nucléaires, etc. La tension électrique est distribuée dans le réseau afin qu'elle puisse servir chaque point du territoire couvert par le réseau. Le contrôle et le monitoring en temps réel de cette distribution au niveau des régions et de chaque foyer nécessitent une architecture permettant d'accéder à chaque point du réseau et ce, dans le but de collecter les informations nécessaires pour exécuter ces tâches de soutien comme l'augmentation de tension et la coupure d'alimentation lorsque nécessaire. Dans les réseaux actuels, ces opérations de contrôle et de monitoring sont effectuées en envoyant des agents sur terrain pour prélever la consommation des foyers et la suspension de service. La variété des ressources énergétiques et l'augmentation du nombre d'utilisateurs et de leurs consommations ont motivé l'introduction d'un autre type de réseaux électriques appelés : Réseaux électriques intelligents (Smart grids). Un réseau intelligent permet le greffage des technologies de l'information et de la communication sur le réseau de distribution de l'électricité dans le but d'économiser l'énergie, réduire les coûts et améliorer sa fiabilité et sa disponibilité. L'évolution des technologies intègre de nouveaux éléments matériels et logiciels au niveau des foyers afin de faciliter les tâches de commandes et de monitoring. Une nouvelle génération de compteurs sera installée au niveau des foyers. II s'agit de compteurs intelligents (Smart meters). Ces compteurs communiquent en temps réel avec des centres de contrôle. Ils permettent de mesurer la consommation énergétique des foyers ou des appareils électriques et électroménagers auxquels ils sont connectés. Une composante indispensable de ce futur système est appelée « Infrastructure avancée de comptage » (AMI), qui devrait fournir des communications bidirectionnelles permettant aux services publics de ne pas seulement garder une trace de la consommation de l'électricité, mais aussi d'informer les consommateurs des derniers prix de l'électricité et d'effectuer la gestion des services à distance, le tout, en temps réel.

Les support physiques de transmission sont primordiaux pour implémenter un réseau électrique intelligent. Il existe plusieurs technologies de communication sans fil et filaires qui pourront être utilisées dans les smart grid tels que la radiodiffusion, les communications micro-ondes, l'accès internet, les satellite de télécommunications, le WiFi, la fibre optique, Bluetooth, les Courants Porteurs en Ligne (CPL)...

Les communication par Courant Porteur en Ligne (CPL) permettent de faire face aux mutations du paysage énergétique et de moderniser le réseau électrique. Ce type de communication CPL consiste à utiliser le réseau électrique pour transmettre des informations. Il s'appuie sur les câbles électriques comme canal de propagation du signal. Grâce aux techniques de modulation, les ingénieurs sont parvenus à faire cohabiter le

courant électrique de basse fréquence (50 Hz) avec des données transmises sur une bande comprise entre 1 et 30 MHz (de $4,3$ à $20,9$ MHz concernant le Home Plug, le standard le plus répandu, développé pour la domotique). Les prises de courant sont présentes partout, quel que soit le type de locaux, privés ou publics. Plus largement, le réseau électrique constitue une infrastructure qui couvre presque tout le territoire, même les zones les moins denses en population d'où l'importance du CPL qui permet un accès généralisé à Internet.

Cependant, comme pour chaque canal de communication, le bruit peut réduire la performance du système de transmission et dégrade la puissance du signal à transmettre. En effet, le canal CPL est affecté par plusieurs limitations telles qu'une sélectivité en temps et en fréquence et un bruit non Gaussien [1] généré par : des bruits de fond, des bruits à bande étroite (BE) et des bruits impulsifs. Notons que les communications CPL-BE s'adaptent à tous les standards [2]. Ces types de bruit diminuent la performance des informations propagées durant la communication d'où la nécessité de proposer des techniques de codage correcteur d'erreurs pour faire face aux perturbations sur le réseau électrique. C'est dans ce contexte que s'inscrivent les travaux de cette thèse.

0.2 Objectif de la thèse

Dans cette thèse, nous allons étudier des codes correcteurs d'erreurs qui peuvent améliorer la qualité de transmission afin d'avoir une communication plus fiable sur un canal bruité. En outre, nous allons proposer une nouvelle construction d'un code correcteur d'erreur appelé LRPC (Low Rank Parity Check) qui sera appliqué dans un canal CPL-BE.

Le principe de fonctionnement des systèmes CPL est simple et consiste à superposer deux signaux : le signal du réseau électrique (50 KHz) et le signal d'information à transmettre ($1 - 30$ MHz). Ces signaux sont présentés dans la figure ci-dessous :

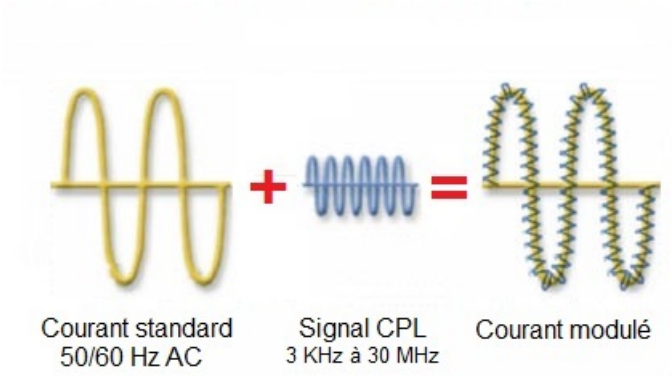


FIGURE 1 – Principe de fonctionnement CPL

D'autre part, le codage réseau constitue une solution intéressante dans le contexte CPL en raison du flux de données transmis et de la grande taille des réseaux CPL-BE.

0.3 Organisation de la thèse

Le manuscrit s'organise en trois chapitres :

- Le premier chapitre présente nos recherches bibliographiques sur le réseau CPL avec sa structure technologique et ses contraintes physiques. Ainsi, la communication CPL-BE pour le smart grid est présenté avec ses défis. Ces recherches permettent d'évaluer nos codes correcteurs d'erreurs utilisés et le niveau d'exigence de performances pour lesquelles ils sont utilisés. Il permet également de positionner notre travail.

- Le deuxième chapitre introduit les codes correcteurs d'erreurs qui peuvent être utilisés afin de faire face aux différents types d'erreurs produits dans le réseau CPL. Nous mettons en œuvre principalement le code à métrique rang appelé LRPC proposé avec sa construction introduite dans ce chapitre.

- Nous exposons dans la première partie du troisième chapitre, un schéma conventionnel selon la norme G3-PLC tout en implémentant un nouveau système codage-décodage afin d'augmenter la performance de la communication sur le réseau CPL et de corriger les motifs d'erreurs du type criss-cross. Cette chaine de transmission comprend deux codes correcteurs d'erreurs concaténés suivies d'une modulation BPSK et puis d'une modulation OFDM. Ensuite, nous comparons le taux d'erreur binaire en fonction du rapport signal sur bruit entre les différents systèmes de codage-décodage.
  Dans la deuxième partie, nous testons ces codes correcteurs d'erreurs dans un canal sélectif en fréquence perturbé avec des bruits impulsifs réels mesurés expérimentalement dans une station électrique au canada (Québec). Nous présentons ensuite les performances du schéma proposé dans un environnement de simulation réaliste.
  Enfin, nous faisons une combinaison entre le code LRPC et le codage réseau pour le réseau CPL et nous montrons les résultats de simulation afin d'évaluer la performance de cette technique.

Finalement, nous présentons une conclusion générale de notre travail et les perspectives de ce travail de thèse.

Chapitre 1 :

Courants Porteurs en Ligne : Principes, normes et applications au Smart Grid (SG)

1.1 Introduction

Le réseau CPL est une technologie qui permet d'utiliser les infrastructures électriques existantes pour transmettre des données hautes fréquences pour différentes applications, par exemple, des réseaux domestiques ou entre des véhicules, en couplant des signaux radio fréquence (RF) sur la ligne électrique. Le réseau CPL peut être classé selon ses fréquences de fonctionnement : Ultra-bande étroite (30 Hz- 3 KHz), Bande étroite (BE) (3-500 kHz) et Broadband (1.8-250 MHz) [24]. Les systèmes CPL présentent de nombreux avantages par rapport aux autres technologies de communication filaire et sans fil. Le premier avantage est que les systèmes CPL fournissent un accès disponible à Internet dans n'importe quel endroit où il y a une prise électrique de courant alternatif (AC), sans la nécessité d'installations supplémentaires. Dans la plupart des cas, la construction d'un réseau de communication utilisant le câblage électrique AC existant est facile à installer et très rentable. Un autre avantage potentiel de la technique CPL est la possibilité de son utilisation pour les applications de réseau intelligent (Smart Grid) car il pourrait offrir la possibilité de contrôler à distance les appareils sans installations supplémentaires [3]. Ce chapitre présente un bref historique de la technologie CPL. En effet, une compréhension de base des principales caractéristiques des systèmes CPL est nécessaire pour l'étude et le développement de nouvelles techniques de correction d'erreurs afin d'améliorer la qualité de transmission. Le développement historique et les progrès actuels dans la technologie CPL sont d'abord décrits. Ensuite, après une brève description de la structure de réseau CPL d'intérieur typique, des informations relatives à la normalisation CPL sont données. Les principales techniques de transmission exploitées par les systèmes CPL et la modélisation des canaux CPL et du bruit sont également fournies. Enfin, une conclusion est donnée dans la dernière section.

1.2 Histoire de la technologie CPL

En premier lieu, les premières applications utilisant la transmission sur les lignes électriques ont été faites pour le contrôle, la ligne de protection, de maintenance et de charge [4]. Par la suite, plusieurs facteurs ont fait du CPL une technologie opérationnelle pour de nombreuses autres applications. Les premiers brevets dans ce domaine remontent au début des années 1900 [5]. En 1913, des répéteurs automatiques de compteurs électromécaniques ont été produits et en 1922, le CPL à bande étroite (CPL-BE) a commencé lorsque les premiers systèmes à fréquence porteuse ont commencé à fonctionner sur des lignes à haute tension dans la gamme de fréquence de 15 à 500 kHz pour des applications de télémétrie. Les études sur les systèmes CPL se sont améliorées et ont gagné en popularité au cours des deux dernières décennies, à mesure que de nouvelles techniques

de modulation et de contrôle des erreurs ont été proposées, ainsi que de nouvelles normes émanant d'alliances industrielles et d'organismes de normalisation. Aujourd'hui, les nouvelles technologies de CPL deviennent prometteuses tant pour les consommateurs que pour les fournisseurs d'énergie. Par conséquent, l'intérêt pour CPL couvre plusieurs applications importantes telles que l'accès Internet haut débit, les applications Smart Grid (mesure et contrôle avancés, prix de l'énergie en temps réel, surveillance du secteur, production d'énergie distribuée, etc.) (LAN) pour les locaux résidentiels et commerciaux, le contrôle de l'éclairage des rues...

1.3 Structure CPL dans l'environnement Indoor

En France, le développement des CPL à l'intérieur des bâtiments n'est soumis à aucune contrainte. La seule limitation est de ne pas créer de bruit par interférence. Pour ce marché indoor, la situation est claire : le Home Plug, norme pour la domotique développée par le consortium Home Plug Power Line Alliance, domine le marché. Les modems CPL établissent un pont entre le matériel informatique et le réseau électrique, comme le ferait un modem analogique entre l'ordinateur et la ligne téléphonique. Dans le cas d'une connexion Internet, le signal provenant de la Toile est récupéré par le routeur CPL puis injecté dans le réseau électrique. N'importe quel ordinateur muni d'un modem CPL peut ainsi accéder à Internet, quelle que soit la prise électrique utilisée, dans la limite des prises gérées par le même compteur électrique. Voici quelques exemples des adaptateurs CPL dans la figure ci-dessous qui sont indispensables pour réaliser un réseau CPL.

(a) RJ-45 (b) USB

FIGURE 1.1 – Adaptateur CPL

Les différents parties d'une structure typique de la topologie d'un réseau électrique européen sont présentés dans la figure 1.2. Nous nous concentrerons dans cette thèse sur la partie du réseau indoor et les différents types de bruit présents.

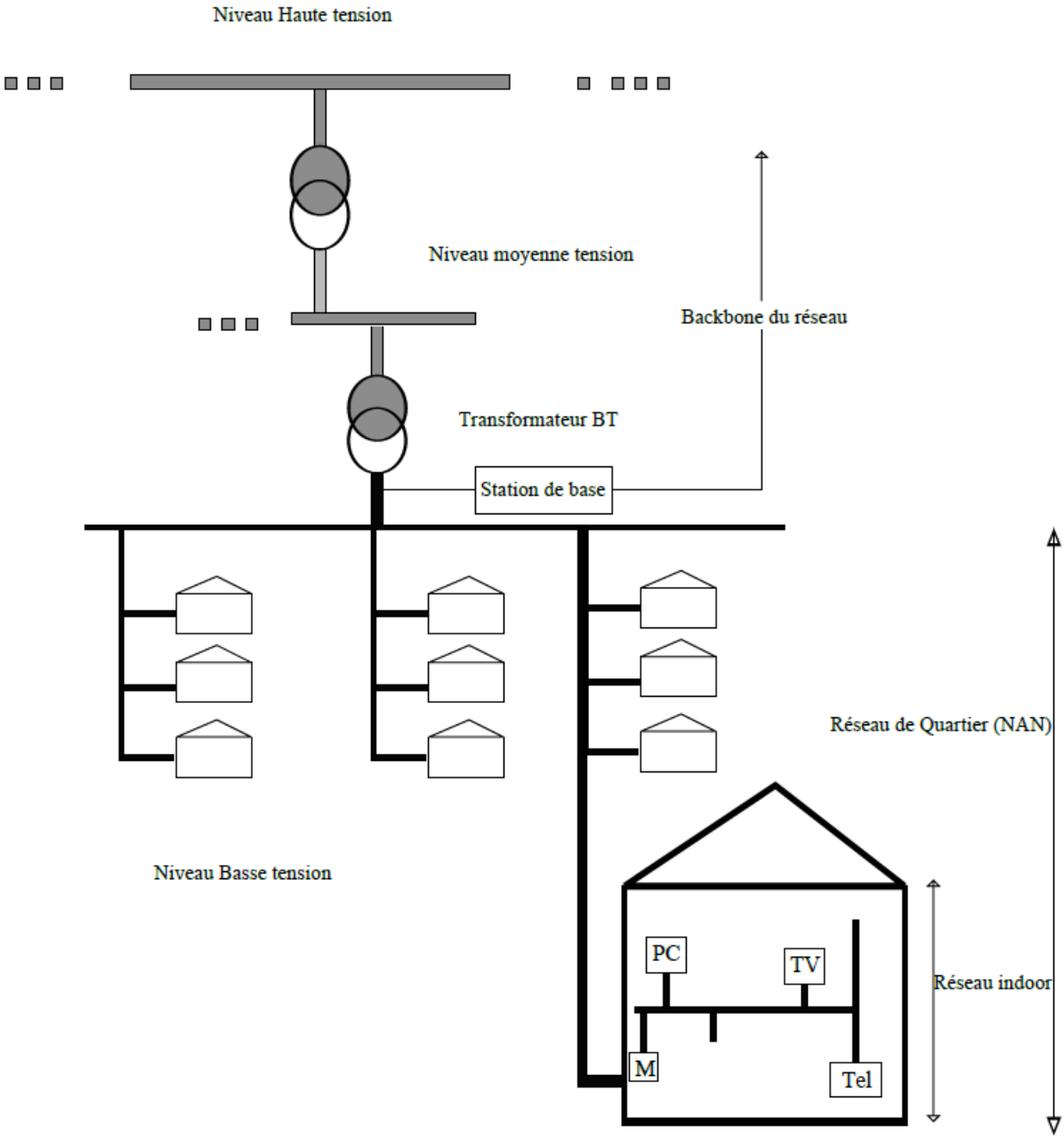


FIGURE 1.2 – Un diagramme de la structure typique d'un réseau électrique européen

1.4 Le réseau CPL-BE pour le Smart Grid (SG)

1.4.1 Caractéristiques du canal

L'utilisation de l'électricité par les consommateurs engendre une variation imprévisible et indépendante des impédances ce qui provoque des perturbations du canal. En outre, le bruit et la réponse fréquentielle ont un comportement cyclo-stationnaire en temps [6].

Autrement dit, le bruit dans le canal dépend de l'amplitude instantanée de la tension du réseau due aux variations synchrones à la fréquence du secteur car les paramètres hautes fréquences des objets connectés au réseau varient aussi en fonction de l'amplitude instantanée de la tension du réseau. Ensuite, le canal CPL est symétrique, cette propriété est vérifiée par [7-8]. Les canaux CPL-BE dépendent aussi des modes de câblage, de la topologie et de la densité des charges connectées au réseau électrique.

1.4.2 Modélisation du canal CPL-BE

Dans cette partie nous allons présenter le comportement du canal CPL-BE selon deux approches différentes :

- Modèle paramétrique de l'évanouissement multi-trajets
- Méthodes standards de la théorie des lignes de transmission

La première approche, appelée aussi "top-down", présentée par une fonction de transfert consiste à calculer le nombre de trajets significatifs, le gain complexe sur chaque trajet et l'atténuation en fonction de la fréquence. Cette méthode est proposée et vérifiée par [9-10]. La deuxième approche sert à calculer le rapport des tensions entre la tension du récepteur et la tension de l'émetteur [11]. Cette approche est connue sous le nom de méthode "bottom-up". La première approche donne un aperçu général sur la totalité des caractéristiques du canal CPL-BE [6] par rapport à la deuxième approche qui présente un avantage car elle permet de rendre compte de la corrélation des fonctions de transfert pour les nœuds, entre l'émetteur et le récepteur, situés sur la même ligne de transmission. Enfin, nous présentons le bruit du canal CPL-BE modélisé et les études qui ont été faites pour faire face aux perturbations dans le canal.

1.4.3 Bruit dans le canal CPL-BE

Différents phénomènes provoquent le bruit dans un canal CPL-BE tels que les objets connectés au réseau électrique et les appareils non connectés au réseau mais qui fonctionnent à la même fréquence que le réseau CPL-BE. Ces perturbations s'additionnent pour former un bruit coloré avec un contenu spectral qui présente une décroissance en fonction de la fréquence en raison de la diminution de la concentration des sources de bruit avec la fréquence [6]. En général, il existe trois types de bruit principal dans un canal CPL-BE :

- Bruit impulsif
  - Bruit impulsif périodique (1)
  - Bruit impulsif périodique (2)
  - Bruit impulsif apériodique
- Bruit à bande étroite

– Bruit de fond coloré

La figure ci-dessous montre le système du réseau CPL-BE avec les types d'erreurs qui proviennent sur ce réseau. Nous distinguons trois catégories de bruit impulsif qui forment

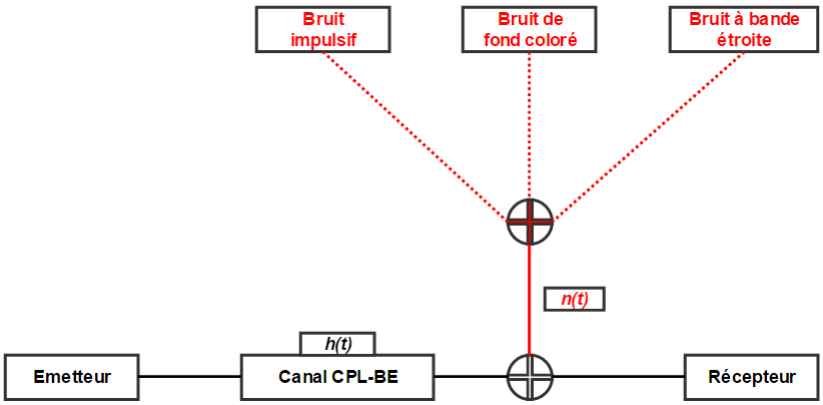
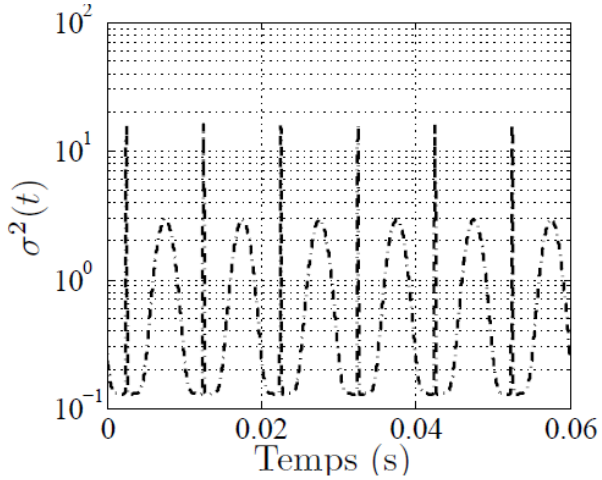


FIGURE 1.3 – Bruit sur le canal CPL-BE

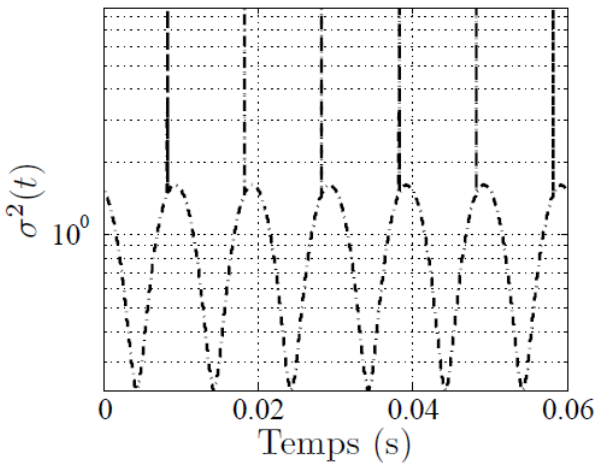
la partie dominante de bruit sur le canal CPL-BE.

1.4.3.1 Bruit impulsif périodique (1)

Le bruit impulsif périodique (1) a été proposé par Katayama [12] et défini comme un bruit gaussien avec une variance qui dépend du temps et de la fréquence. Les figures 1.4 et 1.5 montrent un exemple des variations de la variance et de l'amplitude instantanée du bruit pour les paramètres définis pour deux environnement différents A et B.

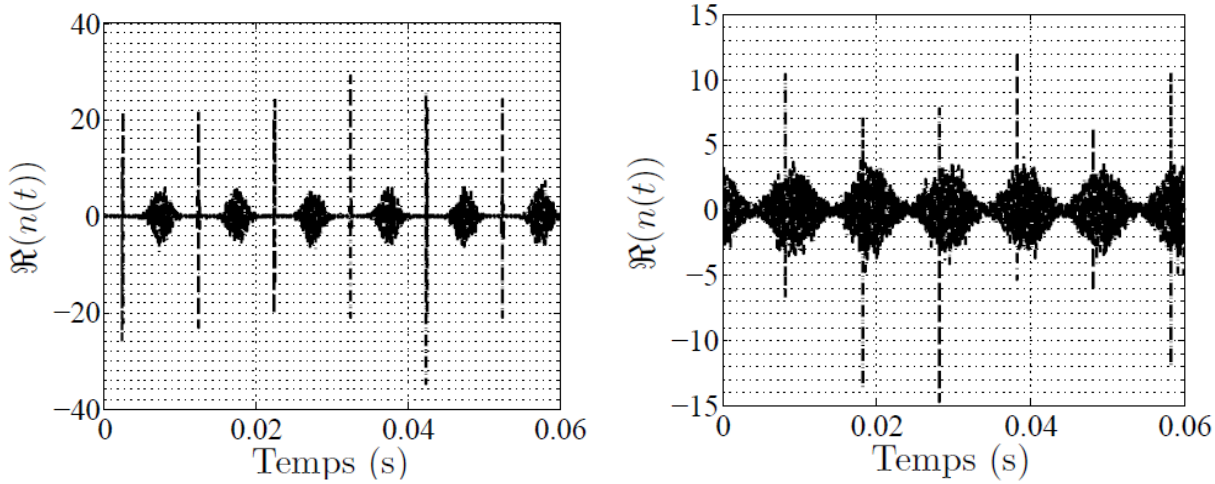


(a) Variance du bruit dans l'environnement A



(b) Variance du bruit dans l'environnement B

FIGURE 1.4 – Variance de l'amplitude instantannée du bruit selon le modèle de Katayama calibré pour deux environnements A et B



(a) Exemple de bruit dans l'environnement A (b) Exemple de bruit dans l'environnement B

FIGURE 1.5 – Exemples de réalisations du bruit selon le modèle de Katayama calibré pour deux environnements A et B

1.4.3.2 Bruit impulsif périodique (2)

Le deuxième type de bruit impulsif périodique, présenté par Nassar [13], est modélisé par le résultat de la convolution d'un bruit blanc Gaussien avec un filtre linéaire variant périodiquement dans le temps. Pour avoir une grande résolution, ce filtre doit avoir un grand nombre de coefficients [14]. Un avantage de ce modèle est qu'il intègre une partie du bruit à bande étroite présents dans un site donné sans avoir besoin de les introduire explicitement.

1.4.3.3 Bruit impulsif apériodique

Il est de nature irrégulier, principalement due aux transitoires causés par la connexion et la déconnexion des appareils électriques. Plusieurs modèles ont été utilisés pour décrire ce type de bruit : Mélange de lois gaussiennes, distribution de Middleton A [15], modèle de Markov [12], etc. Nous constatons qu'avec une apparition d'impulsions suivant la distribution de Poisson, le bruit vu par un récepteur CPL peut être modélisé par un mélange de lois gaussiennes ou par une distribution de Middleton A.

1.4.3.4 Bruit à bande étroite

Ce bruit est une conséquence du "captage" des ondes radio par les câbles électriques [13-16]. Avec ce bruit, une ou plusieurs porteuses OFDM peuvent être bruitées. Selon la nature du bruit, cette interférence peut durer plus ou moins longtemps. Dans les systèmes de télécommunications, nous utilisons un filtre passe-bande après la transposition de

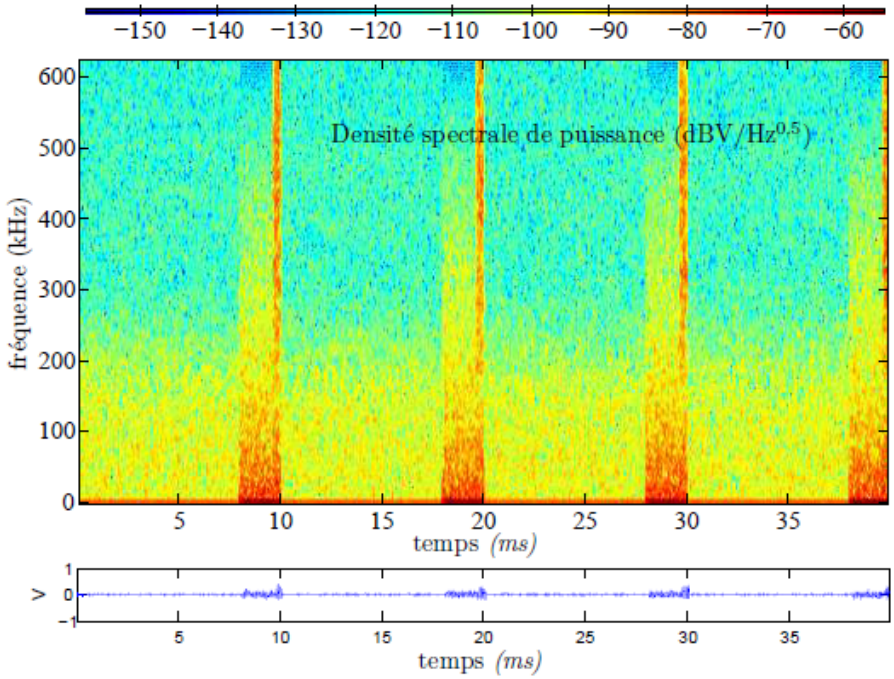


FIGURE 1.6 – Spectrogramme du bruit selon le modèle de Nassar calibré pour une zone donnée

fréquence (mélangeur) qui sert à supprimer les signaux interférents hors-bande. Ce filtre permet d'obtenir le signal modulé autour de sa fréquence porteuse f_c et filtre le bruit large bande pour obtenir un bruit à bande étroite.

Remarque. ***Bruit de fond coloré :*** *Il englobe le reste des types de bruit non inclus dans les catégories précédentes. Nous supposons qu'il est cyclostationnaire.*

1.5 Standards des systèmes CPL

Initialement nous citons les deux normes internationales qui régissent les communications CPL telles que IEEE1901 [17] et (International Telecommunication Union Telecommunication Standardization Sector) ITU-T G.hn [18-19]. D'une part, les produits prêts à être commercialisés à l'IEEE 1901 ont été certifiés soit par HomePlug Powerline Alliance [20], aux Etats-Unis et en Europe, soit par l'alliance HD-PLC [21], principalement au Japon. D'autre part, les produits prêts à l'emploi conformes à l'UIT-T G.hn ont été certifiés par l'alliance HomeGrid Forum [22]. Les produits de la famille HomePlug sont les plus déployés sur le marché.

Dans la figure 1.7 nous représentons l'évolution des générations CPL en fonction du temps :

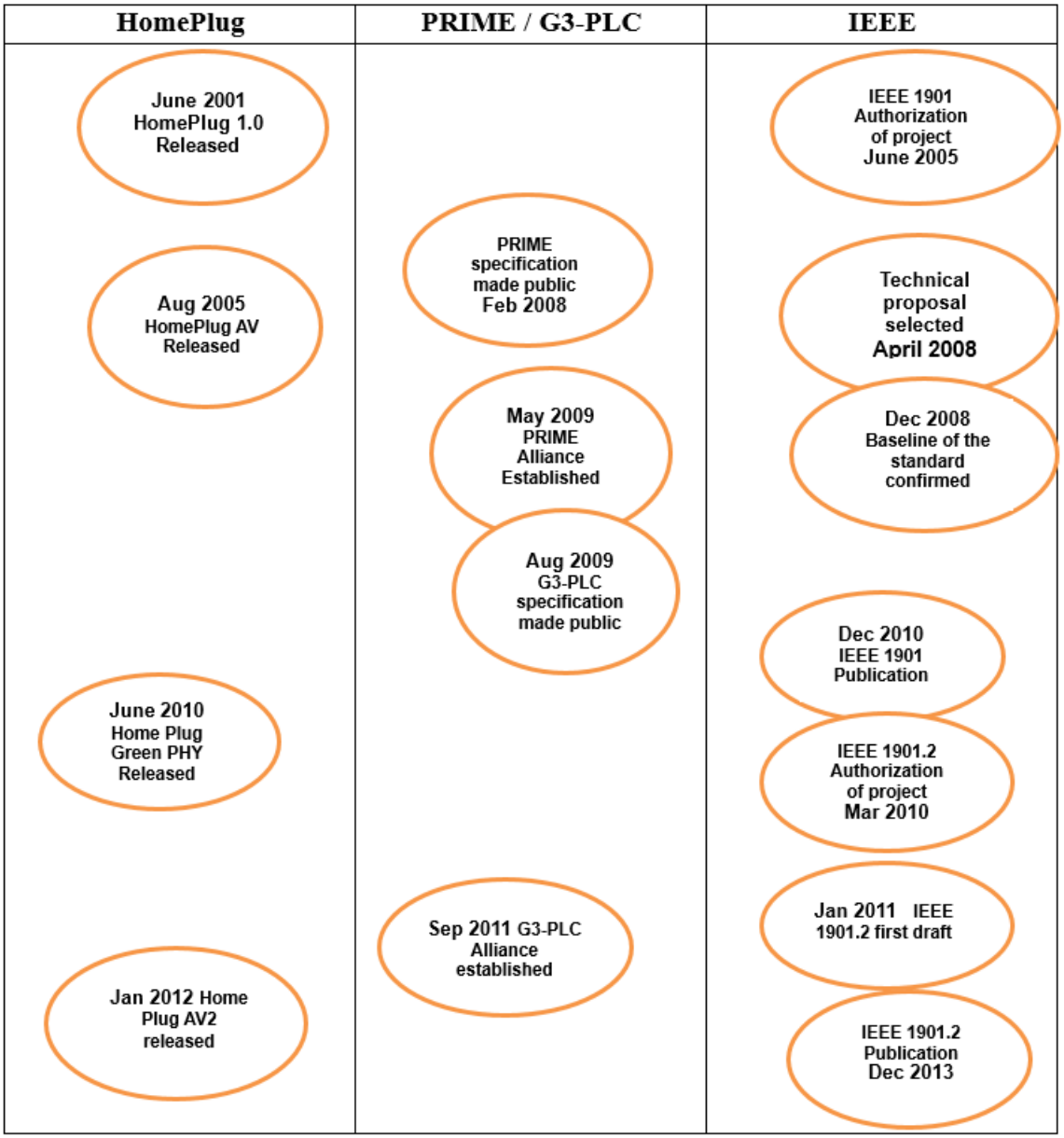


FIGURE 1.7 – Évolution de la technologie CPL

En 1950, les courants CPL sont apparus dans des applications unidirectionnelles tels que l'éclairage publique et la télécommande de relais... Dans les années 1980, des recherches sont menées pour augmenter le débit de transfert des informations en utilisant une bande de fréquence $5 - 500\ kHz$. En 1990, les modems CPL bas débit sont apparus en Europe et aux États-Unis pour la domotique, puis ces modems sont développés en 1997 pour transmettre des données en bidirectionnel. Ensuite, plusieurs entreprises françaises sont arrivées sur le marché avec un processeur 224 Mb/s « le plus rapide au monde » dédiée pour la gestion des énergies dans les bâtiments (technique bas-débit - norme CENELEC EN50065-1), les logiciels et les services équipés du CPL.

Depuis les années 2007, la norme Homeplug AV 200 $Mbits/s$ entre dans le marché avec de nouvelles fonctionnalités (QoS, VLAN, ...). En 2011, plusieurs sociétés, y compris les opérateurs de réseau de distribution (ERDF, Enexis), les fournisseurs de compteurs (Sagemcom, Landis & Gyr) et les vendeurs de puce (Maxim Integrated, Texas Instruments, STMicroelectronics) ont fondé G3-CPL Alliance [23] pour promouvoir la technologie G3-CPL. G3-CPL est le protocole de couche basses (couche physique) pour permettre une infrastructure à grande échelle sur le réseau électrique. G3-CPL peut fonctionner sur bande CENELEC A (35 kHz à 91 kHz) ou CENELEC B (98 kHz à 122 kHz) en Europe, sur bande ARIB (155 kHz à 403 kHz) au Japon et sur FCC (155 kHz à 487 kHz) pour les États-Unis et le reste du monde. [24] La technologie utilisée est l'OFDM échantillonnée à 400 kHz avec une modulation adaptative. La détection et la correction des erreurs sont effectuées à la fois par un code convolutif et par une correction d'erreur de type Reed-Solomon. G3-CPL a été conçu pour une communication extrêmement robuste basée sur des connexions fiables et hautement sécurisées entre les périphériques, y compris les transformateurs de moyenne à basse tension. En décembre 2011, la technologie G3-CPL a été reconnue comme norme internationale à l'UIT à Genève, où elle fait référence à G.9903. [25]. Les réseaux G3-CPL utilisent le multiplexage par répartition de fréquence orthogonale à bande étroite.

1.5.1 Norme G3-CPL

Les Courants Porteurs en Ligne (CPL) n'ont pas été standardisés depuis longtemps, mais seules certaines réglementations ont été établies comme la norme CENELEC EN 50065-1. Le CPL à bande étroite (CPL-BE) pour les applications SmartGrid (SG) a également été lancé. Le comité internationale de régulation doit discuter deux propositions concernant les couches PHY et MAC : G3-CPL, lancé par ERDF et Maxim, et PRIME (PoweRline Intelligent Metering Evolution), initialisé par PRIME Alliance. Dans cette thèse, nous nous concentrerons sur les couches physiques en utilisant la bande CENELEC A et le multiplexage de division de fréquence orthogonale (OFDM) Cyclic Prefix (CP) en combinaison avec le codage Differential Phase Shift Keying (DPSK), connu pour être une technique simple et robuste pour la transmission de données sur des canaux sélectifs en fréquence. Notons que l'OFDM peut être implémenté d'une manière très efficace par la Transformée de Fourier Rapide (FFT). Le système G3-CPL fonctionne à une fréquence d'échantillonnage de $f_s = 400\ kHz$ et utilise une taille FFT de $M = 256$, ce qui conduit à un espacement de sous-porteuse de $\Delta f = 1.65625\ kHz$. Ainsi, en modulant les porteuses n^o 23 à 58, seulement, G3 occupe la plage de fréquence de $35,9$ à $90,6\ kHz$. La figure 1.8 montre le schéma de principe d'un émetteur G3-CPL. Pour la transmission de données, G3-CPL offre trois modes "Robust", "DBPSK" et "DQPSK", ce qui conduit à des paquets

de données de tailles au maximum 133, 235 et encore 235 octets, à un débit de $33,4$ *kbps* maximum (en mode DQPSK) . Dans tous les modes, les données sont protégées par le code

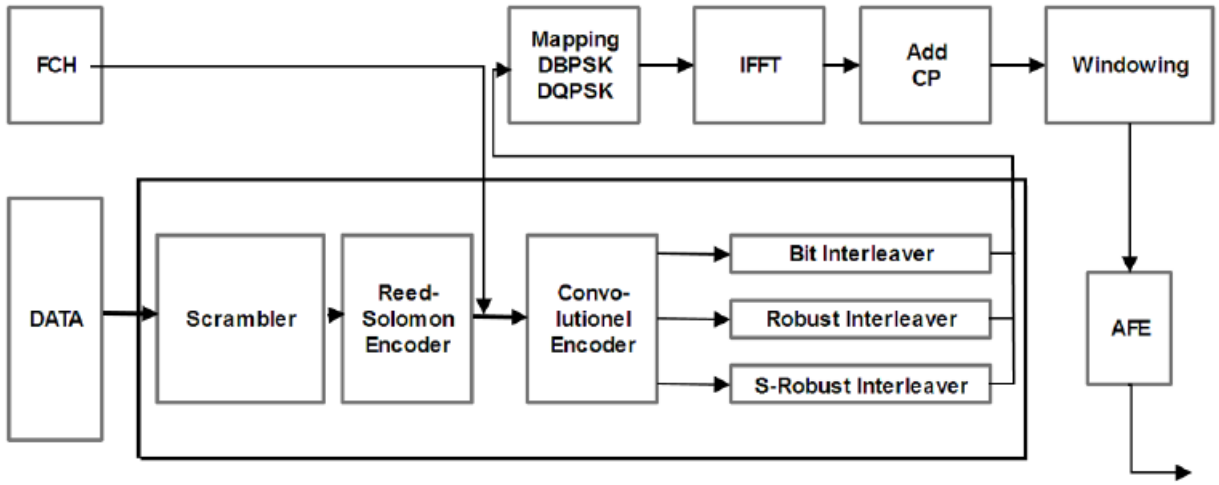


FIGURE 1.8 – Diagramme en block pour un émetteur G3-CPL

convolutif de rendement $1/2$ avec un polynôme générateur $G = [171, 155]$ et entrelacées dans tout le paquet. Les données (DATA) et les données de l'en-tête de contrôle de trame (FCH) en mode Robuste sont en outre répétées six et quatre fois, respectivement, par l'entrelaceur avant la modulation DBPSK (codage de répétition). Les données non FCH sont encodées avec un code Reed Solomon (RS), basé sur $RS(255, 247)$ pour Robuste et $RS(255, 239)$ pour le mode BPSK et DQPSK. Les symboles PSK sont codés de manière différentielle par sous-porteuse dans le temps (t-DPSK), de sorte que les porteuses qui subissent une atténuation ou une perturbation peuvent être désactivées. En outre, les sous-porteuses sont disposées en neuf groupes et un champ "Tone Map" dans le FCH indique lequel d'entre eux est actif. En outre, chaque symbole OFDM est fenêtré par un cosinus surélevé de 8 échantillons, de sorte que l'intervalle de garde est réduit de $L_{CP} = 30$ échantillons à une longueur effective de 14.

1.5.2 PRIME

Dans PRIME, la fréquence d'échantillonnage a été choisie à $f_s = 250\ kHz$, tandis que la taille FFT est $M = 512$, c'est-à-dire que l'espacement entre sous-porteuse représente $\Delta f = 488\ Hz$. Comme les porteuses $n^o\,86$ à 182 sont utilisées pour la transmission, le signal PRIME est situé dans la plage de fréquences 42 à 89 kHz. Le traitement d'un signal dans un émetteur PRIME est représenté sur la figure 1.9 En sélectionnant le schéma de modulation DBPSK, DQPSK ou D8PSK et en allumant ou éteignant le codage convolutif (y compris l'entrelacement), six protocoles peuvent être réalisés pour la transmission de

données. Ainsi, PRIME peut transporter au maximum 2268 octets par paquet à $128,6$ *kbps* en utilisant D8PSK non codé, tandis que son protocole le plus robuste, DBPSK codé, peut transporter 377 octets par paquet à $21,4$ *kbps*. Ainsi, les données FCH sont toujours transmises en utilisant le mode DBPSK codé. Le code convolutif appliqué dans

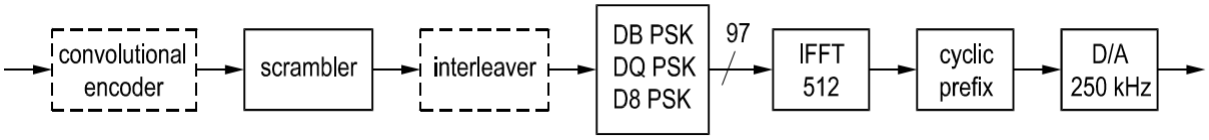


FIGURE 1.9 – Diagramme en block pour un émetteur PRIME. (Les éléments en tirets sont ignorés dans certains protocoles.)

PRIME est le même que dans le G3-CPL, mais l'entrelacement est effectué par symbole OFDM. En outre, le codage différentiel des symboles PSK est effectué par symbole OFDM sur les sous-porteuses (*f*-DPSK). Les deuxième et troisième colonnes du tableau 1.1 donnent un aperçu sur des paramètres du G3-CPL et PRIME respectivement [26-27]. En conséquence, nous remarquons une grande différence entre les deux normes au niveau des codes correcteurs d'erreurs. Ils incluent tous deux le même code convolutif, mais PRIME permet de l'éteindre dans certains modes, tandis que le codage Reed-Solomon est activé dans tous les modes G3-CPL. En outre, selon les spécifications et les résultats de simulation dans [28], le code correcteur d'erreurs appliqué dans G3-CPL est plus puissant que dans PRIME, ce qui nous motive pour mettre en œuvre la norme G3-CPL afin de rendre les transmissions plus fiables en utilisant des codes correcteurs d'erreurs plus performants.

Tableau 1.1 – Paramètres des normes G3-CPL et PRIME

	G3-CPL	**PRIME**
frequency range	$35-91\ kHz$	$42-89\ kHz$
sampling frequency f_s	$400\ kHz$	$250\ kHz$
OFDM		
FFT size M	256	512
length of cyclic prefix L_{CP}	30	48
windowing	yes	no
subcarrier spacing	$\Delta f = 1.5625\ kHz$	$\Delta f = 488\ Hz$
n^o of carriers used (one-sided)	$36\ kHz$	97
max. data rate	33.4 *kbps*	128.6 *kbps*
Forward Error Correction	Reed Solomon code, convolutional code, repitition code	convolutional code
interleaving	per data packet	per OFDM symbol
modulation	DBPSK, DQPSK	DBPSK, DQPSK, D8PSK
differential encoding	in time	in frequency

1.6 État de l'art sur les techniques de codage dans G3-CPL

Le canal CPL-BE peut créer des erreurs en paquets temporelles (sur toutes les sous-porteuses) à cause du bruit impulsif, et aussi peut effacer une porteuse à cause du bruit à bande étroite, ceci peut être interprété comme une erreur en paquet fréquentielle (sur une porteuse) d'où la nécessité d'un codage correcteur d'erreurs pour lutter contre ces types de bruit.

1.6.1 Reed-Solomon dans la spécification G3-CPL

Nous décrivons les schémas de correction d'erreur qui ont été incorporés dans la spécification G3-CPL afin de combattre les différents types d'erreurs généralement rencontrées lors de la transmission dans le canal CPL-BE. Le système G3-CPL est basé sur un schéma de modulation multi-porteuse, qui utilise un grand nombre de sous-porteuses orthogonales étroitement espacées pour transporter des données. Pour obtenir une efficacité spectrale élevée, ces sous-porteuses se chevauchent généralement en fréquence. Cette approche maximise l'utilisation de la bande passante, permettant ainsi des techniques avancées de codage de canaux telles que Viterbi et Reed Solomon [29] utilisées pour des communications robustes ainsi que des débits de données plus élevés. La propriété d'orthogonalité permet également de récupérer chacune des sous-porteuses séparément au récepteur sans interférer entre elles. Le standard G3-CPL utilise la modulation OFDM avec des systèmes de modulation DBPSK, DQPSK et D8PSK avec une taille IFFT de 256. Cette norme utilise un codeur convolutif pour la correction d'erreur directe et inclus l'encodeur Reed-Solomon pour corriger les erreurs de données dûes aux bruits impulsifs. Après l'encodeur convolutif, un bloc d'entrelacement est utilisé. Le but de l'entrelaceur est de fournir une protection contre deux sources d'erreur différentes :

- Une erreur temporelle qui peut corrompre quelques symboles OFDM consécutifs
- Un effet d'évanouissement profond de fréquence qui peut corrompre quelques fréquences adjacentes pour un grand nombre de symboles OFDM

Afin d'obtenir un point de référence pour notre travail, une simulation a été développée dans la bande de Cenelec A pour le système G3-CPL, où le canal a été simulé par un filtre passe-bas avec une fréquence de coupure à 3 dB égale à 88 et 92 kHz suivi d'un générateur de bruit blanc qui ajoute du bruit à la sortie du filtre. Les débits de la couche physique pour les trois modulations sont présentés dans le tableau 1.2. Le rapport signal sur bruit (SNR) du système émetteur G3-CPL détermine lequel des trois modes est sélectionné lors de la communication.

Tableau 1.2 – Débit PHY expérimental

Modulation	**Rendement du code convolutif**	**Débit** ($Kbps$)
DBPSK	1/2	15
DQPSK	1/2	29
D8PSK	1/2	43

La figure 1.10 montre le taux d'erreur bit moyen 'BER' pour le système global de G3-CPL correspondant aux débits de données dans le tableau 1.2. Pour un 'BER' de 10^{-4}, on remarque que le mode DBPSK (1 bit par porteuse) peut fonctionner à un 'SNR' qui est égal à 3 dB (le signal est environ 2 fois supérieur au niveau de bruit) avec un débit de 15 $Kbps$ [30]. Cependant, une solution FSK dans le même état peut fonctionner à un 'SNR' de 12 dB avec un débit de 2 $Kbps$, voir figure 1.11. Le DQPSK qui transmet deux bits sur chaque porteuse fonctionne à un 'SNR' qui vaut 6 dB avec un débit de 29 $kbps$ [31].

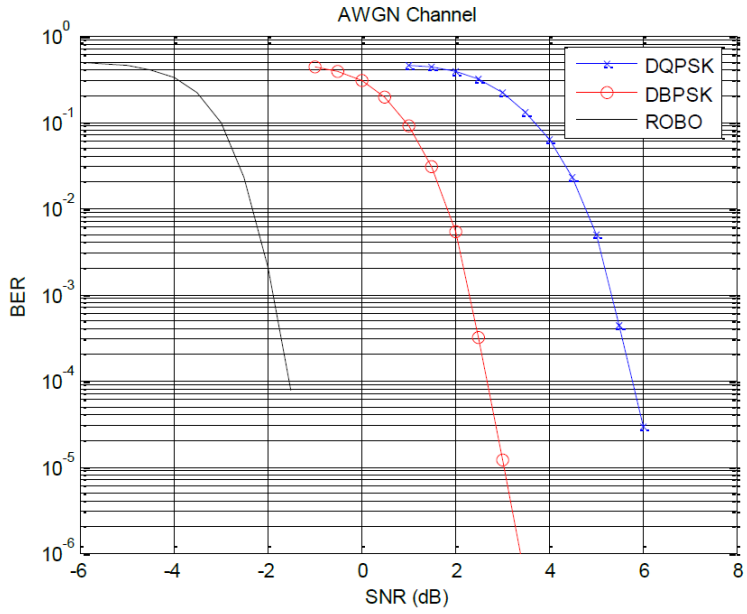


FIGURE 1.10 – Performance d'un système G3-CPL (OFDM)

Ces résultats de simulation présentés montrent les performances supérieures de la couche physique G3-CPL par rapport au FSK. En outre, les succès globaux du déploiement sur le terrain avec les technologies OFDM, en raison de leur fiabilité et de leur débit de données plus élevé, ont démontré aujourd'hui qu'elles peuvent être appliquées pour les applications AMI et Smart Grid du monde réel.

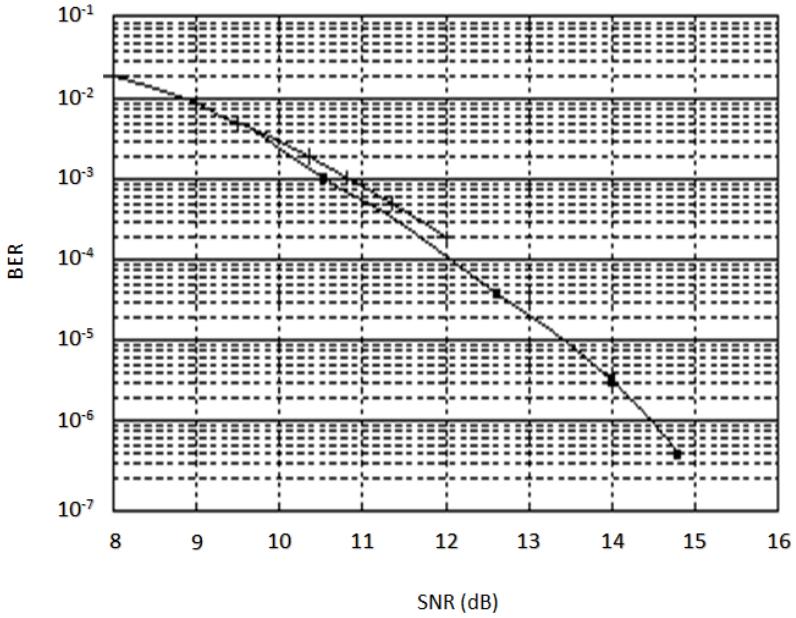


FIGURE 1.11 – Performance d'un système G3-CPL (FSK traditionnel)

1.6.2 Codes LDPC pour le canal CPL-BE

Par ailleurs d'autres recherches ont été effectuées afin d'améliorer la fiabilité du système CPL-BE. Ces études servent à évaluer, par exemple, la performance des codes LDPC (Low Density Parity Check) et à introduire une version optimisée de ces codes lorsqu'ils sont appliqués sur des paquets de taille réduite d'un système CPL-BE. Ensuite, une comparaison sera mise en place au niveau des performances avec celle obtenue lorsque le schéma de codage standard G3-CPL est appliqué sur le système, à savoir le schéma qui concatène le code convolutif avec les codes Reed-Solomon. Les performances des codes LDPC réguliers, ainsi que celle des codes convolutifs concaténés avec les codes Reed-Solomon sur le canal CPL-BE seront présentées dans les figures 1.12 et 1.13. La figure 1.12 montre la performance du scénario de codage de base dans deux conditions de bruit, le bruit de fond avec et sans la présence de bruit impulsif. La figure 1.13 montre la performance des codes LDPC réguliers lorsque le bruit impulsif est absent et présent dans le système. Il ressort des figures 1.12 et 1.13 que toutes les longueurs de paquets (c'est-à-dire la taille : 112 correspond à la longueur du paquet qui comporte 112 symboles OFDM) suivent la même tendance. Comme on peut le voir, les codes convolutifs concaténés avec les codes Reed-Solomon dépassent les codes LDPC réguliers, à l'exception du cas de 12 symboles OFDM formant un seul mot de code. Ceci s'explique car, pour cette longueur de paquet, la redondance introduite par le scénario de codage de base est supérieure à celle des codes LDPC. Par conséquent, la performance de la courbe Eb/N0 résultante semble être inférieure. Il est à noter que lorsque le bruit impulsif se produit, la performance de tous

les scénarios de code se détériore, ce qui est plutôt attendu, car les impulsions ont un effet négatif sur les données d'information. Il a été prouvé que la performance des codes LDPC

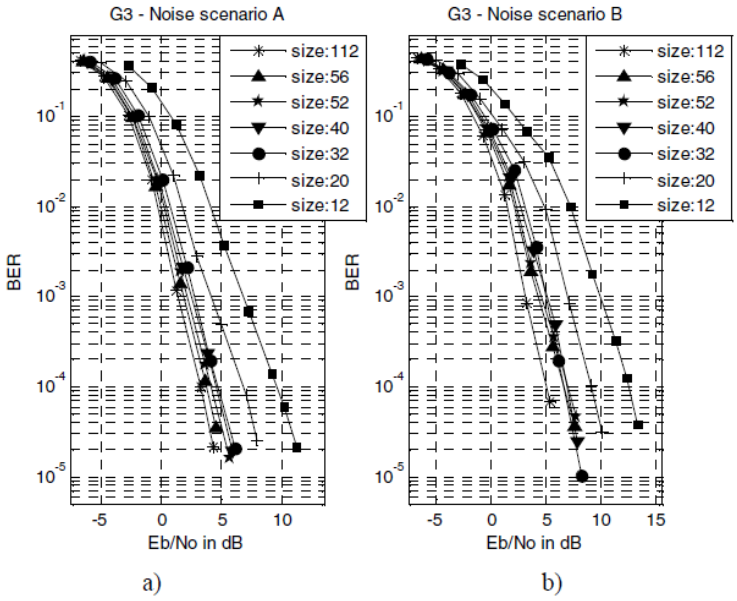


FIGURE 1.12 – Taux d'erreur binaire en fonction de Eb/N0 pour un canal CPL-BE, les codes convolutifs concaténés avec les codes Reed-Solomon, a) scénario de bruit A (absence de bruit impulsif) b) scénario de bruit B (présence de bruit impulsif)

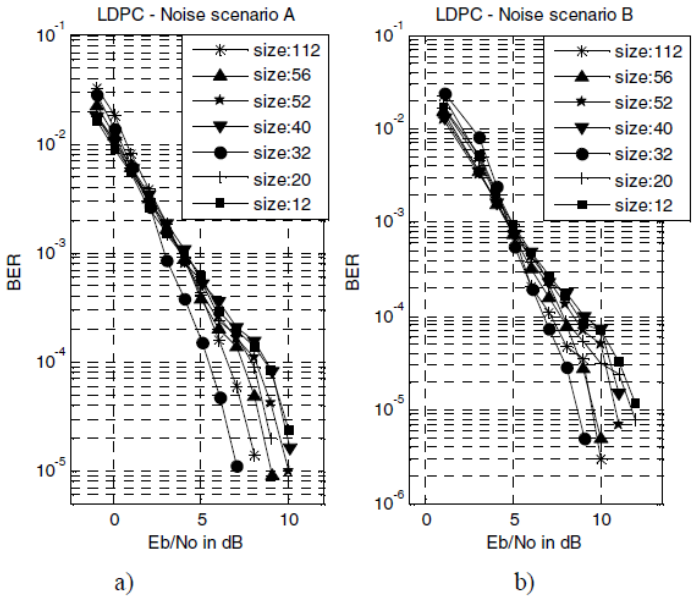


FIGURE 1.13 – Taux d'erreur binaire en fonction de Eb/N0 pour un canal CPL-BE, les codes LDPC réguliers, a) scénario de bruit A (absence de bruit impulsif) b) scénario de bruit B (présence de bruit impulsif)

réguliers peut être améliorée en utilisant des degrés variables pour les nœuds de parité et

les nœuds de variable. On parle alors des codes LDPC irréguliers optimisés, l'optimisation des degrés des nœuds se fait à l'aide de l'outil "évolution de densité" [32]. Les figures 1.14 et 1.15 montrent les performances obtenues avec des codes LDPC irréguliers optimisés.

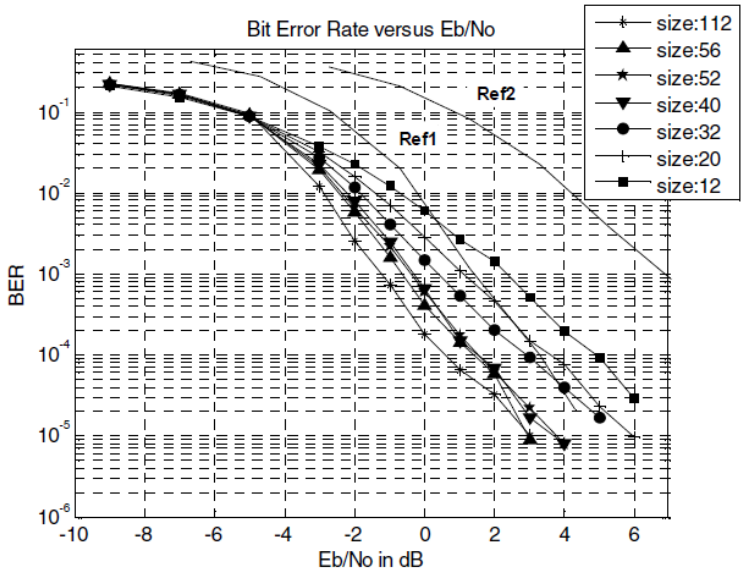


FIGURE 1.14 – Taux d'erreur binaire en fonction de Eb/N0 pour un canal CPL-BE, les codes LDPCoptimisés, scénario de bruit A (absence de bruit impulsif)

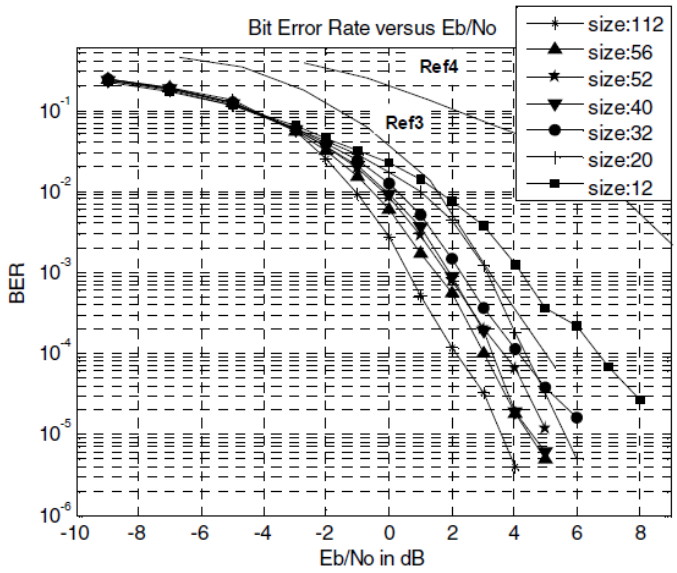


FIGURE 1.15 – Taux d'erreur binaire en fonction de Eb/N0 pour un canal CPL-BE, les codes LDPC optimisés, scénario de bruit B (présence de bruit impulsif)

Les courbes "Ref1" et "Ref2" se réfèrent aux courbes illustrées à la figure 1.12a pour la première et dernière longueur de paquet (taille : 112 et taille : 12) respectivement.

Comme on peut le remarquer à partir de la figure 1.14 et la figure 1.12a, les codes LDPC irréguliers conçus proposés dépassent généralement les systèmes de codage déjà existants utilisés dans la norme G3-CPL d'environ 2 dB et ils ont une meilleure performance que les codes LDPC réguliers. Les courbes "Ref3" et "Ref4" se réfèrent aux courbes illustrées à la figure 1.12b pour la première et la dernière longueur de paquet (taille : 112 et taille : 12) respectivement. Comme on peut le voir sur la figure 1.15, la performance est améliorée en utilisant les codes LDPC irréguliers, par rapport aux schémas de concaténation des codes convolutifs avec les codes Reed Solomon ainsi par rapport au cas des codes LDPC réguliers. Il convient de noter sur la figure 1.15 et la figure 1.12b que l'amélioration de la performance dûe à l'utilisation des codes LDPC optimisés est généralement de l'ordre de $2-3$ dB par rapport aux codes LDPC convolutifs avec les codes RS pour les 6 premières tranches de paquets.

Nous remarquons que les codes LPDC irréguliers donnent de meilleurs performances que les codes LDPC réguliers et peuvent être considérés comme un schéma de codage candidat pour le canal NB-CPL. Une meilleure performance, dans le cas des paquets de taille réduite, est également obtenue par rapport aux codes concaténés convolutifs avec les codes RS utilisés pour la norme G3-CPL.

D'autres études utilisant des Turbo-codes [36] permettent d'aboutir à des performances semblables à celles des codes LDPC optimisés.

1.6.3 Les codes à métrique de rang (Gabidulin) pour les réseaux CPL-BE

Comme nous avons vu précédemment, les schémas classiques rencontrés reposent sur les codes à métrique de Hamming, parmi lesquels les codes Reed-Solomon (RS) et les codes LDPC qui sont des codes en bloc. Cependant, ces codes ne sont pas destinés à combattre les erreurs de type "criss-cross" (figure 1.16). Par conséquent, les auteurs dans [33] ont proposé de remplacer les codes à métrique de Hamming par les codes Gabidulin à métrique de rang qui peuvent corriger une colonne entière ou une ligne d'un mot de code, qui est disposé dans une matrice. Ces codes peuvent donc s'avérer très avantageux dans le contexte CPL puisqu'ils peuvent corriger des sous-espaces complets d'erreurs. Par la suite, la performance de ces codes est comparée avec les codes RS suivant deux étapes : avec et sans la concaténation des codes convolutifs. Le décodage RS se fait à l'aide de l'algorithme Berlekamp-Massey. Pour les codes à distance de type maximum, il existe un algorithme de décodage basé sur un algorithme modifié de Berlekamp-Massey [34]. Le décodeur convolutif utilise l'algorithme Viterbi à entrée souple. La simulation est faite dans un canal NB-CPL, en utilisant la modulation OFDM (les colonnes de la matrice de code contiennent les symboles OFDM), avec toutes les caractéristiques de bruit

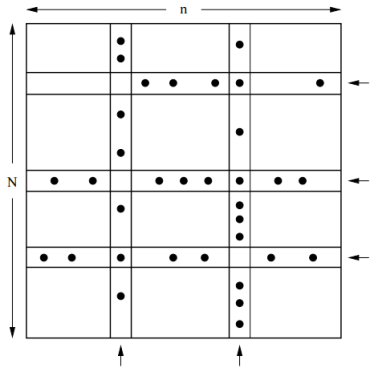


FIGURE 1.16 – Motifs d'erreurs "criss-cross"

indépendantes, y compris le bruit de fond, le bruit impulsif et les interférences à bande étroite.

1.6.3.1 Code Reed-Solomon et code Gabidulin sans concaténation des codes convolutifs

Tout d'abord, nous présentons les simulations qui ont été faites entre un code à métrique de rang de dimension $n = 46$ et de longueur $k = 23$ sur $GF(2^{46})$ et un code RS $(n = 255, k = 127)$ sur $GF(2^8)$. Le rendement de deux codes est $1/2$, très proche du code utilisé par les mécanismes des codes correcteurs d'erreurs des différentes normes BE [35]. Pour ces paramètres, la capacité de correction de ligne et/ou de colonne du code de base simulé est 11, la capacité de correction de colonne du code RS est également 11 et puisque le code RS ne peut pas gérer des erreurs de dimension égale à 2, sa capacité de correction de ligne est 0. Les algorithmes de décodage sont détaillés dans les chapitres suivants. Le mot de code du code Gabidulin est une matrice (46×46) de symboles binaires dans le domaine temps-fréquence. Nous notons que les mots de code utilisés sont de taille sensiblement égale ce qui rend légitime la comparaison des performances.

D'une part, nous exposons la comparaison entre ces deux codes qui corrigent les erreurs en blocs. La figure 1.17 présente la chaîne de communication, lorsque le code Gabidulin

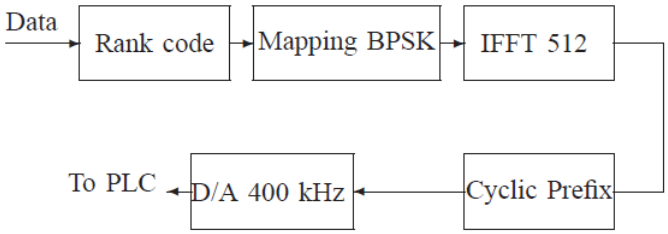


FIGURE 1.17 – Schéma de transmission du code à métrique de rang

est utilisé seul. En l'absence de bruit impulsif et d'interférence à bande étroite : la seule perturbation est le bruit de fond. Il ressort de la figure 1.18 que le code RS est environ $2,5$

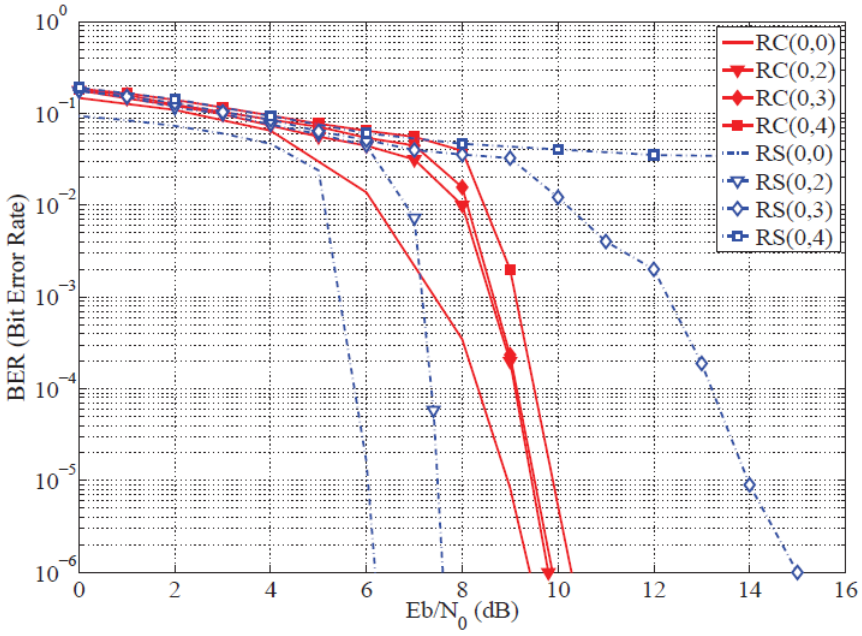


FIGURE 1.18 – Taux d'erreur binaire du code Gabidulin comapré à un code RS avec un nombre différent de sous-porteuses affectées par des interférences à bande étroite

dB supérieur au code Gabidulin (RC) à un BER égal à 10^{-4} dans le cas où il n'y a pas d'interférences à bande étroite ou de bruit impulsif ($RC(0,0)$ et $RS(0,0)$). La structure d'erreur dans les symboles OFDM codés par un code à métrique de rang ne montre pas un comportement efficace lorsqu'il y a peu de bruit à bande étroite ou de bruit impulsif. Ceci est dû à des erreurs individuelles irrégulières augmentant le rang du motif d'erreur et réduisant ainsi la capacité de décodage. Les codes à métrique de rang sont plus efficaces lorsque les erreurs sont confinées dans un nombre réduit de lignes ou de colonnes ce qui signifie que le sous-espace d'erreurs est de taille finie . La figure 1.18 présente également la performance du code à métrique de rang par rapport au code RS en présence de bruit de fond et d'interférences à bande étroite pouvant affecter jusqu'à 4 sous-porteuses. La performance du code RS commence à se détériorer significativement lorsque deux sous-porteuses sont affectées par le bruit à bande étroite. En présence de quatre sous-porteuses affectées par les interférences à bande étroite, les performances du code RS deviennent très faibles et le code RS n'est plus capable de corriger efficacement les erreurs et seul le code à métrique de rang est efficace dans ce cas. En outre, nous constatons une faible sensibilité du code à métrique de rang malgré le nombre croissant d'événements de bruit à bande étroite.

1.6.3.2 Code Reed-Solomon et code Gabidulin avec concaténation des codes convolutifs

D'autre part, une deuxième comparaison a été faite entre un code $RS(255, 215)$ et un code à métrique de rang $RC(46, 38)$ concaténés avec un encodeur convolutif de rendement 1/2. En outre, un schéma d'entrelacement de fréquence temporelle (2D) est utilisé pour réduire l'impact des erreurs de rafale qui se manifestent par beaucoup de symboles erronés à très peu d'écart temporel qui sont difficiles à corriger par des codes convolutifs. Ces paramètres sont choisis conformément aux normes CPL-BE.

En l'absence d'interférence à bande étroite ou de bruit impulsif (voir la figure 1.20), nous notons que les deux codes fonctionnent presque identiquement. Ceci s'explique par le fait que le code convolutif interne arrive à gérer les erreurs introduites par le bruit de fond. Les erreurs de rafale résiduel sont traitées par les codes de blocs externes (Gabidulin ou RS). La figure 1.19 présente le schéma complet de la mise en œuvre du code Gabidulin

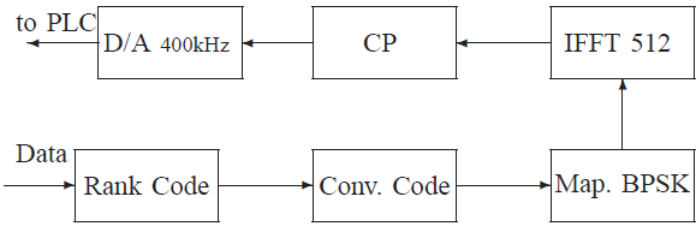


FIGURE 1.19 – Schéma de transmission du code à métrique de rang concaténé avec un code convolutif interne

concaténé avec un code convolutif. En présence de bruit impulsif (voir la figure 1.21), les deux codes ont à peu près la même performance, le code CC-RS est légèrement meilleur que le code CC-Gabidulin. Cependant, en présence du bruit à bande étroite et du bruit de fond (voir la figure 1.22), on peut voir que le code CC-Gabidulin dépasse le système constitué du code RS, du code convolutif et des entrelaceurs. L'apparition d'une interférence à bande étroite (qui affecte les lignes de la matrice de transmission) est correctement corrigée par le code Gabidulin extérieur, si le code convolutif n'a pas réussi à les corriger. En conséquent, le système résultant est robuste contre les bruits impulsifs et les interférences à bande étroite. Et il dépasse clairement la performance des codes RS lorsque l'on considère la concaténation de tels types de codes de blocs avec un code convolutif interne associé à un entrelaceur tel qu'il est mentionné dans les normes.

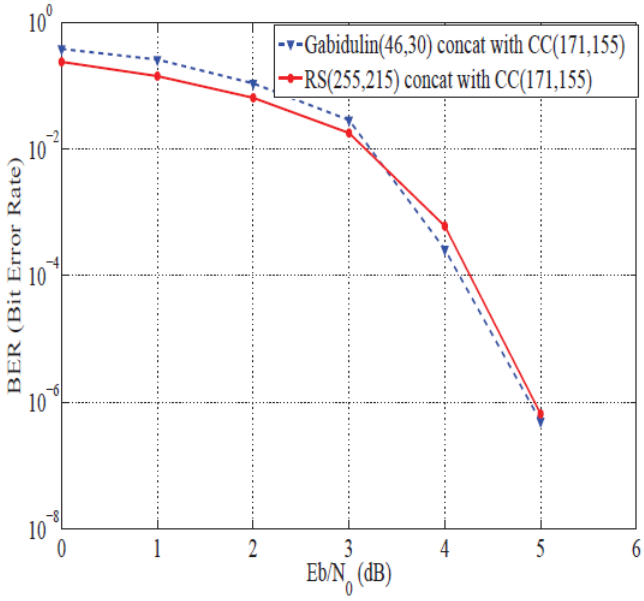


FIGURE 1.20 – Taux d'erreur binaire du code Gabidulin et du code RS concaténés avec un code convolutif (CC) avec uniquement du bruit de fond

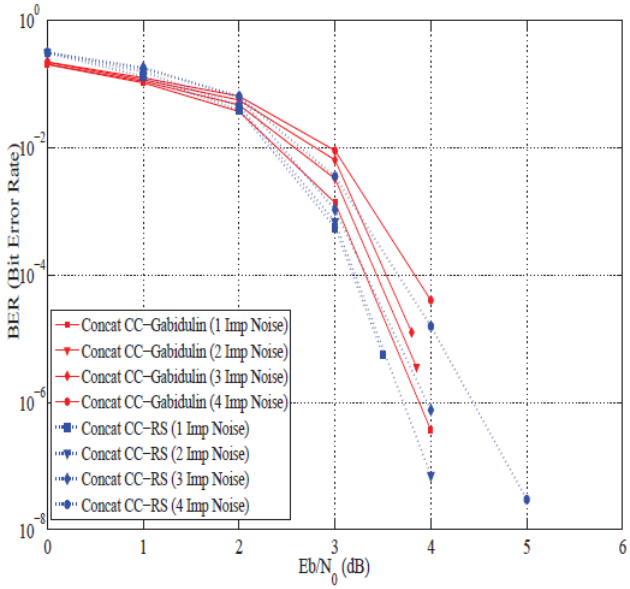


FIGURE 1.21 – Taux d'erreur binaire du code Gabidulin et du code RS concaténés avec un nombre différent de symboles OFDM affectés par le bruit impulsif

1.7 Conclusion

L'objectif de ce premier chapitre était de nous familiariser avec le contexte des Smart Grid et des CPL. Le concept de Smart Grid a tout d'abord été présenté, nous avons introduit ensuite les communications par CPL-BE qui répondent aux besoins de liens

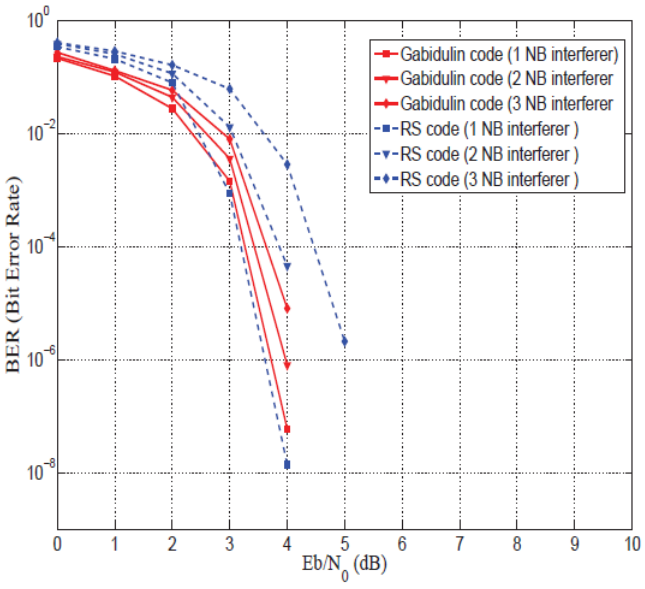


FIGURE 1.22 – Taux d'erreur binaire du code Gabidulin et du code RS concaténés avec un nombre différent des sous-porteuses affectées par les interférences à bande étroite

de communication pour le domaine d'accès Smart Grid. Par ailleurs, les différents types d'erreurs ont été exposés, puis un état de l'art qui permet des mettre en place les codes correcteurs d'erreurs pour faire face aux perturbations dans un canal CPL-BE a été présenté.

En conclusion, il apparait clairement que les développeurs de systèmes CPL sont mis au défi par les caractéristiques très défavorables du canal CPL-BE. Il est indispensable d'avoir recours aux techniques de traitement de signal comme le codage correcteur d'erreurs pour fiabiliser les transmissions sur ce médium. Par conséquent, les caractéristiques particulières du bruit rencontré sur les canaux CPL comme par exemple le bruit à motif criss-cross, doivent être considérés dans la conception et la mise en œuvre de ces codes.

Bibliographie

[1] A.J.H.Vinck, "Coding for a Terrible Channel," in Telecommunications and Information Science and Technologies COST, july 2005.

[2] S. Galli and T. Lys, "Next generation Narrowband (under 500 kHz) Power Line Communications (PLC) standards," China Communications, vol. 12, no. 3, pp. 1–8, March 2015.

[3] S. Galli, A. Scaglione, and Z. Wang. Power Line Communications and the Smart Grid. First IEEE International Conference on Smart Grid Communications (SmartGridComm), pages 303308, October 2010.

[4] M. S. Yousuf and M. El-Shafei. Power Line Communications : An Overview - Part I. 4th International Conference on Innovations in Information Technology (IIT), pages 218222, November 2007.

[5] Pavlidou, N., Vinck, A. H., Yazdani, J., & Honary, B. (2003). Power line communications : state of the art and future trends. IEEE Communications magazine, 41(4), 34-40.

[6] P. J. VAN RENSBURG, "Effective Coupling for Power-Line Communications," Ph.D. dissertation, University of Johannesburg, 2008.

[7] V. Giordano, F. Gangale, G. Fulli, M. S. Jiménez, I. Onyeji, A. Colta, I. Papaioannou, A. Mengolini, C. Alecu, T. Ojala et al., "Smart Grid projects in Europe," JRC Reference Reports, 2011.

[8] P. A. Brown, "Power line communications - past present and future," in International Symposium on Power Line Communications and its Applications , ISPLC, March 1999, pp. 1–8.

[9] M. Tlich, A. Zeddam, F. Moulin, and F. Gauthier, "Indoor Power- Line Communications Channel Characterization up to 100 Mhz ; part ii : Time-Frequency Analysis," IEEE Transactions on Power Delivery, vol. 23, no. 3, pp. 1402–1409, July 2008.

[10] T. Banwell and S. Galli, "On the Symmetry of the Power Line Channel," in International Symposium on Power Line Communications and its Applications, 2001, pp. 325–330.

[11] W. Liu, Emulation of Narrowband Powerline Data Transmission Channels and Evaluation of PLC Systems, ser. Forschungsberichte aus der Industriellen Informationstechnik / Institut für Industrielle Informationstechnik (IIIT), Karlsruher Institut für Technologie. KIT Scientific Publishing, 2013.

[12] M. Katayama, T. Yamazato, and H. Okada, "A Mathematical Model of Noise in Narrowband Power line Communication Systems," IEEE Journal on Selected Areas in Communications, vol. 24, no. 7, pp. 1267–1276, July 2006.

[13] M. Nassar, J. Lin, Y. Mortazavi, A. Dabak, I. H. Kim, and B. Evans, "Local utility Power Line Communications in the 3-500 khz Band :Channel Impairments, Noise, and Standards," IEEE Signal Processing Magazine, vol. 29, no. 5, pp. 116–127, Sept 2012.

[14] A. M. Tonello, "Wideband Impulse Modulation and Receiver Algorithms for Multiuser Power Line Communications," EURASIP Journal on advances in signal processing, vol. 2007, no. 17, 2007.

[15] M. Tlich, A. Zeddam, F. Moulin, and F. Gauthier, "Indoor Power-Line Communications Channel Characterization up to 100 Mhz—part i : one-parameter deterministic model," IEEE Transactions on Power Delivery, vol. 23, no. 3, pp. 1392–1401, 2008.

[16] A.J.H.Vinck, "Coding for a Terrible Channel," in Telecommunications and Information Science and Technologies COST, july 2005.

[17] IEEE. Website : www.standards.ieee.org/findstds/standard/ 1901-2010.html, (accessed 20 august 2015). IEEE Standard 1901- 2010 - IEEE Standard for Broadband over Power Line Networks : Medium Access Control and Physical Layer Specifications, 2010.

[18] ITU-T. Website : www.itu.int/rec/T-REC-G.9960-200910-T/en, (accessed 20 August 2015). G.9960 : United high-speed wireline-based home networking transceivers - System architecture and physical layer specification, 2010.

[19] Oksman, V., & Galli, S. (2009). G. hn : The new ITU-T home networking standard. IEEE Communications Magazine, 47(10).

[20] HomePlug. Website : www.homeplug.org. HomePlug Powerline Alliance.

[21] HD-PLC. Website : www.hd-plc.org. HD-PLC Alliance, HomePlug Powerline Alliance.

[22] HomeGrid. Website : www.homegridforum.org/. HomeGrid Forum Alliance.

[23] http ://www.g3-plc.com/home/

[24] Berger, L. T., Schwager, A., Galli, S., Pagani, P., Schneider, D. M., & Lioe, H. (2014). Current Power Line Communication Systems : A Survey.

[25] Galli, S., & Le Clare, J. (2014). Narrowband Power Line Standards. In MIMO Power Line Communications : Narrow and Broadband Standards, EMC, and Advanced Processing (pp. 271-300). CRC Press.

[26] $http://www.erdfdistribution.fr/medias/Linky/PLC_G3_Physical_Layer_Specification.pdf$

[27] http ://www.prime-alliance.org/portals/0/specs/PRIME-Specv13E201005.pdf

[28] Hoch, M. (2011, April). Comparison of PLC G3 and PRIME. In Power Line Communications and Its Applications (ISPLC), 2011 IEEE International Symposium on (pp. 165-169). IEEE.

[29] Razazian, K., Kamalizad, A., Umari, M., Qu, Q., Loginov, V., & Navid, M. (2011, April). G3-PLC field trials in US distribution grid : Initial results and requirements. In Power Line Communications and Its Applications (ISPLC), 2011 IEEE International Symposium on (pp. 153-158). IEEE.

[30] Razazian, K., Umari, M., Kamalizad, A., Loginov, V., & Navid, M. (2010, March). G3-PLC specification for powerline communication : Overview, system simulation and field trial results. In Power Line Communications and Its Applications (ISPLC), 2010 IEEE International Symposium on (pp. 313-318). IEEE.

[31] Dzung, D., Berganza, I., & Sendin, A. (2011, April). Evolution of powerline communications for smart distribution : from ripple control to OFDM. In Power Line Communications and Its Applications (ISPLC), 2011 IEEE International Symposium on (pp. 474-478). IEEE.

[32] Richardson, T. J., Shokrollahi, M. A., & Urbanke, R. L. (2001). Design of capacity-approaching irregular low-density parity-check codes. IEEE transactions on information theory, 47(2), 619-637.

[33] Kabore, A. W., Meghdadi, V., Cances, J. P., Gaborit, P., & Ruatta, O. (2015, March). Performance of Gabidulin codes for narrowband PLC smart grid networks. In Power Line Communications and its Applications (ISPLC), 2015 International Symposium on (pp. 262-267). IEEE.

[34] Richter, G., & Plass, S. (2004). Fast decoding of rank-codes with rank errors and column erasures. In Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on (pp. 398-398). IEEE.

[35] "IEEE standard for Low-Frequency (less than 500 khz) Narrowband Power Line Communications for Smart Grid Applications," IEEE Std 1901.2-2013, pp. 1–269, Dec 2013.

[36] LIVERIS, Angelos D., XIONG, Zixiang, et GEORGHIADES, Costas N. Compression of binary sources with side information at the decoder using LDPC codes. IEEE communications letters, 2002, vol. 6, no 10, p. 440-442.

Chapitre 2 :

Les codes correcteurs d'erreurs pour les réseaux CPL

2.1 Introduction

Les codes correcteurs d'erreurs sont généralement utilisés pour améliorer la qualité de communication dans les systèmes des télécommunications.

Dans ce chapitre, nous allons présenter les codes Reed-Solomon, les codes LDPC, les codes convolutifs et les codes à métrique rang qui sont préconisés et/ou implémentés dans les systèmes CPL-BE. Nous commencerons par l'étude globale des codes correcteurs d'erreurs, puis nous développerons plus précisément le fonctionnement de chaque code avec ses techniques d'encodage-décodage.

Enfin, nous présenterons le code LRPC que nous avons proposé. Dans le chapitre suivant, ce code sera testé dans un réseau CPL-BE et comparé avec différents codes.

2.2 Théorie des codes

La notion de "codes" a été introduite par Shannon en 1948. Dans son papier [1], il a montré qu'il est possible de faire une transmission fiable sur un canal non-fiable de capacité C. Les codes, selon Shannon, sont définis comme un ensemble fini de vecteurs. Nous supposons que ces vecteurs sont de taille identique N et leur nombre est égale à 2^K. Ces vecteurs peuvent être codés par K bits. Alors, il faut N utilisations du canal pour transmettre K bits. Le rendement R du code est calculé par le rapport K/N. La fiabilité de la transmission sur un canal non-fiable est réalisée lorsque le rendement est inférieur à la capacité $R < C$. A la réception, un décodeur est mis en place qui sert à vérifier l'intégrité des données pour récupérer le message envoyé. Généralement, lors d'une communication le canal présente des erreurs qui empêchent la bonne réception des données. Dans ce cas, le décodeur utilise des règles de maximum de vraisemblance (Maximum Likelihood) [2] pour retrouver le mot de code le plus probable. Il existe, selon le théorème de Shannon en 1948, des codes qui peuvent atteindre une probabilité d'erreur du décodeur à maximum de vraisemblance qui tend vers 0 quand la longueur du code est suffisamment grande. Ce théorème n'est cependant pas constructif et ne donne aucun indice pour trouver ces codes. En outre, la construction de ces codes reste toujours un problème ouvert. Depuis ce jour, les scientifiques cherchent toujours à développer des codes qui permettent d'atteindre un rendement proche de la capacité théorique de Shannon. Le tableau ci-dessous présente l'historique des codes et des algorithmes d'encodage-décodage développés. Les codes linéaires étaient une solution pour l'encodage avec une simple multiplication matricielle par le message à transmettre mais le décodage reste toujours la mission la plus délicate à réaliser. Les scientifiques ont cherché à avoir un code avec une grande longueur N et dimension K sans tenir compte de la complexité de décodage. En revanche, cette complexité limite la longueur du code entraînant un écart entre les

1 :	Bases de la théorie de l'information [1]	1948
2 :	Codes de Golay [3] Code parfait corrigeant 3 erreurs	1949
3 :	Codes de Hamming [4] Code parfait corrigeant 1 erreur	1950
4 :	Codes de Reed Muller découvert par Muller et Reed [5, 6]	1954
5 :	Codes Convolutifs inventé par Elias [7]	1955
6 :	Codes cycliques découvert par Prange [8]	1957
7 :	Codes BCH par Hocquenghem, Bose et Chaudhuri [9, 10]	1959
8 :	Codes de Reed Solomon [11]	1960
9 :	1ère découverte des codes LDPC par Gallager [12]	1962
10 :	Codes concaténés introduit par Forney [13]	1966
11 :	Algorithme de Viterbi [14]	1960
12 :	Algorithme de Berlekamp Massey [15]	1969
13 :	Modulation codées par Underboeck [16]	1982
14 :	Turbo-codes par Berrou, Glavieux et Thitimajshima [17]	1993
15 :	Redécouverte des codes LDPC par MacKay et Neal [18]	1996
16 :	Codes LT découvert par Luby [19]	2002
17 :	Codes Raptor par Shokrolahi [20]	2006
18 :	Codes polaires par Arikan [21]	2009
19 :	Spinal codes par Perry et Balakrishnan [22]	2011

Tableau 2.1 – Historique des codes correcteurs d'erreurs

performances des codes et la limite donnée par Shannon. En 1993, la limite de Shannon fut atteinte par l'invention des turbo-codes basés sur le décodage itératif de deux codes convolutifs récursifs systématiques séparés par un entrelaceur et concaténés en parallèle. Ensuite, en 1996 la redécouverte des codes LDPC par MacKay a permis de trouver une autre classe de codes qui peuvent fonctionner au plus près de la borne de Shannon.

2.3 Les codes Reed-Solomon

Les codes Reed-Solomon sont des codes de correction d'erreurs basés sur des blocs de données avec une large gamme d'applications dans les communications et le stockage numériques. Les codes Reed-Solomon sont utilisés pour corriger les erreurs dans de nombreux systèmes, y compris les dispositifs de stockage (les disques compacts, les DVD, les codes barres) , les communications sans fil ou mobiles (les téléphones cellulaires, les liaisons hyperfréquences), etc. L'encodeur Reed-Solomon prend un bloc de données numériques et ajoute des bits "redondants" supplémentaires. Les erreurs se produisent pendant la transmission ou le stockage pour plusieurs raisons (par exemple bruit ou interférence, rayures sur un CD, etc.). Le décodeur Reed-Solomon traite chaque bloc et tente de corriger les erreurs et de récupérer les données d'origine. Le nombre et le type d'erreurs pouvant être corrigées dépendent des caractéristiques du code Reed-Solomon. Les codes Reed Solomon sont des codes en blocs linéaires. Un code Reed-Solomon est

spécifié comme RS (n, k) avec les symboles s-bit (k bits en entrée et n bits en sortie) tel que $s = \frac{n}{k}$. Cela signifie que l'encodeur prend k symboles de données de s bits chacun et ajoute des symboles de parité pour créer un mot de code symbole de $n \times s$ bits en sortie. Il existe des symboles de parité $n - k$ de s bits chacun. Un décodeur Reed-Solomon peut corriger les symboles t qui contiennent des erreurs dans un mot de code, où $2t = n - k$. La figure 2.1 montre un Reed-Solomon typique (c'est ce qu'on appelle un code systématique car les données sont laisses inchangées et les symboles de parité sont ajoutés).

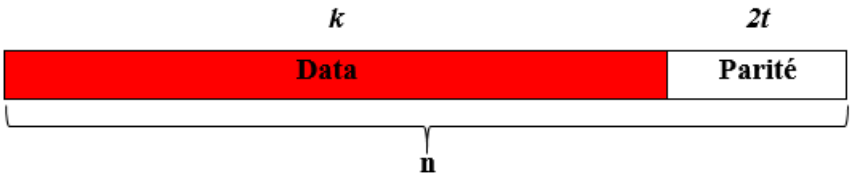


FIGURE 2.1 – Code systématique RS avec les symboles de parité

2.3.1 Encodage des codes Reed-Solomon

Les codes Reed-Solomon sont basés sur l'utilisation des corps de Galois (Galois Field GF) ou de corps finis. Une de ces propriétés est que les opérations arithmétiques (+, -, x, / etc.) sur les éléments du corps conduisent toujours à un résultat qui appartient à ce corps. Un encodeur ou un décodeur Reed-Solomon doit effectuer ces opérations arithmétiques. Ces opérations nécessitent des fonctions matérielles ou logicielles spéciales à mettre en œuvre. Les codes RS sont généralement représentés sous forme polynomiale. Pour obtenir le mode de code $c(x)$, il suffit de multiplier le message $m(x)$ par un polynôme générateur $g(x)$. Tous les mots de code valides sont divisibles par ce polynôme qui prend la forme :

$$g(x) = (x - \alpha)(x - \alpha^2) \cdots (x - \alpha^{2t}), \tag{2.1}$$

Et le mot de code est construit en utilisant :

$$c(x) = g(x).m(x), \tag{2.2}$$

où α est un élément primitif du corps fini $GF(2^8)$ [38, 39].

2.3.2 Décodage des codes Reed-Solomon

Le mot de code reçu $r(x)$ est le mot de code original (transmis) $c(x)$ plus les erreurs $e(x)$:

$$r(x) = c(x) + e(x), \tag{2.3}$$

Un décodeur Reed-Solomon tente d'identifier la position et l'amplitude des t erreurs (ou $2t$ effacements), puis commence à les corriger. Tout d'abord, il commence par le calcul du syndrome, il s'agit d'un calcul similaire au calcul de la parité. Un mot de code Reed-Solomon comporte $2t$ syndromes qui dépendent uniquement d'erreurs (pas sur le mot de code transmis). Les syndromes peuvent être calculés en substituant les racines $2t$ du polynôme générateur $g(x)$ en $r(x)$. Lorsque le mot reçu est un mot de code, alors son syndrome est nul et l'algorithme de correction n'est pas appliqué. Dans le cas où le mot reçu n'est pas un mot de code alors l'algorithme de décodage est appliqué pour déterminer la position des erreurs puis pour trouver le mot de code le plus proche du mot reçu. Cela implique de résoudre un ensemble d'équations à t inconnues. Plusieurs algorithmes rapides sont disponibles pour ce faire. Ces algorithmes profitent de la structure matricielle spéciale des codes Reed-Solomon et réduisent considérablement l'effort de calcul requis. En général, deux étapes sont impliquées :

– Trouver un polynôme de localisation d'erreur

Cela peut être fait en utilisant l'algorithme de Berlekamp-Massey ou l'algorithme d'Euclide. Cependant, l'algorithme Berlekamp-Massey, le plus répandu, tend à conduire à des implémentations matérielles et logicielles plus efficaces.

– Trouver les racines de ce polynôme

2.4 Les codes LDPC

Les codes LDPC ont été inventés par Robert Gallager [23] dans sa thèse de doctorat. Peu de temps après leur invention, ils ont été largement oubliés et réinventés à plusieurs reprises au cours des 30 prochaines années qui ont suivi. Les codes LDPC sont des codes linéaires obtenus à partir de graphes bipartites. Supposons que G soit un graphe avec n nœuds gauches (appelés nœuds de variables) et r nœuds droits (appelés nœuds de contrôle). Le graphique donne naissance à un code linéaire de longueur de bloc n : les n coordonnées des mots de code sont associées aux n nœuds de message. Les mots de code sont ces vecteurs $(c_1, \cdots, c_n)$ tels que pour tous les nœuds de contrôle, la somme (modulo 2) des positions voisines parmi les nœuds de message est nulle. La figure 2.2 montre un exemple de graphe bipartite. Cette représentation graphique est équivalente à une représentation matricielle en regardant la matrice adjacente du graphe. Soit $\mathbf{H}$ une matrice binaire de taille $r \times n$ dans laquelle l'entrée (i, j) est 1 si et seulement si le $i$ème nœud de contrôle est connecté au $j$ème nœud de message dans le graphique. Ensuite, le code LDPC défini par le graphe est l'ensemble des vecteurs $c = (c_1, \cdots, c_n)$ tel que $\mathbf{H}.c^T = 0$. La matrice $\mathbf{H}$ est appelée matrice de contrôle de parité pour le code LDPC (Parity Check Matrix). À l'inverse, toute matrice $r \times n$ binaire donne lieu à un graphe bipartite entre les n nœuds message et r, et le code défini comme espace nulle de $\mathbf{H}$

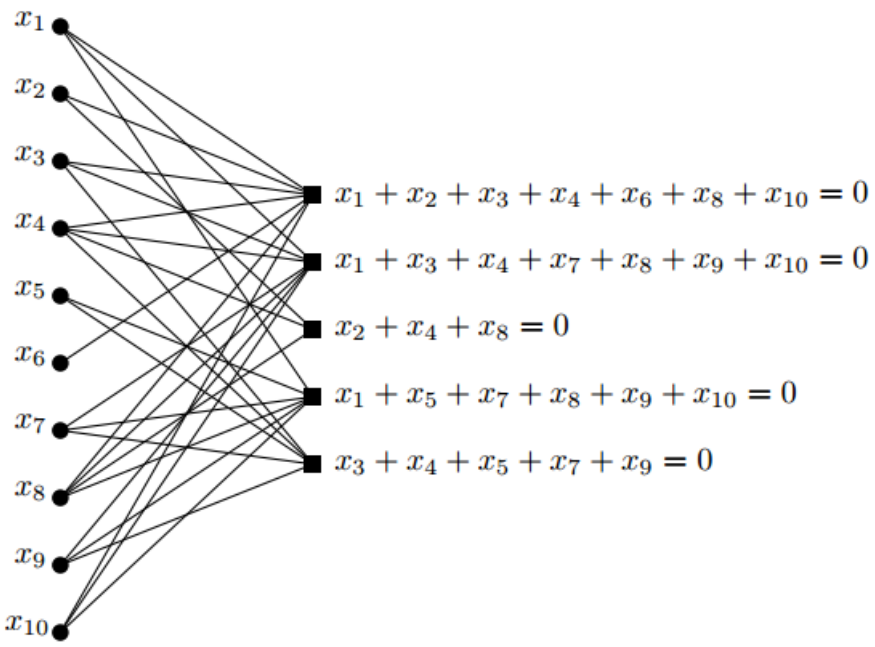


FIGURE 2.2 – Graphe de Tanner d'un code LDPC

est précisément le code associé à ce graphique. Par conséquent, tout code linéaire a une représentation en tant que code associé à un graphique bipartite (notez que ce graphique n'est pas défini uniquement par le code). Cependant, tous les codes linéaires binaires ne sont pas représentés par un graphique avec peu de connexions encore appelé graphe bipartite creuse. [1]Si c'est le cas, le code s'appelle un code LDPC (Low-density Parity-Check). La structure creuse du graphique est une propriété clé qui permet l'efficacité de l'algorithme de décodage des codes LDPC. Le reste de ce chapitre est consacré à l'élaboration de l'algorithme de décodage.

2.4.1 Décodage itératif des codes LDPC

Il existe différents algorithmes de décodage itératifs pour les codes LDPC et ils sont classés en deux catégories principales : les algorithmes de décodage à décision "Hard" et les algorithmes à décision souples. Il existe différents algorithmes pour traiter le décodage des codes LDPC [40]. Les explications détaillées des algorithmes de décodage de décision "durs" et "doux" sont présentées dans la figure 2.3.

1. La sparsité s'applique uniquement aux séquences de matrices. Une séquence de matrices $m \times n$ est appelée c-sparse si mn tend vers l'infini et le nombre d'éléments non nuls dans ces matrices est toujours inférieur à $cmax(m, n)$.

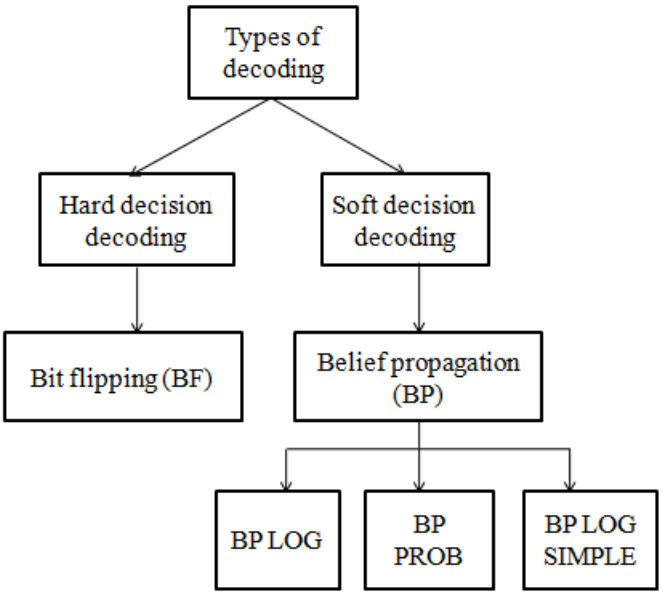


FIGURE 2.3 – Types de décodage des codes LDPC

2.4.2 Décodage à décision "Hard"

Dans ce schéma de décodage dur [41], les nœuds de contrôle trouvent le bit en erreur en vérifiant la validité des équations de parité. On identifie alors les bits qui apparaissent le plus souvent dans les équations de parité non satisfaites et on change les bits impliqués (bit-flipping). L'algorithme de retournement de bits (bit-flipping ou BF) est un exemple de décodage de décision "Hard" [42], [43]. Le décodeur bit-flipping va être immédiatement terminé, chaque fois qu'un mot de code valide a été trouvé. En vérifiant si toutes les équations de vérification de parité sont satisfaites, la procédure est terminée. Nous présentons le détail mathématique de cet algorithme. Soit H la matrice de parité, de taille $m \times n$ à entrées binaires, où $n > m \ggg 1$. Le code binaire C est défini par $C \triangleq \{c \in \mathbb{F}_2^n : C.H^T = 0\}$, où $\mathbb{F}_2$ représente le corps de Galois binaire. Par convention, nous introduisons le code bipolaire $\tilde{C}$ correspondant à C de la manière suivante :

$$\tilde{C} = \{(1 - 2c_1, 1 - 2c_2, \cdots 1 - 2c_n) : c \in C\}$$

Un canal AWGN à entrée binaire est considéré dans ce cas, il est défini par $y = c + z$ avec $c \in C$. Le vecteur $z = (z_1, z_2, \cdots, z_n)$ est un vecteur d'échantillons de bruit blanc gaussien de moyenne nulle et de variance σ^2. Nous posons $N(i)$ et $M(j)$ avec $i \in [1, m]$ et $j \in [1, n]$ les ensembles d'indices suivants tels que : $N(i) \triangleq \{j \in [1, n] : h_{ij} = 1\}$ et $M(j) \triangleq \{i \in [1, m] : h_{ij} = 1\}$ où h_{ij} est le ij-ème élément de la matrice de parité H. En utilisant cette notation nous pouvons écrire la condition de parité ainsi le syndrome $= \prod_{j \in N(i)} x_j = 1 \ \forall i \in [1, m]$ ce qui est équivalent à $(x_1, x_2, \cdots, x_n) \in \tilde{C}$. L'algorithme

bit-flipping est basé sur l'inversion des bits les moins fiables. Normalement, l'inversion est liée à une métrique qui doit être calculée, selon laquelle la décision est prise pour inverser le bit ou non. La fonction d'inversion de la version basique de l'algorithme BF est définie par :

$$\Delta k^{BF}(x) = \sum_{i \in M(k)} \prod_{j \in N(i)} x_j$$

L'objectif de cette fonction d'inversion BF est d'identifier les bits reçus qui participent au plus grand nombre d'équations de parité non satisfaites.

2.4.3 Décodage à décision "Soft"

Le décodage de décision Soft (souple) [42], [43] donne des performances améliorées dans la procédure de décodage des codes LDPC [44]. Il repose sur l'idée de propagation de croyance ou belief propagation (BP) en anglais. Dans un schéma à décodage souple, les messages sont la probabilité conditionnelle que le bit du vecteur reçu soit un "0" ou un "1". L'algorithme de somme produit est un algorithme de décodage de message de décodage de décision Soft. Les probabilités à Priori pour les bits reçus sont les probabilités en sortie du canal à l'initialisation. Les probabilités de bits retournées par le décodeur sont appelées les probabilités à Posteriori. L'algorithme belief propagation [45] est illustré par la méthode de sum product. Nous supposons un système de communication d'un canal AWGN de variance σ^2, $U(u_1, u_2, \cdots, u_n)$ est le signal transmis, $Y(y_1, y_2, \cdots, y_n)$ est le signal reçu, n est le nœud de bits, m est le nœud de contrôle, l'algorithme somme produits (sum-product) dans le processus de décodage est le suivant :

1. Initialisation du nœud de bits n : Calcul des probabilités en sortie du canal
$$\lambda_{n \longrightarrow m}(u_n) = log \frac{P(u_n=0/y_n)}{P(u_n=1/y_n)} = \frac{2y_n}{\sigma^2}$$
2. Initialisation du nœud de contrôle m
$$\Lambda_{m \longrightarrow n}(u_n) = 0$$
3. Mise à jour du nœud de contrôle m
$$\Lambda_{m \longrightarrow n}(u_n) = 2tanh^{-1}\Big\{ \prod_{n' \in N(m) \backslash n} tanh\Big[\frac{\lambda_{n' \longrightarrow m}(u_{n'})}{2}\Big]\Big\}$$
4. Mise à jour du nœud de bits n
$$\lambda_{n \longrightarrow m}(u_n) = \frac{2y_n}{\sigma^2} + \sum_{m' \in M(n) \backslash m} \Lambda_{m' \longrightarrow n}(u_n)$$
5. En supposant que le signal décodé est $\tilde{U}(\tilde{u}_1, \tilde{u}_2, \cdots, \tilde{u}_n)$, nous prenons la décision selon la règle de décodage suivante :
$$\tilde{u}_i = \begin{cases} 0, \text{ si } \lambda_i(u_i) \geq 0 \ \forall i \in \{1, 2, \cdots, n\} \\ 1, \text{ si } \lambda_i(u_i) \leq 0 \ \forall i \in \{1, 2, \cdots, n\} \end{cases}$$
avec
$$\lambda_n(u_n) = \frac{2y_n}{\sigma^2} + \sum_{m \in M(n)} \Lambda_{m \longrightarrow n}(u_n)$$

2.5 Les codes convolutifs

Dans les télécommunications, un code convolutif est un type de code de correction d'erreurs qui génère des symboles de parité via l'application par fenêtre glissante d'une fonction polynomiale booléenne à partir du flux de données entrant. L'application coulissante représente la "convolution" du codeur sur les données, ce qui donne lieu au terme "codage convolutif". La nature glissante des codes convolutifs facilite le décodage en treillis en utilisant un treillis invariant dans le temps. Le décodage de treillis invariant dans le temps permet aux codes convolutifs d'utiliser un algorithme à maximum de vraisemblance avec une complexité raisonnable. C'est l'utilisation de l'algorithme de Viterbi qui permet d'implémenter le maximum de vraisemblance avec une complexité modérée. Les codes convolutifs sont souvent caractérisés par le rendement du code de base et la profondeur (ou mémoire) du codeur $[n, k, K]$. Le rendement du code de base est généralement donné comme n/k, où n est le nombre de bits en sortie du codeur et k est le nombre de bits en entrée. La profondeur est souvent appelée "longueur de contrainte" K, où la sortie est fonction de l'entrée actuelle ainsi que des $K-1$ entrées précédentes. La profondeur peut également être donnée en tant que nombre d'éléments de mémoire v dans le polynôme générateur du code ou le nombre maximum possible d'états du codeur (typiquement 2^v). La description qui suit des encodeurs convolutifs figure dans plusieurs références, comme par exemple [24]. Un encodeur convolutif est une machine d'état fini de Markov qui prend comme entrées des bits d'information et comme sorties des bits de code. Il est représenté par ses polynômes générateurs, son diagramme d'état et/ou son diagramme de treillis. Normalement, les encodeurs convolutifs sont mis en application par un ensemble de registres à décalage linéaire et d'additionneurs (modulo-2). La figure 2.4 représente le circuit généralement utilisé pour un encodeur convolutif de registre à décalage avec un rendement 1/2. Le polynôme générateur de bit de code c_i est

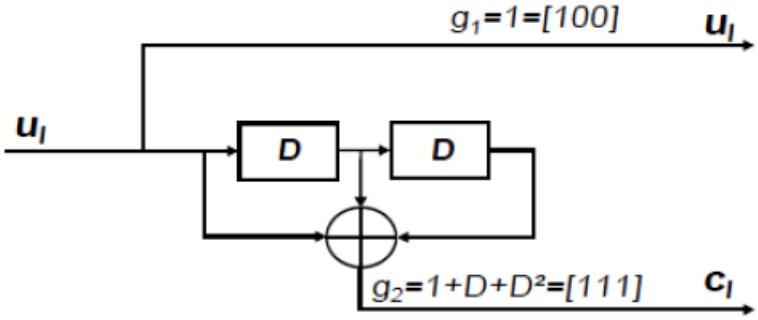


FIGURE 2.4 – Encodeur SC de rendement 1/2

$g_2 = 1 + D + D^2$. Cette formule déclare que les éléments de registre à décalage retardent de respectivement zéro ($D^0 = 1$), un ($D^1 = D$) et deux (D^2) pour obtenir la sortie c_i. Le

polynôme générateur de l'encodeur est $G(D) = [1, 1 + D + D^2]$ où le premier polynôme est égal à 1 puisque le premier bit de code est directement connecté au bit d'information (c-à-d. d'une façon systématique). Alors, l'encodeur est nommé convolutif systématique (systematic convolutional : SC). Puisque le plus grand retard dans le polynôme est celui de l'élément D^2, l'encodeur possède une longueur de mémoire $m = 2$. La longueur de contrainte de l'encodeur est $v = 3$. Elle est déterminée en ajoutant le nombre de(s) entrée(s) à la longueur de mémoire m. Le diagramme d'état de l'encodeur de la figure 2.4 est représenté sur la figure 2.5. Une transition est provoquée par une entrée u_i, notée par $u_i/c_i(u_i, c_i \in \{0, 1\})$. Le nombre de passages possibles d'un état à un autre est limité.

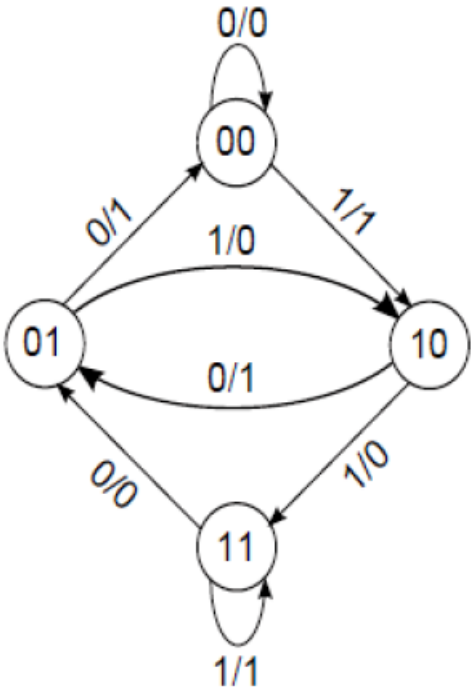


FIGURE 2.5 – Diagramme d'états 1/2

Ainsi, le mot d'information encodé suit un processus d'accès bien déterminé dans le diagramme d'état de l'encodeur convolutif spécifié. Ce processus peut être représenté par un diagramme de treillis. La figure 2.6 représente un chemin de treillis pour le codage de la séquence de bit d'information "00110" qui est encodé avec l'encodeur convolutif de la figure 2.4. Le mot de code correspondant au mot d'information est obtenu en suivant les transitions convenables. En conséquence, la séquence de sortie est "0000111000". Par la suite, les bits de code peuvent être envoyés à travers un canal en utilisant une modulation arbitraire. Les bits de données seront encodés un par un en des bits de code, l'encodeur s'arrêtera après un certain nombre d'états. Il est possible d'ajouter des bits d'information pour avoir à la fin l'état zéro (c-à-d. initialiser les registres à décalage). Quand un encodeur

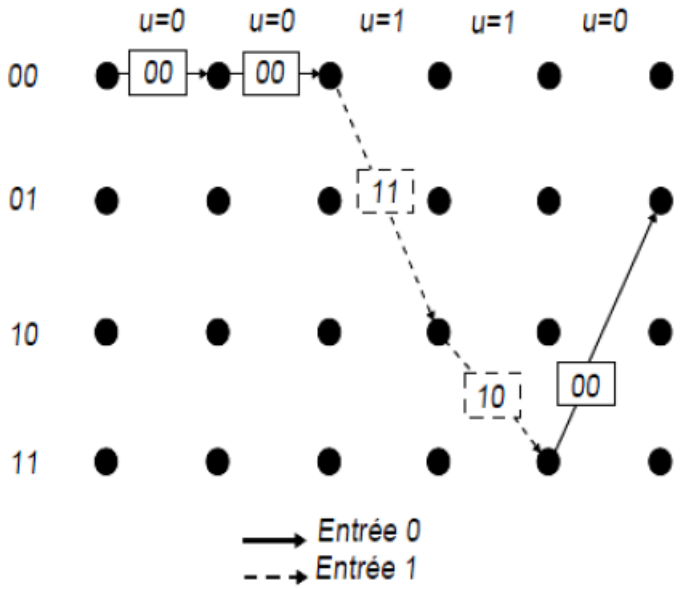


FIGURE 2.6 – Chemin de treillis pour le codage de la séquence de bits d'information "00110"

ne peut pas réaliser cet état final, il s'agit d'un encodeur tronqué.

2.5.1 Encodeur Convolutif Récursif Systématique (RSC)

L'apparition d'encodeur convolutif récursif systématique (recursive systematic convolutional : RSC) est une étape importante dans le codage de canal car leur concaténation en parallèle a donne naissance aux Turbo codes convolutifs. Ce type d'encodeurs a un polynôme de contrôle pour le retour de l'information (Feedback), qui connecte certains éléments des registres à décalage avec l'entrée d'autres éléments par l'intermédiaire d'un additionneur modulo-2. La figure 2.7 représente un exemple d'encodeur RSC de rendement 1/2. Son polynôme générateur est défini par $G(D) = [1, \frac{1+D+D^2}{1+D^2}]$. Un encodeur RSC se caractérise par une réponse impulsionnelle infinie (infinite impulse response : IIR), en raison de ses connexions de contrôle pour le retour de l'information [25]. Ceci a comme conséquence une réponse infinie des "1" et des "0" pour une séquence d'information initiale ne contenant qu'un seul "1". Ainsi, chaque séquence d'information nécessite la détermination d'une séquence de terminaison appropriée. L'encodeur convolutif peut être également représenté à l'aide d'un diagramme d'état, ce qui donne l'état suivant de chaque registre à décalage.

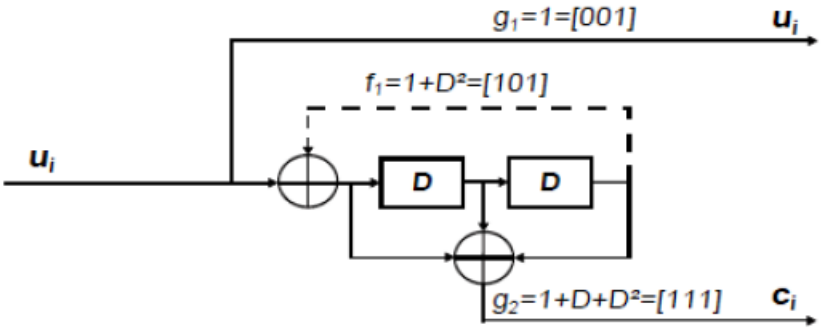


FIGURE 2.7 – Encodeur RSC $(1, 7/5)$

2.5.2 Entrelacement (Interleaver)

L'entrelacement des données codées de manière à rendre les erreurs indépendantes est une bonne solution pour lutter contre les canaux à évanouissements [26]. Ainsi, en utilisant un tel système, les données codées sont réordonnées par un entrelaceur et transmises sur le canal. Au récepteur, après la démodulation, le désentrelaceur réordonne les symboles reçus et les transmet au décodeur. Les erreurs obtenues avec entrelacement n'arrivent plus en bloc, mais de façon indépendante.

2.5.3 Décodage des codes convolutifs

Plusieurs algorithmes existent pour le décodage des codes convolutifs [27]. Pour des valeurs relativement faibles de k, l'algorithme de Viterbi est universellement utilisé car il fournit une performance proche de l'algorithme de maximum de vraisemblance optimal. Les décodeurs Viterbi sont faciles à mettre en œuvre dans le matériel VLSI et dans les logiciels sur les CPU avec des ensembles d'instructions SIMD.

Viterbi et les algorithmes de décodage séquentiels retournent les bits qui forment le mot de code le plus probable. Une mesure de confiance qui consiste à calculer les rapports de vraisemblance logarithmiques (LLR's) des bits transmis peut être ajoutée à chaque bit à l'aide de l'algorithme de Viterbi à sorties souple ou Soft. Les décisions souples maximales a posteriori (MAP) pour chaque bit peuvent être obtenues par l'utilisation de l'algorithme BCJR.

Concernant le décodage des codes convolutifs (NSC ou RSC), on utilise l'algorithme de Viterbi [46] qui approxime au mieux le décodage par maximum de vraisemblance et qui utilise un diagramme en treillis comme celui illustré sur la figure 2.10. Les états sont représentés par l'état des registres à décalage du codeurs (B1 et B2 sur les figures 2.8 et 2.9). Les états communiquent entre eux en fonction de leurs états courant et de la nouvelle entrée (0 ou 1) qui arrive. La suite des états parcourus tout au long du codage

du message à transmettre associée à la suite des bits obtenus en sortie forme le treillis du code. L'algorithme de Viterbi va alors chercher parmi tous les chemins possibles à travers le treillis celui qui minimise la distance entre la séquence reçue et les différentes séquences reconstruites à travers le treillis.

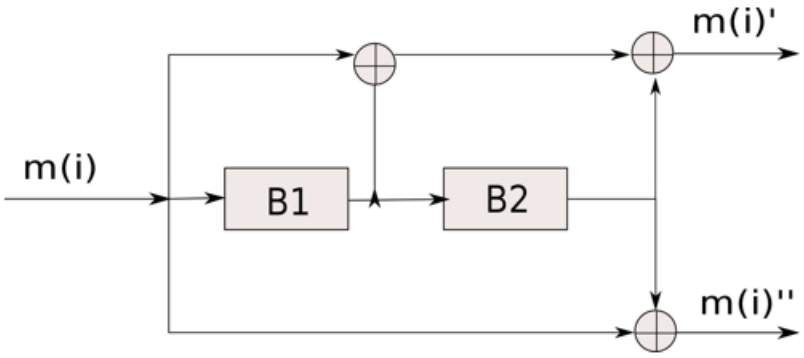


FIGURE 2.8 – Encodeur NSC (non systématique convolutif)

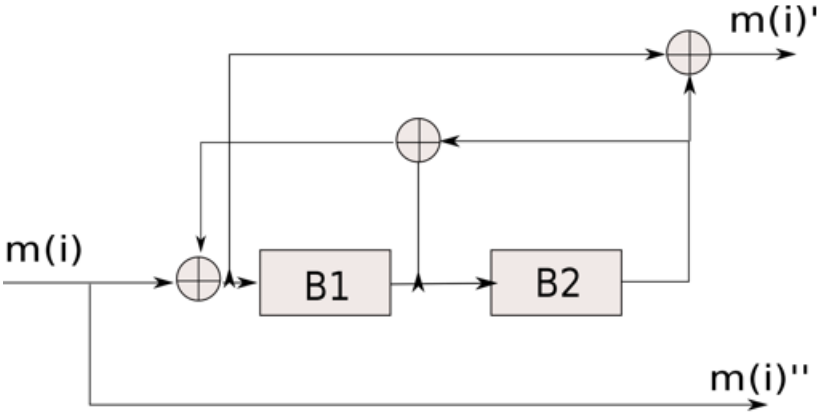


FIGURE 2.9 – Encodeur RSC (récursif systématique convolutif)

2.5.4 Concaténation série de codes

La concaténation des codes est une méthode qui sert à augmenter le pouvoir de correction des codes en travaillant sur la distance minimale d_{min}. Cette technique consiste à encoder en premier lieu le message par le premier code (outer code) puis le mot de code sera ré-encodé par un deuxième code (inner code). La concaténation série des codes RS (outer code) avec les codes convolutifs (inner code) a été utilise dans les réseaux CPL-BE. Ces deux codes sont généralement précédés par un entrelaceur en temps et en fréquence

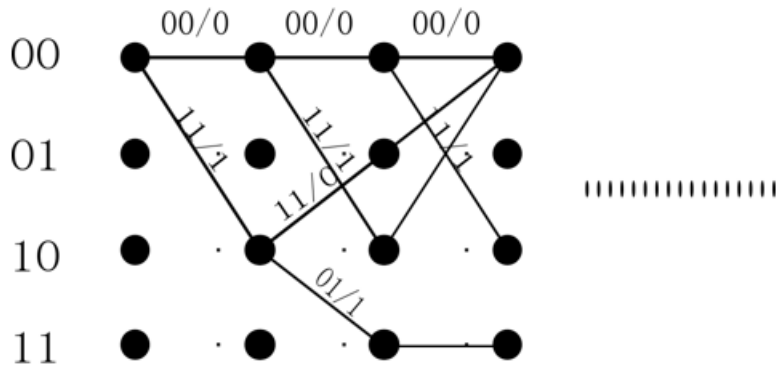


FIGURE 2.10 – Exemple de diagramme en treillis

pour éviter les erreurs en blocs dûes au bruit impulsif et au bruit à bande étroite qui sont difficiles à corriger par les codes convolutifs. Les codes convolutifs utilisent la méthode de zéro tailing bits [2] et terminent l'encodage en mettant tous les bits à zéros [28]. Ces codes utilisent l'algorithme de Viterbi comme algorithme de décodage qui sert à éliminer les erreurs isolés et les codes RS utilisent un algorithme de Berlekamp Massey qui est adapté aux erreurs en blocs.

2.6 Codes correcteurs en métrique de rang

La théorie de la métrique rang a été développé par Gabidulin en 1985, dans la suite des travaux faits par Delsarte comme alternative à la métrique de Hamming. Cette théorie constitue une généralisation des travaux de l'auteur sur les codes qui corrigent des motifs d'erreur matricielles [29]. Gabidulin a pu montrer l'existence d'une famille de codes atteignant la borne du Singleton et décodable en un temps polynomial. Utiliser la métrique de rang pour la détection d'erreurs est souvent peu intéressant, car les canaux réels de communication introduisent rarement une erreur dont le motif peut être modélisé efficacement en métrique rang. Cela est dû à la présence de bruit additif Gaussien ce qui entraîne la présence d'un espace d'erreurs de taille non finie. Cependant, il semble que les outils de cette métrique sont adaptés dans le cadre des canaux CPL-BE et du network coding [30]. En fait ces codes deviennent très efficaces chaque fois que les erreurs appartiennent à des sous-espaces de dimensions réduites. Nous présentons dans un premier temps quelques propriétés de la métrique rang, qui va nous servir pour la construction du code LRPC. Ensuite, nous montrons qu'on peut construire des codes pour cette métrique. Ceux-ci sont les analogues pour la métrique de Hamming des codes de Reed-Solomon généralisés. En conséquence, nous dérivons un algorithme de décodage

2. le nombre de bits à ajouter dépend de la longueur de contrainte du code

en temps polynomial pour les codes de Gabidulin, calqué sur l'algorithme de décodage des codes de Reed-Solomon généralisés [31][32]. Dans tous ce qui suit, nous considérons que n est la longueur de mot de codes C, $\mathbb{F}_{q^m}$ est un corps fini à q^m éléments, où q est une puissance d'un nombre premier. Nous fixons aussi pour la suite de ce chapitre, une base de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$ notée $(\beta_1, \beta_2, \cdots, \beta_m)$.

2.6.1 Métrique rang : définitions et propriétés

Définition 1. *Soit $x = (x_1, x_2, \cdots, x_n) \in \mathbb{F}_{q^m}^n$. Nous appelons le rang de x sur $\mathbb{F}_q$, le rang de la matrice $\boldsymbol{X} = (x_{ij})$, où $x_j = \sum_{i=1}^{m} x_{ij}\beta_i$. Nous le notons sous forme de $Rg(x|\mathbb{F}_q)$.*

Le nombre de vecteurs de rang t dans $\mathbb{F}_{q^m}$ est donné par la formule du binôme de Gauss, en comptant le nombre de matrice de taille $m \times n$ de rang égale à t, dont leurs coefficients sont dans $\mathbb{F}_q$.

$$\begin{bmatrix} m \\ t \end{bmatrix}_q = \prod_{i=0}^{t-1} \frac{q^m - q^i}{q^t - q^i} \tag{2.4}$$

La métrique rang est plus grossière que la métrique de Hamming par la proposition suivante :

Proposition 1. *Soit x un mot de code de $\mathbb{F}_{q^m}$, alors on a : $Rg(x) \leq \omega(x)$, où $\omega(x)$ désigne le poids Hamming du vecteur x.*

Le poids de x désigne le nombre de coordonnées non nulles de x, donc si on écrit x sous forme d'une matrice $\mathbf{X}$ dans la base $(\beta_1, \beta_2, \cdots, \beta_m)$, alors le rang de la matrice $\mathbf{X}$ est plus petit que $\omega(x)$ puisque $\mathbf{X}$ possède $\omega(x)$ colonnes nulles.

Proposition 2. *L'application $x, y \mapsto Rg(x-y)$ est une distance sur $\mathbb{F}_{q^m}^n$, appelée distance rang.*

La distance rang minimale est définie de la même façon que dans le cas d'un code linéaire en distance de Hamming.

2.6.2 Polynômes linéaires : définitions et propriétés

Dans cette partie, nous reprenons les principaux résultats parus dans les articles [33][34][35] de Öre. Nous définissons les q-polynômes. Ensuite, nous étudions la structure de l'ensemble des racines d'un polynôme linéaire. Nous formalisons des résultats déjà connus sur les racines de polynômes linéarisés avec la notion d'espaces vectoriels. Nous

notons q une puissance d'un nombre premier et m un nombre entier. Nous rappelons que $\mathbb{F}_{q^m}$ peut être vu comme un espace vectoriel de dimension m sur $\mathbb{F}_q$.

Définition 2. *Un polynôme linéaire (ou q-polynôme) sur $\mathbb{F}_{q^m}$ de q-degré t est un polynôme de la forme :*

$$P(X) = a_t X^{q^t} + \cdots + a_i X^{q^i} + aX^q + a_0 X, \tag{2.5}$$

où $a_k \neq 0$.

Par la suite, nous notons $[i] = q^i$.

Théorème 1. *L'ensemble des q-polynômes muni des lois + et $\circ$ est un sous-anneau non commutatif de $L(\mathbb{F}_{q^m})$, l'ensemble des applications $\mathbb{F}_q$ linéaires de $\mathbb{F}_{q^m}$ dans $\mathbb{F}_{q^m}$ [34].*

Proposition 3. *Soit deux q-polynômes $P_1(X) = \sum_{i=0}^{t_1} a_i X^i$ et $P_2(X) = \sum_{i=0}^{t_2} b_i X^i$, alors le produit de ces deux polynômes donnent $P_1(X)P_2(X) = \sum_{i=0}^{t_1+t_2} c_i X^i$, où $c_i = \sum_j a_j b_{i-j}^{[j]}$.*

Le point difficile est le calcul de $A \circ B$, à partir des coefficients de A et de B. Ce calcul est réalisé en $O(kk')$ multiplications dans $\mathbb{F}_{q^m}$.

Définition 3. *L'évaluation d'un q-polynôme P sur un vecteur $x = (x_1, \cdots, x_n)$ de longueur n est $(P(x_1), \cdots, P(x_n))$.*

Corollaire 1. ***(Lien entre les polynômes linéaires et la métrique rang).***
Soit x est un vecteur de $\mathbb{F}_{q^m}$. Le vecteur x est de rang t sur $\mathbb{F}_{q^m}$ si et seulement si le q-polynôme V unitaire de plus petit q-degré tel que $V(x) = 0$ est de q-degré t.

2.7 Les codes Gabidulin

2.7.1 Définition et propriétés

Si P est un polynôme linéaire et $x \in \mathbb{F}_{q^m}$, on notera $P(x) = (P(x_1), ..., P(x_n))$.

Définition 4. *Soit $g \in \mathbb{F}_{q^m}$ une famille libre sur $\mathbb{F}_q$.*
Le code de Gabidulin de longueur n, de dimension k, et de support g est l'ensemble des mots obtenus par évaluation d'un q-polynôme de degré au plus $k-1$ sur g :

$$Gab(g,k,n) = \left\{ (P(g_1), ..., P(g_n)) = P(g) | \quad P(z) = \sum_{i=0}^{k-1} p_i z^{[i]} \right\}.$$

La relation entre les codes de Gabidulin et les codes GRS tient aux propriétés communes aux algèbres classiques de polynômes et aux algèbres de polynômes linéarisés.

Proposition 4. ***(MRD)***. *$Gab(g,k,n)$ est un code linéaire optimal en métrique rang, i.e. c'est un code linéaire qui maximise la distance minimale. Soit G une $m \times n$ matrice génératrice de codage dans un corps $\mathbb{F}^q$, si $n \leq m$ sa distance minimale vaut $n-k+1$.*

La distance rang minimale d'un code Gabidulin est définie de la même façon que dans le cas d'un code linéaire en distance de Hamming.

Définition 5. ***(Distance rang minimale)*** *Soit C est un code linéaire de longueur n, de dimension k et de distance minimale (en métrique de rang) d, alors :*

$$d \leq n-k+1$$

Quand $d = n-k+1$, on dit que le code C est un code MRD (Maximum Rank Distance).

Proposition 5. *La matrice génératrice du code engendré par G est de la forme suivante :*

$$A = \left(\begin{array}{cccc|ccc} 1 & 0 & \cdots & 0 & P_1(g_{k+1}) & \cdots & P_1(g_n) \\ 0 & 1 & \cdots & 0 & P_2(g_{k+1}) & \cdots & P_2(g_n) \\ \vdots & \ddots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & P_k(g_{k+1}) & \cdots & P_k(g_n) \end{array}\right)$$

où, pour $i = 1, ..., k$, P_i est l'unique q-polynôme de degré k vérifiant pour tout $j \leq k$, $P_i(g_j) = \delta_{i,j}$.

Une matrice de parité de $Gab_k(g)$ est la matrice

$$A = \left(\begin{array}{cccc} h_1 & h_2 & \cdots & h_n \\ \vdots & \ddots & \ddots & \vdots \\ h_1^{[d-2]} & h_2^{[d-2]} & \cdots & h_n^{[d-2]} \end{array}\right),$$

où, $h = (\lambda_1^{[d]}, \lambda_2^{[d]}, \cdots, \lambda_n^{[d-2]})$ et les λ_i vérifient l'équation

$$\sum_{i=1}^{n} \lambda_i g_i^{[j]} = 0,$$

pour $j = 0, 1, \ldots, n-2$. Ainsi, le code dual de $Gab_k(g)$ est le code $Gab_{n-k}(h)$.

2.7.2 Décodage des codes Gabidulin avec l'algorithme de Berlekamp-Massey modifié

Nous nous intéressons maintenant au décodage des codes de Gabidulin avec l'algorithme de *Berlekamp-Massey modifié* [36].

Supposons que l'erreur d'un mot de code en métrique rang est de la forme :

$$\mathbf{E} = \left(\begin{array}{cc|c|cc} 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 1 & 0 & 0 & 1 \\ \hline 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

C'est une erreur rang car les erreurs se trouvent concentrées sur une colonne uniquement. Si $t \geq 2$, on peut retrouver le mot de code.

Dans toute la section, nous considérons que $\mathbf{C}$ est un code de Gabidulin de langueur n, de dimension k, de distance minimale d dans le corps $\mathbb{F}_{q^m}$, de matrice de parité $\mathbf{H}$ et $y = c + e$ le mot reçu où c un mot de $\mathbf{C}$, e est une erreur et r est le rang de e, avec $2r < d$. Nous calculons

$$s = y.\mathbf{H}^T = e.\mathbf{H}^T.$$

Nous définissons la matrice $\mathbf{Y}$ qui possède des composantes dans le corps $\mathbb{F}_q$ de rang t telle que

$$e = (\mathbf{E}_0, \ldots, \mathbf{E}_{t-1})Y,$$

où $\mathbf{E}_0, \ldots, \mathbf{E}_{t-1} \in \mathbb{F}_q$ sont linéairement indépendants sous $\mathbb{F}_q$.
Nous définissons aussi la matrice $\mathbf{Z}$ comme suit :

$$\mathbf{Z}^T = \mathbf{Y}\mathbf{H}^T = \begin{pmatrix} z_0 & z_0^{[1]} & \cdots & z_0^{[d-1]} \\ \vdots & \vdots & \ddots & \vdots \\ z_{t-1} & z_{t-1}^{[1]} & \cdots & z_{t-1}^{[d-1]} \end{pmatrix}$$

Il est facile de remarquer que $z_0, \ldots, z_{t-1} \in \mathbb{F}_q$ sont linéairement indépendants sous $\mathbb{F}_q$. Donc,

$$(\mathbf{S}_0, \ldots, \mathbf{S}_{d-2}) = (\mathbf{E}_0, \ldots, \mathbf{E}_{t-1}).\mathbf{Z}^T$$

ce qui donne,

$$\mathbf{S}_i^{[-i]} = \sum_{j=0}^{t-1} \mathbf{E}_j^{[-i]} z_j, i = 0, ..., d-2.$$

Donc, nous obtenons $d-1$ équations et $2t$ inconnues, notons aussi que t n'est pas connu aussi, il suffit de trouver une seule solution pour ce système pour récupérer e.
Soit $P(X)$ un q-polynôme de q-degré t qui a comme solutions $\mathbf{E}_0, \ldots, \mathbf{E}_{t-1}$ sous $\mathbb{F}_q$ et $P_0 = 1$, nous l'appelons *polynôme d'erreur*, nous définissons aussi *l'équation clé* dans le théorème suivant :

Théorème 2. *Soit P polynôme d'erreur, nous avons*

$$P(X) \circ S(X) = F(X) mod X^{[d-1]},$$

où $S(X)$ est le polynôme linéaire du syndrome et $F(X)$ est un polynôme auxiliaire avec $deg_q(F) < t$.

Preuve

– D'après la définition de polynôme linéaire, nous avons

$$P(X) \circ S(X) = \sum_{i=0}^{t+d-2} \left(\sum_{j+k=i} P_j S_k^{[j]} \right) X^{[i]}$$

Tout les coefficients sont nuls pour $i \leq d-1$ à cause de modulo, il reste à montrer que $F_i = 0$ pour $t \leq i \leq d-2$. Ensuite,

$$F_i = \sum_{j+k=i} P_j S_k^{[j]} = \sum_{j=0}^{i} P_j S_{i-j}^{[j]} = \sum_{j=0}^{i} P_j \left(\sum_{l=0}^{t-1} E_l z_l^{[i-j]} \right)^{[j]} = \sum_{l=0}^{t-1} z_l^{[i]} \left(\sum_{j=0}^{i} P_j E_l^{[j]} \right)^{[j]} = 0,$$

car E_l sont des racines de $P(X)$.

Nous devons donc résoudre le système $\sum_{j=0}^{i} P_j S_{i-j}^{[j]} = 0$ pour $t \leq i \leq 2t-1$ ce qui s'écrit :

$$S. \begin{pmatrix} P_t \\ P_{t-1} \\ \vdots \\ P_1 \end{pmatrix} = \begin{pmatrix} -S_t \\ -S_{t+1} \\ \vdots \\ -S_{2t-1} \end{pmatrix}, \tag{2.6}$$

avec,

$$S = \begin{pmatrix} S_0^{[t]} & \cdots & S_{t-1}^{[1]} \\ S_1^{[t]} & \cdots & S_t^{[1]} \\ \vdots & \ddots & \vdots \\ S_{t-1}^{[t]} & \cdots & S_{2t-1}^{[1]} \end{pmatrix}$$

Nous remarquons que S est inversible, ce qui donne l'unicité de la solution. Cette solution peut être trouvée en utilisant l'algorithme de Berlekamp-Massey modifié.
Nous pouvons voir l'équation **(2.6)** comme un registre à décalage [36] comme la figure 2.11 l'illustre :

Le problème de résolution de *l'équation clé* est équivalent au problème de recherche de plus petit registre à décalage FSR (Feedback Shift Register) qui génère la séquence du syndrome.

Nous commençons l'itération par $i = 0$, puis nous initialisons la longueur du registre l_i par 0 et $P(X) = X$. A chaque itération i, nous créons un registre qui génère les $i+1$ syndromes qui ont une longueur l_i.

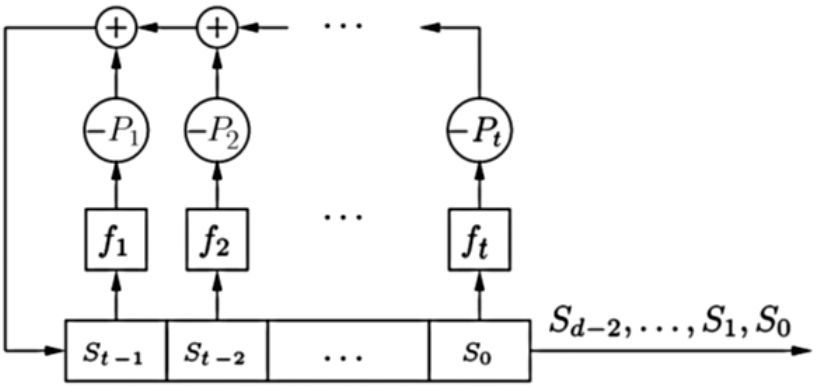


FIGURE 2.11 – Polynôme d'erreur sous forme d'un registre à décalage [36].

Définition 6. *Le discriminant de la $i-$ème itération est défini par :*

$$\Delta_i = S_i + \sum_{j=1}^{l_i} P_j^{(i)} S_{i-j}^{[j]} = \sum_{j=0}^{l_i} P_j^{(i)} S_{i-j}^{[j]}$$

Pour le cas $\Delta_i = 0$, nous posons $P^{(i+1)}(X) = P^{(i)}(X)$ et l'itération est terminée.

Théorème 3. *Si $\Delta_i \neq 0$, le polynôme linéaire est obtenu par :*

$$P^{(i+1)}(X) = P^{(i)}(X) - \Delta_i \Delta_m^{-[r-m]} \circ P^{(m)}(X),$$

avec $m < i$. Donc, le nouveaux discriminant $\Delta'_i = 0$.

Preuve

– Il suffit de vérifier que $\Delta'_i = \sum_{j=0}^{l_{i+1}} P_j^{(r+1)} S_{i-j}^{[j]} = 0$.

Nous avons prouvé que $l_{i+1} = max(l_i, r + 1 - l_i)$ et que l'algorithme de Berlekamp-Massey modifié pour la métrique rang génère le plus petit registre à décalage FSR.
Nous pouvons résumer l'algorithme dans le schéma 2.12 suivant. Maintenant, nous pouvons résumer toutes les différentes étapes de l'algorithme de décodage :

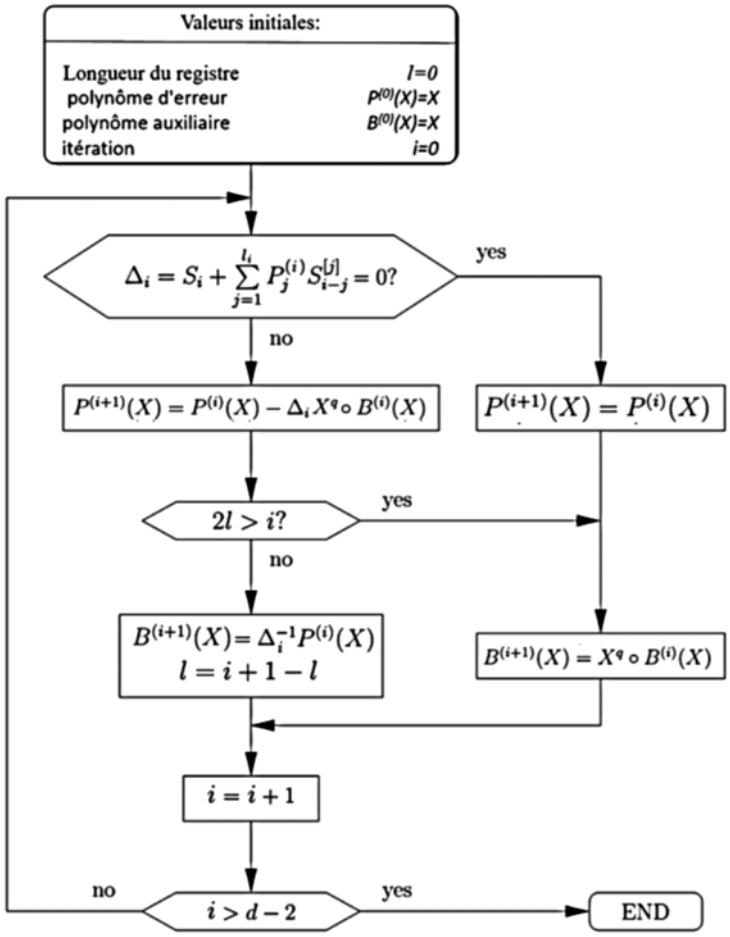


FIGURE 2.12 – Algorithme de Berlekamp-Massey modifié [36].

Algorithm 1: Berlekamp-Massey

Entrée: Le mot reçu y.

La matrice $\mathbf{H}$.

Sortie : le mot de code c.

1- Calculer le syndrome.

2- Résoudre le système **(1)** avec l'algorithme de Berlekamp-Massey modifié pour obtenir $P(X)$.

3- Calculer $E_0, \ldots, E_{t-1}$ les racines de $P(X)$.

4- Résoudre le système $S_i^{[-i]} = \sum_{j=0}^{t-1} E_j^{[-i]} z_j, i = 0, ..., d-2$.

5- Calculer Y par multiplications matricielles.

6- Calculer $e = (E_0, \ldots, E_{t-1})\mathbf{Y}$.

Retourne $c = y - e$.

2.8 Les codes LRPC

2.8.1 Low Rank Parity Check Codes

L'idée de ces codes est de généraliser l'approche des codes LDPC classiques pour la distance de *Hamming* à la métrique de rang. Il y a une analogie entre matrices de faible densité et matrices à faible rang.

Dans cette partie, nous présentons les principaux résultats issus de [37].

Définition 7. *Un code LRPC est un code de rang d, de longueur n et de dimension k dans $\mathbb{F}_{q^m}$, ce code admet comme matrice de parité $\boldsymbol{H}(h_{ij})$ de taille $(n-k)\times n$ telle que le sous espace vectoriel de $\mathbb{F}_{q^m}$ généré par ses coefficients h_{ij} est de dimension au plus d. Nous appelons cette dimension le poids de $\boldsymbol{H}$. En notant F le sous-espace vectoriel de $\mathbb{F}_{q^m}$ généré par les coefficients h_{ij} de $\boldsymbol{H}$, nous notons $\{F_1, F_2, \ldots, F_d\}$ une de ses bases.*

2.8.2 Écriture des équations du syndrome dans le corps $\mathbb{F}_q$ pour les codes LRPC

La structure particulière des codes LRPC permet d'exprimer formellement les équations du syndrome dans $\mathbb{F}_{q^m}$ en équations dans la base $\mathbb{F}_q$, il permet d'obtenir un algorithme de décodage très efficace, que nous allons décrire dans la prochaine section. Nous décrivons dans ce qui suit, la façon d'obtenir une telle transformation, en particulier, nous introduisons une matrice ${\mathbf{A}_H}^r$, qui sera utilisée pour la procédure de décodage.

Supposons que l'erreur $e(e_1, ..., e_n)$ de poids r se situe dans un espace d'erreur E de dimension r généré par une base $\{E_1, E_2, \ldots, E_r\}$, puis tous les $e_i (1 \leq i \leq n)$ peuvent être écrits sous la forme $e_i = \sum_{j=1}^{r} e_{ij} E_j$. La matrice $\mathbf{H} = (h_{ij})$ est réalisée de telle sorte que les h_{ij} appartiennent à un espace F de dimension d généré par $\{F_1, F_2, \ldots, F_d\}$, alors pour tout $1 \leq i \leq n-k, 1 \leq j \leq n$, $h_{ij} = \sum_{l=1}^{d} h_{ijl} F_l$, avec $h_{ijl} \in \mathbb{F}_q$.

Supposons en outre que la dimension de l'espace $< F_1E_1, F_1E_2, .., F_1E_r, F_2E_1, ..., F_dE_r >$ est exactement rd, il est alors possible d'exprimer les équations du syndrome $\mathbf{H}.e^t = s$ dans $\mathbb{F}_{q^m}$ en équations dans la base $\mathbb{F}_q$, en exprimant formellement les e_i dans la base $\{E_1, E_2, \ldots, E_r\}$ et les coordonnées du syndrome dans le produit des bases $< F_1E_1, F_1E_2, .., F_1E_r, F_2E_1, ..., F_dE_r >$.

Plus formellement, il existe une matrice ${\mathbf{A}_H}^r$ de taille $(n-k)rd \times nr$ dans $\mathbb{F}_q$ tels que les équations du syndrome $\mathbf{H}.e^t = s$ dans $\mathbb{F}_{q^m}$ deviennent un système d'équations ${\mathbf{A}_H}^r.e'^t = s'$ dans $\mathbb{F}_q$, où s' correspond à un vecteur de taille $(n-k)rd$ dans $\mathbb{F}_q$ correspondant aux coordonnées du syndrome s, $(s_1, ..., s_n - k)$, où chaque s_i est écrit dans la base $< F_1E_1, F_1E_2, .., F_1E_r, F_2E_1, ..., F_dE_r >$ du produit de deux espaces $< E.F >$, et où e' est un

vecteur de dimension égale à nr sur $\mathbb{F}_q$ correspondant aux coordonnées d'erreur $(e_1, ..., en)$, en supposant que chaque e_i est écrit dans la base $\{E_1, E_2, \ldots, E_r\}$. Si l'on procède de cette façon la matrice ${\mathbf{A}_H}^r$ de taille $nr \times (n-k)rd$ ne dépend que des coordonnées h_{ij} écrit dans la base $\{F_1, F_2, \ldots, F_d\}$, et donc ${A_H}^r$ ne dépend pas de l'erreur e, mais de façon unique de sa dimension r. Pour des différents erreurs e, on a juste à calculer s et s' dans le produit de deux espaces $< E.F >$ puis résoudre le système ${\mathbf{A}_H}^r.e'^t = s'$.
En effet,

$$\mathbf{H}.e = \begin{pmatrix} h_{1,1} & h_{1,2} & \cdots & h_{1,n} \\ h_{2,1} & h_{2,2} & \cdots & h_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ h_{n-k,1} & h_{n-k,2} & \cdots & h_{n-k,n} \end{pmatrix} \times \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{pmatrix} = \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_{n-k} \end{pmatrix}$$

Alors,

$$\begin{cases} h_{1,1}e_1 + h_{1,2}e_2 + \ldots + h_{1,n}e_n = s_1 \\ h_{2,1}e_1 + h_{2,2}e_2 + \ldots + h_{2,n}e_n = s_1 \\ \vdots \qquad\qquad\qquad\qquad\qquad \vdots \\ h_{n-k,1}e_1 + h_{n-k,2}e_2 + \ldots + h_{n-k,n}e_n = s_1 \end{cases}$$

Or,

$$h_{ij}.e_j = \begin{pmatrix} h_{ij1} \\ h_{ij2} \\ \vdots \\ h_{ijd} \end{pmatrix} . \begin{pmatrix} e_{j1} & e_{j2} & \cdots & e_{jr} \end{pmatrix} = \begin{pmatrix} h_{ij1}e_{j1} & h_{ij1}e_{j2} & \cdots & h_{ij1}e_{jr} \\ h_{ij2}e_{j1} & h_{ij2}e_{j2} & \cdots & h_{ij2}e_{jr} \\ \vdots & \vdots & \ddots & \vdots \\ h_{ijd}e_{j1} & h_{ijd}e_{j2} & \cdots & h_{ijd}e_{jr} \end{pmatrix}$$

Et,

$$s_i = \begin{pmatrix} s_{i11} & s_{i12} & \cdots & s_{i1r} \\ s_{i21} & s_{i22} & \cdots & s_{i2r} \\ \vdots & \vdots & \ddots & \vdots \\ s_{id1} & s_{id2} & \cdots & s_{idr} \end{pmatrix}$$

Si nous développons chaque équation, nous obtiendrons,

$$\begin{pmatrix} \sum_{j=1}^{n} h_{1j1}e_{j1} & \sum_{j=1}^{n} h_{1j1}e_{j2} & \cdots & \sum_{j=1}^{n} h_{1j1}e_{jr} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{j=1}^{n} h_{1jd}e_{j1} & \sum_{j=1}^{n} h_{1jd}e_{j2} & \cdots & \sum_{j=1}^{n} h_{1jd}e_{jr} \\ \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{j=1}^{n} h_{(n-k)j1}e_{j1} & \sum_{j=1}^{n} h_{(n-k)j1}e_{j2} & \cdots & \sum_{j=1}^{n} h_{(n-k)j1}e_{jr} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{j=1}^{n} h_{(n-k)jd}e_{j1} & \sum_{j=1}^{n} h_{(n-k)jd}e_{j2} & \cdots & \sum_{j=1}^{n} h_{(n-k)jd}e_{jr} \end{pmatrix} = \begin{pmatrix} s_{111} & s_{112} & \cdots & s_{11r} \\ \vdots & \vdots & \ddots & \vdots \\ s_{1d1} & s_{1d2} & \cdots & s_{1dr} \\ \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ s_{(n-k)11} & s_{(n-k)12} & \cdots & s_{(n-k)1r} \\ \vdots & \vdots & \ddots & \vdots \\ s_{(n-k)d1} & s_{(n-k)d2} & \cdots & s_{(n-k)dr} \end{pmatrix}$$

En transformant l'équation matricielle en un système, nous parvenons à :

$$\begin{cases} \sum_{j=1}^{n} h_{1j1}e_{j1} = s_{111} \\ \vdots \\ \sum_{j=1}^{n} h_{1j1}e_{jr} = s_{11r} \\ \vdots \\ \sum_{j=1}^{n} h_{1jd}e_{j1} = s_{1d1} \\ \vdots \\ \sum_{j=1}^{n} h_{1jd}e_{jr} = s_{1dr} \\ \vdots \\ \vdots \\ \sum_{j=1}^{n} h_{(n-k)j1}e_{j1} = s_{(n-k)11} \\ \vdots \\ \sum_{j=1}^{n} h_{(n-k)j1}e_{jr} = s_{(n-k)1r} \\ \vdots \\ \sum_{j=1}^{n} h_{(n-k)jd}e_{j1} = s_{(n-k)d1} \\ \vdots \\ \sum_{j=1}^{n} h_{(n-k)jd}e_{jr} = s_{(n-k)dr} \end{cases}$$

Ce qui donne,

$$
\left\{\begin{array}{ccccccccccccccccccc}
h_{111}e_{11} & + & 0 & + & \cdots & + & 0 & + & \cdots\cdots & + & h_{1n1}e_{n1} & + & 0 & + & \cdots & + & 0 & = & s_{111} \\
0 & + & h_{111}e_{12} & + & \cdots & + & 0 & + & \cdots\cdots & + & 0 & + & h_{1n1}e_{n2} & + & \cdots & + & 0 & = & s_{112} \\
 & & \vdots & & & & & & & & & & & & & & & & \vdots \\
0 & + & 0 & + & \cdots & + & h_{111}e_{1r} & + & 0 & + & \cdots\cdots & + & 0 & + & \cdots & + & h_{1n1}e_{nr} & = & s_{11r} \\
 & & \vdots & & & & & & & & & & & & & & & & \vdots \\
 & & \vdots & & & & & & & & & & & & & & & & \vdots \\
h_{11d}e_{11} & + & 0 & + & \cdots & + & 0 & + & \cdots\cdots & + & h_{1nd}e_{n1} & + & 0 & + & \cdots & + & 0 & = & s_{1d1} \\
0 & + & h_{11d}e_{12} & + & \cdots & + & 0 & + & \cdots\cdots & + & 0 & + & h_{1nd}e_{n2} & + & \cdots & + & 0 & = & s_{1d2} \\
 & & \vdots & & & & & & & & & & & & & & & & \vdots \\
0 & + & 0 & + & \cdots & + & h_{11d}e_{1r} & + & 0 & + & \cdots\cdots & + & 0 & + & \cdots & + & h_{1nd}e_{nr} & = & s_{1d2} \\
 & & \vdots & & & & & & & & & & & & & & & & \vdots \\
 & & \vdots & & & & & & & & & & & & & & & & \vdots \\
 & & \vdots & & & & & & & & & & & & & & & & \vdots
\end{array}\right.
$$

Par conséquent,

$$
A_H^r = \begin{pmatrix}
h_{111} & 0 & \cdots & 0 & \cdots & \cdots & h_{1n1} & 0 & \cdots & 0 \\
0 & h_{111} & \cdots & 0 & \cdots & \cdots & 0 & h_{1n1} & \cdots & 0 \\
\vdots & & & & & & & & & \\
0 & 0 & \cdots & h_{111} & \cdots & \cdots & 0 & 0 & \cdots & h_{1n1} \\
\vdots & & & & & & & & & \\
\vdots & & & & & & & & & \\
h_{11d} & 0 & \cdots & 0 & \cdots & \cdots & h_{1nd} & 0 & \cdots & 0 \\
0 & h_{11d} & \cdots & 0 & \cdots & \cdots & 0 & h_{1nd} & \cdots & 0 \\
\vdots & & & & & & & & & \\
0 & 0 & \cdots & h_{11d} & \cdots & \cdots & 0 & 0 & \cdots & h_{1nd} \\
\vdots & & & & & & & & & \\
\vdots & & & & & & & & & \\
\vdots & & & & & & & & & \\
h_{(n-k)11} & 0 & \cdots & 0 & \cdots & \cdots & h_{(n-k)n1} & 0 & \cdots & 0 \\
0 & h_{(n-k)11} & \cdots & 0 & \cdots & \cdots & 0 & h_{(n-k)n1} & \cdots & 0 \\
\vdots & & & & & & & & & \\
0 & 0 & \cdots & h_{(n-k)11} & \cdots & \cdots & 0 & 0 & \cdots & h_{(n-k)n1} \\
\vdots & & & & & & & & & \\
\vdots & & & & & & & & & \\
h_{(n-k)1d} & 0 & \cdots & 0 & \cdots & \cdots & h_{(n-k)nd} & 0 & \cdots & 0 \\
0 & h_{(n-k)1d} & \cdots & 0 & \cdots & \cdots & 0 & h_{(n-k)nd} & \cdots & 0 \\
\vdots & & & & & & & & & \\
0 & 0 & \cdots & h_{(n-k)1d} & \cdots & \cdots & 0 & 0 & \cdots & h_{(n-k)nd}
\end{pmatrix}
$$

La construction précédente peut être considérée comme la décomposition formelle de la matrice $\mathbf{H}$ dans la base de produit des deux espaces $< E.F >$:
$< F_1E_1, F_1E_2, .., F_1E_r, F_2E_1, ..., F_dE_r >$.

Définition 8. *Avec la notation précédente, nous considérons une matrice* $(n-k)rd \times nr$ $\boldsymbol{A}_H^r = (a_{ij})$. *Dans un premier temps* $a_{ij} = 0$ *et après on écrit* $a_{u+(v-1)r+(i-1)rd,u+(j-1)r} = h_{ij}$ *pour* $1 \leq u \leq r$, $1 \leq i \leq n-k$, $1 \leq j \leq n$ *et* $1 \leq v \leq d$

Notation 1. *On note par* $\boldsymbol{A}_H$ *la* $nr \times nr$ *sous-matrice inversible de* $\boldsymbol{A}_H^r$, *on note* $\boldsymbol{D}_H = \boldsymbol{A}_H^{-1}$ *une matrice de décodage de* $\boldsymbol{H}$.
La matrice $\boldsymbol{D}_H$ *permet de récupérer directement les valeurs de* e_{ij}

2.9 L'algorithme de décodage des codes LRPC

2.9.1 L'idée générale

L'idée générale de l'algorithme est d'utiliser le fait que le poids de la matrice de parité est petit et que l'espace généré par les coordonnées du syndrome $< s_1, ..., s_{n_k} >$ permet de récupérer tout l'espace produit $P =< F.E >$ entre le support de l'erreur et la base de $\mathbf{H}$. En connaissant les espaces P et F, on peut récupérer l'espace E, après il sera facile de retrouver l'erreur e en résolvant un système linéaire. Cette méthode est similaire à la procédure de décodage des codes RS.

2.9.2 L'algorithme général de décodage

Considérons un $[n, k]$ LRPC code $\mathbf{C}$ de petit poids d dans $\mathbb{F}_{q^m}$, avec une matrice génératrice G et une matrice de parité $\mathbf{H}$ de taille $(n-k) \times n$ tel que ses coefficients h_{ij} sont engendrés par $\{F_1, F_2, \ldots, F_d\}$ et que H est choisie telle que D_H existe.

Supposons que nous avons reçu $y = x\mathbf{G} + e$ pour x dans $\mathbb{F}_{q^m}^k$ et e dans $\mathbb{F}_{q^m}^n$ de rang r tel que $\{E_1, E_2, \ldots, E_r\}$ est une base de $< e_1, ..., e_n >$.

Nous considérons l'algorithme général de décodage suivant, cet algorithme a une probabilité d'échec que nous allons présenter dans la prochaine section, nous allons donner quelque paramètres pour lequel l'algorithme fonctionne.

Algorithme 1 : Algorithme général du décodage LRPC

1. **Comptage d'espace syndrome**
   Nous commençons par calculer le syndrome, après nous calculons l'espace syndrome $< s_1, ..., s_{n-k} >$.
2. **Trouver le support E de l'erreur**
   Nous définissons $S_i = F_i^{-1}S$ et nous calculons le support d'erreur $E = S_1 \cap S_2 \cap ... \cap S_d$.
3. **Trouver l'erreur e**
   Nous écrivons $e_i (1 \leq i \leq n)$ dans la base $\{E_1, E_2, \ldots, E_r\}$ tel $e_i = \sum_{j=1}^{r} e_{ij} E_j$.
   $e' = (e_{11}, e_{12}, ..., e_{nr})$.
   Nous écrivons s_i dans la base $P =< E.F >$.
   Nous essayons de récupérer e' à partir du système $\mathbf{A}_H^r.e' = s'$.
4. **Trouver le message x**
   Trouver x depuis le system $x.\mathbf{G} = y - e$.

2.9.3 L'exactitude de l'algorithme

Nous allons prouver l'exactitude de l'algorithme dans le cas idéal quand $dim(< E.F >) = rd, dim(S) = rd$ et $dim(S_1 \cap S_2 \cap ... \cap S_d) = r$, nous allons voir dans la prochaine section que ceci correspond au cas général.

Étape 1 : La première étape de l'algorithme est évidente.

Étape 2 : Nous allons prouver que $E \subset S_1 \cap S_2 \cap ... \cap S_d$. Puisque S est le produit des deux espaces E et F, nous avons $F_i.E_j \in S$, pour $1 \leq j \leq r$, donc $E_j \in S_i$ et $E \subset S_i$, d'où $E \subset S_1 \cap S_2 \cap ... \cap S_d$. Par hypothèse $dim(S_1 \cap S_2 \cap ... \cap S_d) = dim(E)$ ce qui implique l'égalité de E et $S_1 \cap S_2 \cap ... \cap S_d$.

Étape 3 : Après avoir trouvé E, on écrit e_i dans la base de E, dans cas on a nr inconnus et $(n-k)m$ équations donc il faut que r soit plus petit que $\frac{(n-k)m}{n}$.

2.9.4 La probabilité d'échec

Nous considérons les trois différentes probabilité d'échec, le cas où $dim(< E.F >) = rd$ est vérifié avec une probabilité supérieure à $r\frac{q^{rd}}{q^m}$, le cas où $E = S_1 \cap S_2 \cap ... \cap S_d$ est vérifié avec une probabilité supérieure à $r\frac{q^{rd(d+1)/2}}{q^m}$ et le cas où $dim(S) = rd$ est vérifié avec une probabilité inférieure à $q^{(n-k)-rd-1}$.

2.9.5 La complexité de décodage

L'étape 2) et l'étape 3) sont les plus coûteuses dans l'algorithme 1. Pour l'étape 2) la complexité de l'intersection des espaces vectoriels conduisent à $4r^2d^2m$ opérations dans le corps de base. Dans l'étape 3) la complexité est n^2r^2 pour trouver e_{ij} en utilisant la matrice $\mathbf{D}_H$.
Remarquons que $\mathbf{D}_H$ peut être calculée et stockée dans la mémoire du codeur.

Si nous résumons les différents sections, nous obtenons le théorème suivant

Théorème 4. *Soit $\boldsymbol{H}$ une matrice duale de taille $(n-k)\times n$ d'un code LRPC de petit rang $d \geq 2$ sur $\mathbb{F}_{q^m}$, l'algorithme 1 décode une erreur aléatoire e de poids r tel que $rd \leq n-k$, avec une probabilité de succès égale à $1-q^{-(n-k-rd)}$ et une complexité égale à $r^2(4d^2m+n^2)$.*

2.10 Conclusion

Nous avons consacré ce deuxième chapitre à la présentation de quelques codes correcteurs d'erreurs qui sont de bons candidats à une utilisation sur des canaux CPL-BE. Nous avons considéré deux catégories de codes à savoir les codes de Hamming et les codes à métrique de rang. Dans la première catégorie, nous avons présenté les codes RS, LDPC ainsi que les codes convolutifs. Pour la deuxième catégorie, nous avons détaillé tout d'abord les codes Gabidulin et enchainé par la suite par la présentation du code proposé nommé Low Rank Parity Check (LRPC). Le nouveau code proposé est à la base destiné à la cryptographie. Néanmoins, due à sa matrice de parité de faible rang, ce code est adapté à la nature des erreurs qui peuvent être présentes dans un canal CPL (erreurs criss-cross). En plus, le code proposé LRPC présente une complexité de $\mathcal{O}(t^2(16m+N^2))$ plus faible que le code Gabidulin $\mathcal{O}(tNm^2)$ tandis que ce dernier ne présente pas une probabilité d'échec de décodage. Dans le chapitre suivant, nous allons évaluer les performances du code LRPC et les comparer avec ceux des codes RS adoptés par la norme G3-CPL.

Bibliographie

[1] C. E. Shannon, "A mathematical theory of communication," Bell System Technical Journal, vol. 27, pp. 379–423 and 623–656, July and October 1948.

[2] http ://math.unice.fr/ diener/probas/Vraisembl.pdf

[3] M. J. Golay, "Notes on digital coding," Proc. ire, vol. 37, no. 6, p. 657, 1949.

[4] R. W. Hamming, "Error detecting and error correcting codes," Bell System technical journal, vol. 29, no. 2, pp. 147–160, 1950.

[5] D. E. Muller, "Application of boolean algebra to switching circuit design and to error detection," Electronic Computers, Transactions of the IRE Professional Group on, no. 3, pp. 6–12, 1954.

[6] I. Reed, "A class of multiple-error-correcting codes and the decoding scheme," Information Theory, IRE Professional Group on, vol. 4, no. 4, pp. 38–49, 1954.

[7] P. Elias, "Coding for noisy channels," IRE Conv. Rec, vol. 3, no. pt 4, pp. 37–46, 1955.

[8] E. Prange, Cyclic Error-Correcting codes in two symbols. Air Force Cambridge Research Center, 1957.

[9] A. Hocquenghem, "Codes correcteurs d'erreurs," Chiffres, vol. 2, no. 2, pp. 147–56, 1959.

[10] R. C. Bose and D. K. Ray-Chaudhuri, "On a class of error correcting binary group codes," Information and control, vol. 3, no. 1, pp. 68–79, 1960.

[11] I. S. Reed and G. Solomon, "Polynomial codes over certain finite fields," Journal of the Society for Industrial & Applied Mathematics, vol. 8, no. 2, pp. 300–304, 1960.

[12] R. Gallager, "Low-density parity-check codes," Information Theory, IRE Transactions on, vol. 8, no. 1, pp. 21–28, 1962.

[13] G. D. Forney, "Concatenated codes," Massachusetts Institude of Technology, Cambridge, Massachusetts, Tech. Rep. 440, December 1965.

[14] A. Viterbi, "Error bounds for convolutional codes and an asymptotically optimum decoding algorithm," Information Theory, IEEE Transactions on, vol. 13, no. 2, pp. 260–269, 1967.

[15] J. Massey, "Shift-register synthesis and BCH decoding," Information Theory, IEEE Transactions on, vol. 15, no. 1, pp. 122–127, 1969.

[16] G. Ungerboeck, "Channel coding with multilevel/phase signals," Information Theory, IEEE Transactions on, vol. 28, no. 1, pp. 55–67, 1982.

[17] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error correcting coding and decoding : Turbo-codes," in Communications, 1993. ICC 93. Geneva. Technical Program, Conference Record, IEEE International Conference on, vol. 2. IEEE, 1993, pp. 1064–1070.

[18] D. J. MacKay and R. M. Neal, "Near Shannon limit performance of low density parity check codes," Electronics letters, vol. 32, no. 18, p. 1645, 1996.

[19] M. Luby, "LT codes," in Foundations of Computer Science, 2002. Proceedings. The 43rd Annual IEEE Symposium on. IEEE, 2002, pp. 271–280.

[20] A. Shokrollahi, "Raptor codes," Information Theory, IEEE Transactions on, vol. 52, no. 6, pp. 2551–2567, 2006.

[21] E. Arikan, "Channel polarization : A method for constructing capacity achieving codes for symmetric binary-input memoryless channels," Information Theory, IEEE Transactions on, vol. 55, no. 7, pp. 3051–3073, 2009.

[22] J. Perry, H. Balakrishnan, and D. Shah, "Rateless spinal codes," in Proceedings of the 10th ACM Workshop on Hot Topics in Networks. ACM, 2011, p. 6.

[23] R. G. Gallager, Low Density Parity-Check Codes. MIT Press, Cambridge, MA, 1963.

[24] C. Schlegel and L. Perez, "Trellis and Turbo Coding," IEEE Press. 2002.

[25] A. Burr, "Turbo-codes : the ultimate error control codes," Electronics and Communication Engineering Journal. August 2001.

[26] J. L. Ramsey, "Realization of optimum interleavers," IEEE Trans. on Inform.Theory. vol. 16, p.338-345, May 1970.

[27] *https* : *//en.wikipedia.org/wiki/Convolutional*$_c$*ode*

[28] W. Liu, Emulation of Narrowband Powerline Data Transmission Channels and Evaluation of PLC Systems, ser. Forschungsberichte aus der Industriellen Informationstechnik / Institut für Industrielle Informationstechnik (IIIT), Karlsruher Institut für Technologie. KIT Scientific Publishing, 2013.

[29] E. M. Gabidulin. Theory of codes with maximal rank distance. Problems of Information Transmission, 1985.

[30] C. FAURE. Etudes de systèmes cryptographiques construits à l'aide de codes correcteurs, en métrique de Hamming et en métrique rang. Thèse de Doctorat. 2009.

[31] P. Loidreau. Métrique Rang et Cryptographie. Mémoire d'habilitation à diriger les recherches, 2007. Université Paris-VI.

[32] R.M. Roth . Maximum-Rank array co des and their application to criss-cross error correction. IEEE Transactions on Information Theory, vol. 37, n°2, mars 1991, pp. 328-336.

[33] O. Öre. Theory of non-commutative polynomials. The Annals of Mathematics, vol.34, 1933, pp. 480-508.

[34] O. Öre. On a special class of polynomials. Transaction of the American Mathematical Society, vol.35, 1933, pp. 237-246.

[35] O. Öre. Contribution to the theory of finite fields. Transaction of the American Mathematical Society, vol.36, 1934, pp. 243-274.

[36] G. Richter et S. Plass. Error and erasure decoding of rank-codes with a modified Berlekamp-Massey algorithm. In : 5th Int. ITG Conference on Source and Channel Coding(SCC 04) . 2004

[37] P. Gaborit, O. Ruatta, G. Murat et G. Zémor. Low Rank Parity Check Codes and their application in cryptography. WCC 2013, 167-179

[38] S. Sahuguède, "Codage de canal pour les communications optiques," Ph.D. dissertation, Université de Limoges, 2009.

[39] M. Luby, "LT codes," in Foundations of Computer Science, 2002. Proceedings. The 43rd Annual IEEE Symposium on. IEEE, 2002, pp. 271–280.

[40] Sonia, Geeta Arora, "Implementation of different decoding techniques for QC-LDPC codes," IJESRT Volume 4 issue 6 June 2015.

[41] Kai Zhang, Xinming Member and Zhongfeng wang, "High Throughput Layered Decoder Implementation for Quasi-Cyclic LDPC Codes", IEEE, vol. 27, no. 6, August 2009.

[42] Chinna Babu.J, S.Prathyusha, "Hard Decision and Soft Decoding Algorithms of LDPC and Comparison of LDPC With Turbo Codes, RS Codes and BCH Codes," IRF International Conference, 27th july-2014.

[43] Monica V.Mankar, Abha Patil and G.M.Asutkar, "Single mode Quasi-cyclic LDPC Decoder Using Modified Belief Propagation," IEEE 2014.

[44] Yaqi Li, Bo Rong, Bo Liu, Yiyan Wv and Gilles Gagnon, "Rate-compatible LDPC-RS Product Codes Based on Raptor-like LDPC codes", IEEE 2013.

[45] https ://zh.wikipedia.org/wiki/

[46] GLAVIEUX, Alain, ADDE, Patrick, BATTAIL, Gérard, et al. Codage de canal-des bases théoriques aux turbo-codes (sous la direction de Alain GLAVIEUX). 2005.

Chapitre 3 :

Les codes LRPC et leur application dans les réseaux intelligents

3.1 Introduction

Nous étudions dans ce chapire, l'utilisation des codes LRPC, conçus à l'origine pour les applications de cryptographie, dans le cadre des communications dans les réseaux CPL. En particulier, nous proposons une nouvelle conception de code et un algorithme de décodage probabiliste efficace. L'idée principale du décodage des codes LRPC est basée sur des calculs d'espaces vectoriels sur un champ fini $\mathbb{F}_q$. Les LRPC, de faible rang, peuvent être considérés comme identiques aux codes de contrôle de parité à faible densité LDPC. Nous comparons les performances de ces codes LRPC avec les codes RS pour un canal de communication de type CPL-BE.

3.1.1 Modernisation du système électrique

Les réseaux électriques nécessitent de nouveaux systèmes pour gérer la consommation d'énergie. Par exemple, ces exigences intègrent la climatisation, le chauffage électrique et les appareils vidéo ou audio. Plus précisément, une grille intelligente comprend une combinaison de mesures de gestion de l'énergie qui contiennent principalement des compteurs intelligents et des ressources énergétiques renouvelables. Un élément commun aux systèmes de réseaux intelligents prévus est la nécessité de techniques de traitement numérique pour obtenir rapidement des informations hautement fiables sur la consommation d'énergie dans les locaux du client. En d'autres termes, la gestion de l'information en temps réel est un point crucial pour un réseau intelligent. En ce qui concerne la transmission d'informations, le réseau courant porteurs en lignes (CPL) a été reconnu comme une solution clé pour connecter les différentes entités du système de grille intelligente. Par exemple, dans une étude antérieure, [1] différentes technologies sont étudiées, y compris CPL. Les auteurs d'une étude antérieure [2] fournissent un sondage sur les opportunités potentielles offertes par CPL pour les applications de grille intelligente et décrivent l'application potentielle de PLC dans le réseau intelligent. Cependant, en raison de la présence d'un canal de propagation sévère, assurer des communications fiables sur les canaux PLC reste une tâche difficile. En fait, le canal PLC est doublement sélectif en temps et en fréquence [3] ; Il est affecté par un bruit de fond impulsif coloré et par d'autres sources de bruit impulsif et d'interférence à bande étroite comme le montre la figure 3.1.

3.2 Idée générale du schéma proposé

Les principales difficultés dans les communications CPL viennent du fait que nous devons faire face aux bruits impulsifs et à bande étroite et les atténuer, ce qui est un problème de traitement du signal difficile. Pour lutter contre l'influence des bruits impulsifs

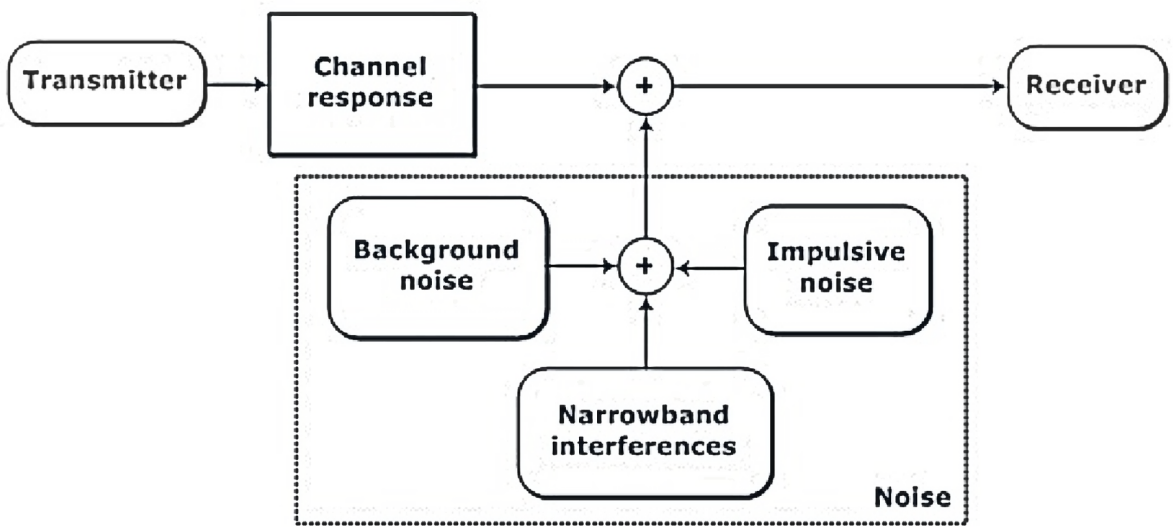


FIGURE 3.1 – Modèle du canal CPL Indoor

et à bande étroite, les solutions classiques dans la littérature suggèrent d'utiliser des techniques de codage d'erreur telles que la combinaison d'un code de bloc Reed-Solomon (RS) concaténé avec un code convolutif et séparé par un entrelaceur pour obtenir une motif d'erreur isolée à l'entrée du décodeur du code convolutif [4]. Parmi ces codes basés sur la métrique de Hamming, les codes Reed-Solomon peuvent détecter et corriger les erreurs en blocs mais ne sont pas immunisés contre les modèles d'erreur croisés qui apparaissent souvent dans les communications CPL. Les modèles d'erreur croisés (criss-cross) sont des blocs d'erreur qui sont concentrés sur une partie donnée de la grille temps-fréquence de la transmission [5]. Cela signifie que plusieurs sous-porteuses adjacentes à la fréquence ainsi que plusieurs créneaux temporels consécutifs rencontrent des distorsions sévères en raison de la présence de signaux parasites. Les codes Gabidulin ou les codes à métrique de rang qui peuvent récupérer des sous-espaces d'erreur complets dépassent nettement les performances des codes Reed-Solomon pour ce type d'erreurs. Le schéma que nous proposons dans ce chapitre est basé sur la conception de codes à métriques de rangs en utilisant une structure d'origine particulière qui s'appelle Low Rank Parity Check (LRPC).

L'objectif principal de notre travail est d'étudier et de comparer les performances des codes LRPC avec celles des codes RS déjà mentionnés dans les différentes normes PLC Narrowband (NB). Les auteurs dans une étude précédente [5] utilisent un code à métrique de rang pour lutter contre les erreurs croisées dans le contexte d'une transmission multiporteuses de type OFDM. Dans un travail antérieur réalisé par Sarr et al [6], les auteurs ont étudié l'impact du bruit impulsif à bande étroite dans un récepteur à bande étroite ZigBee pour les canaux blancs gaussiens, Rayleigh et Rician aditifs. Les résultats ont montré que l'influence du bruit impulsif est proche de celle d'un bruit gaussien ou

d'un bruit de Rayleigh selon le rapport signal sur bruit. En outre, un certain nombre d'applications de grille intelligente (SG) nécessitent un débit de données élevé et une large bande passante. Compte tenu des caractéristiques du canal CPL, les codes à métriques de rang peuvent être utilisés pour combattre le bruit impulsif et les interférences à bande étroite existant dans le canal CPL-BE. En outre, en plus des résultats présentés dans une étude précédente [4], nous étudions la performance des codes à métriques de rang sur les canaux CPL en utilisant les codes RS des différents Normes CPL-BE comme repères.

3.3 Description du canal de communication CPL

La communication par les courants porteurs en lignes électriques (CPL) a été appliquée en tant que méthode d'accès au réseau dans les réseaux publics de distribution d'électricité et les réseaux intérieurs (Indoor). En fait, de nombreuses applications, y compris les pompes à chaleur ou l'alimentation électrique des voitures, peuvent être supportées par des canaux de communication CPL. Les caractéristiques des réseaux CPL et les applications de différentes méthodes de modulation numérique ont fait l'objet d'une enquête approfondie. Toutefois, en raison des problèmes de réglementation, l'idée de mettre en place des services Internet par le biais du réseau de distribution a été partiellement suspendue. Malgré cette limitation, CPL est reconnu comme un bon outil pour contrôler les données de transfert et pour surveiller les périphériques distants chaque fois que la bande passante de transmission requise n'est pas trop importante. Un exemple illustrant est le transfert de données lié à la surveillance des moteurs électriques à basse tension industriels. Il existe 2 méthodes possibles pour la modélisation des canaux CPL. Le premier applique les méthodes utilisées pour la modélisation des canaux radio. Le canal CPL est supposé être un environnement de propagation composé de trajets multiples. La deuxième alternative s'applique aux méthodes utilisées pour modéliser les réseaux de distribution d'électricité. Les matrices de paramètres de chaîne décrivant la relation entre la tension d'entrée et de sortie et le courant du réseau 2 ports peuvent être appliquées pour la modélisation de la fonction de transfert d'un canal de communication.

Construire des canaux de communication CPL fiables est une tâche difficile. Cela s'explique principalement par la présence de charges non adaptées, ce qui se traduit par des canaux sélectifs doublement en temps et en fréquences [7]. Les paramètres de la fonction de transfert de canal peuvent être déterminés de manière empirique selon l'environnement de propagation multi-path [8] [9]. Un modèle statistique du canal peut être dérivé en considérant les paramètres dans l'expression de la fonction de transfert comme variables aléatoires. Dans ce chapitre, nous réutilisons le canal modèle dérivé d'une étude précédente dans [10].

1- *Bruit CPL-BE :* L'interférence de bande étroite est considérée dans une bande de

fréquence allant jusqu'à 500 kHz ; Cette source de bruit est un processus cyclo-stationnaire en temps et en fréquence superposé au courant principal à 50 Hz. Pour obtenir ses caractéristiques dans le domaine du temps et de la fréquence, les auteurs d'une étude précédente [3] ont proposé un modèle qui a été adopté par la norme IEEE1901.2. Dans le modèle précité, chaque période de bruit est séparée en blocs L ($L = 3$). Pendant chaque bloc, les perturbations sont stationnaires. Chaque bloc est défini par une forme spectrale et son propre filtre de mise en forme. Avec l'aide du modèle ci-dessus, le bruit du canal CPL peut être considéré comme équivalent à la convolution d'un signal de bruit gaussien blanc additif $m[\tau]$ avec un système linéaire périodiquement variable $h[x, \tau]$ donné par :

$$s[x] = \sum_\tau h[x, \tau]m[\tau] = \sum_{i=1}^{L} \mathbf{1}_{[a,b]}(x) \sum_\tau h_i[\tau]m[\tau]$$

Où $\mathbf{1}_{[a,b]}(x)$ est la fonction indicatrice de l'intervalle $[a, b]$, il est égal à 1 si x appartient à $[a, b]$, et 0 ailleurs, et $h[x, \tau] = \sum_{i=1}^{L} h_i[\tau]\mathbf{1}_{[a,b]}(x)$ pour $0 \leq x \leq N - 1$. Les filtres linéaires inversés dans le temps $h_i[x]$ sont adaptés aux filtres spectraux pour chaque bloc du spectre de fréquence.

CPL-G3 est une norme développée par l'industrie (Maxim et Electricite Reseau Distribution France) pour les systèmes CPL.

1- CPL-G3 [10] : Ici, nous avons considéré les paramètres de la couche physique de la norme CPL-G3. La fréquence d'échantillonnage du système est $f_s = 400\ kHz$. En raison de la sélectivité en fréquence, CPL-G3 comprend une transformée de Fourier rapide de taille 256, avec un espacement de $\triangle f = 1.65625\ kHz$. La figure 3.2 montre le diagramme

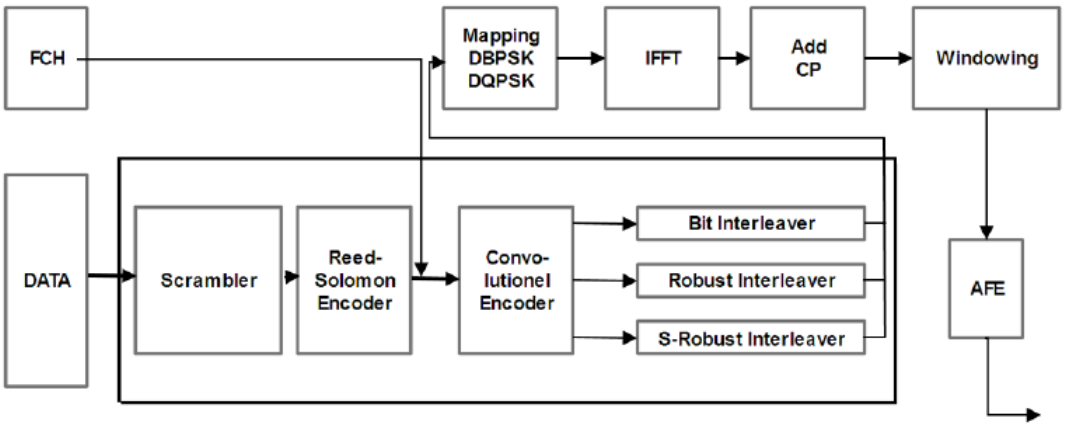


FIGURE 3.2 – Diagramme en block pour une émetteur G3-CPL

schématique de l'émetteur susmentionné qui était déjà montré dans le premier chapitre. Nous disposons de 3 types de modes standard pour la transmission de données : Robustes, Differential Quaternary Phase Shift Keying, et Differential Binary Phase Shift Keying. Ainsi, selon la qualité du canal, nous modifions l'efficacité spectrale des signaux d'émission

Tableau 3.1 – Periodic impulsive variations

Main Current Frequency	Inter Arrival Time	Impulsive Noise Variation
60 Hz	8 mS	[0.5 - 2.8] mS
50 Hz	10 mS	[0.625 - 3.5] mS

Tableau 3.2 – Parameters of PLC-G3 and PRIME

	PLC-G3	PRIME
Frequency range	[35-91]Khz	[42-89]Khz
Symbol duration	640 μs	–
Sampling frequency f_s	400 Khz	250 Khz
OFDM FFT size	256	512
Length of cyclic prefix CP	30	48
Windowing	yes	No
Subcarrier spacing $\triangle f$	1.5625 kHz	488 Hz
Max. data rate	33.4 Kbps	128.6 Kbps
Forward Error Correction	RS, Conv, repetition codes	Convolutional code
Modulation	DBPSK, DQPSK in time	DQPSK in frequency

pour optimiser le débit de données. Nous avons 2 tailles de données de 133 et 235 octets avec un débit de données maximal de $33,4$ *kbps* pour le mode DQPSK. Comme le montre la figure 3.2, un code convolutif du rendement 1/2 avec le polynôme générateur G = [171,133] est utilisé pour protéger les données d'entête de la trame dans tous ces modes. En mode robuste, en cas de canaux à fading sévères, les données peuvent être répétées 4 et 6 fois avant le mapping BPSK. Les données d'en-tête de contrôle (non-Frame) sont protégées avec la concaténation d'un code Reed-Solomon avec un code convolutif. Le code Reed-Solomon possède les paramètres RS(n, k) suivants,$n = 255$ et $k = 247$ pour Robust, et $n = 255$ et $k = 239$ pour les autres modules. Dans le système G3-CPL, nous avons observé expérimentalement que les paramètres périodiques du bruit impulsif varient selon le paramètres suivant, voir tableau 3.1 :

Pour plus d'informations sur ce système, une étude a été faite dans [11]. 2-PLC-PoweRline Intelligent Metering Evolution (PRIME) : La troisième colonne du tableau 3.2 ci-dessus présente une vue d'ensemble des paramètres PRIME [11].

3.3.1 Construction de la matrice de parité du code LRPC

Dans cette section concernant les codes à métriques de rang LRPC [13], nous fournissons le matériel nécessaire pour comprendre la base du codage des canaux avec ces types des codes. Nous définissons un nouveau type de code de rang appelé LRPC avec une construction originale pour la vérification de parité et la matrice génératrice. En outre, nous décrivons un nouveau algorithme du décodage basé sur des calculs d'espaces vectoriels sur un champ fini $\mathbb{F}_q$. Nous présenterons une construction spécifique

de la matrice de vérification de parité $\mathbf{H}(h_{ij})$ à partir de laquelle nous dérivons la matrice génératrice $\mathbf{G}$ sous une forme systématique [12][14]. Cette méthode conduit à trouver une matrice de rang faible. Nous présentons les étapes de construction ci-dessous :

1- Nous générons une matrice appelée $\omega_d(d, q^d)$ formée par tous les vecteurs dans $(\mathbb{F}_q)^d$, cette matrice possède un $rang = d$.

2- Toujours dans le corps $(\mathbb{F}_q)^m$, pour obtenir une matrice $\omega_m(m, q^d)$ avec m lignes, nous étendons la matrice ω_d en ajoutant des lignes $(m - d)$ sous cette forme : $(\alpha, \cdots, \alpha)$ / $\alpha \in \mathbb{F}_q$. Par cette méthode, nous obtenons une matrice $\omega_m(m, q^d)$ avec m lignes du rang égal à d.

Remarque : Nous avons $Rang(\omega_m) = Rang(\omega_d) = d$.

3- Nous écrivons les colonnes de ω_m (de longueur m) dans $\mathbb{F}_{q^m}$. Nous désignons par $\mathbf{D}$ l'ensemble des éléments comme $\mathbf{D} = \{\alpha_1, \cdots, \alpha_{q^d}\} \subset \mathbb{F}_{q^m}$.

4- A partir de l'ensemble $\mathbf{D}$, nous construisons la matrice de contrôle de parité $\mathbf{H}$ avec $\mathbf{H} = (h_{ij})$ pour $1 \leq i \leq n-k, 1 \leq j \leq n$ / $h_{ij} \in \mathbf{D}$.

Remarque : $\mathbf{H}$ s'appelle la matrice de vérification de parité avec un faible $rang = d$.

3.3.2 Décodage du code LRPC

La matrice génératrice $\mathbf{G}$ est obtenue par la relation :

$$\mathbf{G}.\mathbf{H}^T = 0$$

Nous considérons que le message envoyé est codé par la matrice $\mathbf{G}$, nous recevons à l'entrée du décodeur :

$$y = xG + e$$

où, x est le message à transmettre et e la base d'erreur. L'algorithme du décodage utilisé pour faire face aux erreurs considérés dans le canal CPL est le suivant (figure 3.3) :

Considérons un exemple du code LRPC avec des paramètres de petites valeurs pour expliquer la construction de la matrice $\mathbf{A}_H^r$ et le fonctionnement de l'algorithme du décodage. Nous choisissons un code $\mathbb{F}_{2^{11}} \cong \mathbb{F}_2[\alpha] = \{0, 1, \alpha, \cdots, \alpha^9\} \cong \mathbb{F}_2[X]/(P)$ où le polynôme Conway $P(X) = X^{11} + X^2 + 1$ est choisi comme un polynôme primitif. Nous considérons un code de longueur $n = 6$ et une dimension $k = 3$. Supposons que l'erreur

Algorithm Decoding algorithm

Input:

$\mathbf{H}$, ▷ Parity check matrix

y, ▷ Received word

d, ▷ Low rank of $\mathbf{H}$

Output:

e, ▷ Error

x, ▷ Message

1: $s \leftarrow \mathbf{H}.y^t$
2: $S \leftarrow < s_1, \ldots, s_{n-k} >$
3: **for** $i := 1$ **to** d **do**
4: $\quad S_i \leftarrow F_i^{-1} S$
5: **end for**
6: $E \leftarrow S_1 \cap S_2 \cap \ldots \cap S_d$
7: $\{E_1, E_2, , E_r\} \leftarrow$ **basis**(E)
8: $s' \leftarrow (s_{111}, \ldots, s_{11r}, \ldots, s_{(n-k)dr})$
9: $e' \leftarrow$ **Resolve**$(A^r_{\mathbf{H}}, s')$ ▷ $A^r_H.e' = s'$
10: $(e_{11}, e_{12}, \ldots, e_{nr}) \leftarrow e'$
11: **for** $i := 1$ **to** n **do**
12: $\quad e_i \leftarrow \sum_{j=1}^{r} e_{ij} E_j$
13: **end for**
14: $x \leftarrow$ **Resolve**$(G, y - e)$ ▷ $x.G = y - e$

FIGURE 3.3 – Algorithme du décodage proposé pour les codes LRPC

appartient à un sous-espace de dimension égale à 1 ($r = 1$) généré par $E_1 = \alpha$. Nous supposons que les coefficients de la matrice $\mathbf{H}$ appartiennent à un espace de dimension égale à 2 ($d = 2$) généré par $F_1 = 1$ et $F_2 = \alpha^2$. Supposons que la matrice $\mathbf{H}$ est donnée par :

$$\mathbf{H} = \begin{pmatrix} 1 & \alpha^2 & 1 & 1+\alpha^2 & 0 & 0 \\ 0 & \alpha^2 & 1 & \alpha^2 & 1 & 1+\alpha^2 \\ 1 & 0 & \alpha^2 & 0 & 0 & 1+\alpha^2 \end{pmatrix} \tag{3.1}$$

Et nous recevons un mot $y = x + e$ où x est un mot de code et e est un vecteur d'erreur de rang 1 égal à :

$$e = (0, \alpha, 0, 0, 0, \alpha) \tag{3.2}$$

L'algorithme du décodage procède alors comme suit.

1. Détermination de l'espace du syndrome

$$s = \mathbf{H}y^t = \mathbf{H}e^t = \begin{pmatrix} \alpha^3 \\ \alpha \\ \alpha + \alpha^3 \end{pmatrix} \tag{3.3}$$

Comme α et α^3 sont linéairement indépendants sur $\mathbb{F}_2$, l'espace S généré par les coordonnées du syndrome est $S =< \alpha, \alpha^3 >$.

2. Calcul du support d'erreur :

$$S_1 =< 1^{-1}\alpha, 1^{-1}\alpha^3 >=< \alpha, \alpha^3 >$$
$$S_2 =< (\alpha^2)^{-1}\alpha, (\alpha^2)^{-1}\alpha^3 >=< \alpha^{-1}, \alpha >$$

L'élément α^{-1} n'appartient pas à S_1, donc $S_1 \cap S_2 =< \alpha >= E$.

3. Détermination de l'erreur en écrivant les coordonnées dans le corps de base : Décomposons les coordonnées du syndrome s dans la base $\{F_1E_1, F_2E_1\}$. L'élément obtenu est noté $s_{\mathbb{F}_2}$:

$$s_{\mathbb{F}_2} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} \tag{3.4}$$

Décomposons chaque coefficient de $\mathbf{H}$ en vecteur colonne dans la base $\{F_1, F_2\} = \{1, \alpha^2\}$ afin d'obtenir la matrice $\mathbf{A}_H^r$:

$$\mathbf{A}_H^r = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \tag{3.5}$$

Nous avons choisi la matrice $\mathbf{H}$ de façon à ce que $\mathbf{A}_H^r$ soit carrée inversible, ainsi $\mathbf{A}_H^r = \mathbf{A}_H$ et

$$\mathbf{D}_H = \mathbf{A}_H^{-1} = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix} \tag{3.6}$$

Pour retrouver le vecteur d'erreur nous calculons

$$\mathbf{D}_H \times s_{\mathbb{F}_2} = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix} \times \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = e^t$$

Nous retrouvons bien les coordonnées du vecteur erreur écrites dans la base $\{E_1\}$.

3.4 OFDM Mapping Desription

Les signaux de transmission multiporteuses OFDM, qui sont souvent utilisés sur le canaux doublement sélectif en temps et en fréquence, peuvent être représentés sous une forme matricielle. La colonne d'une matrice représente un symbole OFDM. Selon le codeur Reed-Solomon, le signal est codé d'abord en utilisant un encodeur convolutif puis on utilise un entrelaceur 2D, pour plus de détails sur cet entrelaceur, le lecteur peut se référer à une étude préalable dans [10]. Une simple transformation cartographique série / parallèle décrite dans la figure 3.4 est utilisée dans nos simulations.

Selon le codeur LRPC, le signal transmis est une matrice avec des éléments appartenant à $\mathbb{F}_2$, ou un vecteur d'éléments dans l'extension du sous-espace $\mathbb{F}_{2^N}$. Pour mieux illustrer cette cartographie, nous considérons un vecteur à partir du codeur avec des éléments dans $\mathbb{F}_{2^N}$: $a = M \times G = (a_1, a_2, \cdots, a_n), M = (m_1, \cdots, m_k)$ étant le message à envoyer. Maintenant, nous pouvons présenter le vecteur a avec des entrées dans $GF(2^N)$ en tant que matrice $\mathbf{A}$ avec des entrées dans $\mathbb{F}_2$:

$$\mathbf{A} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,t} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,t} \\ \vdots & \vdots & \ddots & \vdots \\ a_{f,1} & a_{f,2} & \cdots & a_{f,t} \end{pmatrix}$$

– f représente le nombre de sous-porteuses utilisés.
– t est le nombre de symboles OFDM envoyés sur le canal.

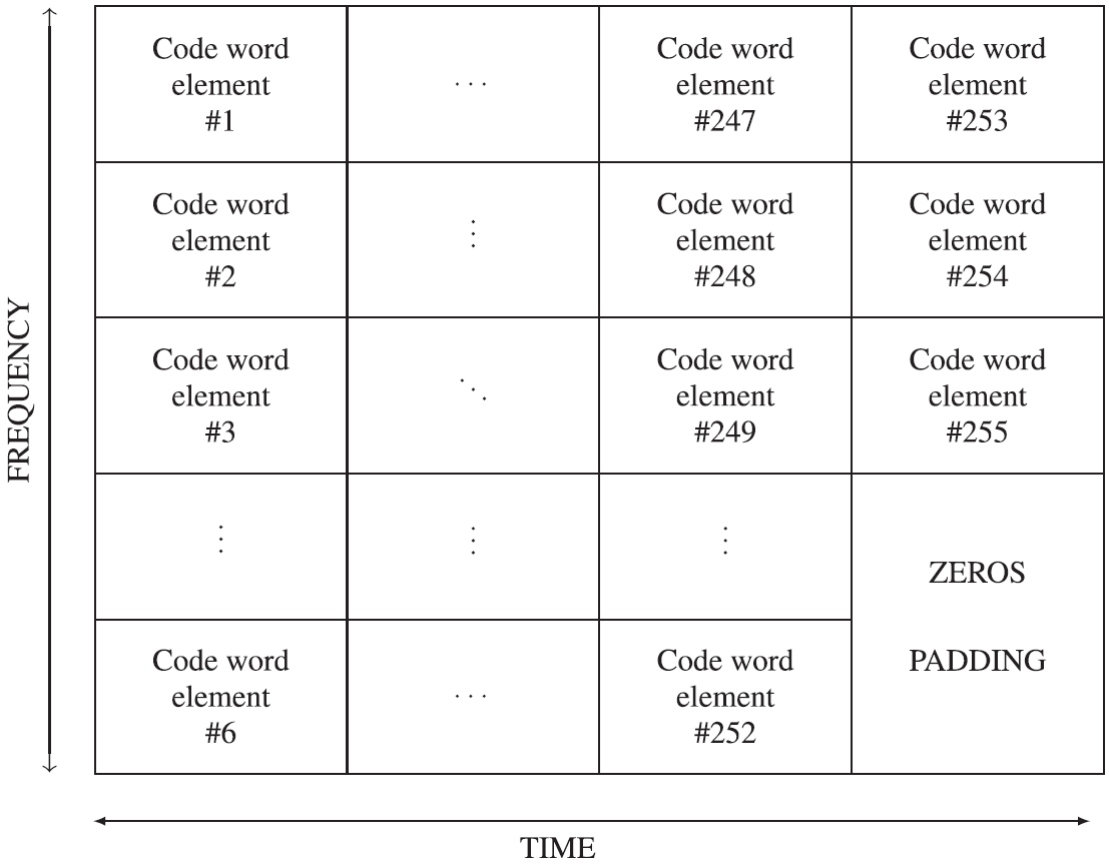


FIGURE 3.4 – Mapping du code RS avant la Transformée de Fourier Rapide Inverse

Nous notons ici que les 2 codes (contrôle de parité de rang faible et codes Reed-Solomon) sont "mappés" en utilisant un nombre identique de sous-porteuses. Afin de clarifier ces différents types de bruit, la figure 3.5 visualise les erreurs sur une très petite image, transmise dans le temps en tant que colonnes et dans le domaine des fréquences en tant que lignes. Ces matrices correspondent au modèle d'erreur (error pattern), les valeurs "x" correspondant aux emplacements d'erreur et 0 indique l'absence d'erreurs.

3.5 Résultats de simulation du schéma proposé [15]

Pour évaluer les performances du code LRPC, un système G3-CPL complet a été implémenté dans MATLAB. Ici, nous comparerons le code proposé LRPC $(46, 23)$ avec le code Reed-Solomon $(255, 127)$, celui-ci utilise un rendement de taux $1/2$ (généralement la concaténation du Code convolutif et du code RS lorsqu'ils ne sont pas associés à la répétition codes). Le mot de code du code LRPC est une matrice (46×46) de symboles

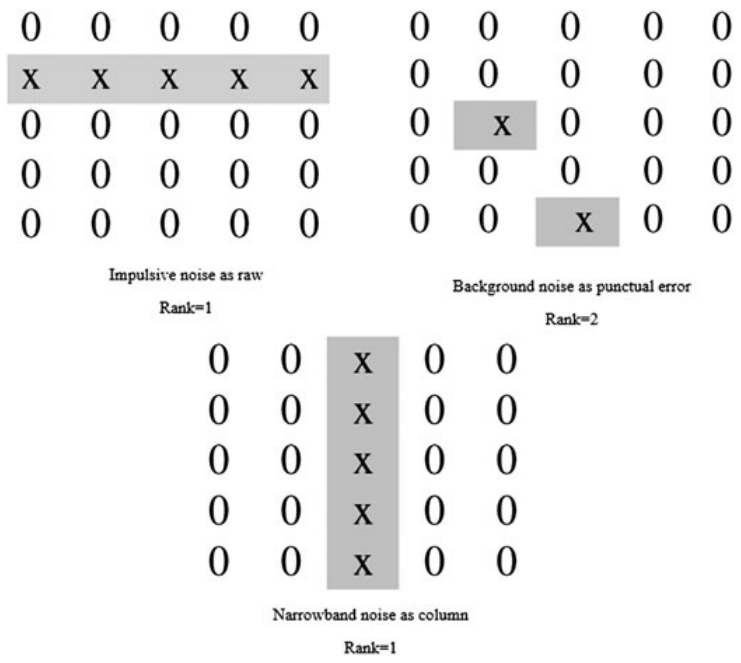


FIGURE 3.5 – Différents types de bruit sur un canal CPL [16]

binaires dans le domaine temps-fréquence. Cette taille a été choisie afin de garantir que la complexité du décodage de LRPC est à peu près similaire à celle des codes RS, voir tableau 3.3 de la page 82. Le décodage du code Reed-Solomon est effectué à l'aide de l'algorithme Berlekamp-Massey [17]. Nous simulons un canal CPL avec toutes les caractéristiques de bruit indépendantes (bruit impulsif, interférence à bande étroite). Nous notons que les mots de code utilisés sont de la même taille pour les 2 codes. En bref, pour les paramètres sélectionnés, les codes LRPC fonctionnent à peu près avec la même complexité que les codes RS, voir le tableau 3.3.

Tableau 3.3 – Analyse de la complexité du décodage

Reed-Solomon	LRPC
Complexity parameters of RS $q = 2, n = 255, m = 8, t = 64$	Complexity parameters of LRPC $q = 2, N = m = 46, t = 12, d = 2$
Standard decoding complexity $\mathcal{O}(tnm^2)$ in $\mathbb{F}_q$ [4]	Standard decoding complexity $\mathcal{O}(t^2(16m + N^2))$ in $\mathbb{F}_q$ [13]

Le diagramme en blocs du système de communication du code LRPC proposé est représenté sur la figure 3.6. Dans les différents résultats de simulation, LRPC (i, j) désigne un code à métrique de rang avec i le nombre des symboles OFDM affectés par le bruit impulsif et j le nombre des sous-porteuses affectés par des interférences à bande étroite .

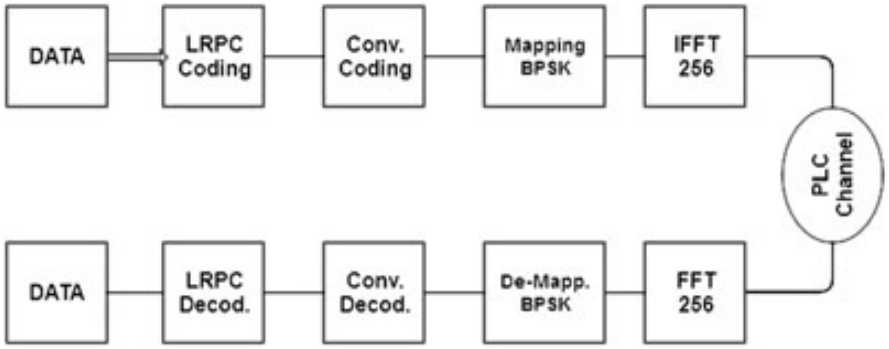


FIGURE 3.6 – Schéma du code LRPC proposé (LRPC). BPSK ; FFT, Fast Fourier Transform ; IFFT, Transformée de Fourier Inverse rapide ; CPL, Courant porteurs en lignes

Schéma de communication avec des interférence à bande étroite BE

La figure 3.7 illustre les performances du code LRPC avec un code RS en présence de bruit de fond et des interférences à bande étroite qui affectent 3 sous-porteuses. Nous commençons à comparer les 2 codes sans bruit impulsif et des interférences BE désignées par LRPC (0,0) et RS (0,0) : la seule perturbation est le bruit de fond. Nous observons que le code LRPC est plus efficace lorsque les erreurs sont confinées dans les lignes et les colonnes.

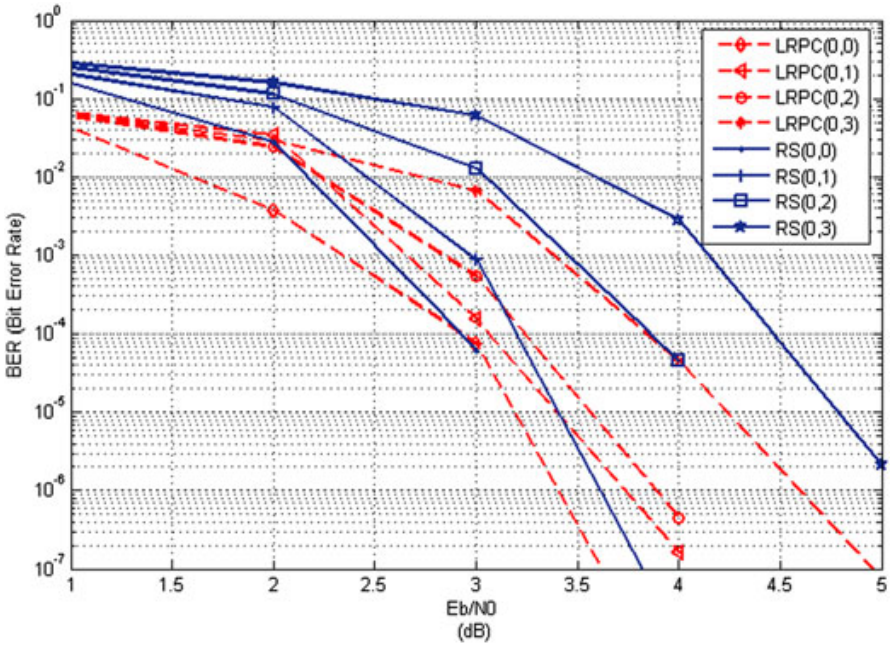


FIGURE 3.7 – Taux d'erreur binaire (BER) du code LRPC avec un code Reed-Solomon (RS) avec un nombre différent de sous-porteuses affectées par des interférences à bande étroite

La figure 3.8 montre que le code LRPC est meilleur que le code RS pour un certain nombre de symboles OFDM, comme dans les cas de LRPC (0,1) et LRPC (0,2). Cependant, pour les valeurs 3 et 4, nous remarquons que les codes RS deviennent meilleurs que le LRPC. Ceci est dû à la nature probabiliste des codes LRPC. Nous illustrons cette limitation probabiliste par un calcul simple ci-dessous.

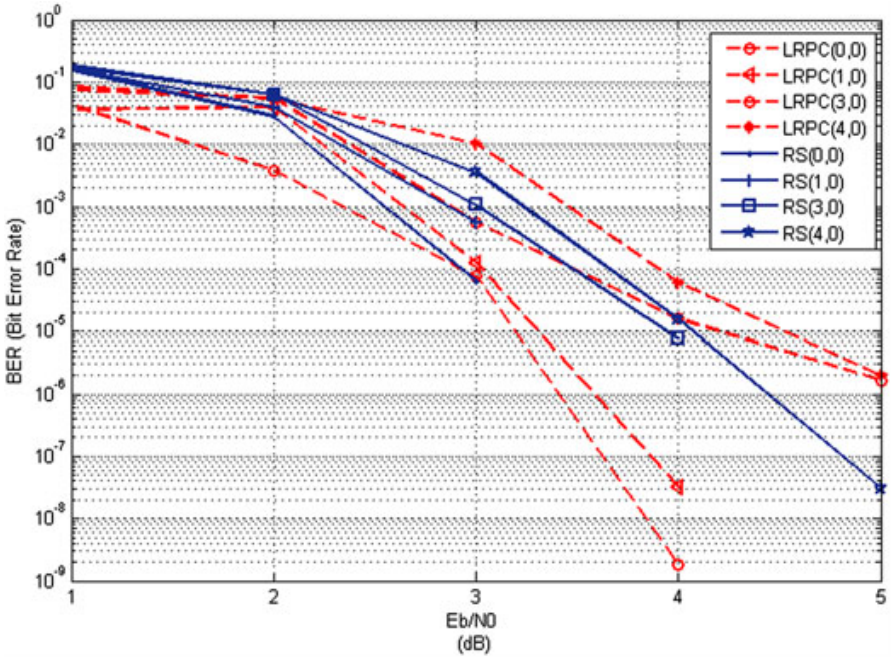


FIGURE 3.8 – Taux d'erreur binaire (BER) du code LRPC par rapport à un code Reed-Solomon (RS) avec un nombre différent des symboles OFDM affectés par un bruit impulsif

Pour mieux illustrer cette faiblesse, nous choisissons un taux BER cible de 10^{-6} pour un code LRPC. En effet, pour pouvoir corriger avec une probabilité supérieure à $1-10^{-6}$, il faut respecter ces relations :

$$\begin{aligned} 2^{-(n-k-2e)} &\leq 10^{-6} \simeq = 2^{-3\times 6} \\ 2^{-(n-k-2e)} &\leq = 2^{-18} \\ n-k-2e &\geq 18 \qquad (*) \\ \left(\tfrac{n-k}{2}\right) -9 &\geq e \end{aligned}$$

Nous notons que la capacité de correction pour un code RS est $\left(\frac{n-k}{2}\right)$, c'est à dire CAP_{RS} - $\epsilon \geq CAP_{LRPC}$.

Note : n, d sont respectivement la longueur et la dimension du code LRPC, e est l'erreur rang du code, et ϵ désigne les erreurs dues au manque de la capacité de correction.

Exemple : pour $n = 512$, $k = \left(\frac{n}{2}\right)$, $\left(\frac{n-k}{2}\right) = 128$ voir equation (*).

Cela signifie que, à condition que le sous-espace d'erreur dépasse moins de 119 symboles OFDM, LRPC décodera avec succès. Pour les grandes tailles, le décodage n'est pas garanti.

3.6 Conclusion

Dans ce chapitre, nous avons développé un nouveau système robuste au bruit impulsif et aux interférences à bande étroite. Nous avons également étudié les performances de ce nouveau code LRPC avec un schéma de transmission complet selon la norme G3-CPL dans un environnement bruyant des interférences CPL-BE. Le code LRPC (46, 23) sur $GF(2^{46})$ a été implémenté et comparé avec un code RS (255, 127) ; La taille des mots de code utilisés est sensiblement égale. Nous avons choisi la modulation OFDM avec une taille FFT = 256 sous-porteuses et une modulation BPSK conformément aux normes CPL-BE actuelles. Les résultats indiquent que, dans les conditions de canal et de bruit considérées, le code à métrique de rang LRPC introduit est plus performant que le code RS utilisé dans la norme CPL-G3 concaténé avec un code convolutif.

Bibliographie

[1] V. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. Hancke, "Smart grid technologies : Communication technologies and standards," IEEE Transactions on Industrial Informatics, vol. 7, pp. 529– 539, Nov 2011.

[2] S. Galli, A. Scaglione, and Z. Wang, "Power line communications and the smart grid," in First IEEE International Conference on Smart Grid Communications, (SmartGridComm), pp. 303–308, Oct 2010.

[3] M. Nassar, A. Dabak, I. H. Kim, T. Pande, and B. Evans, "Cyclostationary noise modeling in narrowband powerline communication for smart grid applications," in IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 3089–3092, March 2012.

[4] Kabore AW, Meghdadi V, Cances JP, Gaborit P, Ruatta O. Performance of Gabidulin codes for narrowband PLC smart grid networks. Power Line Communications and its Applications (ISPLC), 2015 International Symposium on, Austin, TX USA, IEEE ; March 2015 : 262–267.

[5] G. Richter and S. Plass, "Fast decoding of rank-codes with rank errors and column erasures," in International Symposium on Information Theory. ISIT 2004. Proceedings., pp. 398–398, 2004.

[6] Sarr, N. B., Boeglen, H., Agba, B. L., Gagnon, F., Vauzelle, R. (2016, April). "Partial discharge impulsive noise in 735 kV electricity substations and its impacts on 2.4 GHz ZigBee communications". In 2016 International Conference on Selected Topics in Mobile & Wireless Networking (MoWNeT) (pp. 1-7). IEEE.

[7] O. G. Hooijen, "On the relation between netwok-topology and power line signal attenuation," ISPLC, 98.

[8] M. Zimmermann and K. Dostert, "A multipath model for the powerline channel," IEEE Transactions on Communications, vol. 50, pp. 553–559, Apr 2002.

[9] Masood B, Baig S. Channel modeling of NB-PLC for smart grid. 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, Cyprus,IEEE ; 2015.

[10] "IEEE standard for low-frequency (less than 500 khz) narrowband power line communications for smart grid applications," IEEE Std 1901.2-2013, pp. 1–269, Dec 2013.

[11] Draft Standard for PoweRline Intelligent Metering Evolution (PRIME), 1.3A ed., PRIME Alliance Technical Working Group, May 2010. [Online]. Available : http ://www.prime-alliance.org/portals/0/specs/PRIME-Specv1 3 E 201005.pdf

[12] E. M. Gabidulin, "Theory of codes with maximum rank distance,"Problems on Information Transmission, vol. 21, pp. 1–12, Jan 1985.

[13] P. Gaborit, G. Murat, O. Ruatta and G. Zémor, Low Rank Parity-check codes and their application to cryptography. in Proc. WCC 2013.

[14] Abdul KarimY,Vahid M, Jean-Pierre C.Narrowband interference mitigation with LRPC code and OFDM for smart grid applications. Signal Processing and Communication Systems, 2016. ICSPCS 2016. 10th International Conference on, Gold Coast, Australia, IEEE ; 2016.

[15] Abdul Karim Y, Vahid M, Jean-Pierre C. Low Rank Parity Check Codes against Reed-Solomon Codes for Narrow-band PLC smart grid networks. 2016 International Conference on Computer & Communication Engineering ICCCE, Kuala Lumpur, Malaysia ; 2016.

[16] Kabore AW, Meghdadi V, Cances J-P, et al. Performance of rank metric codes for narrow-band PLC smart grid networks ; 2015.

[17] Richter, Gerd, and Simon Plass. "Error and erasure decoding of rank-codes with a modified Berlekamp-Massey algorithm." ITG FACHBERICHT (2004) : 203-210.

Chapitre 4 :

Combinaison des codes LRPC et du codage réseau aléatoire dans les réseaux de capteurs sans fil

4.1 Introduction

Les futurs systèmes de communication sans fil consisteront en une multiplicité de réseaux de capacités différentes. Dans ce chapitre, nous étudions l'influence du bruit impulsif sur des canaux sans fil. Les réseaux sans fil peuvent rencontrer de graves distorsions en raison de la présence de signaux parasites générés dans certaines centrales électriques dédiées aux applications de réseaux intelligents (SG). En fait, les effets environnementaux graves des stations à haute tension doivent être pris en considération, en particulier le bruit impulsif doit être pris en compte. Tout d'abord, pour faire face à ce genre d'environnement hostile, nous proposons un schéma de codage efficace dans un canal à système mono-utilisateur, lorsqu'une source transmet des données directement à une destination. La première partie de ce chapitre consiste à intégrer des codes de correction d'erreur en conjonction avec l'utilisation des systèmes OFDM. Nous évaluons, en termes de BER et PER, l'impact des codes de Gabidulin (RC), des codes LRPC et des codes polaires en utilisant des mesures réelles de bruit impulsif dans un canal multi-trajets réaliste. L'analyse des performances montre que les schémas de codage proposés sont très efficaces pour éliminer le bruit impulsif en mode mono-utilisateur. En outre, nous élargissons notre approche pour montrer l'efficacité des codes à métrique de rang dans les réseaux de capteurs sans fil (WSN), lorsque les données transmises traversent plusieurs nœuds intermédiaires pour atteindre la destination finale. Les capteurs permettent la collecte et le traitement des informations, mais lorsqu'un nœud cesse de fonctionner correctement, des erreurs peuvent se produire tout au long du réseau et les données ne sont pas reçues à l'utilisateur final. Pour augmenter la fiabilité du système, nous avons appliqué une technique de codage réseau avancée (NC) basée sur les codes LRPC (Low Rank Parity Check). Puisque nous vérifions la performance des codes LRPC avec des erreurs en blocs, nous présentons dans ce chapitre un nouveau mécanisme de codage d'erreur utilisant des codes LRPC dans un système multi-utilisateurs sans fil. Nous considérons le problème de la collecte de données dans les WSN, lorsque chaque lien entre deux nœuds présentent des erreurs de bruit impulsif avec un canal AWGN. En outre, le code LRPC est considéré comme un code externe qui code les données au moment de la transmission et du décodage à la station de traitement final (BS) concaténée avec un code convolutif en tant que code interne utilisant la technique du Decode-and-Forward (DF) à chaque niveau de nœud . En outre, nous calculons une approximation de la théorie de la probabilité de décodage pour le code LRPC dans le cas du codage réseau. Finalement, les méthodes proposées sont évaluées en termes de PER.

4.2 Bref aperçu sur le codage réseau linéaire aléatoire

Les réseaux de capteurs sans fil sont un réseau sans infrastructure composés de dispositifs de capacité de traitement à contraintes énergétiques limitées, qui sont éventuellement équipés d'une capacité à démoduler les signaux qui transitent. Dans la deuxième partie de ce chapitre, nous considérons le scénario de collecte de données dans lequel des capteurs localisés envoient des données à une station de base (BS) comme l'illustre la figure 4.1. Notons que les capteurs sont généralement alimentés par des piles, et donc, nécessitent une faible consommation d'énergie pour maximiser leur durée de vie. Avec une gamme de transmission limitée, la collecte de données nécessite l'utilisation de stations relais pour atteindre la station de base (BS).

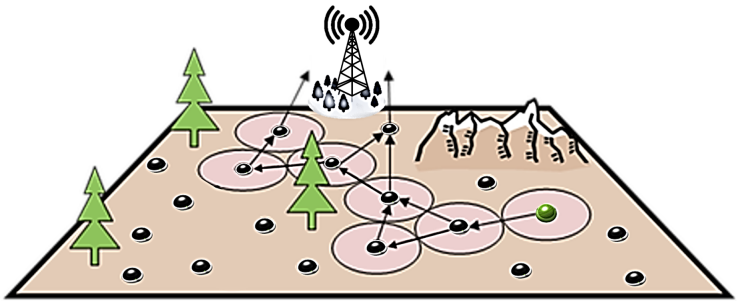


FIGURE 4.1 – Scénario de collecte de données dans les WSN.

Récemment, l'efficacité énergétique a reçu une attention considérable lors de la conception de protocoles de communication [1]. Cependant, la réception d'un nombre élevé de données de broadcast et de multicast sur un système WSN consomme les ressources énergétiques du réseau et peut rendre le réseau incapable de transporter le trafic normal. Par conséquent, de nouvelles solutions qui maintiennent une consommation d'énergie limitée présentes à la fois dans le système WSN et dans les capteurs sont nécessaires. En raison de la rareté d'approvisionnement en énergie des réseaux de capteurs sans fil (WSN) et des caractéristiques énergétiques peu coûteuses et limitées des capteurs, il est nécessaire de concevoir une architecture du réseau afin d'optimiser la consommation d'énergie. Le codage réseau (NC) a récemment été introduit pour réduire le trafic dans les réseaux généraux. Beaucoup de travaux ont étudié cette idée dans les réseaux câblés et sans fil. En effet, le codage réseau (NC) s'avère être une solution appropriée pour augmenter le débit de données et réduire la consommation d'énergie pour les réseaux de capteurs sans fil (WSN). Le codage réseau a d'abord été introduit dans [2] et, comme il a été démontré, cela permet d'améliorer considérablement l'efficacité du réseau en réduisant le nombre de transmissions. En effet, une topologie de nœud utilise des fonctions algébriques pour combiner les paquets de données et les envoyer à un autre. Ce processus est répété

par chaque nœud jusqu'à ce que les paquets atteignent les destinations. Le codage réseau linéaire aléatoire (RLNC) [3] est une classe de codage de réseau qui utilise un code linéaire généré de façon aléatoire par chaque nœud du réseau. Il suppose que les données sont des vecteurs sur un corps fini et que chaque nœud du réseau effectue une combinaison linéaire aléatoire de tous les paquets reçus et les transmet aux nœuds voisins. Néanmoins, si des erreurs de paquets se produisent, les paquets erronés sont combinés avec les paquets corrects, ce qui corrompt l'ensemble de la combinaison. Afin de résoudre les problèmes d'effacement et de paquets erronés, deux approches ont été utilisées dans la littérature de recherche. La première approche consiste à utiliser les codes LT [4]. Ils sont une solution bien connue au problème de la communication fiable sur un canal d'effacement de paquets. La deuxième approche consiste à utiliser des codes à métriques de rang et c'est cette solution que nous allons développer dans la suite de ce chapitre. Il est prouvé que les codes à métrique de rang sont efficaces contre les erreurs de combinaisons des paquets. Kötter et Kschischang ont testé la performance des codes en métriques rang sur les schémas RLNC. Nous nous concentrons principalement sur la proposition d'un algorithme de codage-décodage pour les réseaux de capteurs sans fil qui peut être appliqué à des normes comme la norme IEEE 802.15.4.

4.3 Idée du codage réseau linéaire

La figure 4.2 illustre un exemple de codage classique et un codage réseau. Considérons un système qui agit comme relais d'information, tels que un routeur, un nœud dans un réseau ad-hoc, ou un nœud dans un réseau P2P (Peer to Peer). Dans le codage classique lors de la transmission d'un paquet d'informations destinées à une autre nœud, il retransmet tout simplement la même information. Avec le codage réseau, le nœud permet de combiner un certain nombre de paquets qu'il a reçu ou créés dans un ou plusieurs paquets sortants [5].

Pour bien illustrer cette idée, les figure 4.3 et 4.4 présentent le temps de transmission nécessaire pour les deux techniques. Si nous souhaitons transmettre deux paquets a et b, le temps d'envoi de ces paquets par un commutateur (Switch) dans le cas du codage classique est $4t$, cependant, le temps que dure cette transmission dans le cas du codage réseau est réduite à $2t$ [6].

Pour décrire plus précisément cette technique, supposons que chaque paquet se compose de L bits. Nous pouvons interpréter s bits consécutifs d'un paquet comme un symbole dans le corps $\mathbb{F}_2$, avec chaque paquet composé d'un vecteur des symboles. Avec le codage réseau linéaire, les paquets sortants sont des combinaisons linéaires des paquets d'origine, où l'addition et la multiplication sont effectuées dans le corps $\mathbb{F}_2$. La combinaison linéaire des paquets de longueur L résulte d'un paquet codé également de taille L.

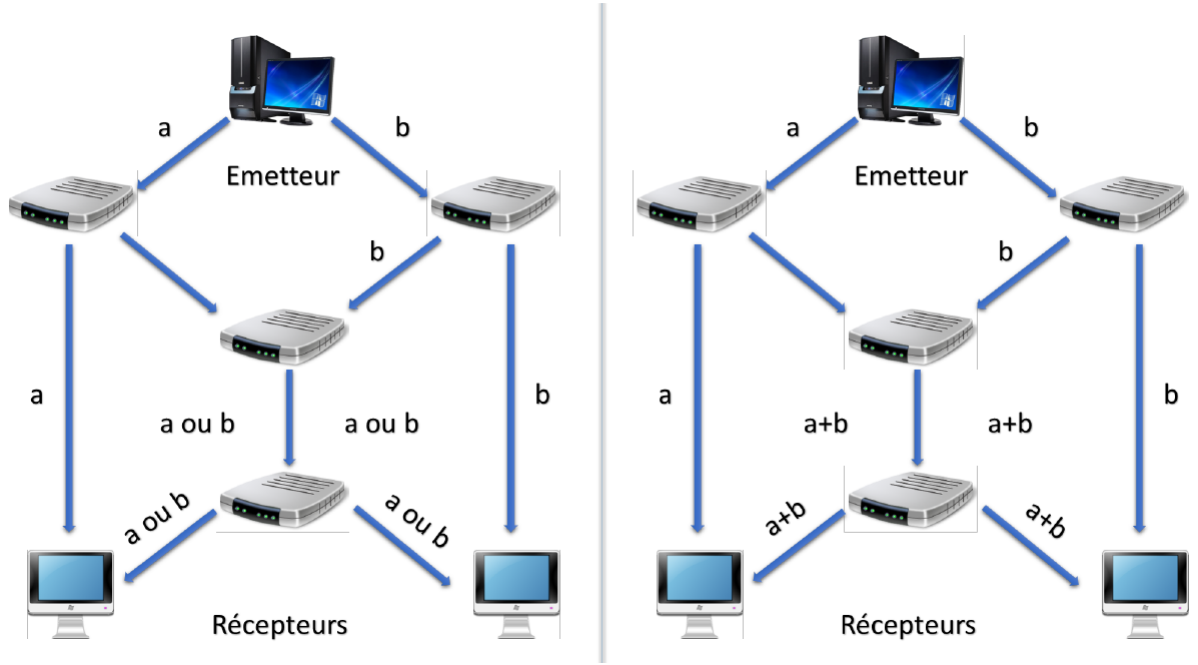


FIGURE 4.2 – Exemple du codage classique Vs codage réseau

FIGURE 4.3 – Exemple de codage classique

Supposons que chaque paquet est de longueur L bits. on peut considérer que chaque s bits de paquet est un élément q dans $\mathbb{F}_{2^s}$ qui donne un vecteur de $\frac{L}{s}$ symboles. Dans le codage réseau linéaire la sortie du nœud est une combinaison linéaire des paquets d'origine [7].

4.3.1 Expression théorique du codage réseau linéaire

Supposons que le nombre de paquets à coder est n paquets $M1, \cdots, Mn$ générés par une ou plusieurs sources. Avec un codage réseau linéaire [6], chaque paquet est associé à un vecteur de coefficients $g_1, \cdots, g_n \in \mathbb{F}_{2^s}$ ce qui peut s'écrire :

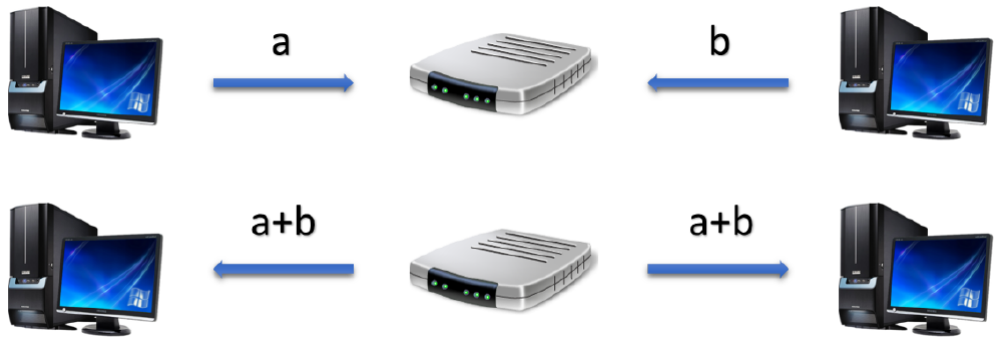


FIGURE 4.4 – Exemple du codage réseau

$$X = \sum_{i=1}^{n} g_i M_i.$$

On considère que les paquets sont des vecteurs de $\frac{L}{s}$ symboles, la combinaison linéaire doit être réalisée pour chaque position du vecteur c-à-d,

$$X_k = \sum_{i=1}^{n} g_i^k M_i$$

où $0 \leq k \leq \frac{L}{s} - 1$ et M_i^k et X_k sont respectivement les k$^{\text{ème}}$ symboles de M_i et de X. En plus des données combinées X, le vecteur des coefficients $g = (g_1, \cdots, g_n)$ est également stocké dans le paquet combiné. Ces informations ont un coût supplémentaire pour la transmission, mais ce coût diminue proportionnellement avec l'augmentation des longueurs de blocs de données. Des paquets combinés peuvent également être recombinés dans des nouveaux nœuds intermédiaires. Supposons qu'un nœud intermédiaire reçoive un ensemble de paquets combinés reçus $(g^1, X^1), \cdots, (g^t, X^t)$, où g^j est le vecteur de codage du j$^{\text{ème}}$ paquet combiné X^j. Après avoir choisi de façon aléatoire uniforme un ensemble de coefficients $h_1, \cdots, h_t$, ce nœud peut générer un nouveau paquet combiné (g', X') en faisant la combinaison linéaire suivante :

$$X' = \sum_{i=1}^{t} h_i X^i$$

Le vecteur de codage correspondant g' est alors

$$g'_i = \sum_{j=1}^{t} h_j g_i^j$$

Cette opération peut être répétée dans plusieurs nœuds dans le réseau [6].

4.3.2 Décodage

Il est tout d'abord nécessaire que pour chaque paquet reçu, le récepteur connaisse le vecteur des combinaisons linéaires totales de ce vecteur en fonction des paquets sources. Il

réalise ensuite la combinaison linéaire inverse (qui correspond à une inversion de matrice) pour retrouver les paquets sources [5].
Par exemple, supposons qu'un nœud reçoive l'ensemble de paquets $(g^1, X^1), \cdots, (g^t, X^t)$. Pour récupérer les paquets sources $M_1, \cdots, M_n$, il doit résoudre le système de s équations linéaires avec n inconnues :

$$X = G.M \Leftrightarrow \begin{cases} X_1 = \sum_{i=1}^{n} g_i^1 M_i \\ X_2 = \sum_{i=1}^{n} g_i^2 M_i \\ \cdots \\ X_t = \sum_{i=1}^{n} g_i^t M_i \end{cases}$$

où les inconnues sont les paquets sources M_i. Si le nombre d'équations linéairement indépendantes est supérieur ou égal au nombre de paquets sources, le système d'équations peut être résolu et les n paquets sources, $M_1, \cdots, M_n$, peuvent être récupérés [6].

Au niveau pratique, il faut noter que l'augmentation du nombre de paquets sources n codés nécessite une augmentation de la quantité de mémoire au niveau du récepteur. En effet, le récepteur doit stocker tous les paquets reçus jusqu'à ce qu'il reçoive au moins n paquets indépendants. En plus de la mémoire, la taille du bloc codé n a une conséquence sur le délai de décodage des paquets. Afin de réduire les besoins en mémoire, le délai et la complexité de calcul, la taille des matrices de décodage doit être limitée [7][8], [6].

4.4 La métrique de rang et ses applications au codage réseau

Les codes à métriques de rang sont des codes sous-espace qui présentent une propriété intéressante pour récupérer un sous-espace d'erreur de dimension finie même si toutes les données détectées sont fausses avant décodage.

Nous utilisons la forme d'onde impulsionnelle obtenue à partir des mesures d'une simulation faite dans le laboratoire Xlim-Poitier (voir figure 4.5). Sur cette figure, nous avons des échantillons mesurés dans une amplitude d'impulsion puissante de 735 kV d'une sous-station électrique. En raison de sa courte période, le bruit impulsif vient fortement perturber le spectre du signal transmis. Pour faire face à ce bruit impulsif, des codes de correction d'erreur sont proposés pour récupérer les données perdues.

Typiquement, lorsqu'un bruit impulsif survient, nous devons faire face à un ensemble d'erreurs telles que celles décrites dans la figure 4.6. Cet ensemble d'erreurs est habituellement connu dans la littérature sous la forme d'un motif d'erreur croisé (criss-cross) décrit dans le chapitre précédent et cela implique que la deuxième ligne de la matrice reçue soit effacée.

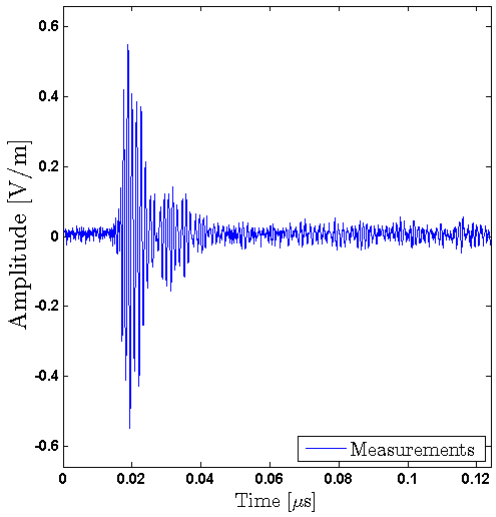


FIGURE 4.5 – Mesures réelles du bruit impulsif

0	0	0	0	0
e	e	e	e	e
0	0	0	0	0
0	0	0	0	0
0	0	0	0	0

FIGURE 4.6 – Bruit impulsif, Rang=1

Dans cette partie, nous examinons trois types de codes : les codes Gabidulin, les codes LRPC, et les codes polaires.

Les codes Gabidulin utilisent l'algorithme de Berlkamp-Massey pour le décodage, tandis que les codes LRPC utilisent la procédure utilisée dans la figure 3.3. Ensuite, nous observons à partir de [9] que le nombre de sous-espace t-dimensionnel de l'espace vectoriel m-dimensionnel sur $GF(q)$ est le coefficient gaussien. La définition du coefficient Gaussien est donné par :

$$\begin{bmatrix} m \\ t \end{bmatrix} \triangleq \prod_{i=0}^{t-1} \frac{q^m - q^i}{q^t - q^i} \tag{4.1}$$

A partir de l'équation (4.1), nous pouvons déduire le nombre des matrices de rang t dans $GF(q^{m\times N})$ définie par :

$$S(m,N,q,t)=\prod_{i=0}^{t-1}\frac{(q^m-q^i)(q^N-q^i)}{q^t-q^i} \tag{4.2}$$

Ensuite, nous pouvons obtenir le nombre des matrices de rang $\leq t$ dans $GF(q^{m\times N})$:

$$B(m,N,q,t)=\sum_{i=0}^{t}S(m,N,q,i) \tag{4.3}$$

Ces relations nous aident plus tard à calculer l'approximation théorique de la probabilité du décodage pour les codes à métrique de rang dans le contexte du codage réseau linéaire aléatoire (**R**andom **L**inear **N**etwork **C**oding).

4.4.1 Les codes polaires

Les codes polaires sont une classe de codes avec une structure permettant d'atteindre la capacité des canaux en utilisant un algorithme de codage-décodage de complexité $O(NlogN)$ où N est la longueur du code. L'architecture du codage basée sur le circuit discret de transformation de Fourier rapide qui permet d'obtenir des taux de codage différents à condition que certains bits soient gelés [10]. L'algorithme du décodage se déroule en mettant à jour les LLR (Log Likelihood Ratio : Teux de vraisemblance) à la sortie des différents étages intermédiaires selon certaines règles de base [10]. De plus, l'ensemble des simulations repose sur une bibliothèque de codes polaires développée au sein de l'équipe "ReSyst".

4.5 Architecture proposé du RLNC

Dans cette partie, nous allons présenter la combinaison des codes correcteurs d'erreurs dans une topologies aléatoire des réseaux de capteurs sans fil (WSN). Ensuite, nous allons appliquer le principe du codage réseau linéaire aléatoire avec ces codes et puis décrire le modèle du réseau proposé.

En outre, une approximation théorique de la probabilité du décodage des codes Gabidulin et LRPC dans le contexte du codage réseau sera exprimée.

4.5.1 Codage réseau linéaire aléatoire

Description du modèle : la source envoie une matrice $(m \times k)$ qui contient un ensemble de vecteurs. Nous considérons que les vecteurs sont les paquets à transmettre et chaque élément dans un vecteur représente un symbole sur $GF(q)$. Ensuite, la matrice $(m \times k)$ sera codée par un code [N, k] LRPC pour obtenir un vecteur $\mathbf{C}$ sur $GF(q^m)$ qui peut être considéré comme une matrice sur $GF(q^{m\times N})$. La matrice $\mathbf{C}$ contient les paquets codés qui seront combinés avec les coefficients des nœuds. Comme on peut le voir sur la figure 4.7, ces coefficients forment une matrice à chaque niveau du réseau. Le décodage n'est possible que lorsque cette matrice n'est pas singulière. Comme les capteurs sont très limités en terme de ressources radioélectriques, nous avons besoin de nœuds intermédiaires pour permettre à la station source de communiquer avec la station finale de traitement. Nous désignons $\mathbf{A}_i$ la matrice et i le niveau de nœud du réseau. À la destination finale, l'entrée du décodeur LRPC reçoit la matrice $\mathbf{Y}$ qui est exprimée par :

$$\mathbf{Y} = \prod_{i=0}^{L} \mathbf{A}_i.\mathbf{C} + \mathbf{E} \tag{4.4}$$

Où L est le nombre de tous les niveaux, $\mathbf{A}_i$ est la matrice du canal de niveau i et $\mathbf{E}$ $\in (GF(q))^{m\times N}$ est la matrice d'erreur additive qui corrompt les paquets. Nous désignons $\mathbf{A} = \prod_{i=0}^{L} \mathbf{A}_i$ la matrice du canal réseau.

La matrice $\mathbf{E}$ contient la matrice d'erreur de rang $\mathbf{E}^{(r)}$ et la matrice d'erreur du canal $\mathbf{E}^{(n)}$. La matrice d'erreur de rang est due à des paquets erronés, si nous multiplions cette matrice par une matrice de rang complet, le rang ne change pas. Par conséquent, pour 1 $\leq i \leq L$, nous avons la relation ci-dessous :

$$rank(\mathbf{E}^i) = rank(\prod_{i=0}^{L} \mathbf{A}_i.\mathbf{E}^i) = rank(\mathbf{E}^{(r)}) \tag{4.5}$$

Nous décrivons dans cette partie comment l'erreur de canal $\mathbf{E}^{(n)}$ peut affecter les paquets. Les coefficients gaussiens sont délimités par $4q^{t(N-t)}$ [11]. De (4.2), nous pouvons prouver que le nombre de matrices de rang t est borné supérieurement par :

$$S_e(m, N, q, t) \leq 4q^{t(N+m-t)} \tag{4.6}$$

Nous supposons une répartition uniforme des erreurs. Ensuite, la probabilité P_e que le rang de matrice d'erreur est inférieure à t est exprimée par :

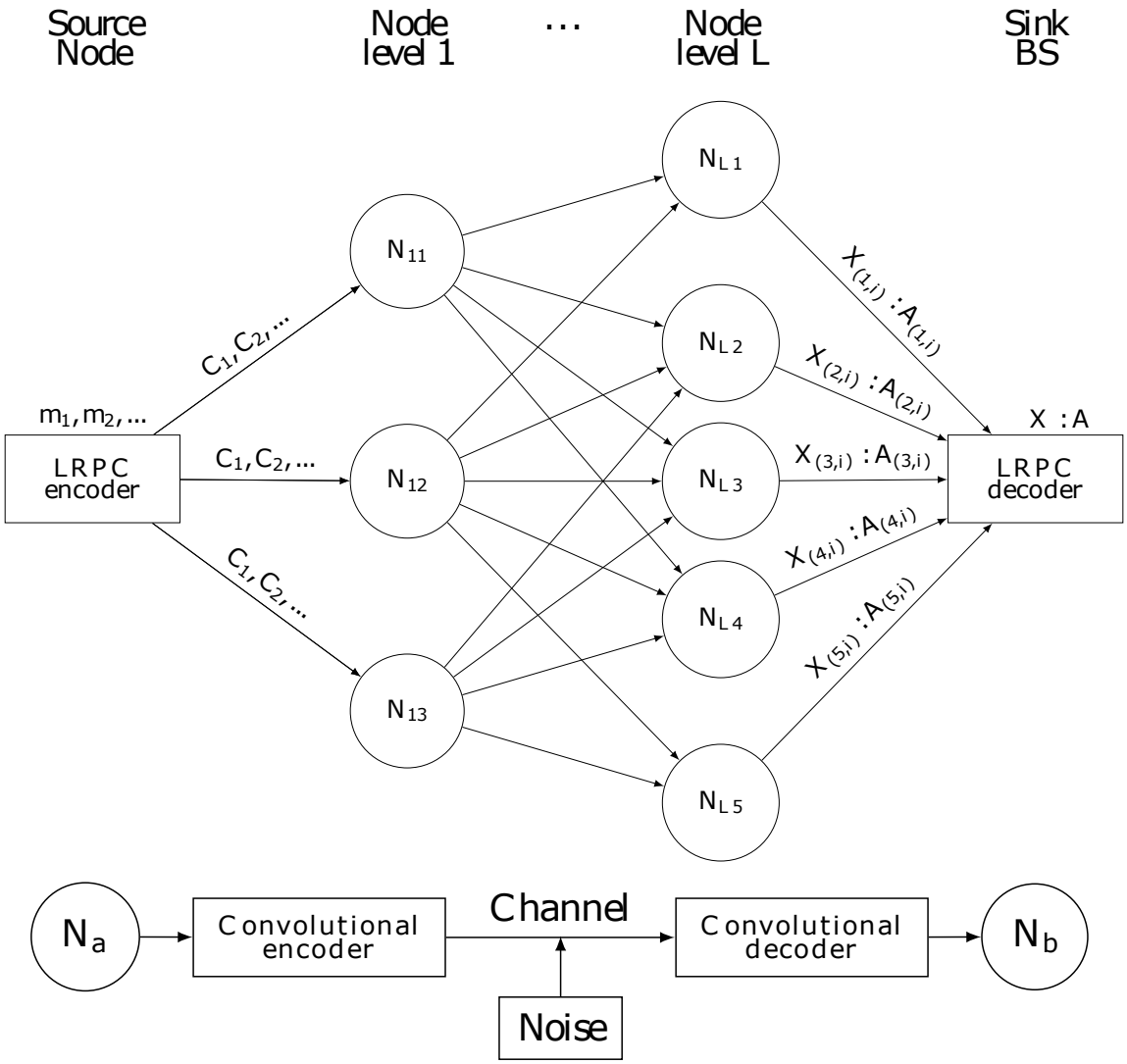


FIGURE 4.7 – Le modèle du réseau de capteurs proposé comprenant un nœud source qui utilise un codeur LRPC, une station de base qui utilise un décodeur LRPC et huit nœuds relais utilisant un code convolutif et le RLNC.

$$P_e \leq \frac{4t.q^{t(N+m-t)}}{q^{mN}} \tag{4.7}$$

Nous notons que lorsque nous multiplions $\mathbf{A}_i$, dans chaque niveau, par la matrice de canal, les erreurs lignes changent et se transforment en erreurs colonnes comme nous pouvons le voir dans la figure 4.8, où un modèle d'erreur typique dans notre réseau RLNC est illustré. Ensuite, le produit de $\mathbf{A}_i$ et $\mathbf{E}_i^{(n)}$ est ajouté à l'erreur de canal du niveau $i+1$ et donne lieu à la matrice de canal d'erreur $\mathbf{E}_{i+1}^{(n)}$. Cette opération sera répétée à chaque étape du réseau jusqu'à la station finale de réception (BS). D'autre part, si L le nombre de niveau est important, dans presque tous les cas, la matrice d'erreur $\mathbf{E}^{(n)}$ devient une matrice à rang complet et, dans ce cas, le code à métrique de rang n'arrive pas à décoder

ce type d'erreurs.

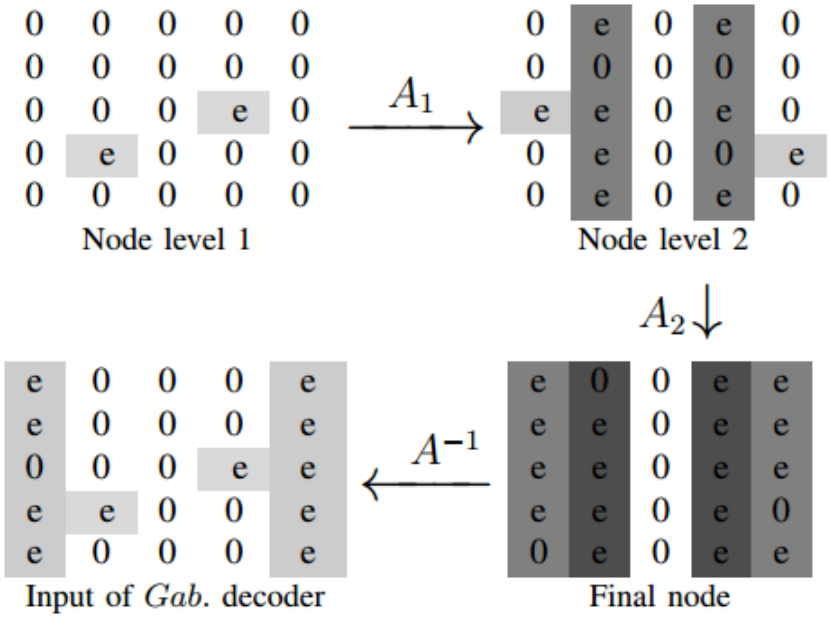


FIGURE 4.8 – Exemple de transmission des paquets dans un réseau RLNC en présence d'erreurs de canal.

Soit r le nombre de colonnes non nulles de $\mathbf{E}^{(n)}$, où la matrice $(m \times r)$ est choisie au hasard. Cela signifie que la probabilité que le rang de $(m \times r)$ soit inférieur à t vérifie l'équation suivante :

$$P_M^{(r)} = \frac{B(m, r, q, t)}{q^{mr}} \tag{4.8}$$

Où $B(m, r, q, t)$ est définie dans l'équation (4.3).

Pour calculer la probabilité du décodage d'erreur pour les codes LRPC, nous supposons que p_s est le taux de symboles de canal. La probabilité qu'une erreur se produise dans une colonne de matrice $\mathbf{C}$ soit :

$$p_c = 1 - (1 - p_s)^{mL}$$

Soit P_{gab} la probabilité d'erreur de paquet pour les codes Gabidulin dans RLNC, nous avons :

$$P_{gab} = \sum_{i=t+1}^{N} \binom{N}{i} p_c^i (1 - p_c)^{N-i} \times (1 - P_M^{(i)}) \tag{4.9}$$

Tableau 4.1 – Paramètres OFDM

Parameters	**Values**
Number of subcarriers	512
Channel bandwidth	5 MHz
Subcarrier Spacing	488 Hz
Symbol time	100.8 μs
Guard time	11.2 μs

Preuve. La probabilité que l'erreur se produise dans i colonnes de N est $p_c^i(1-p_c)^{N-i}$. La probabilité que le code à métrique de rang ne puisse pas récupérer les erreurs lorsque $i \leq t$ est égal à 0. Lorsque $i > t$, la probabilité que le rang de la matrice soit supérieur à t est $(1 - P_M^{(i)})$, où $P_M^{(i)}$ est exprimé dans l'équation (4.8) . Dans le cas du code LRPC, P_{LRPC} peut être exprimé comme suit :

$$P_{LRPC} = \sum_{i=1}^{N} \binom{N}{i} p_c^i (1-p_c)^{N-i} \Bigg(min(1, q^{-(1+(N-k)-i.d)}) - \sum_{j=1}^{min(t,i)} q^{-(1+(N-k)-i.d)} \frac{S(m,i,q,j)}{q^{mL}} \Bigg) \quad (4.10)$$

Note : $P_{LRPC} \approx P_{gab}$ pour $d = 2$.

4.6 Les résultats de simulation dans un canal AWGN avec un bruit impulsif dans un scénario P2P

Les résultats obtenus à partir du schéma de transmission conçu, représenté dans la figure 4.9, sont discutés dans ce paragraphe. Le schéma proposé évalue les deux codes à métrique de rang lorsqu'un seul utilisateur envoie des données directement à une seule destination (finale). Nous montrons la performance des schémas de codage proposés, en termes de taux d'erreur binaire (BER), dans un canal AWGN avec du bruit impulsif. Comme le montre la figure 4.9, les schémas de codage proposés sont simulés avec la modulation BPSK et OFDM, avec une taille de bloc de 512 porteuses. Les paramètres sont représentés dans le tableau 4.1.

Pour faire face à des erreurs isolées, nous ajoutons un code convolutif concaténé avec le code LRPC. Ce code est généré par la matrice génératrice G = [171,133] sous forme

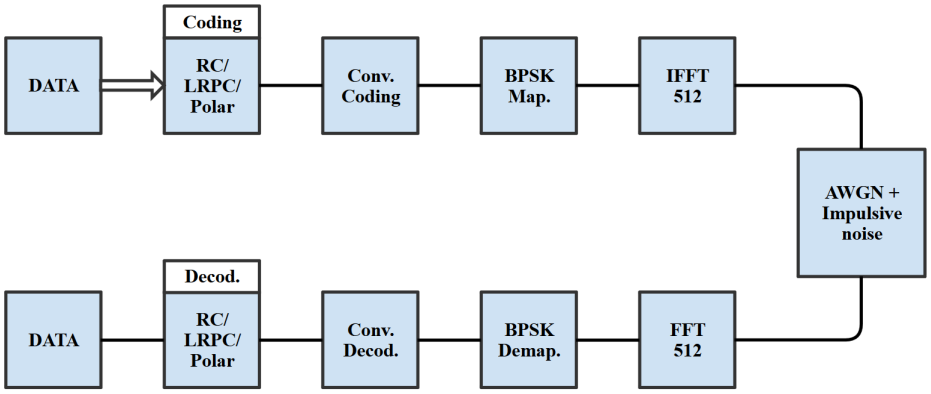


FIGURE 4.9 – Schéma de transmission

octale. Dans cette partie, nous ne discutons que des résultats de simulation de $RC(n, k)$ et de $LRPC(n, k)$, avec $n = 16$ et $k = 8$, sur $GF(2^{16})$. Notons que le bruit impulsif mesuré est ajouté au flux de symboles. Pour les schémas du décodage, nous utilisons l'algorithme Berlekamp-Massey modifié pour les codes RC (Gabidulin), et l'algorithme décrit dans la figure 3.3, pour les codes LRPC. Dans la fig. 4.10, nous comparons les performances obtenues à partir des systèmes RC et LRPC avec les données non codées à travers un canal de bruit impulsif mesuré.

En se référant à la figure 4.10, nous observons un gain important comparé au cas non codé. Le BER cible de 10^{-6} est obtenue à un Eb/No de 3.5 dB et 5 dB pour RC et LRPC respectivement. Le système RC dépasse le schéma LRPC de 2 dB à un BER de 10^{-6}. Ceci est dû au fait que LRPC fonctionne avec une probabilité d'échec du décodage donnée par rapport aux codes RC, voir [12].

4.6.1 Application à un canal réaliste

Dans cette section, nous considérons un environnement multi-path. Pour cela, nous utilisons une approche de modélisation de canal basée sur un traçage déterministe des rayons qui prend en compte les caractéristiques de l'environnement de transmission. L'outil logiciel utilisé s'appelle RaPSor et l'environnement réaliste choisi pour la simulation est le Laurentides qui est une sous-station électrique importante située au Québec (Canada).

4.6.1.1 Description et simulation 3D

RaPSor (Ray Propagation Simulator) est un outil de simulation de propagation radio entièrement développé par le laboratoire XLIM [13]. Il est basé sur un traçage de rayons $3D$ associé aux lois de l'optique géométrique (GO) et à la Théorie Uniforme de la Diffraction (UTD) pour le calcul de plusieurs chemins entre un émetteur et un récepteur. Pour un lien

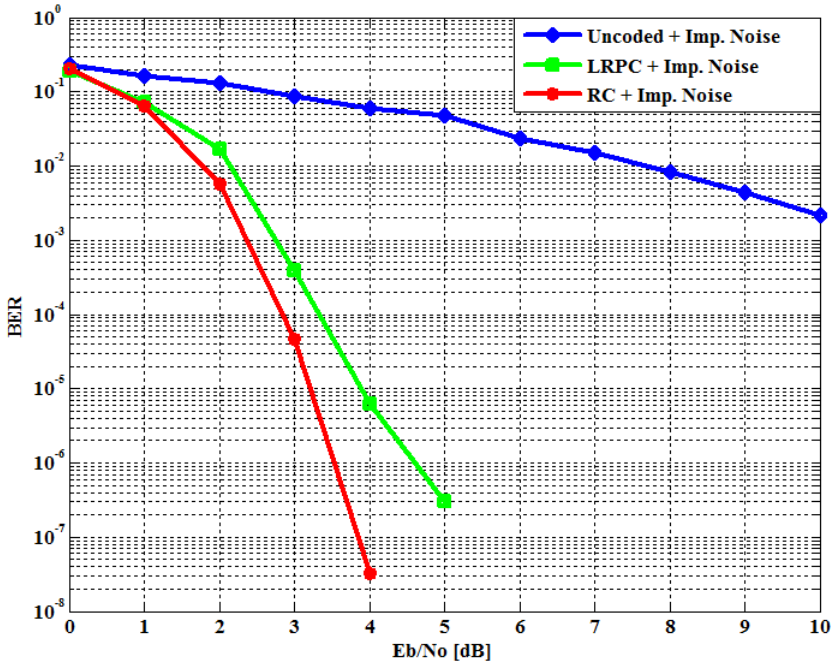


FIGURE 4.10 – Performances de BER pour les codes RC, LRPC et le système non codé en présence de bruit impulsif sur un canal AWGN.

émetteur-récepteur, ce simulateur est capable d'identifier et de caractériser la combinaison existante de multitrajets [14]. En outre, nous avons accès aux caractéristiques de chacun de ces chemins (atténuation, phase, délai ...). Par conséquent, nous pouvons obtenir la Réponse Impulsionnelle du Canal (CIR) noté $h(t, \tau)$ pour le point choisi comme dans [15] :

$$h(t, \tau) = \sum_{i=0}^{N} a_i(t)\delta(t - \tau_i(t))$$

L'environnement réaliste correspond à la sous-station électrique des Laurentides HV au Québec (Canada) avec une superficie de $1300m \times 800m$. Les équipements et les appareils présents dans la sous-station sont notamment des transformateurs, des disjoncteurs, des interrupteurs, etc. Dans le scénario de transmission considéré, un nœud de collecte de données (DGN) est positionné sur une tour dans l'environnement (voir la figure 5). Un nœud récepteur est positionné sur un transformateur. Il est placé sur un poteau d'éclairage de $60m$ de haut comme représenté sur la figure 4.11. Dans cette figure, nous pouvons noter qu'il existe plusieurs chemins en raison des interactions entre le signal et les objets présents dans la sous-station. Le chemin direct a une puissance de -87 dBm associée à un retard de 699 ns. Les caractéristiques des chemins secondaires significatifs résultants de la combinaison des interactions entre les réflexions et les diffractions sont présentées dans le tableau 4.2. Nous utilisons Ri pour les réflexions et Di pour les diffractions où i est le nombre du chemin.

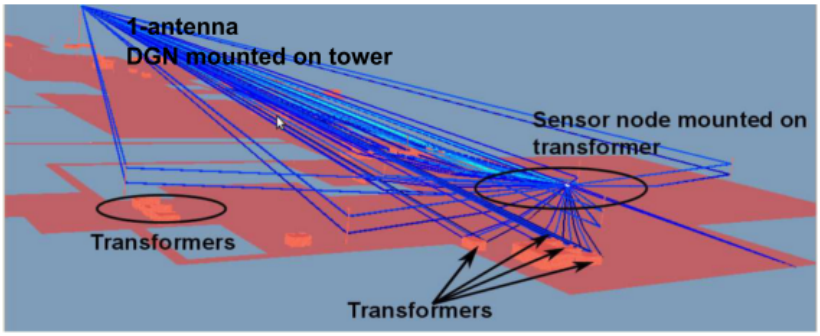


FIGURE 4.11 – Sous-station HV avec des capteurs et les positions DGN montrant l'interaction des rayons avec les objets en sous-station

Tableau 4.2 – Exemple de caractéristiques RI de RaPSor

Nature	**Power** (dBm)	**Delay (ns)**
R2	-114	708
R8, D8	-170	735
R20, D20	-154	2014

Cependant, pour pouvoir utiliser ce type de CIR dans un simulateur de système de communication, nous devons traiter les données.

- Extraction de données du CIR (atténuation, retard, phase)
- Calcul du champ vectoriel
- Échantillonnage
  - Récupération de l'indice
  - Calcul de la somme vectorielle
- Normalisation de la puissance

Dans la figure 4.12, le premier chemin à 699 ns est composé d'un chemin LOS et de plusieurs chemins NLOS. Le deuxième chemin est ainsi constitué de plusieurs chemins NLOS et ainsi de suite. Le modèle du canal résultant est sélectif en fréquence. Le délai maximal et la bande passante de cohérence associée sont respectivement 733 ns et $1,3$ MHz.

Après avoir obtenu l'atténuation normalisée, nous procédons à la recherche des coefficients de cette voie multipath par échantillonnage en aval (downsampling) du taux de transmission de symboles de la transmission. Nous obtenons enfin un CIR équivalent :

$$C = \sum_k \sqrt{P_k} e^{j\phi_k} \delta(t - kT)$$

Avec P_k est la puissance associée au composant multipath $k-th$ équivalent et ϕ_k sa phase. T est la période des symboles d'émission. Pour la partie des résultats de la

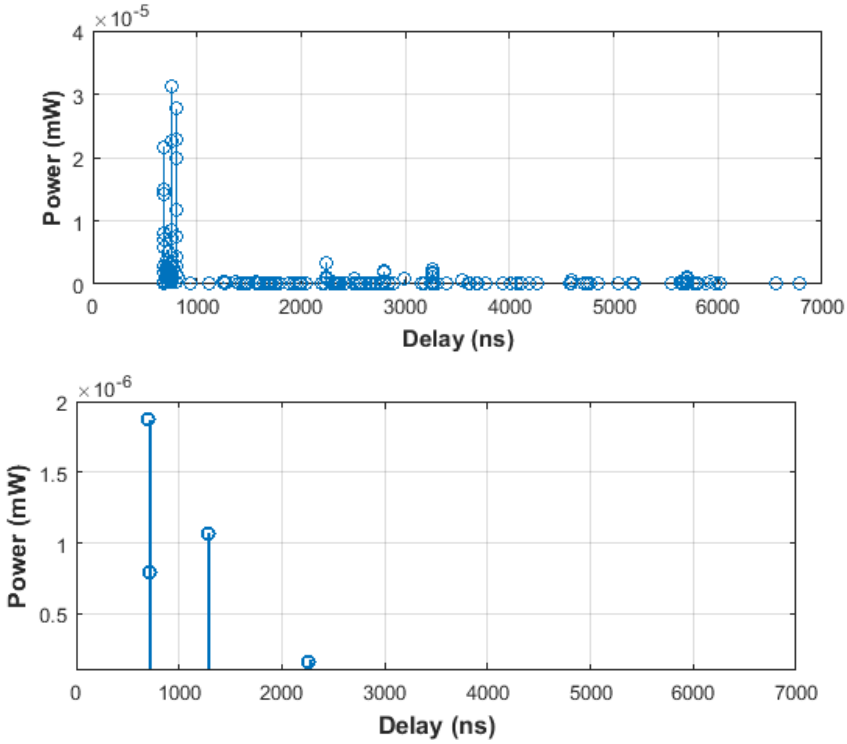


FIGURE 4.12 – Réponse Impulsionnelle (IR) de RaPSor avant et après l'échantillonnage

simulation, nous considérerons deux débits de données : 54 *Mbps* et 100 *Mbps*.

4.6.1.2 Résultats des simulations

Dans cette section, nous présentons des résultats de simulation numériques qui illustrent les performances de la chaîne de transmission, y compris le schéma de codage proposé et la modulation OFDM dans les canaux multipath et impulsifs. Les taux d'erreur Binaire (BER) et Paquet (PER) en fonction de Eb/No dans différentes configurations sont calculés.

a) Premier débit à 54 *Mbps* : la charge utile des données est de 150 octets. Nous obtenons une réponse impulsionnelle équivalente du canal avec trois coefficients (voir tableau 4.3). Dans notre simulation, nous choisissons une FFT de V_{512} selon la norme

Tableau 4.3 – Coefficients des RI pour WIFI IEEE 802.11g ($54 Mbits/s$)

C_1	C_2	C_3
0.5+0.5i	0.32-0.38i	0.43+0.25i

choisie (WIFI IEEE 802.11g). Compte tenu du retard du premier composant multipath, nous obtenons le CIR final équivalent :

$$V_{512} = [\underbrace{0 \cdots 0 \cdots 0}_{86} \quad C_1 \quad C_2 \quad C_3 \quad \underbrace{0 \cdots 0 \cdots 0 \cdots 0}_{423}]$$

Ensuite, une FFT (Fast Fourier Transform) est appliquée à $V_5 12$ pour obtenir H_k qui représente la réponse en fréquence du canal à la tonalité k. Pour chaque support k, nous obtenons le Y_k reçu comme indiqué ci-dessous :

$$Y_k = H_k X_k + noise$$

Ce signal est ensuite égalisé par la multiplication avec le conjugué de H_k : $H_k^* Y_k$. ***b)*** Deuxième débit à 100 $Mbps$: nous considérons ici un débit binaire cible de 100 $Mbps$. Compte tenu du même CIR, nous obtenons maintenant les coefficients de la réponse impulsionnelle équivalente du canal dans le tableau 4.4. Pour comparer ces résultats

Tableau 4.4 – Coefficients des RI pour LTE-Advanced (100 $Mbits/s$)

C_1	C_2	C_3	C_4	C_5	C_6
0.6+0.41i	0.24-0.27i	0.23+0.26i	0.2-0.25i	0.19-0.2i	0.18+0.09i

avec un système de codage du canal puissant, nous utilisons comme référence, un code polaire de taux 1/2 avec une taille de paquet de 1500 octets. Dans la figure 4.13, nous comparons le BER des différents schémas à savoir RC, LRPC, code polaire et les données non codées. Ces différents schémas de codage sont examinés dans le canal multipath réaliste en présence de bruit impulsif. Comme prévu, nous notons une dégradation de la performance par rapport aux résultats obtenus dans la figure 4.10. En revanche, nous obtenons un gain important pour les trois codes par rapport au cas non codé. Ces gains sont au moins égaux à 10 dB à un BER de 10^{-5}. Le BER de RC à 10^{-5} est atteint lorsque Eb/No est égal à $5,5$ dB. Pendant ce temps, pour les codes LRPC et polaires, Eb/No est égal à 6 dB et $9,5$ dB, respectivement. En comparant les trois schémas de codage, nous pouvons facilement voir que les codes RC et LRPC sont plus efficaces que le code polaire dans ce canal multipath. Le code RC a un gain de 4 dB par rapport au code polaire lorsque le BER de 10^{-5} est considérée. Nous pouvons conclure que les codes polaires ne sont pas conçus pour s'attaquer au bruit impulsif. Cependant, nous comaprons aussi nos résultats à ceux obtenus dans [16]. Ils ont utilisé un entrelaceur de domaine temporel associé à un égaliseur MMSE (Minimum Mean Square Error) [17] en présence de bruit impulsif sur un canal multipath de Rayleigh. Le gain est d'environ 20 dB pour un BER $= 10^{-5}$.

Ensuite, nous considérons un débit de données de 100 $Mbps$. Ici, nous évaluons le scénario considéré dans un canal multipath sélectif en fréquence. La bande passante de cohérence du canal ($1,3$ MHz) est inférieure à la bande passante du signal (40 MHz). Comme le montre la figure 4.14, le BER pour les données non codées est constant et égal

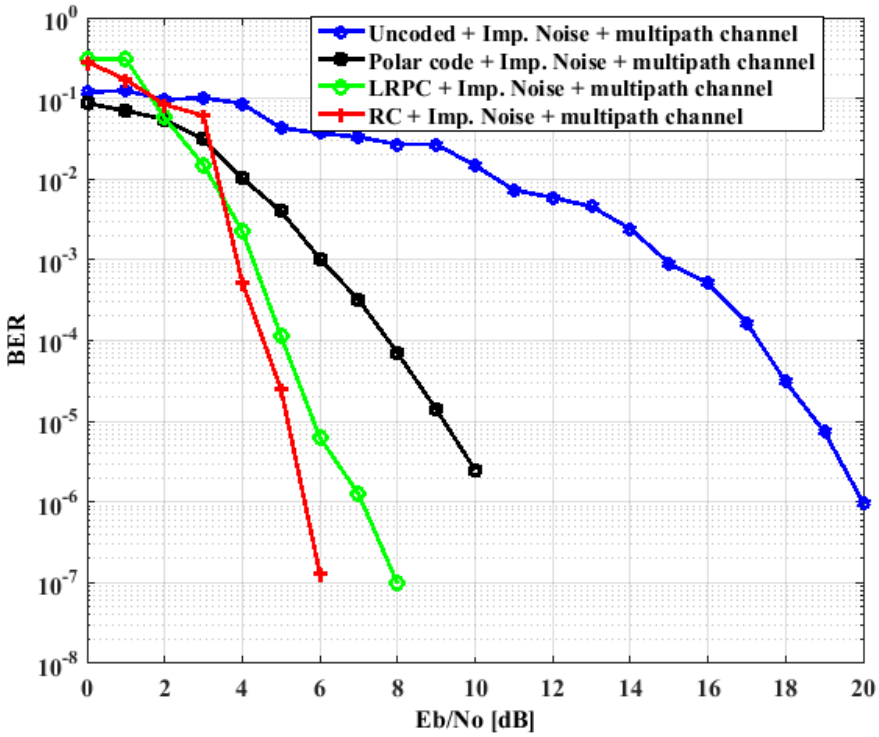


FIGURE 4.13 – Performances de BER pour RC, LRPC, code polaire et système non codé en présence de bruit impulsif dans un canal multipath réaliste (1^{er} débit de données)

à 10^{-1}. Par rapport à la figure 4.13, pour les trois schémas proposés, l'écart avec le cas non codé augmente significativement de plus de 3 dB à un BER de 10^{-5}.

Le taux d'erreur de paquet (PER) est également un paramètre très important pour caractériser la qualité de service QoS. Pour tester les performances d'un récepteur terminal d'accès, les PER sont simulés et les résultats sont représentés sur la figure 4.15 et 4.16 pour les deux débits de données. La figure 4.15 montre que le PER de RC à 10^{-2} est atteint lorsque Eb/No est égal à $10,5$ dB. Dans le cas de LRPC et du code polaire, pour la même cible BER, Eb/No est égal à 11 dB et 13 dB, respectivement.

En outre, le PER pour 100 $Mbps$ est illustré dans la figure 4.16. Le rapport signal sur bruit Eb/No pour les trois schémas proposés est compris entre 11 dB et 14 dB à un PER égal à 10^{-2}. En résumé, les deux codes à métriques de rang sont plus efficaces que le code polaire.

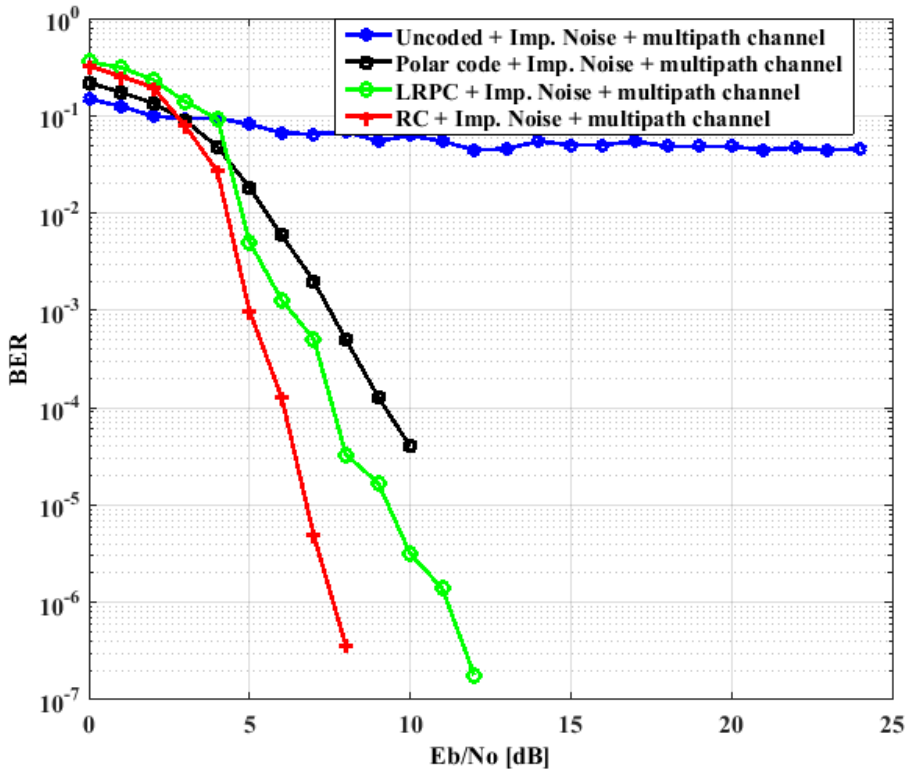


FIGURE 4.14 – Performances de BER pour RC, LRPC, code polaire et système non codé en présence de bruit impulsif dans un canal multipath réaliste ($2^{\text{ème}}$ débit de données)

4.7 Les résultats de simulation de RLNC dans un canal AWGN avec un bruit impulsif dans un réseau de capteurs sans fil

Dans cette section, nous évaluons la performance des codes LRPC par rapport aux codes Gabidulin (RC) avec les codes RS sur un canal du bruit impulsif dans le contexte des réseaux de capteurs sans fil. Nous considérons dans nos simulations de nombreux scénarios de transmission. Tout d'abord, à la source, les données sont codées par un code LRPC. Ensuite, au premier niveau de nœuds intermédiaires, un code convolutif avec un taux de codage $0,5$ est utilisé pour protéger les données pour la transmission dans les nœuds relais. Du deuxième niveau de nœuds intermédiaires au niveau $L-th$ $(L=8)$, chaque nœud utilise un décodeur convolutif puis il ré-encode les données en utilisant le même codeur convolutif. Par conséquent, nous utilisons la technique du Decode-and-Forward (DF). Lorsque les données atteignent la destination finale, elles seront décodées à l'aide du décodeur LRPC. Dans le second cas, nous remplaçons les codes LRPC concaténés avec les codes convolutifs par des codes Gabidulin suivis des codes Reed-Solomon. Nous montrons également la performance des codes Gabidulin utilisés uniquement dans notre modèle

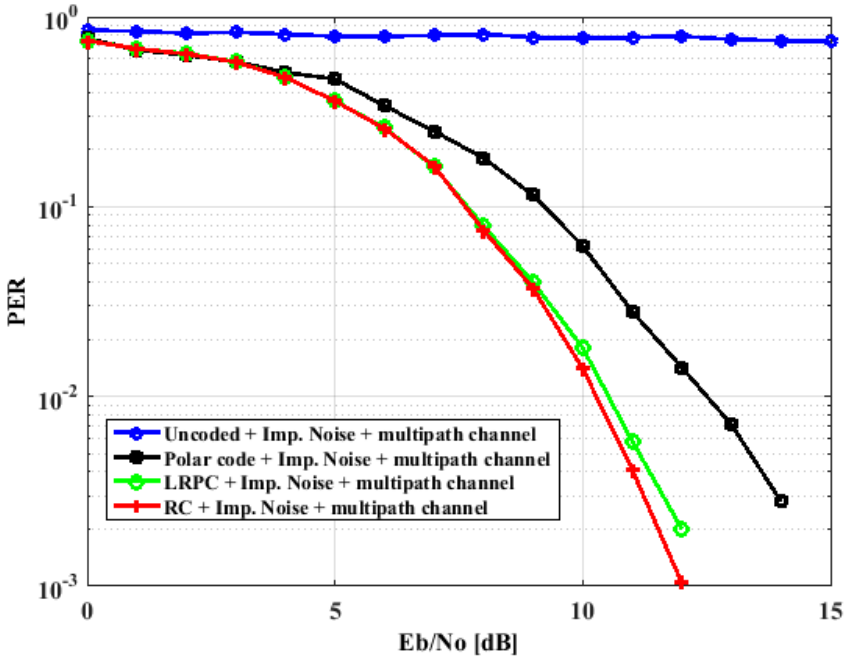


FIGURE 4.15 – Performances de PER pour RC, LRPC, code polaire et système non codé en présence de bruit impulsif dans un canal multipath réaliste (1er débit de données)

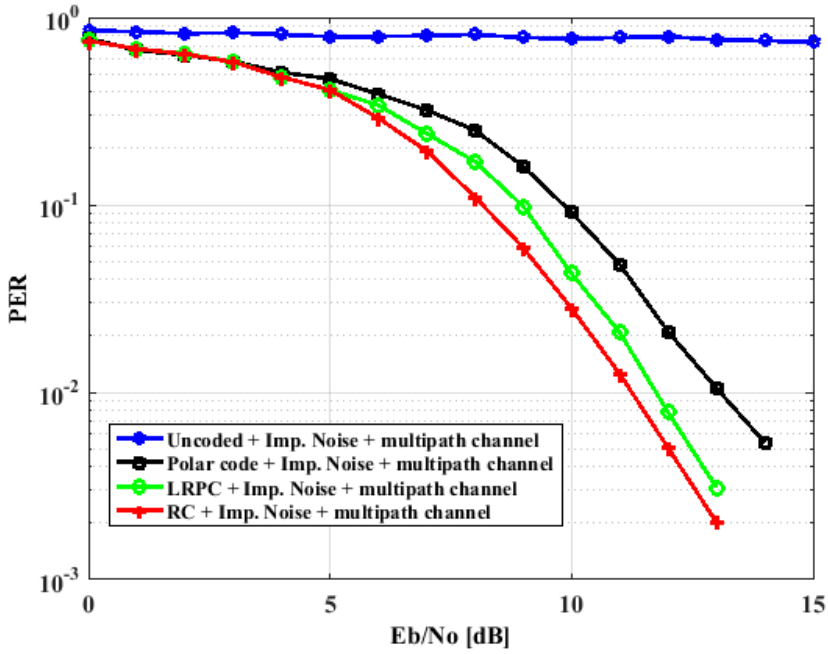


FIGURE 4.16 – Performances de PER pour RC, LRPC, code polaire et système non codé en présence de bruit impulsif dans un canal multipath réaliste (2èmedébit de données)

de réseau proposé. De plus, nous présentons les résultats de l'approximation théorique pour la probabilité d'erreur du décodage (LRPC, Gabidulin). Pour les codes LRPC et

Gabidulin, nous prenons comme paramètres [46,32] dans $GF(2^{46})$. Par conséquent, ici, le taux de codage est d'environ 0,66. Pour ces paramètres, les capacités de correction de rang du code LRPC simulé et du code Gabidulin sont 7 ($\frac{N-k}{2} = \frac{46-32}{2}$). Le paramètres utilisé pour le code Reed-Solomon est [511,236] sur $GF(2^9)$. Pour l'encodeur convolutif, nous utilisons un entrelaceur pour améliorer la correction d'erreur. Pour tous les cas, le message initial est une matrice de taille $(m \times k)$ $((46 \times 32)$ dans cette simulation) et le message codé est une matrice de taille $(m \times k)$ $((46 \times 100)$ dans cette simulation). Le taux de code total est $0,32$.

$LRPC - CC(i)$ désigne un code LRPC concaténé avec un code convolutif avec i les paquets erronés transmis par les nœuds en panne et indique un résultat théorique. La même notation est adoptée pour les différents autres codes. Dans la figure 4.17, nous comparons les différents codes en présence de bruit de fond uniquement en raison des erreurs de canal et de l'absence d'erreur de rang. Nous observons que le $LRPC - CC$ est meilleur que le $Gabidulin - RS$ avec un gain de codage de 2 dB. En outre, il surpasse environ 3 dB le code Gabidulin à un PER de 10^{-4}.

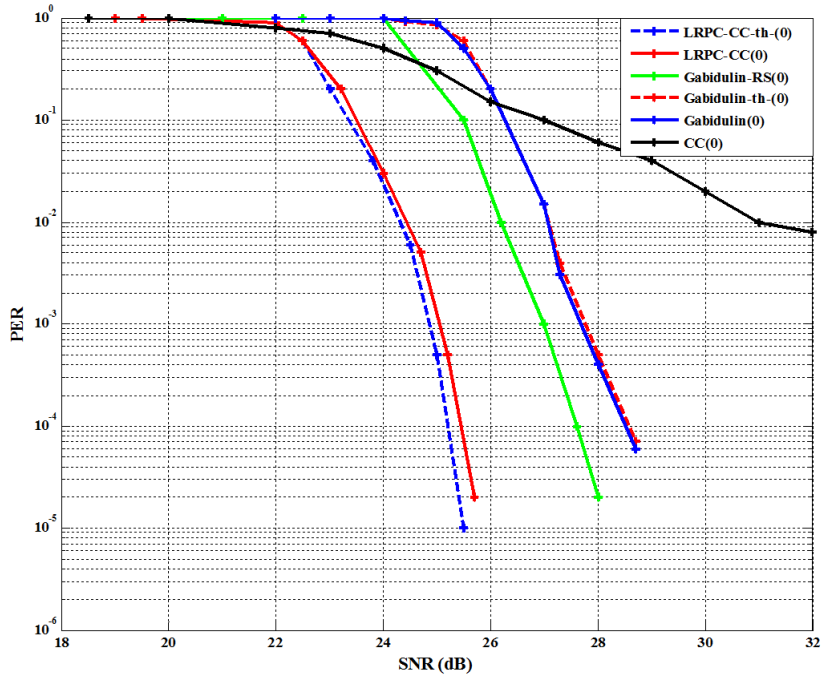


FIGURE 4.17 – Taux d'erreur de paquets (PER) pour les différents codes avec uniquement du bruit de fond

La courbe théorique de $LRPC - CC$ quantifie avec précision la relation entre Eb/No (SNR) et la probabilité d'erreur de paquet. L'emploi d'un code à métrique de rang sans utiliser le code Hamming n'a pas de contribution bénéfique à l'égard des erreurs de canal. C'est en raison de la propriété du bruit blanc, chaque symbole a une forte probabilité de générer une erreur de rang et réduisant ainsi la capacité de correction d'erreur. En effet,

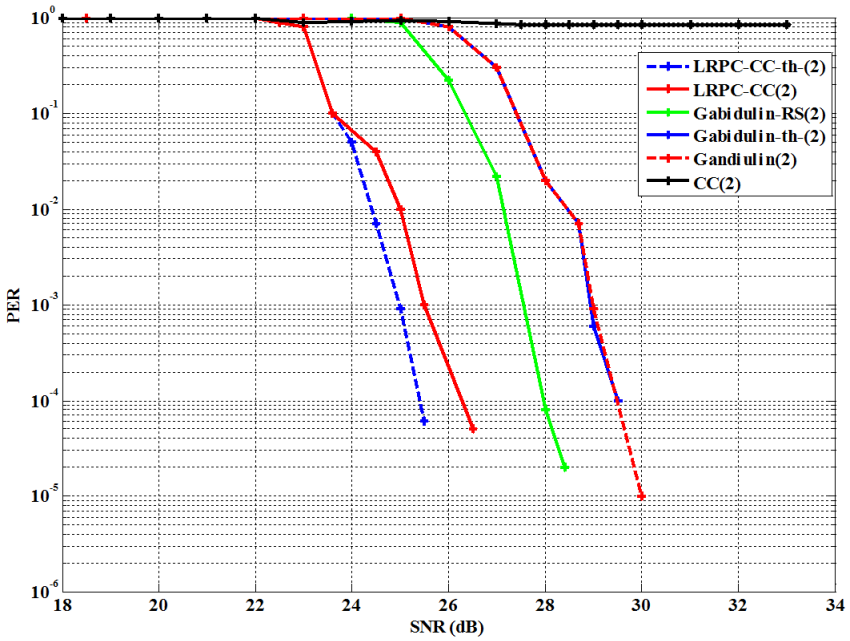


FIGURE 4.18 – Taux d'erreur de paquets (PER) pour les différents codes avec le bruit de fond et deux paquets erronés injectés sur le réseau.

ce résultat est prévisible pour le code Gabidulin puisque les codes à métriques de rang sont plus efficaces lorsque les erreurs sont confinées dans les lignes ou dans les colonnes. C'est la raison de l'utilisation d'un code Hamming dans notre cas pour réduire l'impact des erreurs de canal.

Dans la figure 4.18, nous montrons les performances du réseau avec deux paquets erronés affectés par une défaillance de nœuds. La performance du code à métrique de rang varie légèrement en fonction du nombre de paquets erronés. Les codes concaténés présentent une très bonne performance par rapport au code convolutif CC. En outre, les codes Gabidulin succèdent à la procédure de correction dans ce cas. Pour calculer les résultats théoriques, pour le code $LRPC-CC$ et Gabidulin avec 2 paquets erronés, nous avons remplacé la capacité de correction d'erreur t par $t-2$ dans les équations (4.9) et (4.10).

4.8 Comparaison de la complexité

La complexité des codes ne serait pas complète sans une comparaison de leurs complexités de décodage. Le décodage RLNC montre une complexité très importante : $\mathcal{O}(m^3)$, où m est le nombre de paquets générés pour chaque transmission [18]. Pour un codage réseau linéaire, la complexité vaut $\mathcal{O}(m^2)$.

Pour les codes LRPC, si N est le nombre de symboles par mot de code et k le nombre

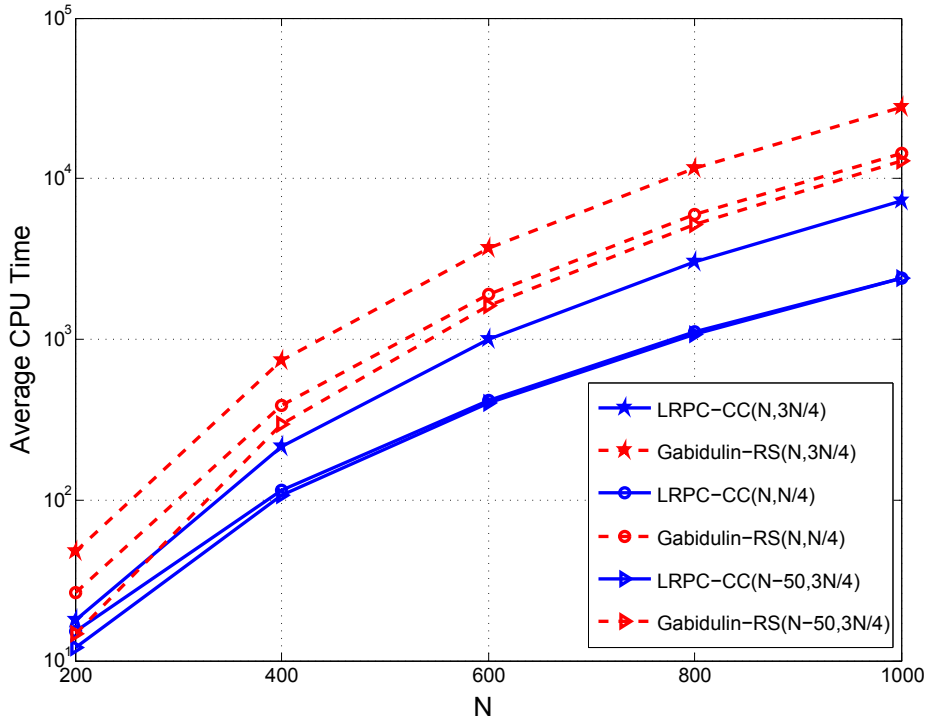


FIGURE 4.19 – Comparaison de la complexité entre un code LRPC concaténé avec un code convolutif et une concaténation d'un code Gabidulin avec un code Reed-Solomon pour différentes valeurs de m et k en fonction de N.

de symboles par message, la complexité globale de l'algorithme est $\mathcal{O}(m(Nk)^2)$ in $\mathbb{F}_q$, voir [19]. La complexité d'un décodeur basé sur l'algorithme de Vitterbi pour un code convolutif est $\mathcal{O}(N\sqrt{N})$ [20]. La complexité globale du code convolutif, utilisée pour mL fois, est $\mathcal{O}(mN\sqrt{N}L)$. Ainsi, l'algorithme proposé a une complexité $\mathcal{O}(m(N-k)^2 + mN\sqrt{N}L)$.

Pour les codes de Gabidulin, une modification significative a été faite pour réduire la complexité de la procédure de décodage. La complexité globale de l'algorithme, lorsque $N = m$, est approximativement $\mathcal{O}(Nm^2(log(m))$ sur $\mathbb{F}_q$, voir [21]. La complexité totale du code Gabidulin-RS est $\mathcal{O}(m^2N(log(m) + t))$ sur $\mathbb{F}_q$.

Nous présentons des résultats numériques pour les complexités du code LRPC concaténées avec un code convolutif et un code Gabidulin concaténés avec un code Reed-Solomon pour les mêmes paramètres (m, k), en fonction de N, tel que décrit dans la figure 4.19. Pour les paramètres de la simulation, prenons $L = 200$ et $d = 2$. Nous pouvons observer clairement le gain de performance des codes concaténés proposés en termes de complexité par rapport aux codes Gabidulin-RS.

4.9 Conclusion

Dans ce chapitre, le codage dans la couche physique est proposée qui vise à atténuer le bruit impulsif généré par les sous-stations électriques. Les performances du système lors de l'utilisation des codes Gabidulin (RC), les codes LRPC et les codes polaires, dans un schéma de modulation OFDM, ont été étudiées dans un scénario P2P. Les résultats montrent que la couche physique proposée permet d'éliminer efficacement tout bruit impulsif qui perturbe la transmission. En effet, lorsqu'un code à métrique de rang et un code convolutif sont concaténés en présence de bruit impulsif, le BER et le PER résultants sont significativement meilleurs que ceux obtenus lors de l'utilisation d'un code polaire. En outre, nous notons que les résultats obtenus pour un taux de données de 54 $Mbps$ sont meilleurs que ceux obtenus pour 100 $Mbps$, c'est-à-dire que nous n'utilisons pas complètement la diversité de fréquences du régime et cela peut constituer un nouveau domaine de recherche. Dans la deuxième partie de ce chapitre, nous avons étudié le problème de collecte de données dans les WSN et nous avons proposé un nouveau algorithme de collecte de données efficace basé sur la concaténation de deux techniques de codage. La méthode proposée tient compte non seulement des erreurs dues à la nature du canal sans fil, mais également des erreurs introduites par un utilisateur malveillant ou à cause d'échecs de nœud. En fait, nous avons utilisé les codes LRPC, testés dans un scénario P2P, comme code externe, et nous avons utilisé le code convolutif comme code interne pour faire face aux erreurs du canal sans fil. Nous avons dérivé l'expression exacte de la probabilité du décodage des codes Gabidulin et LRPC dans le cas du codage réseau aléatoire. Il vaut la peine de mentionner que les paquets codés à une métrique de rang ne sont décodés que dans le puits BS, dont la capacité de calcul est beaucoup plus élevée que les capteurs. Ainsi, l'algorithme proposé peut être directement implémenté dans un WSN réaliste. Les résultats des simulations prouvent que notre algorithme est supérieur à la méthode basée sur le codage de réseau proposée dans la littérature [12]. En conclusion, compte tenu des résultats de cette étude, la mise en place de codes à métriques de rang dans des capteurs réels dédiés aux applications Smart Grid est fortement encouragée afin d'optimiser la fiabilité globale de la communication système.

Bibliographie

[1] S. Zarifzadeh, N. Yazdani, and A. Nayyeri, "Energy-efficient topology control in wireless ad hoc networks with selfish nodes," Computer Networks, vol. 56, no. 2, pp. 902 – 914, 2012.

[2] R. Ahlswede, N. Cai, S. yen Robert Li, and R. W. Yeung, "Network information flow," IEEE TRANSACTIONS ON INFORMATION THEORY, vol. 46, no. 4, pp. 1204–1216, 2000.

[3] T. Ho, R. Koetter, M. Medard, D. R. Karger, and M. Effros, "The benefits of coding over routing in a randomized setting," 2003.

[4] M. Luby, "Digital fountain, inc. luby@ digitalfountain. com," 2002.

[5] C. Fragouli, J-Y. Le Boudec, et J. Widmer. Network coding : an instant primer. ACM SIGCOMM Computer Communication Review, vol. 36, no. 1, pp. 63-68, January 2006.

[6] A. Mahmino. Application du Codage Réseau aux Architectures à Garanties de Qualité de Service (QoS). Institut National Polytechnique de Toulouse. 2009.

[7] T. Ho, M. Médard, J. Shi, M. Effros, et D. R. Karger. On randomized network coding. In Proceedings of the 41st Allerton Conference on Communication, Control, and Computingin, October 2003.

[8] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, et B. Leong. Toward a random operation of networks. IEEE Transactions on Information Theory, vol. 2001, pp. 1-8, 2004.

[9] E. M. Gabidulin, "Theory of codes with maximum rank distance,"Problems on Information Transmission, vol. 21, pp. 1-12, Jan 1985.

[10] E. Arikan, "Channel polarization : A method for constructing capacity achieving codes", IEEE International Symposium On Information Theory, ISIT 2008.

[11] R. Koetter and F. R. Kschischang, "Coding for errors and erasures in random network coding," IEEE Transactions on Information Theory, vol. 54, no. 8, pp. 3579–3591, 2008.

[12] Yazbek, Abdul Karim, et al. "Low Rank Parity Check Codes Against Reed-Solomon Codes for Narrow-Band PLC Smart Grid Networks." Computer and Communication Engineering (ICCCE), 2016 International Conference on. IEEE, 2016.

[13] *http : //rapsor.sourceforge.net/index.php*

[14] C. Lièbe et al., "Ultra-Wideband Indoor Channel Modelling Using Ray-Tracing Software for through-the-Wall Imaging Radar," International Journal of Antennas and Propagation, vol. 2010, Article ID 934602, 14 pages, 2010.

[15] O. J. Oyedapo, "Optimization of transmissions in wireless sensor networks by closed-loop cooperative MIMO in perturbed environment", Thesis, University of Poitiers, 2014.

[16] K. Al-Mawali et al, "Joint Time-domain/Frequency-domain Impulsive Noise Redction in OFDM -based Power Line Communications", ATNAC 2008.

[17] *https* : *//en.wikipedia.org/wiki/Minimum_mean_square_error*

[18] P. Garrido, C. W. Sørensen, D. E. Lucani, and R. Agüero, "Performance and complexity of tunable sparse network coding with gradual growing tuning functions over wireless networks," in 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Sept 2016, pp. 1–6.

[19] P. Gaborit, G. Murat, O. Ruatta, and G. Zémor, "Low rank parity check codes and their application to cryptography," in Proc. WCC, 2013, pp. 168–180.

[20] S. Patel, "A lower-complexity viterbi algorithm," in Acoustics, Speech, and Signal Processing, 1995. ICASSP-95., 1995 International Conference on, vol. 1. IEEE, 1995, pp. 592–595.

[21] A. Wachter-Zeh, V. Afanassiev, and V. Sidorenko, "Fast decoding of gabidulin codes," Designs, Codes and Cryptography, vol. 66, no. 1, pp. 57–73, 2013.

Chapitre 5 :

Conclusion générale et perspectives

Nous avons proposé et implémenté un nouveau code correcteur d'erreur appelé LRPC pour les réseaux CPL-BE pour les réseaux intelligents (SG). Les performances du code proposé ont été comparée avec les normes existantes dans le CPL-G3. Plusieurs contraintes étaient un défi telles que la complexité des codes correcteurs d'erreur au niveau du décodage et le taux d'erreur bloc des transmissions. En outre, le codage réseau linéaire aléatoire a été mise en place en utilisant le code LRPC comme code externe entre la source et la destination finale et les codes convolutifs comme codes interne entre les nœuds intermédiaires.

5.1 Conclusion

Le concept de Smart Grid a tout d'abord été présenté, nous avons introduit ensuite les communications par CPL-BE qui répondent aux besoins de liens de communication pour le domaine d'accès SG. En revanche, les canaux de communication sur les réseaux CPL-BE présentent différents types de bruit qui dégradent les performances du réseau, d'où l'intérêt d'utiliser les codes correcteurs d'erreurs afin de fiabiliser la communication au niveau du réseau SG. La première partie de cette thèse est consacrée à l'étude des caractéristiques du réseau CPL-BE, ainsi les différents types de bruit dans ce réseau. Pour cela, un état de l'art qui permet des mettre en place les codes correcteurs d'erreurs pour faire face aux perturbations dans un canal CPL-BE tels que les codes Reed-Solomon qui sont adaptés pour la norme G3-CPL existante, les codes Gabidulin, les codes convolutifs et les codes LDPC. Ensuite, nous avons proposé le code à métrique de rang (LRPC) concaténé avec les codes convolutifs dans un réseau CPL-BE, où les transmissions sont perturbées par des bruits impulsifs, par des interférences à bande étroite, dont les motifs sont de type criss-cross, et des erreurs isolés. Les codes à métrique de rang sont particulièrement adaptés pour lutter contre les erreurs criss-cross. Ainsi que les codes convolutifs sont utilisés pour corriger les erreurs isolés. Ce schéma de transmission a été simulé sur Matlab et comparé avec les codes Reed-Solomon concaténés avec les codes convolutifs selon la norme existante G3-CPL. Les résultats ont montré que les performances de notre schéma proposé sont plus performantes que les normes déjà existantes sans autant d'être plus complexes.

Dans la deuxième partie, un travail en collaboration avec Xlim-poitier a été réalisé. Des bruits impulsifs qui sont mesurés dans un environnement réaliste dans une station haute tension à Canada ont été utilisé pour tester le code LRPC proposé. Les performances du système lors de l'utilisation des codes Gabidulin (RC), les codes LRPC et les codes polaires, dans un schéma de modulation OFDM, ont été étudiées dans un scénario P2P multi-trajets. En plus, des coefficients des canaux sélectifs en fréquence ont été calculés pour deux débits différents 54 $Mbps$ et 100 $Mbps$. En effet, lorsqu'un code à métrique de rang et un code convolutif sont concaténés en présence de bruit impulsif, le BER et le

PER résultants sont significativement meilleurs que ceux obtenus lors de l'utilisation d'un code polaire. En outre, nous notons que les résultats obtenus pour un taux de données de 54 $Mbps$ sont meilleurs que ceux obtenus pour 100 $Mbps$, c'est-à-dire que nous n'utilisons pas complètement la diversité de fréquences du régime et cela peut constituer un nouveau domaine de recherche. Dans la suite de la thèse, le concept de codage réseau a été étudié dans le contexte des réseaux de capteurs sans fils. Le principe du modèle proposé est de faire un codage LRPC à la source et puis transmettre les données dans un champ de captage tels que les nœuds intermédiaires sont placés aléatoirement. Il s'agit aussi de faire un codage-décodage convolutif entre tous les nœuds jusqu'à la destination finale. Enfin, les données subissent un décodage LRPC à la destination finale. Ce schéma présenté est simulé sur Matlab et les résultats montrent des bonnes performances du code LRPC concaténé avec les codes convolutifs cette fois-ci dans un contexte de codage réseau linéaire aléatoire. Pour bien valider notre travail, nous avons comparé ces performances avec les codes Gabidulin et les codes Ree-Solomon, les codes Gabidulins concaténés avec les codes convolutifs et les codes convolutifs.

Pour conclure, nous avons proposé des algorithmes qui permettent de lutter contre les bruits de type criss-cross dans des différents contextes et qui ont de bonnes performances malgré une faible complexité.

5.2 Perspectives

Je conclus ce travail de recherche par une discussion sur les directions de recherche possibles pour l'amélioration de la fiabilité du code LRPC proposé. Tout d'abord, une implémentation des algorithmes développés sur la cible matérielle la plus efficace parmi les processeurs classiques, reconfigurables ou circuits dédiés peut former une perspective intéressante de ce travail. Ensuite, l'amélioration de la construction de la matrice génératrice du code LRPC afin d'éviter le problème de décodage probabiliste pour le rendre plus fiable dans les réseaux CPL-BE et les réseaux de capteurs sans fils. La réduction de la complexité de décodage peut être aussi une piste futur de recherche. En outre, la modulation OFDM peut être remplacer par une nouvelle technique de modulation O-QAM [1] qui est une modulation basée sur le principe de l'OFDM mais qui permet d'utiliser des formes d'ondes bien localisées en temps et en fréquence. De plus, cette modulation est construite de telle sorte à conserver la même efficacité spectrale que l'OFDM sans intervalle de garde afin de de mieux interfacer avec les codes à métrique de rang.

Bibliographie

[1] Skrzypczak, A., Javaudin, J. P., & Siohan, P. (2006, September). Overlapped selective mapping for pulse-shaped multi-carrier modulations. In Vehicular Technology Conference, 2006. VTC-2006 Fall. 2006 IEEE 64th (pp. 1-5). IEEE.

Liste des publications

Publications internationales dans des revues à comité de lecture :

1. Performance of rank metric codes for interference constrained wireless sensor networks soumis à IET Wireless Sensor Systems Journal.
2. Yazbek, AK, El-qachchach, I, Cances, J-P, Meghdadi, V. Low rank parity check codes and their application in PLC Smart grid networks. Int J Commun Syst. 2017 ; e3256.doi :10.1002/dac.3256.

Conférences internationales avec actes et comité de lecture :

1. New Concatenated Code Schemes for Data Gathering in WSN's using Rank Metric Codes soumises à WCNC 2018.
2. Ndéye Bineta Sarr, Abdul Karim Yazbek, Herve Boeglen, J.P. Cances, Rodolphe Vauzelle, François Gagnon, " An Impulsive Noise Resistant Physical Layer for Smart Grid Communications." Communications, 2017. ICC'17. IEEE International Conference on. IEEE, 2017.
3. Yazbek, Abdul Karim, Jean-Pierre Cances, and Vahid Meghdadi. "Narrowband interference mitigation with LRPC code and OFDM for smart grid applications." Signal Processing and Communication Systems (ICSPCS), 2016 10th International Conference on. IEEE, 2016.
4. ABDUL KARIM, Yazbek, IMAD, El-Qachchach, JEAN-PIERRE, Cances, et al. Low Rank Parity Check Codes Against Reed-Solomon Codes for Narrow-Band PLC Smart Grid Networks. In : Computer and Communication Engineering (ICCCE), 2016 International Conference on. IEEE, 2016. p. 470-474.

Les codes à métrique de rang et leurs applications dans les réseaux Smart Grid

Résumé : Cette thèse a pour cadre les transmissions sur les réseaux CPL-BE et les réseaux de capteurs à faible capacité. L'état de l'art classique sur la protection de l'information dans la transmission par réseaux de capteurs fait référence à l'utilisation de codage distribué où les relais implémentent des opérations de parité (mélange des flux) sur les data issues des capteurs. Cependant, il est difficile, de par la nature variable de la qualité des liens en liaisons sans fil, de contrôler la qualité du codeur équivalent construit et de maintenir ses performances au cours du temps. C'est pourquoi nous nous sommes orientés dans cette thèse vers la recherche de schémas de codage différents qui résistent mieux à la variation de qualité des liaisons à travers le réseau. Notre choix s'est porté sur le codage par sous-espace inspiré des travaux de Gabidulin. Le but est de former un code qui utilise une métrique simple et résistante pour sécuriser les transmissions sur le réseau. Les codes à métrique de rang répondent bien à ce besoin car il n'y a qu'à contrôler le rang de la matrice obtenue en réception pour vérifier l'intégrité de la transmission. Les codes à métrique de rang et leur algorithme de décodage ont été étudiés dans un premier temps. Puis, les performances du code LRPC proposé concaténé avec les codes convolutifs sont testées dans des schémas de transmission des contextes différents.

Mots clés : Réseaux intelligents, Bruit impulsif, Interférence à bande étroite, Codes à métrique de rang, Code LRPC, Modulation OFDM.

Rank metric codes and their applications in Smart Grid networks

Abstract : This thesis considers the context of transmissions on CPL-BE networks and low-capacity sensor networks. The state of the art on information protection intransmission by sensor networks refers to the use of distributed coding, where therelays implement parity operations (mixing of streams) on data transmitted by thesensors. However, due to the varying nature of the quality of the wireless links, it is difficult to control the quality of the equivalent encoder constructed and to maintain its performance over time. Therefore, in this thesis, we have focused on the search for different coding schemes that are better resist the variation in the quality of the links across the network. Our choice was based on the sub-space coding inspired by Gabidulin's work. The goal is to form a code that uses a simple and resistant metric to secure transmission across the network. Rank metric codes respond well to this need because it only has to control the rank of the matrix obtained in reception to verify the integrity of the transmission. The rank metric codes and their decoding algorithm were studied in a first step. Then, the performance of the proposed LRPC code concatenated with the convolutional codes is tested in transmission schemes of different contexts.

Keywords : Smart Grid, Impulsive noise, Narrowband interference, Rank metric codes, Low Parity Check Code, OFDM.

XLIM - UMR CNRS n° 521
16, Rue Atlantis - 87280 Limoges-France