Erasure Correcting Codes for Opportunistic Spectrum Access (OSA).

Muhammad Moazam Azeem

CONSERVATOIRE NATIONAL DES ARTS ET MÉTIERS

le cnam

Ecole Doctorale EDITE:
Informatique, Télécommunication et Électronique de Paris

THÈSE DE DOCTORAT

Présentée par : **Muhammad Moazam Azeem**

Soutenue le : **01 Juillet 2014**
Pour obtenir le grade de : **Docteur du Conservatoire National des Arts et Métiers**

Discipline : **Radiocommunications**

Spécialité : **Télécommunications**

Codes à effacements pour l'accés opportuniste au spectre (OSA)

RAPPORTEURS

Jean-Pierre Cances, Professeur	ENSIL, Limoges, France
Jérôme Lacan, Professeur	ISAE, Toulouse, France

EXAMINATEURS

David Declercq, Professeur	ENSEA Cergy Pontoise, France
Jean-François Helard, Professeur	INSA, Rennes, France
Iness Ahriz, Maître de Conférences	CNAM, Paris, France

Membre invité

Patrick Tortelier	Orange Labs, Paris, France

Directeurs

Didier Le Ruyet, Professeur	CNAM, Paris, France

CONSERVATOIRE NATIONAL DES ARTS ET MÉTIERS	le cnam

Doctoral School EDITE:
Informatics, Telecommunications and Electronics (Paris)

PhD THESIS

Presented by : **Muhammad Moazam Azeem**

Defended on : **01 July 2014**

To obtain the Degree of : **Doctor of Philosophy (PhD) of Conservatoire National des Arts et Métiers**

Discipline : **Radiocommunications**

Specialization : **Telecommunications**

Erasure Correcting Codes for Opportunistic Spectrum Access (OSA)

Reviewers

Jean-Pierre Cances, Professor	ENSIL, Limoges, France
Jérôme Lacan, Professor	ISAE, Toulouse, France

Examiners

David Declercq, Professor	ENSEA Cergy Pontoise, France
Jean-François Helard, Professor	INSA, Rennes, France
Iness Ahriz, Assistant Professor	CNAM, Paris, France

Invited member

Patrick Tortelier	Orange Labs, Paris, France

Thesis supervisor

Didier Le Ruyet, Professor	CNAM, Paris, France

Dedication

To my Father Muhammad Azeem, Mother
and
all Teachers

Acknowledgements

The research work presented in this report was carried out at Orange Labs, France-Telecom, Paris in collaboration with CNAM, Paris. Working at Orange Labs was an excellent opportunity as it is an organization with excellent and encouraging R&D environment and with valuable innovative ideas. I am really thankful to all persons who have helped me in the completion of my thesis.

First of all, I would like to thank Patrick Tortelier, Project Manager at Orange Labs, and Didier Le Ruyet, Professor at CNAM, for supervising my thesis. I explored a lot of new ideas during this period and learned a lot of new techniques, my supervisors always guided me to the right scientific approach and they encouraged me whenever I had new ideas during this research period.

I would like to thank Jean-Philippe Desbat, the team manager, who supported in all administrative tasks and Laurent Labeguerie who prepared the administrative letters at the right time. I would like to thank all jury members who examined my thesis.

I would like to thank my all family members, specially to my brother Muhammad Faysal Azeem, for their continuous encouragement and support. Last but not the least, I cannot forget the moral support of my parents at different stages and their endless love that helped a lot to achieve my goals.

Résumé

Les années récentes ont vu l'explosion du trafic sur les réseaux mobiles depuis l'apparition de nouveaux terminaux (smartphones, tablettes) et des usages qu'ils permettent, en particulier les données multimédia, le trafic voix restant sensiblement constant. Une conséquence est le besoin de plus de spectre, ou la necessité de mieux utiliser le spectre déjà alloué. Cela passe en particulier par de nouvelles méthodes pour gérer la manière dont plusieurs utilisateurs se partagent une même ressource spectrale.

Parmi les nouveaux schémas d'accès dynamique au spectre qui ont été conçus pour une meilleure utilisation du spectre, nous considérerons les schémas dits opportunistes (opportunistic spectrum access, OSA, en anglais) dans lesquels un ou plusieurs utilisateurs dits secondaires (SU) peuvent utiliser la ressource spectre pendant les périodes d'inactivité de l'utilisateur légitime, dit utilisateur primaire (PU).

Comme il n'y a pas de coordination entre les utilisateurs secondaire(s) et primaire, avant toute transmission les premiers doivent mettre en oeuvre des traitements pour détecter les périodes dans lesquelles l'utilisateur primaire transmet, ce qui est le scénario considéré dans cette thèse.[1]

Cette opération de détection doit être effectuée le plus rapidement possible pour ne rater aucune des possibilités qui se présentent, ce qui est incompatible avec une détection infaillible. En conséquence l'utilisateur secondaire est confronté à deux types d'erreurs dans ce processus de détection :

- Une *fausse alarme* lorsque un utilisateur primaire est détecté alors que personne ne transmet en réalité. Il y a alors une occasion manqué d'utiliser le canal.

- Une *non détection* de l'utilisateur primaire en train de transmettre. Il y a alors une collision entre les paquets transmis, avec perte des données correspondantes ; on parle d'effacements.

Le canal vu par l'utilisateur secondaire est un canal à effacement en mode paquet. La solution consistant à retransmettre les paquets perdus ne ferait qu'empirer les choses : il faudrait en effet un acquittement pour chaque paquet transmis, et une retransmission de ceux qui n'ont pas été reçus, c'est-à-dire de nouvelles tentatives d'accès secondaire au spectre.

Nous considérons donc une autre approche, reposant sur l'utilisation de codes correcteurs d'effacements en mode paquet. Il s'agit d'une technique bien connue dans le cas de la diffusion d'un même contenu à un grand nombre de destinataires (multicast, ou broadcast), par exemple pour le MBMS. Mais ces solutions reposent en général sur des codes longs, sans rendement prédéfini (rateless codes), tels les codes LT, ou les codes Raptor.

[1] Il est tout a fait possible d'envisager une collaboration entre utilisateurs primaire et secondaire, sous la forme de licence dite secondaire, l'utilisateur primaire avertissant l'utilisateur secondaire des périodes disponibles. Dans ce cas il n'est plus besoin de détection, mais nous ne considérons pas ce schéma dans notre travail

Afin de minimiser la latence et la complexité des codage et décodage nous abordons dans cette thèse l'utilisation de codes cours connus (BCH, Golay, ...) ou de combinaisons de codes courts (codes produits). Nous introduisons une métrique pour mesurer l'efficacité des codes en question du point de vue d'une utilisation secondaire du spectre et nous montrons qu'il est possible de l'optimiser en cherchant un bon compromis *fausse-alarme/non-détection* pour l'opération de détection.

La dernière partie de la thèse aborde un scénario dans lequel il n'y a plus d'utilisateur primaire, tous les utilisateurs ayant le même droit à transmettre dans le canal. Il peut s'agir par exemple de réutilisation spatiale du spectre de TV numérique (les TV white spaces) ou, plus intéressant, de stations WiFi connectées à un même point d'accès. Dans ce dernier cas on sait qu'il existe un protocole qui a pour but d'éviter les collisions entre les différents terminaux (CSMA/CA). Nous décrivons une modification de la couche MAC du 802.11 consistant à réduire les différents temps consacrés à attendre (SIFS, DIFS, backoff, ...) afin d' accèder plus souvent au canal, au prix de quelques collisions supplémentaires qu'il est possible de récupérer en mettant en œuvre des codes correcteurs d'effacements.

Les simulations effectuées montrent que cette technique permet d'améliorer les débits agrégés de tous les utilisateurs avec une garantie sur la qualité de réception.

Mots-clés : La radio cognitive, Opportuniste du spectre accès, Canal à effacement binaire, Codes correcteurs d'effacements, Graphe de Tanner, Les codes de produit, L'efficacitè spectrale, Processus de dètection, CSMA/CA, Protocoles MAC.

Abstract

There is a need of either more spectrum or to use existing spectrum more efficiently due to dramatic increase in the demand of limited spectrum. The emergence of new devices especially the smartphones and tablets having a lot of new applications have rocketed the wireless traffic in recent years and this is the cause of main surge in the demand of radio spectrum. Among the new dynamic access schemes designed to use the spectrum more efficiently opportunistic spectrum access (OSA) is currently addressed when one or more secondary users (SU) are allowed to access the channel when the PU is not transmitting. There is no coordination between PU and SU when dealing with OSA and SU needs sensing to detect PU's idle periods in the channel before starting the transmission, this is one of the main challenges that is addressed in this thesis. The sensing operation must be performed as quickly as possible in order to seize maximum opportunities as they appear but it suffers from two kinds of impairments: False alarms when there is no PU while the detection stage decides there is one; as a consequence the SU experiences a missed opportunity to use the channel. Conversely, it may happen that there is actually a PU but it is not detected by the SU. The result is a collision between PU and SU and a loss of data of both users. Due to the possible loss of packets during collisions the SU's link can be modelled as an erasure channel. If retransmission of data is done the channel would even worsen the problem (the SU would have to find another opportunity to send a retransmission request).

The erasure correcting codes are therefore envisioned to recover the lost data and we address the short erasure correcting codes for the recovery of erased data in opportunistic spectrum access (OSA). The main advantage of using short codes is their low decoding complexity. There is a need to define a parameter to estimate the secondary spectrum access. we define this parameter as efficiency of SU and optimize it in-terms of spectrum utilization keeping into account sensing impairments, code parameters and the activity of PU. Various decoding methods are compared and Tanner graph based approach is selected due to lower decoding complexity. The performance enhancement of short codes for better erasure recovery is also addressed and the concatenation of short codes is described to build more powerful product codes in case the collision rate is high.

Finally, the spectrum access for multiple secondary users is addressed when there is no primary and each user has equal right to access the channel. The interesting scenarios are Cognitive radio networks and WiFi where 802.11 protocol gives the specification for MAC layer. With the increasing number of users in the network waiting time is increased and in order to avoid the long delays to access the channel the parameters of MAC protocol can be modified. When the waiting time is reduced the collisions among multiple users are increased and there is a need to envision erasure correcting codes to recover the lost data due to collisions. The analytical approximation for global collision rate is provided and it is compared with the simulation results, the effect of codes at various collision rates is analysed for multiple users. The expression for global throughput for multiple users is estimated and simulation curves are plotted by modifying the parameters of 802.11. The

throughput curves achieved by retransmission and using various erasure correcting codes are compared. This modification in MAC layer will reduce the long waiting time to access the channel, as the number of users are increased, using erasure correcting codes at the expense of redundancy.

Keywords: Opportunistic Spectrum Access, Cognitive Radio, Binary Erasure Channel, Erasure Correcting Codes, Tanner graph, Product Codes, Spectral Efficiency, Spectrum Sensing, CSMA/CA, MAC Protocols.

Acronyms

OSA	Opportunistic Spectrum Access
DSA	Dynamic Spectrum Access
CR	Cognitive Radio
SDR	Software Defined Radio
$CTMC$	Continuous-Time Markov Chain
$POMDP$	Partially Observable Markov Decision Process
FCC	Federal Communications Commission
$SPTF$	Spectrum Policy Task Force
UWB	Ultra Wide Band
DFH	Dynamic frequency hopping
PU	Primary User
SU	Secondary User
pdf	probability distribution function
BEC	Binary Erasure Channel
ROC	Receiver Operating Characteristic
P_{FA}	False Alarms Probability
P_{ND}	Non detection Probability
N	Number of samples
T	Sensing Time
P_D	Detection Probability
$AWGN$	Additive White Gaussian Noise
C	Channel Capacity
BSC	Binary Symmetric Channel
GF	Galois Field
n	Length of the code
k	Dimension of the code
R	Rate of the code
d	minimum distance of the code
FEC	Forward Error Correction
SPC	single parity check
$SPCPC$	single parity check product
MDS	Maximum Distance Separable
WER	Word Erasure Rate
BER	Bit Erasure Rate

p	Input Erasure probability
p_r	Residual Probability
p_f	Failure Probability
PER	Packet Erasure Probability
BM	Branch Metric
PM	Path Metric
η_c	Efficiency
η_u	Efficiency without Coding
η_{max}	Maximum Achievable Efficiency
$CSMA/CD$	Carrier Sense Multiple Access with Collision Detection
$CSMA/CA$	Carrier Sense Multiple Access with Collision Avoidance
$DIFS$	Distributed inter-frame space
$SIFS$	Short inter-frame space
BO	Backoff
U	Successful Transmission Time
B	Busy Period
I	Idle Period
S	Throughput
λ	Arrival Rate
μ	Mean arrival rate

Table of contents

List of Figures

List of Tables

Chapter A

Résumé des travaux de thèse

Contents

A.1 Introduction

A.1.1 Définition du problème

Il y a une augmentation significative des besoins de bande de fréquence en raison de l'émergence des smartphones et tablettes au cours de ces derniéres années. Les bandes de fréquences sont toutes attribuées et il y a un risque élevé de pénurie. Il y a donc nécessaire d'utiliser le spectre de manière plus efficace. Dans cette thèse, nous traitons du système

d'accés dynamique et opportuniste au spectre (OSA) qui décrit l'accès primaire/secondaire au spectre. L'utilisateur principal (PU) est l'utilisateur autorisé pendant que l'utilisateur secondaire (SU) peut avoir accès à la spectre lorsque l'utilisateur primaire (PU) ne transmet pas. La partie non utilisée du spectre appartenant à l'utilisateur primaire (PU) peut être utilisé par un utilisateur secondaire (SU) avec le schéma de l'OSA. Cet accés à la SU est possible par l'utilisation de la radio cognitive qui a été introduite par Mitola dans sa thèse [1]. L'objectif principal de la radio cognitive est de permettre la meilleure utilisation du spectre en exploitant les trous laissés par l'utilisateur primaire. En outre, il n'existe pas de coordination entre l'utilisateur primaire et secondaire dans le schéma de l'OSA. L'utilisateur secondaire qui accède au canal opportuniste doit écouter d'abord le canal afin d'éviter toute interférence avec le PU. Cependant, la détection n'est pas parfaite et il a deux types de défauts qui sont les fausses alarmes et non détection. Les fausses alarmes se produisent quand un utilisateur principal est détecté, c'est à dire que l'étape de détection détecte le PU dans le canal alors que le canal est libre. Les non détections se produisent lorsque l'utilisateur principal n'est pas détecté alors que le canal est occupé. Les conséquences des fausses alarmes sont des occasions manquées sur le canal et les non détections entrainent une collision avec l'utilisateur primaire. Lors de la collision, les données envoyées par l'utilisateur primaire sont perdues et déclarées effacées. Afin de récupérer les effacements, certaines techniques doivent être utilisées afin de garantir la meilleure qualité de service (QoS) pour l'accés primaire/secondaire. La solution possible est d'avoir un canal de retour et retransmettre les données perdues sur demande, mais cela peut conduire à des retards et des ressources supplémentaires. Une autre solution qui sera considérée dans cette thèse est l'utilisation de l'effacements (FEC) des codes d'exploitation du côté récepteur pour récupérer les données perdues. La récupération des données perdues en raison de collisions entre plusieurs utilisateurs est un défi majeur que nous allons aborder dans la thèse.

A.1.2 Contribution de la thèse

Nous avons proposé l'utilisation de codes de correction d'effacements afin de mitiger les fausse alarmes et l'impact des non-détections dans les systèmes d'accès opportunistes au spectre. Les pertes de données en cas de collision peuvent être vues comme des effacements et récupéré l'aide de codes de correction d'effacements.

Décodage et analyse de la performance des codes à effacements:

Nous avons utilisé le codage de canal en ajoutant de la redondance aux paquets d'information

pour permettre la correction des l'effacements. Les codes correcteurs d'effacement sont envisagés à la couche d'application. Nous nous concentrons sur ces codes de raison de la faible complexité de décodage et nous utilisons le décodage à base de graphe de Tanner pour les codes de effacements courts. La performance des codes courts est encore améliorée par le choix d'une matrice de contrôle appropriée pour laquelle des équations de parité supplémentaires sont ajoutés pour obtenir étendu matrice de contrôle de parité H_e.

Le décodage à base de graphe de Tanner normal et étendu est comparé à la méthode de recherche exhaustive pour divers codes courts. La différence de performance des deux techniques est ensuite analysée et nous avons justifié l'apport du décodage à base de graphe de Tanner vis à vis de la recherche exhaustive. La correction d'effacements en utilisant le graphe de Tanner au niveau du paquet est moins complexe que le décodage de Viterbi. Les limites analytiques pour les codes SPCPC sont calculées et ces résultats d'analyse sont comparés avec les résultats des simulations pour diverses probabilités d'entrée d'effacements. Le décodage de Viterbi modifié qui fonctionne sur des effacements est décrit pour les trois techniques de décodage: le décodage à base de graphe de Tanner, la recherche exhaustive et décodage de Viterbi.

Analyse de la performance de l'accès au spectre secondaire de l'OSA:
Une contribution importante est de trouver le point de fonctionnement optimal sur la courbe ROC afin d'améliorer l'efficacité de l'accès au spectre secondaire. L'expression de l'efficacité est calculée et les paramètres les plus importants sont définis. Les effets des paramètres de détection et de l'activité du PU sur l'efficacité sont analysés et les effets de l'utilisation de divers codes correcteurs d'effacement sont analysés. Un grand nombre de simulations sont effectuées pour atteindre différents niveaux d'efficacité en utilisant différents codes avec différents taux, distance minimale et longueur. Les codes des produits sont construits par concaténation et les courbes d'efficacité sont tracées à l'aide de divers codes de produit. Nous avons comparé l'efficacité maximale obtenue pour différents codes courts en fonction de la probabilité de détection et de l'activité du PU et avons d'optimisé l'efficacité de l'accès au spectre secondaire. Nous avons conclu qu'il existe un compromis entre l'efficacité maximale, les propriétés de ce code (taux, distance minimale, etc) et les probabilités de détection.

Analyse du débit des utilisateurs secondaires multiples en accés multiple:
La dernière partie de la thèse porte sur l'accès secondaire multiple. Nous avons abordé l'application des réseaux de radio cognitive où plusieurs utilisateurs accèdent au canal de

télévision espaces blancs (scénario intéressant est WiFi 802.11af) et WiFi fonctionnant à 2,4 et 5 bandes de fréquences GHz. Nous avons décrit les protocoles MAC pour les réseaux CR pour les protocoles aléatoires, puis nous avons adapté les paramètres de protocole MAC en réduisant le temps d'attente pour accéder au canal. En réduisant la valeur du backoff, les collisions entre plusieurs utilisateurs augmentent et nous envisageons les systèmes de correction d'effacements pour corriger les données effacées. Nous avons calculé analytiquement la probabilité de collision entre plusieurs utilisateurs secondaires et comparé avec les résultats de la simulation. Nous avons tracé le taux de collision d'entrée et la probabilité de défaillance de divers codes en modifiant les paramètres de protocole MAC.

Lorsque le nombre d'utilisateurs augmente, nous devons aussi augmenter la valeur de backoff pour réduire le taux de collision avec l'objectif de maximiser le débit global. Nous avons donné l'expression mathématique permettant d'estimer le débit global pour plusieurs utilisateurs secondaires et tracer les résultats de la simulation à l'aide de divers codes correcteurs d'effacements. Les codes courts donnent de meilleures performances lorsque le taux de collision est faible, mais lorsque les taux de collision augmentent alors les codes plus puissants deviennent plus efficaces. Nous avons aussi proposé une approche pour déterminer le point optimal pour un débit global. Nous constatons que le débit optimal est fonction des paramètres de protocole MAC, les paramètres du code dont la longueur, la taux et la distance minimale et le nombre d'utilisateurs dans le réseau.

A.2 Décodage des codes correcteurs d'effacement

A.2.1 Canal d'effacements binaire (BEC) et codes.

Dans cette section, nous montrons que des codes courts binaires peuvent être envisagées pour la récupération d'effacements. En fait, tout code classique (codes BCH ou Golay, pour n'en nommer que quelques-uns) peut être utilisé, pour les raisons suivantes:

A.2.2 Décodage basé sur le graphe de Tanner

Par exemple fig. A.1 représente le graphe de Tanner associé à la matrice de contrôle de parité de la (7,4) Code de Hamming suivante:

$$\mathbf{H} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \tag{A.1}$$

La première équation du graphe de Tanner correspond à la première ligne de contrôle de

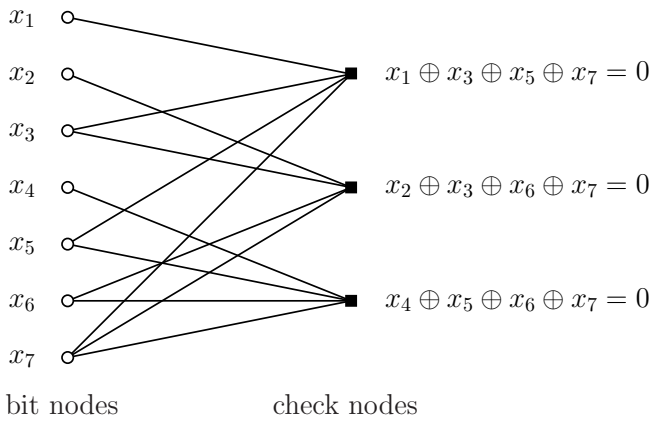

Figure A.1: Tanner graphique de Hamming (7,4) Code

la matrice de parité **H**, la deuxième équation correspond à la deuxième ligne de **H** matrice et dernière équation correspond à la troisième ligne de de la matrice **H**. L'algorithme de

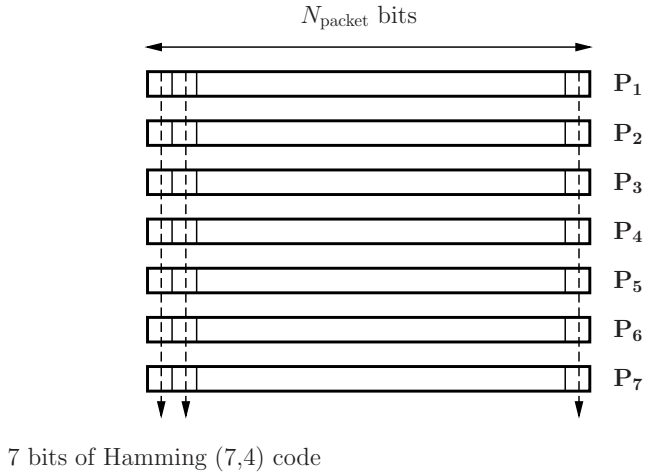

Figure A.2: Passage des bits aux paquets

décodage à base de graphe de Tanner peut être appliquée lorsqu'il s'agit de paquets plutôt que de bits, à la différence que de contrôle de parité équations impliquent désormais une opération de ou exlusif sur les paquets; par exemple, la première équation de contrôle de parité devient $\mathbf{P_1} \oplus \mathbf{P_3} \oplus \mathbf{P_5} \oplus \mathbf{P_7} = \mathbf{0}$ où $\mathbf{P_1} \ldots \mathbf{P_7}$ sont tels que l'ensemble de $i = 1 \ldots N$ bits de chaque paquet est un mot de code du code de Hamming comme décrit dans la figure A.2.

A.2.3 Comparaison de graphe de Tanner à la recherche exhaustive pour le code Golay (24,12,8)

Nous passons maintenant à un bien meilleur code qui est le code de Golay (24,12,8). Nous obtenons le polynôme énumérateur $T(x)$ ci-dessous.

$$T(x) = 110x^4 + 2277x^5 + 19723x^6 + 100397x^7 + 343035x^8 + \dots \tag{A.2}$$

Plusieurs modèles de 4,5,6 et 7 effacements ne sont pas entièrement récupérés, bien que nous ayons pris $d = 8$. Si nous utilisons la matrice de contrôle étendue $\mathbf{H}_e$, la performance du code augmente. Utilisation de la matrice de parité étendue de l'article mentionné ci-dessus, $\mathbf{H}_e$ avec 34 lignes au lieu de 12, l'énumérateur à deux variables devient:

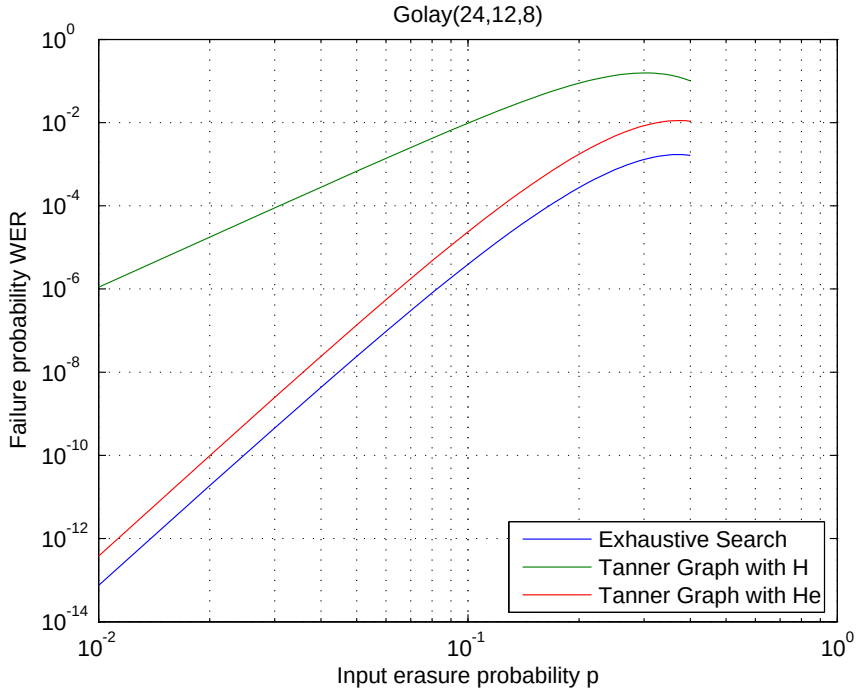

Figure A.3: Comparaison des performances de la recherche exhaustive et du décodage sur graphe de Tanner pour le code de Golay (24,12,8).

$$T_{ext}(x) = 3598z^8x^8 + 82138x^9 + \dots \tag{A.3}$$

Nous voyons que tous les modèles d'effacements de poids de 1 à 7 sont récupérés et que la distance minimale d-1 est égale à 7. Il y a 759 modèles d'effacements de poids 8, 12144

modèles d'effacements de poids 9, etc ... qui ne sont pas récupérés ce qui correspond à la capacité maximale de correction d'effacement.

$$T_{exh}(x) = 759x^8 + 12144x^9 + 91080x^{10} + 425040x^{11} + \dots$$

La comparaison du décodage basé sur le graphe de Tanner et sur la recherche exhaustive pour le code de Golay(24,12,8) avec matrice de parité normale et étendue est donné dans la figure figure3.11. On constate qu'il y a beaucoup de différence dans les performances selon les matrices **H**.

A.3 Application des codes correcteurs d'effacement court pour OSA

A.3.1 Les paramètres d'efficacité

Nous devons définir un critère pour comparer les performances de correction d'effacements des différents codes courts (Golay, Hamming, BCH, ...) et des longs codes comme les codes LDPC par exemple. Le principal paramètre est le taux (nombre de paquets d'informations transmis) du SU, mais d'autres paramètres sont également importants. L'efficacité dépend de l'activité du PU P_{on}. Une forte valeur de P_{on} implique que la probabilité d'accés au secondaire sera limitée. Il dépend également de la probabilité de fausse alarme P_{FA} et de la probabilité de détection P_{ND}. Nous avons introduit une référence qui correspond à un détecteur idéal ($P_{FA} = 0$ et $P_{ND} = 0$). Dans ce cas, le SU serait en mesure d'avoir la possibilité d'utiliser toutes les périodes d'inactivité du PU; dans un certain nombre $t \gg 1$ de créneaux temporels consécutifs, une moyenne $t \times P_{off}$ sont libres et le nombre moyen de paquets d'informations correctement transmises par le SU est donné par:

$$N_p(ideal) = t \times P_{off} \tag{A.4}$$

C'est le meilleur scénario qui puisse être atteint par un SU avec un détecteur idéal, car il n'y a pas de paquets de redondance (il n'y a pas de collision) et toutes les opportunités sont utilisées pour transmettre les paquets de données du SU. Alors que dans le scénario réel, nous devons prendre en compte la détection troubles, le nombre moyen de paquets transmis par le SU sur $t \gg 1$ créneaux horaires alors égal à $N_p(real)$, qui est donné par:

$$N_p(real) = t \times \Big(P_{on}\, P_{ND} + P_{off}\ (1 - P_{FA}) \Big) \tag{A.5}$$

Nous avons la probabilité de collision p conditionnellement à la transmission de la transmission du SU:

$$p = \frac{P_{on}\, P_{ND}}{P_{on}\, P_{ND} + P_{off}\ (1 - P_{FA})} \tag{A.6}$$

Le nombre moyen de mots de code transmis par le SU est alors égal à $N_p(real)/n$ et $(1 - p_f)$ est la fraction des mots de code qui sont entièrement récupérés après décodage. Enfin, nous devons prendre en compte le taux de code, cela signifie que nous ne disposons que de k paquets d'information pour n paquets transmis. Le nombre moyen de paquets d'informations reçus plus de $t \gg 1$ devient:

$$N_p(info) = k \times \frac{N_p(real)}{n} \times (1 - p_f)$$

L'efficacité $\eta_c = N_p(info)/N_p(ideal)$ est donnée par:

$$\eta_c = \frac{1}{P_{off}}\, \frac{k}{n} \left(P_{on}\, P_{ND} + P_{off} \times (1 - P_{FA}) \right) (1 - p_f) \tag{A.7}$$

L'évolution de lefficacité η_c pour différents codes ayant des taux différents est cohérente puisque les codes sont comparés pour la même valeur de P_{on} et η_c directement proportionnel au débit.

A.3.2 Influence du taux et de la distance minimale du code

Nous abordons maintenant l'influence du code utilisé sur la récupération des effacements. Nous observons deux comportements différents selon que l'activité de PU est élevé ou non. Lorsque le PU est souvent actif, par exemple pour $P_{on} = 0.7$, nous observons deux phénomènes intéressants. Tout d'abord, il n'y a pas un grand écart d'efficacité entre le code de Golay (24,12) utilisant la matrice de contrôle normale et un code de Hamming (15,11).

Les deux codes ont une efficacité proche de 25 % en dépit de leurs différentes capacités de correction d'effacements (distance minimale $d = 8$ pour le code de Golay et $d = 3$ pour le code de Hamming). Le facteur limitant est le rendement du code et l'utilisation de contrô le de parité matrice ordinaire du code de Golay laisse plusieurs d'effacements de taille inférieure à $d - 1 = 7$ non récupérées [2, 3]. Les résultats sont différents en utilisant la matrice de contrôle étendue H_e donnée dans [2, 3], l'efficacité augmente à plus de 40% parce que nous pouvons maintenant récupérer tous les modes d'effacements de taille jusqu'à $d - 1$, comme le montre la fig. A.4.

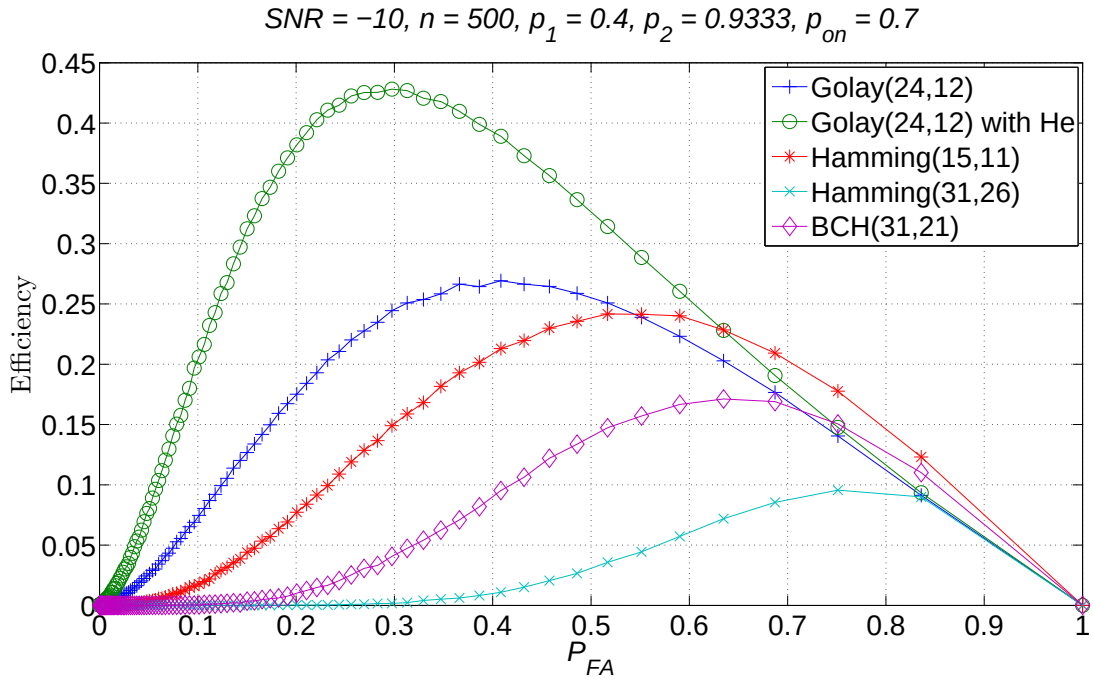

Figure A.4: Comparaison de plusieurs codes, $P_{on} = 0.7$

A.4 Performance du MAC avec les codes correcteurs d'effacement

Dans cette section, nous le cas où plusieurs utilisateurs peuvent accéder au canal comme par exemple dans la TV espaces blancs (WiFi 802.11af) en utilisant le régime Carrier Sense Multiple Access Collision Avoidance (CSMA/CA) régime. Le protocole 802.11 fournit les spécifications pour l'accés multiple (MAC) et la couche physique (PHY) pour mettre en œuvre le réseau local sans fil (WLAN) à l'aide de 2,4 ou 5 bandes de fréquence GHz.

Nous décrivons le schéma CSMA/CA en détail avec l'interaction des couches physiques et couche MAC et les modifications dans le protocole 802.11 existant. Le but est de trouver un point optimal pour un débit global pour plusieurs utilisateurs en réduisant la valeur du backoff BO et en introduisant l'effacement des codes correcteurs pour récupérer les collisions. Le débit optimal est fonction des paramètres de protocole MAC, les paramètres importants sont la longueur, le taux et la distance minimale du code ainsi que le le nombre d'utilisateurs dans le réseau. En outre, si le nombre d'utilisateurs dans le système augmente, des codes correcteurs d'effacement plus efficaces sont nécessaire.

A.4.1 Transmission de flux de MAC avec récupération d'effacements

Le débit de transmission et de réception modifié de la couche MAC est représenté dans la 5.2. Il ressort de l'organigramme de la transmission et de réception qu'il y a deux états d'attente: le temps DIFS sans interruption et le temps backoff (BO) sans interruption. Cette modification du régime CSMA/CA classique réduit les retards dus au DIFS et au BO.

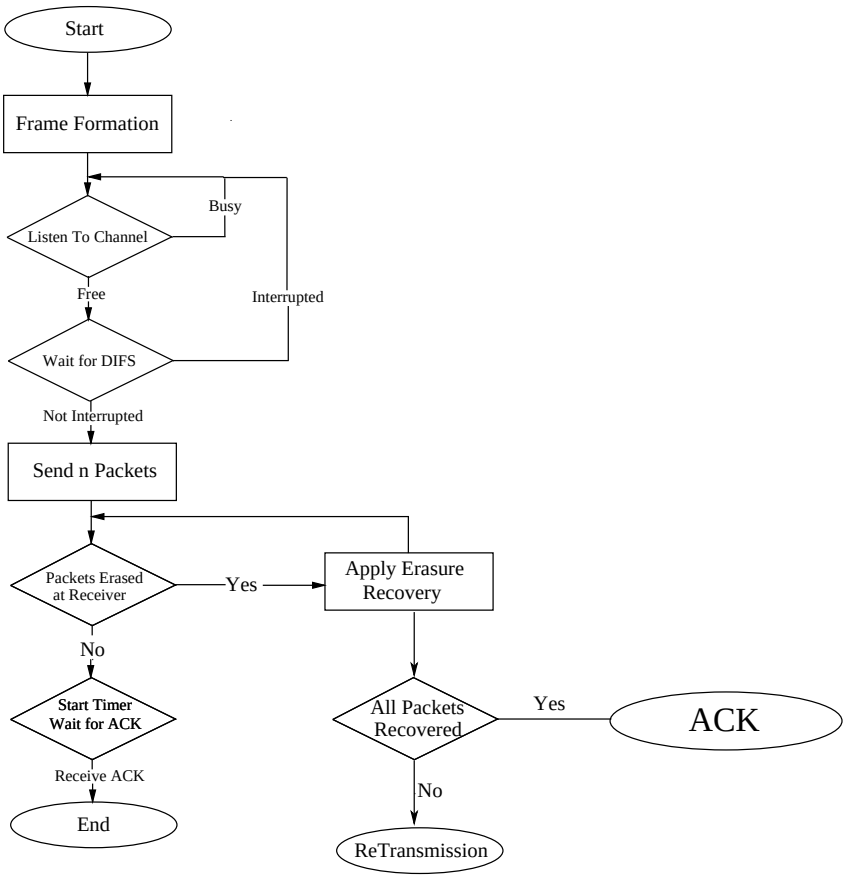

Figure A.5: Diagramme utilisant CSMA/CA avec récupération d'effacements

A.4.2 Résultats de la simulation

Dans cette section, le débit global du protocole CSMA/CA basé sur la protocole MAC est calculé. L'expression générale de débit S est donnée par:

$$S = \frac{U}{B + I} \tag{A.8}$$

où U = temps de transmission réussie des utilisateurs secondaires, B = période d'occupation du canal, I = période d'inactivité du canal lors de la prise en compte des paramètres de protocole MAC utilisant CSMA/CA. L'expression du débit global peut aussi s'écrire:

$$S = \frac{N_{OK}}{N_{OK}(DIFA + SIFS + BO + T_{packets}) + N_{NotOK}(DIFA + SIFS + BO + T_{packets})} \tag{A.9}$$

où N_{OK} = Nombre de paquets reçus avec succès, N_{NotOK} = Nombre de paquets non reçus, $T_{paquets}$ = temps total de transmission d'un paquet. On peut aussi écrire l'expression de débit comme suit:
S = Nombre de paquets réussies / Temps total
où S est mesurée en paquets/sec.

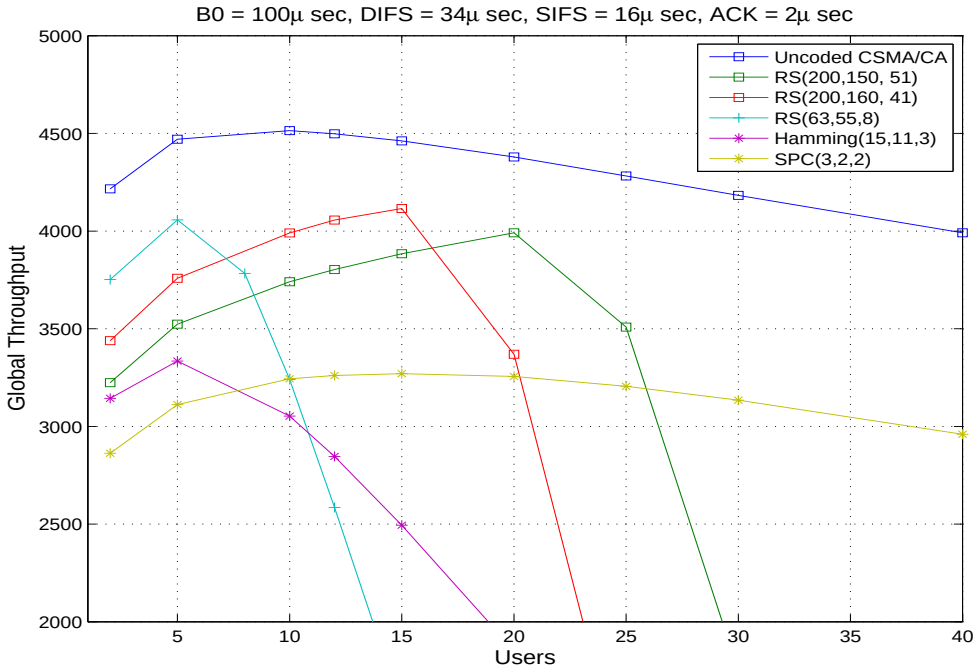

Figure A.6: Débit global en utilisant plusieurs utilisateurs secondaires

La figure 5.9 montre que le débit global est initialement plus élevé avec BO = 100 μsec quand il y a peu de nombre d'utilisateurs secondaires, comme le nombre d'utilisateurs augmente alors le débit global commence à diminuer. Le débit global diminueé de 4500 à 4000 paquets/sec lorsque les utilisateurs passent de 2 à 40. La courbe bleue montre le débit

global du système de retransmission, le débit obtenu avec la retransmission et sans codes d'effacements correction entraîne des délais très longs avec un taux de collision plus élevé. Les courbes de débit globaux sont ensuite tracées en utilisant différents codes correcteurs d'effacement qui montrent que le débit maximum atteint est comparable à celui obtenu avec le débit de retransmission de données. Cette différence est due au rendement du code, mais si aucun codage se fait alors divers paquets effacées par des collisions entre plusieurs SU ne sont pas récupérables et des retransmissions de données sont nécessaire.

A.4.2.1 Taux de collision et le débit global avec BO = 100

Avec les mêmes paramètres que ceux utilisés dans la figure 5.9 pour le CSMA/CA, les courbes de probabilités de collisions et les courbes de probabilité d'effacements résiduelles sont données dans la figure 5.10 pour BO = 100 μsec. Il est clair que la probabilité de défaillance du code Reed-Solomon RS (200,150,51) est égal à zéro jusqu'à 20 utilisateurs et tous les paquets sont récupérés effacées lorsque la probabilité de collision est de 10 % comme indiqué par la courbe bleue. En outre, si le nombre d'utilisateurs augmente pour le point d'accès donné alors des codes plus puissants sont nécessaires pour récupérer les données perdues.

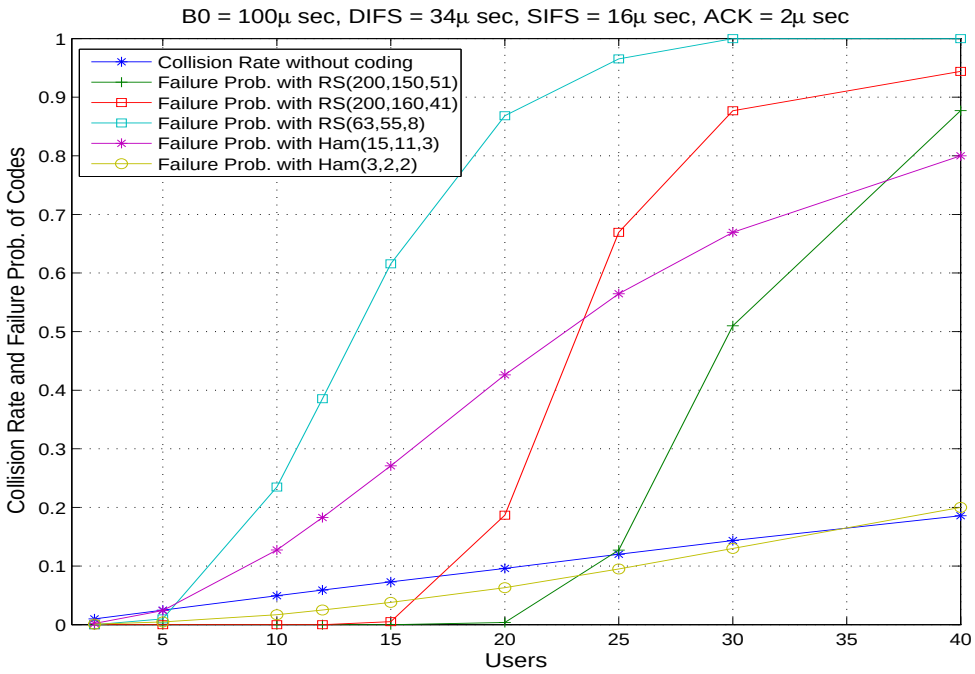

Figure A.7: Taux de collision et probabilité de défaillance de codes

A.5 Conclusions

Dans cette thèse, nous avons étudié divers régimes d'accès au spectre, y compris l'accés opportuniste au spectre. Nous avons proposé une solution pour optimiser l'efficacité de l'utilisateur secondaire à l'aide de l'accés opportuniste au spectre (OSA). Nous avons proposé d'utiliser les codes correcteurs d'effacement pour récupérer les données perdues en raison de collisions entre l'utilisateur primaire et secondaire, l'objectif est d'optimiser l'accès au spectre secondaire pour le régime OSA.

Nous avons proposé des techniques pour optimiser les performances des codes correcteurs d'effacements et de leur décodage. La performance des différents codes correcteurs d'effacement en utilisant diverses méthodes de décodage y compris la recherche exhaustive et le décodage de Viterbi est comparée dans le contexte OSA. L'approche basée sur le graphe de Tanner est proposée pour le décodage en raison de la complexité de décodage limitée et ses bonnes performances. Pour optimiser les performances de codes courts, différentes solutions sont également proposées comme l'utilisation d'une matrice de contrôle augmentée qui apporte un gain significatif de performance. Les détails sur la concaténation des codes courts pour construire des codes plus puissants en termes de récupération d'effacements sont proposées. Les limites analytiques sur taux d'effacements résiduelle pour les codes composants sont calculés et ces limites analytiques sont comparées aux résultats de simulation.

Nous avons modélisé le trafic primaire et secondaire en utilisant un le modèle On/Off de Gilbert et calculé l'expression de la probabilité de collision qui dépend de l'activité du PU et des probabilités de détection. Différentes courbes de simulation sont tracées pour voir l'effet de l'activité de PU, des probabilités de fausse détection et des paramètres de code sur l'efficacité. Il est observé que lorsque le PU est très actif dans le canal, l'efficacité du SU est réduite et que lorsque le PU est peu actif, le SU atteint le niveau de efficacité plus élevé. La performance de correction d'effacement a également un impact élevé sur l'efficacité. Les codes correcteurs d'effacement courts et les codes produits sont plus efficaces en termes de complexité de décodage.

Nous avons proposé une solution pour optimiser le débit global de plusieurs utilisateurs dans le réseau secondaire. Nous avons calculé le taux de collision analytiquement et comparé avec les résultats de la simulation lorsque plusieurs utilisateurs secondaires sont présents. Nous constatons que te taux de collision augmente lorsque que le temps d'attente pour

accéder au canal est réduit et que le nombre d'utilisateurs augmente.

Afin de récupérer les données perdues en raison de collisions, nous avons proposé d'utiliser à court effacements des codes correcteurs. Nous avons montré que pour atteindre un point optimal pour un débit global, il y a toujours un compromis entre le nombre utilisateurs secondaires, la valeur de BO et la capacité de correction des codes d'effacement.

Chapter 1

Introduction

Contents

1.1 Problem Definition

There is a dramatic increase in the access of limited spectrum for the mobile services especially with the emergence of smartphones and tablets in recent years. This is the cause of surge in the demand of radio spectrum. In fact, the useful frequencies are quite completely allocated and there is a high risk of spectrum shortage, so there is a need of either more spectrum or to use existing spectrum more efficiently. The thesis address the second item, especially more flexible spectrum access schemes. A lot of papers have address this problem to depart from Command and Control model that assigns the frequency band to some license holder once for all ensuring that there is only one licensed spectrum holder. In fact, some more flexible schemes have been designed to increase spectrum utilization by dynamic sharing the spectrum and their detailed classification can be found in [4]. In this thesis, we deal with the Dynamic/Opportunistic Spectrum Access (OSA) scheme that describes the primary/secondary access to the spectrum, the primary user (PU) is the licensed user while the secondary user (SU) can have access to the spectrum when the

primary user (PU) is not transmitting. The unused part of the spectrum owned by the primary user (PU) can be utilized by a secondary user (SU) with OSA scheme. This access to the SU is possible by the use of Cognitive radio that was introduced by Mitola in his dissertation [1]. The main objective of Cognitive Radio is to obtain the best available spectrum from the temporary unused spectrum referred as a spectrum hole. Moreover, there is no coordination between primary and secondary user in OSA scheme. The sensing therefore becomes a complimentary part of this scheme as secondary user that accesses the channel opportunistically must listen the channel first in order to avoid interference with the PU. However, sensing is not perfect and it has two types of impairments, these are False alarms and Non detection. False alarms occur when a primary user is detected, i.e. the detection stage detects the PU in the channel while the channel is free and Non detection occurs when the primary user is not detected while the channel is occupied. The consequences of False alarms are missed opportunities to the channel and Non detection results to a collision with primary user. During the collision, data sent when primary is present, are lost and declared as **erased**. In order to recover the lost/erased data due to collisions some techniques must be used in order to guarantee the better Quality of Service (QoS) for primary/secondary access. The possible solution can be a feedback channel and retransmit lost data on request but this may lead to further delays and extra resources. The other solution is the use of forward erasure correcting (FEC) codes operating at receiver side to recover the lost data that will be focused in this thesis. Furthermore, when there are multiple users to access spectrum then Listen Before talk schemes are used, the best scenarios of multiple users access are WiFi in TV white spaces and WiFi operating at 2.4 and 5 GHz. The 802.11 protocol provides the specifications for Media Access Control (MAC) and physical layer (PHY) to implement wireless local area network (WLAN). Due to conjunction of multiple users there are long waiting times as many users try to access the channel and each user has to wait long time to start its transmission. If the long waiting time is reduced and the parameters of MAC protocol are modified then there is a risk of collisions among multiple users and this problem has to be addressed. Moreover, hidden node problem is a known cause of non detection and there is possibility of collisions among multiple users. The recovery of lost data due to collisions among multiple users is a challenge and we address it in the thesis.

1.2 Objective of the thesis

Maximize the Efficiency of Secondary User for OSA

In order to use spectrum efficiently Opportunistic Spectrum Access scheme will be focussed in this thesis. As the data is lost due to sensing impairments, the objective of thesis is to recover this lost/erased data due to collisions for better Quality of Service (QoS) of primary and secondary transmission. The sensing impairments: False alarms and Non detection are not independent and their relationship can be plotted using Receiver Operating Characteristic (ROC) curve, our objective is to find a good functioning point on the ROC curve with minimum collisions and better erasure recovery using various erasure recovery codes. This optimal functioning point on ROC curve will result to maximize the efficiency of secondary spectrum access for OSA. For secondary/opportunistic spectrum access, the secondary user link that will be chosen with the selection of sub channels, is modelled as an erasure channel and we assumed that either data is received correctly or it is not received and will be considered as erased. The short erasure correcting codes will be used to recover the erased data that will reduce the use of extra resources as delays. This is another objective of the thesis. We will use erasure correcting codes for the recovery of lost data due to sensing impairments. We suppose that the data is already protected at physical layer with error correcting codes, we deal with the case when the error correcting mechanism at the physical layer fails and the erroneous data is not passed to the upper layers, the corrupted data is considered as erased at the application layer and erasure correcting codes are used for data recovery at application layer without changing the existing legacy system and this is one of the main objectives of the thesis.

Optimize the performance of erasure correcting codes and decoding:

To optimize the performance of short codes is another main objective of the thesis. When dealing with secondary user network using OSA we focus on short codes which are more suitable due to lower decoding complexity and lower latency. There is also a need to find good decoding method for erasure recovery of erased data for OSA. The objective is to compare the performance achieved for various erasure correcting codes using different decoding methods including Tanner graph, Exhaustive search and Viterbi decoding and choose the suitable decoding method. To enhance the performance of short codes is another objective as long codes are not suitable due to higher decoding complexity and higher latency. The performance of short codes can be greatly improved by the proper choice of parity check

matrix when using Tanner graph based approach. Moreover, the more efficient codes with the concatenation of short codes are addressed to enhance the erasure recovery capability, for example with the concatenation of Single Parity Check (SPC) codes, Single Parity Check Product (SPCPC) codes are constructed which are more powerful in terms of erasure recovery capability.

Optimize the Global Throughput of Multiple Secondary Users:

Finally, the scenario of multiple users is addressed when there is no primary/secondary scenario and there are multiple users in the channel with equal access to the spectrum via CSMA/CA scheme. The goal is to optimize the global throughput of multiple secondary users. The interesting scenario for multiple users access is the use of TV white spaces where WiFi 802.11af can be implemented using Career Sense Multiple Access Collision Avoidance(CSMA/CA) scheme. The second example of multiple users access is WiFi, as the number of users increase in the channel the waiting time to access the channel increases also and the objective is to reduce this long waiting time. If the waiting time is reduced among multiple secondary users then there will be collisions among multiple secondary users, the transmitted data is lost due to collisions. The lost data will be considered as erased and there is a need to recover this lost data that is another challenge that has to be addressed. Moreover, if the no.of users in increased then the value of BO should be increased to some extant in order to aviod too many collisions. The objective is to maximize the global throughput for multiple secondary users. In fact, there is a trade off among number of users, collision probability and erasure correcting codes to recover the erased data.

1.3 Contribution of the thesis

We have envisioned the use of erasure correcting codes to overcome the False alarms and Non detection impairments of sensing in opportunistic spectrum access schemes. Non transmitted data because of primary user (PU) activity, or data lost during collisions can be seen as erasures and recovered with the help of erasure correcting codes.

Decoding and Performance analysis of Erasure Correcting Codes:

We used channel coding by adding redundancy to the information packets to allow the erasure recovery of lost packets. The erasure correcting codes are envisioned at application layer to perform erasure recovery. We focus on short codes due to low decoding complexity and we use the Tanner graph based decoding for short erasures codes in principal to recover

lost data packets. The performance of short codes is further improved by choosing a proper parity check matrix, the extra parity check equations are added to get extended parity check matrix H_e and with Tanner graph based decoding of erasure codes, the performance of short codes is enhanced. The Tanner graph based decoding with usual and extended **H** matrix is compared with the Exhaustive search approach for various short codes. The difference in performance of both techniques is then analysed and we explained why Tanner graph approach is given preference over Exhaustive search. Moreover, the erasure recovery using Tanner graph based approach is done at packet level and we analysed that its decoding is less complex than Viterbi decoding (the complexity of Viterbi decoding becomes too high at packet level). The concatenation of short codes to construct more powerful codes is also addressed in this thesis; for example concatenation of single parity check (SPC) codes form Single Parity Check Product (SPCPC) codes that are more powerful in-terms of erasure recovery with less encoding and decoding complexity. The analytical bounds for SPCPC to estimate their performance are computed and these analytical results are compared with the simulation results for various input erasure probabilities. The modified Viterbi decoding that operate on erasures is described with examples and the three decoding techniques: Tanner graph based decoding, Exhaustive search and Viterbi decoding are also compared using various examples.

Performance Analysis of secondary spectrum access for OSA:
One major contribution is to find the optimum functioning point on ROC curve to enhance the efficiency of secondary spectrum access. The optimal functioning point depends on the sensing impairments, activity of the PU and the parameters of the code including the length, rate and minimum distance. The primary and secondary traffic are modelled using two state On/Off Gilbert models and the analytical formulae are calculated for input collision probability and for the efficiency of the SU. The expression for efficiency is computed and parameters that will affect the efficiency are defined. The effects of sensing parameters and PU's activity on efficiency are analysed and the effects of using various erasure correcting codes having different parameters on efficiency are analysed. A lot of simulations are performed to achieve various efficiency levels using different codes having different parameters including their rate, minimum distance and length. The product codes are constructed through concatenation and the efficiency curves are plotted using various product codes. We have compared the maximum efficiency achieved by various short codes under different parameters of sensing and PU's activity and tried to optimize the efficiency for secondary

spectrum access. We also used long codes to compute the efficiency and observed that the long LDPC codes are capacity achieving but their decoding complexity and latency is too high. We summarized that there exists a trade-off among maximum achievable efficiency, the code properties (rate, minimum distance, etc.) and sensing impairments.

Throughput Analysis of Multiple Secondary Users using MAC:
The last part of thesis is about multiple secondary access. We addressed the application of cognitive radio networks where multiple users access the channel in TV white spaces (interesting scenario is WiFi 802.11af) and WiFi operating at 2.4 and 5 GHz frequency bands. We have described the MAC protocols for CR networks for random protocols and then we have changed the parameters of MAC protocol by reducing the waiting time to access the channel. By reducing the value of backoff the collisions among multiple users increase and we envision the erasure recovery schemes to recover the erased data. We calculated the collision probability analytically among multiple secondary users and compared it with simulation results. We plotted the input collision rate and failure probability of various codes by changing the parameters of MAC protocol. We analysed that each code has different failure probability depending on the collision rate. When the no.of users is increased then we increase the value of BO to reduce the collision rate as the goal is to maximize the global throughput. We have given the expression for estimating the global throughput for multiple secondary users and plotted the simulation results using various erasure correcting codes. The short codes give better performance when collision rate is low but as the collision rate increases then more powerful codes become more effective. Moreover, we proposed the solution to find an optimal point for global throughput. It is observed that the optimal throughput depends on the parameters of MAC protocol, the parameters of the code including the length, rate and minimum distance and the number of users in the network. This modification in the CSMA/CA based MAC protocol will improve the spectrum throughput in-terms of re-usability among multiple secondary users at the expense of redundancy that we have introduced for erasure recovery.

1.4 Structure of the thesis

Chapter 1 describes the background, problem definition, objective, and main contributions of the thesis. Chapter 2 is about state of the art and it gives a detailed classification of various spectrum access schemes. Various traffic models including On/Off are then explained used for the traffic modelling of primary and secondary users. Spectrum sensing

techniques are also described including energy detection. The properties of erasure channel and erasure correcting codes are given with their associated decoding. The last part of the chapter describes MAC protocols and Random Access Protocols in detail. The performance of various erasure correcting codes is given in Chapter 3 using Tanner graph based decoding and Exhaustive search. It is then explained how the performance of short codes can be enhanced. Decoding of Single parity Check (SPCPC) Codes is then given and finally the Viterbi decoding for erasures is described. The applications of short erasure correcting codes for erasure recovery are given in Chapter 4. Primary and secondary traffic is modelled using two state On/Off Gilbert model and the parameters for efficiency are estimated for secondary spectrum access. Simulation results are then given for various values of P_{on} activity of the PU for various short codes, LDPC codes, and product codes. The comparison of efficiencies achieved for secondary reuse of spectrum using various short and long codes is done in this chapter. The spectrum access scheme for multiple users is described in Chapter 5 and the performance of MAC protocols is analysed. Parameters of MAC protocol for 802.11 are given and it is explained how the global throughput is affected if the parameters of CSMA/CA based MAC protocols are changed and erasure recovery schemes are used. The analytical probability for the collision is also calculated and compared with simulation results. The last part of this chapter is about simulation results for multiple users for various CSMA/CA parameters. The chapter 6 is about conclusions and prospects.

Chapter 2

State of the Art

Contents

2.1 Spectrum Access Schemes

Since the demand in radio spectrum has increased and a large portion of the spectrum is underutilized, we will describe various spectrum access schemes in this section. Measurement results presented in a report by the Federal Communications Commission (FCC)'s Spectrum Policy Task Force (SPTF) shows that more than 60% of the licensed spectrum below 6 GHz remains unused [5]. In this report it was advised to manage spectrum access allowing dynamic use of spectrum. FCC therefore allowed to use the secondary spectrum access to improve the spectrum utilization [5]. There are new spectrum access schemes

which depart from today Command&Control scheme. These schemes have flexibility and range from dynamic exclusive use to opportunistic schemes. A detailed classification can be found in [4, 6, 7]. The figure 2.1 shows a detailed classification of the spectrum access models.

In fact the spectrum access models are categorized into four types. The first type is **Command and control** when the regulatory body explicitly defines the rule for use of spectrum and this spectrum is assigned to entities for use. Examples for such spectrum usage include the band used for government organisations, military applications, and aeronautical applications, etc. With the increasing demand of dynamic access to the spectrum, there is no more higher interest for regulatory bodies in command and control type of spectrum assignment and only a small part of spectrum is managed in this mode. The second type is of **Exclusive-use** when the license of specific spectrum band is assigned and the owner has exclusive right to use that spectrum under certain rules. There are further two models of spectrum band assignment under this type. These are the *Long-term Exclusive-use* and *Dynamic Exclusive-use* models. For Long-term Exclusive-use, there are further two possibilities; fixed use and flexible use. During the fixed use, the regulatory body assigns the service and technology specific details and these parameters cannot be changed during the license duration and this is existing standard for various European and Asian countries. For flexible-use, the licensee can change the service or technology specific details used in the band during the assigned period of license time. Example for this service is the TV broadcast service that can be changed to IPTV service using cellular service. For Long-term Exclusive-use, the owner and the duration of license never changes. However, in the Dynamic Exclusive-use, the operator has exclusive rights to the spectrum but the identity of owner and/or type of use can be changed.

The third type of spectrum use is **Secondary use** when there is primary or licensed owner for the spectrum band and many secondary users share the spectrum band opportunistically. This spectrum use can be further categorized into *spectrum underlay* and *spectrum overlay* approach. The spectrum underlay approach is very conservative approach to the spectrum use when the secondary users transmissions are done under very low power in order to avoid any possible interference to the primary users. The primary users in this case have interference free transmissions. The secondary users transmissions in this case will have short range operations. Ultra Wide Band (UWB) is the best example of spectrum underlay approach. UWB has many interesting applications including sensor data

collection, short range personal network connection, etc. In spectrum overlay approach, the spectrum gaps or white spaces are accessed opportunistically either in time or spatial domain. The approach was initially explored in DARPA xG program [8]. This spectrum overlay approach is also known as Dynamic Spectrum Access(DSA), NeXt Generation (xG) Networks or Cognitive Radio Networks. The idea of Cognitive cycle for cognitive radio was initially given by Mitola [1]. This scheme of Dynamic/Opportunistic spectrum access (DSA/OSA) is proposed to improve the spectral efficiency. The unused part of the spectrum owned by the primary user (PU) can now be used by the secondary user (SU) which is possible by the use of cognitive radios [1, 8–12]. The development in Software Defined radio (SDR) has made possible the powerful and flexible radio interfaces [13, 14]. The main

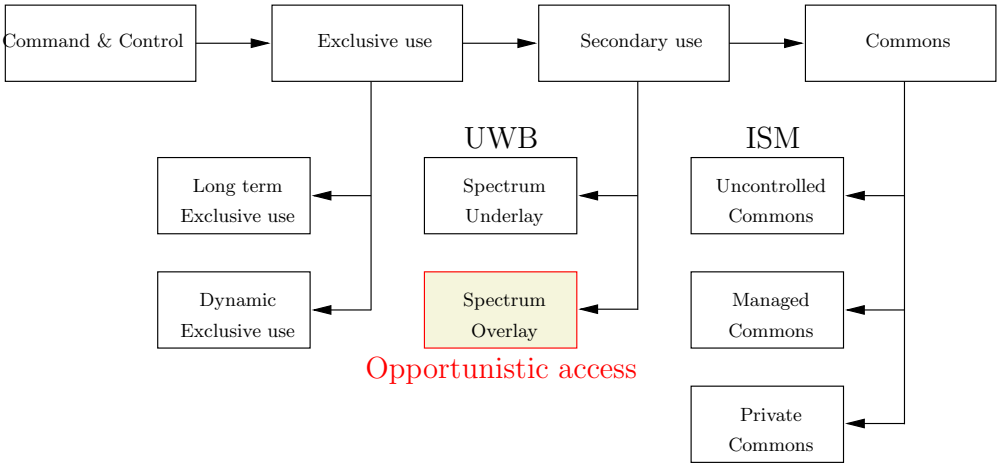

Figure 2.1: Buddhikot's Classification [4]

functionality of the cognitive radio includes the detection of the unused available spectral bands, the selection of the best available channels to meet the secondary user requirement and the maintenance of the channel (e.g., the recovery of lost data during transmission to different spectral bands) [15–17]. The main objective of Cognitive Radio is to obtain the best available spectrum from the temporary unused spectrum referred as a spectrum hole. Various studies on Opportunistically accessing the spectrum are described in [18–29]. In the presence of PU, secondary users equipped with cognitive radio devices may be allowed to transmit when the PU is in idle state by protecting its activity. However, during the transmission of secondary user, the sensing stage continues to sense the spectrum and if primary user is detected, secondary user must stop its transmission and make available spectrum for primary transmission. This is one of the main bottlenecks of SU spectrum

utilization.

The fourth type of spectrum usage is **Commons** which is unlicensed and available for common public and it is shared spectrum. Nobody can claim this spectrum for exclusive use and it is a public resource. This Common spectrum is further categorized into three types which are *Uncontrolled Common*, *Managed Common*, and *Private Common*. Uncontrolled common is the simplest form of all the commons when any entity has no exclusive licence to the band and any entity can have many number of devices operating in this band. The examples of unlicensed bands are ISM(2.4 GHz), U-NII(5GHz) unlicensed bands. In this model there is no protection from interferences, the entities operating in this band may suffer from two kinds of interferences. These are Uncontrolled interferences and Controlled Interferences. Uncontrolled interferences are due to the entities that are outside the network and do not follow the MAC protocol used by the network. The examples of such entities are Bluetooth and microwave ovens that are operating in 2.4GHz band. The controlled interferences are due to broadcast wireless links that create interference to the neighbouring links. The managed commons is also a shared, free of cost and unlicensed spectrum that is used by the devices having multiple technologies. Managed commons provides all three operational scenarios including peer-to-peer/Ad-Hoc, macro and micro cell. An example of managed common band is 50 MHz block in 3650-3700 MHz for government use commons. Private common is a new concept that is introduced by FCC and this concept allows the use of advanced technologies. For example, the primary/license holder may specify protocol and specific hardware, software for devices. The license holder in this case offers private common service either by signalling the spatial or temporal white spaces or allowing the entity performing sensing approved by the primary licensee.

2.1.1 Opportunistic Spectrum Access Related Works

Many works for OSA have been done in order to improve the performance of spectrum access using theoretical modelling and analysis. There also exist some cognitive radio platforms and standards which are used as testbeds and assess the theoretical predictions. Experimental set-up using the Berkeley Emulation Engine 2 (BEE2) platform [30] to compare different sensing techniques, to develop metrics and test cases to measure the sensing performance are proposed by the researchers at the University of California. Using this BEE2 platform, research on spectrum sensing using energy detection and sensing with cooperation is tested by experiments, which shows the practical performance limits of energy detection

under real noise and interference in wireless systems. A distributed genetic algorithm based cognitive radio engine is proposed in the center for wireless telecommunications at Virginia Tech. [31]. This cognitive engine focuses on how to provide CR capability to MAC data link and physical layers. The Open Access Research Test-bed for Next-Generation Wireless Networks (ORBIT) [32] to perform experiments on Cognitive radio has been developed by researchers at Rutgers University. IEEE 802.22 [33] aims to reuse the TV white spaces without harmful interference to TV incumbents. A CR based PHY and MAC for dynamic spectrum sharing of free TV channels is evaluated in [34], which studies the coexistence of primary and secondary user, spectrum sensing, spectrum management, QoS, reliability and their impact on the network performance. Dynamic frequency hopping (DFH) is recently proposed in IEEE 802.22 [33], where the sensing is performed on the intended next working channels in parallel to the data transmission in current working channel and no interruption is needed for sensing. The IEEE P1900 [35] is an existing standard focusing on next generation radio and spectrum management. One important role of this standard is to provide reconfigurable networks and terminals in a heterogeneous wireless environment.

2.2 Traffic Models and Secondary Access

2.2.1 Traffic Models

There are many system models to describe the activity of PU and these are helpful for estimating the efficiency of SU to opportunistically access the spectrum. The channel occupancy can be described by either continuous or discrete slot structure. The difference between continuous and discrete structure is that for continuous time channel occupancy the user does not check whether the channel is busy or free while for the slotted structure the user starts its transmission at the beginning of time slot. The continuous time structure is not divided into time slots while the discrete structure is divided into time slots. For

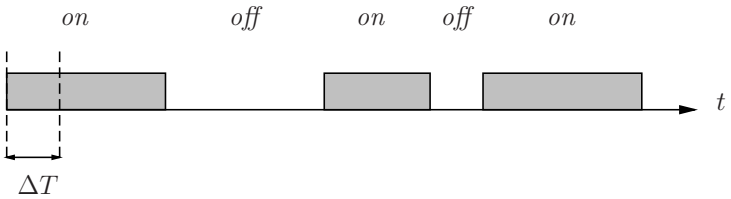

Figure 2.2: Time activity of the PU

the Opportunistic Spectrum Access (OSA) scheme the activity of PU can be modelled

as the succession of active and idle periods as the measurement results reported in [36] have shown. This activity, as sketched in figure 2.2, can be modelled with a two-state Gilbert model [37, 38] with given transition probabilities between state *On* (while PU is transmitting) and state *Off* (when PU is idle) as shown in figure 2.3. In this model it is assumed that the whole frequency band is divided into subbands of a number υ with respective widths $B_1, B_2, ..., B_\upsilon$. Each subband is either occupied (while the primary user is transmitting) or idle during each time slot ΔT as sketched.

p_1 is the transition probability from state *On* to state *Off*, conversely p_2 is the transition probability from state *Off* to state *On*. The steady state probabilities P_{on}, P_{off} of the channel to be active or idle are given by the classical formula:

The On/Off model is not really a semi-Markov model since the transitions occur at periodic ticks, but it can be converted to a semi-Markov model provided the probability distribution function(pdf) of time is derived in On and Off states. The activity of PU cannot be controlled as it is variable and it is the main challenge for SU to achieve guaranteed quality of service. For various values of P_{on}, the SU may achieve various efficiency levels. The secondary user listen continuously to the channel in order to detect the idle time slots, and sensing is normally required for this purpose. A part of the time-slot T_s is reserved for sensing the channel, while the remaining $T - T_s$ will be used for SU's transmission if no PU activity is detected.

$$P_{on} = \frac{p_2}{p_1 + p_2}, \quad P_{off} = \frac{p_1}{p_1 + p_2}$$

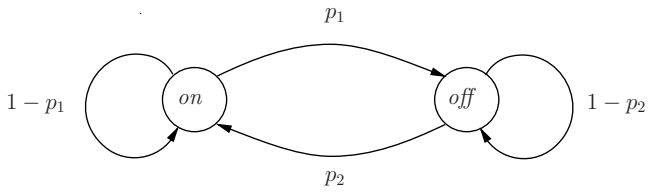

Figure 2.3: Simple On/Off model

When both the primary and secondary networks are slotted then the Partially Observable Markov Decision Process (POMDP) based model is proposed for OSA scheme [39]. Decentralized MAC protocol is a practical example for this scenario when there is no central controller and secondary users independently search spectrum opportunities. The secondary user need not to monitor the channel at all time, rather it monitors the channel when it intends to transmit the data. This is energy efficient scheme for OSA system in

case of Ad-Hoc Networks.

PU traffic also can be modelled as Poisson process. The arrival of PU in the subchannels i can be modelled using Poisson process with arrival rate λ_i, where the number of events in the time interval $(t, t+\tau)$ follows a Poisson distribution with parameter $\lambda_i\tau$. This relationship is expressed as:

$$P[X = k] = \frac{e^{-\lambda\tau}(\lambda\tau)^k}{k!} \qquad k = 0, 1, \ldots, \tag{2.1}$$

where $X = k$ are the number of events in time interval $(t, t+\tau)$. When modelling the PU traffic as Posisson process, Spectrum pooling concept [40] can be used to estimate the efficiency of SU when the spectrum is divided into multiple subbands in order to minimize the interference of PU. The secondary user's communication is done by combining these idle subbands and a communication link is maintained. If the PU arrives to the channel the performance of SU starts decreasing slowly. A very simple channel selection scheme is studied in [41] using On/Off model [42], [43], [44], [45] to minimize interference to the PU that has continuous time channel occupancy and can appear any time in the channel while the secondary user's network is assumed time slotted that performs periodic sensing to find the idle slots.

For OSA when both the primary and secondary users do not have slot structure, Continuous-Time Markov Chain (CTMC) process is proposed [46]. To dynamically access the N parallel channels occupied by the primary user can be done by performing periodic channel sensing and the complete system states can be modelled using a 2^N-state continuous-time Markov chain (CTMC) process. The idle slots are sensed among the bursty traffic of primary transmissions and then the transmission in a single channel is done by the secondary user. Bluetooth is a practical example for this scenario.

WLAN OSA system does not have slot structure, therefore, the description of the system in continuous time is required. In this case, the system should contain specific informations: The channel state, the transition probabilities, and the system duration in that particular state. The use of semi-Markov model is useful for this WLAN OSA system. In WLAN standard, acknowledgement is sent after each data packet transmission. The channel occupancy for WLAN system can be modelled by a two state semi-Markov chain, the details are given in [47]. Furthermore, after the successful transmission, the stations must follow a backoff mechanism in order to continue the further transmission and to have equal rights among all stations. The state transition is done in this way and the second

step is to find the occupied duration of each state. To find the statistical distribution of idle state is challenging and to estimate this time, there are several distributions that fit for statistical behaviour of traffic, for example the load Empirical CDF distribution for UDP traffic can be chosen.

2.3 Spectrum sensing

There is usually no synchronization between the primary and secondary users in OSA scheme and sensing is required to detect the presence of PU in case of dynamic traffic or to detect the coexistence of SUs in case of static traffic (TV white spaces for example) [48,49] (the scenario is 802.11af protocol or LTE femtocells in TV band). Sensing gives the information about the spectrum usage and the existence of primary users in geographical area. This awareness can be obtained via geolocation and databases using the beacons or by local spectrum sensing at the CR. The idle periods between the bursty transmissions of wireless local area network (WLAN) can be used opportunistically. The Energy Detector based Sensing is commonly used due to low computational and implementation cost. The waveform based Sensing, cyclostationarity based Sensing, radio identification based Sensing, matched-Filtering based sensing are other types of sensing which are described in [50]. Cooperating Sensing, centralized sensing, distributed sensing, external sensing are also important types of sensing. History based prediction can also be used for the future profile of the spectrum. More sensing algorithms for Cognitive Radio applications can be found in [51–53].

Energy Detection approach for spectrum sensing is preferred for cognitive radio due to its simplicity and low computational and implementation complexities. The cognitive radio user do not has prior arrival information of primary user within a given frequency band and generally the cognitive/secondary user do not has enough information about channel idle or busy states for secondary transmission. With this insufficient information for secondary user, energy detection approach is preferred to detect the primary user's signal irrespective of its structure. Energy detection approach compares the energy of received signal for a given frequency band to a threshold value. If the energy of signal is above a given threshold then the frequency band is declared as busy otherwise the frequency band is declared and it can be used by the secondary user. However, the spectrum sensing is not perfect and there are some limitations in detecting the signal. These limitations of spectrum sensing problem can be formulated using binary hypothesis [54].

$$\begin{aligned} \mathcal{H}_0 : y[n] &= w[n] \qquad n = 1, 2, ..., N \\ \mathcal{H}_1 : y[n] &= x[n] + w[n] \qquad n = 1, 2, ..., N \end{aligned} \tag{2.2}$$

where $\mathcal{H}_0$ denotes the null hypothesis showing that the samples of received signal $y[n]$ correspond to noise samples $w[n]$ and no primary signal exist in the spectrum band. The other hypothesis $\mathcal{H}_1$ indicates that the signal of primary/licensed user $x[n]$ is present in the spectrum band, where N indicates the number of samples during the signal observation duration and it is called sensing period T_s. The number of these samples are limited as the whole idle period is not spent for sensing. The remaining idle period is used for secondary transmission once no PU's transmission is detected. In ideal case, the detection stage would select $\mathcal{H}_1$ when the primary user's signal is present or $\mathcal{H}_0$ in case no signal is detected.

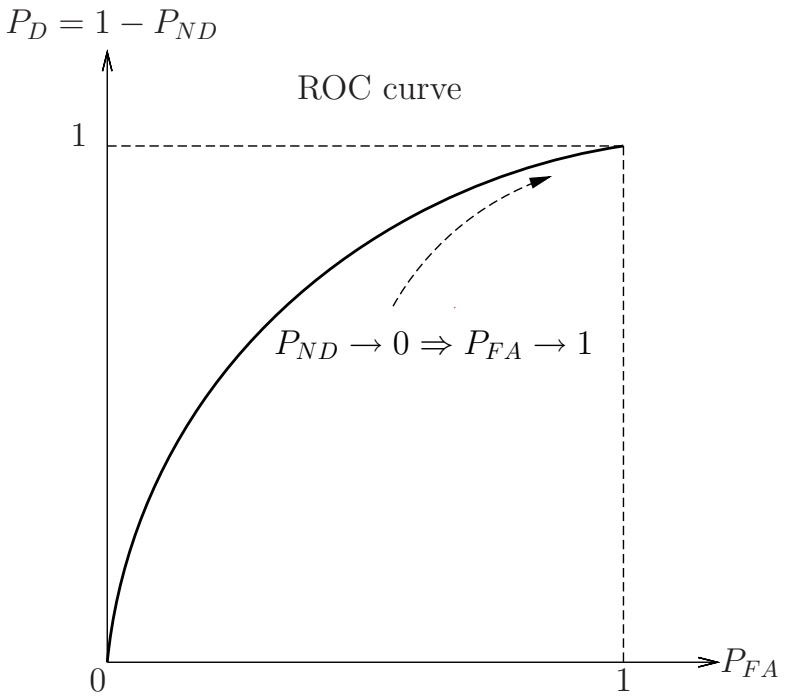

Figure 2.4: Typical ROC curve, the trade-off between P_{ND} and P_{FA}

Spectrum sensing is not perfect and it has two types of impairments which are False Alarms and Non Detection. False alarms occur when a primary user is detected, i.e. the detection stage selects $\mathcal{H}_1$ while the channel is free [51] and Non detection occurs when the primary user is not detected while the channel is occupied, i.e. the detection stage selects $\mathcal{H}_0$. The consequences of these False Alarms and Non-Detection are missed opportunities

to access the channel and collisions with primary user. During a collision, data sent when primary is present, are lost and declared as **erased**.

Respective probabilities $P_{FA} = P(\mathcal{H}_1/\mathcal{H}_0)$ (false alarm) and $P_{ND} = P_{ND} = 1 - P_D = P(\mathcal{H}_0/\mathcal{H}_1)$ (non detection) are not independent and their relationship can be plotted using Receiver Operating Characteristic (ROC) as shown in figure 2.4. It is unfortunately not possible to have at the same time small false alarm and non detection probabilities, more exactly $P_{ND} \to 0 \Rightarrow P_{FA} \to 1$. There is a trade off for the choice of a functioning point on the ROC curve. Detection performance is better when the SNR is higher; same result when the number N of samples is higher (corresponds to a higher sensing time T_s. The Fig. 2.5 describes the fact that as the value of SNR is getting better for example from -20dB to -5dB, the functioning point is moving and it is possible to get better functioning point with reduced values of P_{FA} and P_{ND}, i.e. with the possibility of reduced missed opportunities to access the channel and with lower collisions.

The classical energy detection approach measures the energy for given frequency band during observation time also called sensing time and decides the current channel state S_i as busy when hypothesis $\mathcal{H}_1$ is selected i.e., if the measured energy is greater than the predefined threshold or idle in case the measured is less then the defined threshold i.e., when $\mathcal{H}_0$ is selected.

$$T_i(Y_i) = \sum_{n=1}^{N} |y_i[n]|^2 \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \lambda \tag{2.3}$$

Where $T_i(Y_i)$ is the statistic test computed during the $i-th$ sensing symbols over the signal vector $(y_i[1], y_i[2], ..., y_i[N])$ and λ is threshold that distinguish between two hypotheses of equation 2.2. Closed-form expression for the detection probability (P_D) and false alarm probability (P_{FA}) can be calculated based on statistic of $T_i(Y_i)$. For Gaussian approximation, test statistics follow a central and non-central chi-square distribution with $2N$ degrees of freedom under hypothesis $\mathcal{H}_0$ and $\mathcal{H}_1$ [54]. Furthermore, for lower SNR, the number of samples for detecting the presence of primary signal should be large ($N \gg 1$) to achieve specific performance. Based on the sensing observation, the central limit theorem can be applied to estimate the test statistic as Gaussian:

$$T_i(Y_i) \sim \begin{cases} \mathcal{N}(N\sigma_w^2, 2N\sigma_w^4), & \mathcal{H}_0 \\ \mathcal{N}(N(\sigma_x^2 + \sigma_w^2), 2N(\sigma_x^2 + \sigma_w^2)^2), & \mathcal{H}_1 \end{cases} \tag{2.4}$$

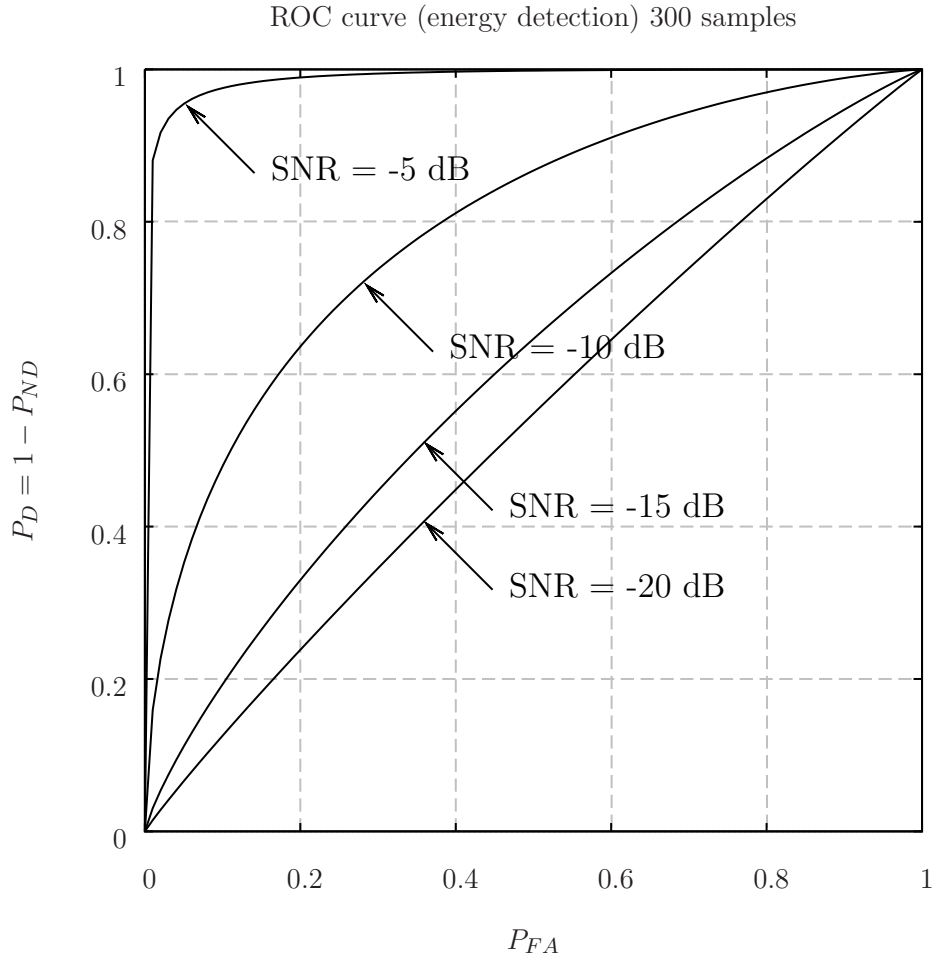

Figure 2.5: ROC curves for various values of SNR

where σ_x^2 is the power of primary user's signal and σ_w^2 is the noise variance. In case if Additive White Gaussian Noise (AWGN) is considered, P_D and P_{FA} can be calculated as follows:

$$P_D = P\{T_i(Y_i) > \lambda\}_{\mathcal{H}_1} = \mathcal{Q}\left(\frac{\lambda - N\left(\sigma_x^2 + \sigma_w^2\right)}{\sqrt{2N\left(\sigma_x^2 + \sigma_w^2\right)^2}}\right) \tag{2.5}$$

$$P_{FA} = P\{T_i(Y_i) > \lambda\}_{\mathcal{H}_0} = \mathcal{Q}\left(\frac{\lambda - N\sigma_w^2}{\sqrt{2N\sigma_w^4}}\right) \tag{2.6}$$

The decision threshold λ is an important parameter that can be chosen for an optimal trade-off between P_{FA} and P_D but this threshold requires the values of noise and signal powers. However, the noise power can be estimated while the received signal power is

difficult to calculate because it depends on various parameters including propagation and transmission characteristics. The threshold is normally chosen to satisfy values of P_{FA} that only needs the noise power for estimation [55]. By solving the equation 2.6 the expression of λ is calculated that gives the threshold value required for the detection probability P_D.

$$\lambda = \left(\mathcal{Q}^{-1}\left(P_{FA}\right)\sqrt{2N} + N\right)\sigma_w^2 \tag{2.7}$$

By substituting the value of equation 2.7 into equation 2.8 and dividing the equation by σ_w^2 gives:

$$P_D = \mathcal{Q}\left(\frac{\mathcal{Q}^{-1}\left(P_{FA}\right)\sqrt{2N} - N\gamma}{\sqrt{2N\left(1+\gamma\right)}}\right) \tag{2.8}$$

This equation can further be written as :

$$P_D = 1 - P_{ND} = \mathcal{Q}\left(\frac{\mathcal{Q}^{-1}\left(P_{FA}\right) - \sqrt{\frac{N}{2}} \times SNR}{1 + SNR}\right), SNR = \sigma_x^2/\sigma_w^2 \tag{2.9}$$

One of the main objectives of the work is to find a good functioning point on ROC curve that will optimize the spectral efficiency of secondary access. The activities of PU and SU

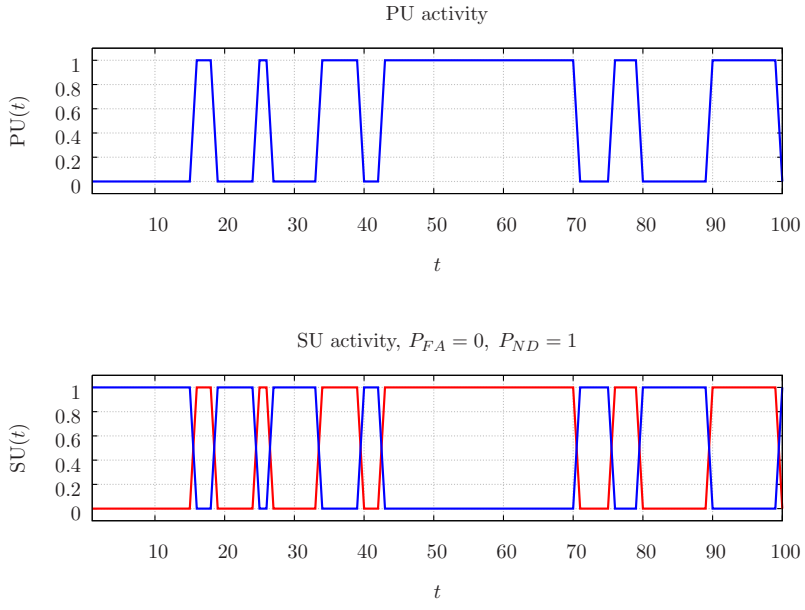

Figure 2.6: SU activity; successful access (blue), collisions (red)

are now plotted using On/Off model and using the ROC curves of figure 2.5 with equations

2.6 and 2.9 for various values of P_{FA} and P_{ND} keeping other parameters constant. We will observe the different cases of spectrum access and collisions between PU and SU as the functioning point moves on the ROC curve in figures 2.6 to 2.8. The functioning point is

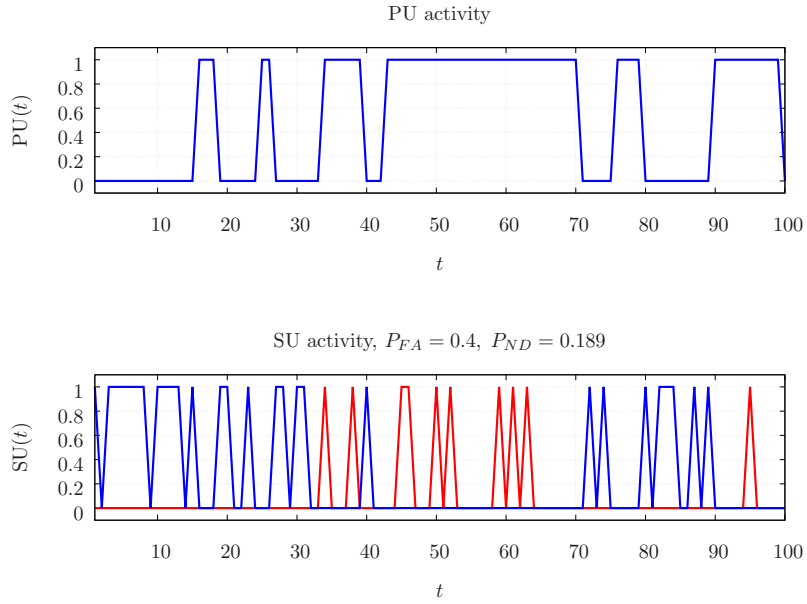

Figure 2.7: SU activity; successful access (blue), collisions (red)

moved by assigning various values to P_{FA} and P_{ND} and the effect of these probabilities in terms of successful access to the spectrum and collision with the PU can be seen in figures 2.6 to 2.8. The blue line shows the successful access to the spectrum and the red line shows the collision to the PU's that will lead to the loss of data for both primary and secondary user. The figure 2.6 shows that when the value of $P_{FA} = 0$ and $P_{ND} = 1$, the secondary user is always transmitting as if no sensing were performed, so that there is a collision when PU is on. In this case there are no false alarms but there is always collision with the PU, it means when the activity of PU is high the activity of SU is also high and both are transmitting. The x-axis shows the time ticks and y-axis shows the activities of primary and secondary user. The figure 2.7 shows when the value of $P_{FA} = 0.4$ and $P_{ND} = 0.189$, the secondary user is not always transmitting but it is missing the idle slots most of the time due to false alarms, so that there are collisions when PU is on but some opportunities are missed due to 40% probability of False alarms. This is clear that the collision probability is very low but at the same time there is no access to the channel most of the time due to False alarms. The figure 2.8 shows when the value of $P_{FA} = 1$ and $P_{ND} = 0$ the secondary

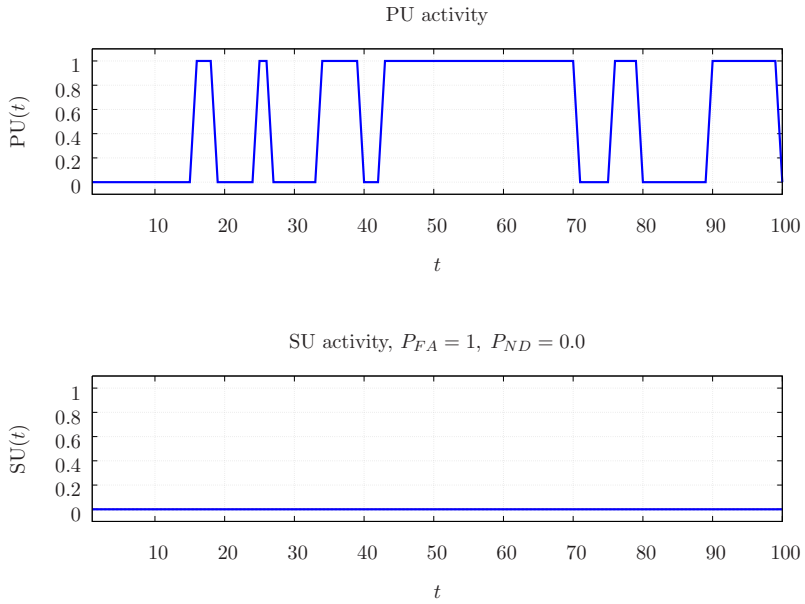

Figure 2.8: SU activity; successful access (blue), collisions (red)

user is not transmitting at all and as the result there are no collisions when PU is on but at the same time there is no access to the channel as the probability of False alarms is 100 %. There are two extreme access schemes: First, there are no false alarms but the SU is always transmitting and there are always collisions, this is an aggressive approach. There are no collisions but there is no access to the channel, this is a conservative approach and SU will not be able to transmit. In fact, there exist a good functioning point to be in between conservative and aggressive approach to have better secondary transmission. Furthermore, these is a need to use Forward Erasure Correction to recover the lost data due to primary/secondary collisions. These are few important challenges to be addressed for opportunistic spectrum access.

2.4 Erasures Codes and associated Decoders

2.4.1 Background

The transmission of data is an essential part of digital world. The transmission of data includes the uploading and downloading of videos, files, texts and it includes the cellular calls and messages of wireless world. They are then transmitted through channel and reconstructed at the receiver. The wireless channel is more sensitive due to shadowing,

interference of multiple users, and fading, etc. To transmit the information reliably through wireless channel is an important topic of information theory.

The theoretical work developed by pioneers specially "Claude Shannon" developed the foundation for communication systems in such a way that the information can be transmitted reliably at any rate lower than the channel capacity and conversely, the reliable transmission is not possible at rate higher than the channel capacity. These techniques are collectively known as coding theory by introducing redundancy to the transmitted information. For any digital communication system, data is transmitted through channel, and the component that add redundancy to the original information is called channel encoder and the component that recover the source information from the encoded information is known as channel decoder. The codes help to represent source information efficiently in the presence of noise introduced by the channel at the receiver.

In channel coding, the message across noisy channel is transmitted using codes with the source information and redundant information to recover the original information the sink even in the presence of channel noise. In general, the codes with lower encoding and decoding complexities and with lower delays are suitable to achieve reliable transmission close to channel limit known as *Shannon capacity*. This capacity is an upper bound on the rate of information that can be transmitted reliably over a communications channel. The "information" channel capacity of a discrete memoryless channel is defined by the following equation:

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

where X represents the input of the channel and Y represents the output where the mutual information $I(X,Y)$ is given by the following equation:

$$I(X,Y) = H(X) - H(X|Y)$$

The reliable transmission is required and the transmitted information should be generated at the sink/receiver even if some data is distorted or lost during the transmission. At the receiver side the received bits are decoded to recover the transmitted information and then the decoded bits are used to reconstruct the source at the receiver. According to Shannon theorem for a given noisy channel with channel capacity C with information transmitted at rate $\mathbf{R}$, if

$$\mathbf{R < C}$$

then there exist the codes which allow the small error probability at the receiver side, that means theoretically it is possible to transmit information without an error at rate below the limiting rate **C**.

There exist a lot of channels models including Binary Symmetric Channel (BSC), Binary Erasure Channel (BEC). The binary erasure channel is one of the simplest channel model and can be used to model data networks when bits are either received correctly or lost due to various reasons including extra delays, buffer overflows, interferences,...etc. In BEC the encoded bits are either received correctly or declared as erased if not received correctly. The coding in binary erasure channel is facilitated by the fact that bits are never corrupted these are considered as lost and the only concern for coding is to find the value of lost/erased bits giving the location of erasures. The lost or erased bits can further extend to packet level.

Figure 2.9 depicts the **Binary Erasure Channel (BEC)**, a transmitter sends bits(zeros or ones) and the receiver either receives the bits and if not these are declared as "erased". The channel input denoted by x is binary input: $x \in \{0, 1\}$ and the output is denoted as y. The possible output values are $\{0, 1, \epsilon\}$. where p indicates the erasure probability.

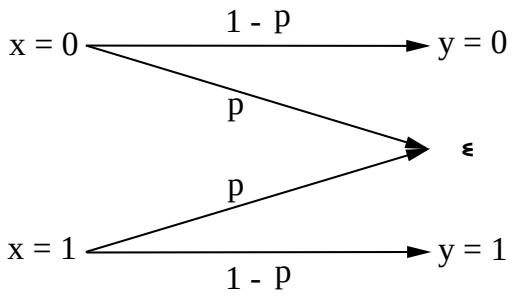

Figure 2.9: Binary Erasure Channel

The erasure channel is memoryless and the capacity of this channel is calculated as follows:

$$\Pr(x|y) = \begin{cases} 1 & \text{if } y = x, \\ 0 & \text{if } y \neq x, \\ \frac{1}{2} & \text{if } y = \epsilon \end{cases}$$

$$P_r(X = 0) = P_r(X = 1) = 1/2$$

$$H(X|Y) = \sum_{x \in X} \sum_{y \in Y} P_r(X = x_i, Y = y_j) \times \log_2 \frac{1}{P_r(X = x_i | Y = y_j)}$$

$$H(X|Y) = 2 \times \left(\frac{1-p}{2}\right) \times \log_2 \left(\frac{1}{1}\right) + 2 \times \left(\frac{p}{2}\right) \times \log_2 \left(\frac{1}{1/2}\right) = p$$

$$I(X,Y) = H(X) - H(X|Y) = 1 - p$$

2.4.2 Block codes

There are two families of error correction codes. **Block codes:** Hamming, BCH, Reed-Solomon, Turbo, Turbo Product, LDPC, Concatenated Codes (Serial and parallel) and **Convolutional codes** [56–69].

Main parameters of a code are the rate R (related parameter to redundancy that is introduced to allow correction), the minimum distance d, the length n (number of bits after coding) and dimension k (number of information bits before coding) and the code rate is calculated as

$$R = k/n$$

There exist always a trade-off among the parameters R, d, n, and k to choose an appropriate code for erasure recovery [70], [71]. Block code is defined with a finite codeword length, a $\mathcal{C}$ (n, k, d) has n = length, k = dimension, d= minimum distance, these three parameters are not independent. The Hamming distance (also known as the minimum distance) d of a linear code is the smallest Hamming distance between any pair of code vectors in the code and it is defined by the following expression:

$$d = \min_{\mathbf{x} \neq \mathbf{y}} d(\mathbf{x}, \mathbf{y})$$

and the Singleton bound says that

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

The minimum distance can be written as:

$$d = n - (k + i) + 1, \quad i \geq 0$$

When $i = 0$, the code is a maximum Distance Separable code. It is theoretically possible

to correct t_c erasures where t_c is given as:

$$t_c = n - (k + i) = d - 1$$

Moreover, if the codeword is constructed by appending parity symbols to the information data, it is called a "systematic" code. If the systematic encoding is done then the codeword can be written as: $(d_1, d_2, d_3, ..., d_k, r_1, r_2, ..., r_{n-k})$ and the information packets can be separated very easily at the receiver side while decoding. For systematic codes the generator matrix $\mathbf{G}$ is written in the form:

$$\mathbf{G} = [\mathbf{I_k A}]$$

and Parity check matrix $\mathbf{H}$ is written as:

$$\mathbf{H} = [\mathbf{A^T I_{n-k}}]$$

When dealing with binary erasure channel (BEC), the information bits are encoded using erasure correcting code to recover the lost data. In fact, the error correction is done already at physical layer to correct the errors within a packet while the error position is not known, the examples of error correcting codes are turbo-codes, LDPC and a lot of other short codes. While, erasure correction is done at application layer and no modification is done at PHY layer. Bits which are not correctly decoded at the PHY layer (if there are too much interference residual errors after error correction) are declared as erased. The recovery of these lost bits is performed by an erasure correcting code. The main difference is that when using erasure correcting code the positions of erased packet are known (i.e. each packet has its identifier).

2.4.3 Binary Linear Codes

A block code $\mathcal{C}$ is called a binary linear (n, k) code if its 2^k code words form a k-dimensional subspace of the vector space of all n-tuple over the Galois Field GF(2). It is also defined as a (n, k) linear code over GF(2) is a k-dimensional subspace of vector space V_n that are spanned by k linearly independent vectors. The binary linear codes has the property that the output of an information source is a sequence of binary digits "0" or "1". Each information block consists of k information digits as shown in figure 2.10 and there are a total of 2^k distinct information blocks.

The encoder transforms each input information block $\mathbf{u}$ into a binary n-tuple $\mathbf{v}$ with

$n > k$. This n-tuple $\mathbf{v}$ is referred as the code word (or code vector) of the information block $\mathbf{u}$. There are 2^k distinct code words. GF(2) is the set of $\{0, 1\}$ together with two operations of addition and multiplication (modulo 2) satisfying a given set of properties.

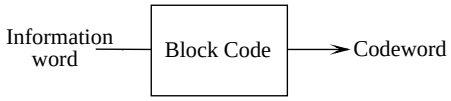

Figure 2.10: Block Codes encoding

The "vector space" V_n over GF(2) is a subset of GF(2^n) with two operations of addition and multiplication (modulo 2) satisfying a given set of properties and the "subspace" is a subset of a vector space which is itself a vector space. The set of vectors $\mathbf{v_0}, ..., \mathbf{v_{k-1}}$ is linearly independent if $a_0\mathbf{v_0}+\mathbf{a_1v_1}+...+\mathbf{a_{k-1}v_{k-1}} = \mathbf{0}$ that implies $a_0 = a_1 = ... = a_{k-1} = 0$. Any codeword $\mathbf{c}$ can be written as a linear combination of k basic vectors $(\mathbf{v_0}, ..., \mathbf{v_{k-1}})$ as follows: $\mathbf{c} = \mathbf{u_0v_0} + \mathbf{u_1v_1} + ... + \mathbf{u_{k-1}v_{k-1}}$, where $(\mathbf{u_0}, \mathbf{u_1}, ..., \mathbf{u_{k-1}})$ is the data to be encoded.

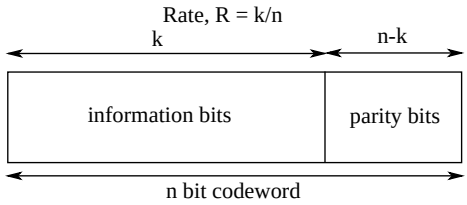

Figure 2.11: Codewords with $n - k$ redundancy

Generator matrix is described as the rows of the generator matrix which are the basis vectors $v_0, ..., v_{k-1}$. The codeword $\mathbf{c}$ is obtained by multiplying $\mathbf{G}$ by $\mathbf{u}$: $\mathbf{c} = \mathbf{u}.\mathbf{G}$. To construct the (6,3) linear code spanned by the basic vectors [100011], [010110], and [001101] with data $\mathbf{u} = [\mathbf{011}]$ is encoded to $\mathbf{c} = 0.[100011] + 1.[010110] + 1.[001101] = [011011]$.

Now the **Parity check matrix** is defined, if $\mathcal{C}$ is a $[n, k]_q$ linear code then its dual denoted as $\mathcal{C}^\perp$ is given as $[n, n-k]_q$ linear code. Since a linear code is a subspace of $\mathbf{F}$ then its dual or orthogonal space is $\mathcal{C}^\perp = \{z \in \mathbf{F} \mid \langle \mathbf{z} \cdot \mathbf{c} \rangle = \mathbf{0} \, \forall \, \mathbf{c} \in \mathcal{C}\}$, where $\langle z, c \rangle = \sum_{i=1}^{n} z_i c_i$ and $(\mathcal{C}^\perp)^\perp = \mathcal{C}$. $\mathbf{H}$ is parity check matrix for $\mathcal{C}$ which is, in fact, a generator matrix for dual code $\mathcal{C}^\perp$. This $\mathbf{H}$ matrix will be used in decoding to estimate the error/erasures in the codeword.

The generator matrix is related to the parity check matrix by the equation $\mathbf{H}.\mathbf{G^T} = \mathbf{0}$

where $\mathbf{G^T}$ denotes the transpose of $\mathbf{G}$. This implies that, for any codeword $\mathbf{c}$, the product of the parity check matrix and the encoded information block should be zero $\mathbf{H}.\mathbf{c^T} = \mathbf{0}$.

2.4.3.1 Reed–Solomon (RS)

RS codes are non-binary cyclic error-correcting codes build over GF(2^m). The important features of RS codes is that the minimum distance of (n, k) RS code is $n - k + 1$. RS codes are Maximum Distance Separable (MDS) code and they are famous for correcting multiple-burst bit-errors. The basic building block of RS codes is a symbol that is composed of m binary bits, where m is a number greater than 2. For any given m, the length of RS codes composed of m bit symbols is $2^m - 1$, for example, the length of the RS codes with 8 bit symbols is $2^8 - 1 = 255$. If the channel loss is higher then the receiver may not receive k out of n symbols and the retransmission is necessary for the duplicate of previously transmitted symbols. This may decrease the efficiency of channel and increase the encoding and decoding complexity of the code.

2.4.3.2 Low-density parity-check (LDPC) codes

LDPC codes are a class of linear codes and there were first introduced by Gallager in his PhD thesis in 1960. The name comes from the characteristic of their parity-check matrix which contains only a few 1's in comparison to the amount of 0's. Their main advantage is that they provide a performance which is very close to the capacity for a lot of different channels and require linear time complex algorithms for decoding. Like other linear block codes LDPC can be described via sparse parity-check matrix. In fact, completely randomly chosen codes are good with high probability but encoding complexity of such codes is usually high because there is no structure that can be used to encode and to decode [72–76].

In many cases they allow a higher code rate and also a lower error floor rate and their code length should be longer to yield good results. The feature of LDPC codes to perform near the channel limit exits only for large block lengths. The large block length results in large parity-check and generator matrices and the encoding complexity will be quite high.

2.4.3.3 Digital Fountain codes

Digital Fountain codes are sparse-graph codes designed for channels with erasures such as broadcast transmission where files are transmitted in multiple small packets, each of which is received without error or not received. The transmitter transmits the packets at receiver

without any knowledge of which packets are received. Once the receiver has received N packets, where N is slightly greater than the original file size K, the whole file can be recovered. Fountain codes are rateless in the sense that the number of output packets that are generated from the original data are limitless and transmitted packets are generated on the fly. These codes can be used to provide the protection against erasures caused by a primary user appearance over a secondary user link. Digital fountain codes are capable of

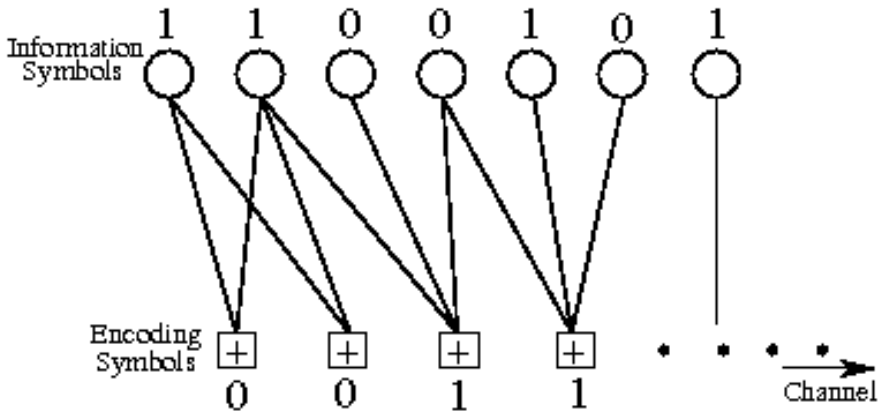

Figure 2.12: LT Encoding

protecting from the effects of packet loss irrespective of the loss model of secondary user link. By recovering lost data packets without requesting retransmission from the sender, these codes provide reliability in various applications such as multicast, parallel downloading, video streaming, etc. The examples of digital fountain codes are Luby Transform Codes (LT Codes) and Raptor Codes. These codes have ability to generate a potentially limitless amount of encoded data from any original set of source data. These codes can recover the original data from a subset of successfully recovered encoded data regardless of which encoded data has been received. Fast encoding and decoding algorithms operate at nearly symmetric speeds that grow only linearly with the amount of source data to be processed and independently of the actual amount of network loss. Fountain codes are recently used for broadcast applications [77], [78]

LT codes are practical rateless codes [79, 80] for binary erasure channel. These codes were presented by Luby in 1998 for the purpose of scalable and fault tolerant distribution of data over computer networks. LT codes are very efficient as the transmitter does not need any acknowledgement (ACK) from the receiver. The data block file is divided into k equal

length symbols of length l bits and infinite number of encoded symbols of same length l can be generated using these information symbols. Using LT codes, k information symbols can be recovered from any $k + \epsilon$ encoding symbols. The encoding process of LT codes is now provided: the degree d of an encoding symbol is determined and then the degree is chosen randomly from a given node degree distribution where d distinct information symbols at random are chosen uniformly and these are the neighbours of the encoding symbol. XOR operation is assigned to the chosen d information symbols to have encoding symbol. Moreover, the degree distribution $P(x)$ comes from the fact that we can draw a bipartite graph as shown in figure 2.12 that consists of the information symbols as variable nodes and the encoding symbols as factor nodes. The degree distribution of LT codes determines their performance as explained in [81].

Now the decoding process is described: A decoder needs to know the neighbouring nodes of each encoding symbol. The information can be transmitted in several ways, one way is that the encoder and decoder share a random number generator seed, and the decoder obtains the neighbouring node of each encoding symbol by generating the random linear combinations that are synchronized with encoder. The encoding symbols of degree one, i.e., the nodes which are connected to one information symbol are released to recover their unique neighbour. The released encoding symbols are then helpful to recover other neighbour information symbols. One by one information symbol is chosen to be processed, the edges connecting to the information symbol to its neighbour encoding symbols are removed and the value of each encoding symbol changes according to the information symbol. The decoding process is continued by iterating the above procedure. The decoding process completes if all information symbols are recovered at the end. For example, any received encoding symbol can recover the associated information symbol but if the encoding symbol is erased, the associated information symbol cannot be recovered. In order to prevent the failure, the transmitter have to send more encoding symbols than k to recover the erased information symbol and this distribution leads to extra encoding symbols.

Raptor codes are the extended step of the LT codes [82]. For LT codes, the decoding complexity increases as k becomes large. Raptor codes have linear time encoding and decoding complexity. These codes have first pre-coding of the source symbols by an appropriate fixed erasure code, LDPC for example. Raptor codes are the first known class of fountain codes with linear time encoding and decoding. Raptor codes give a significant the-

oretical and practical improvement over LT codes. A symbol can be of any size from single byte to hundreds of bytes. The probability that the message can be recovered increases with the number of symbols received above k and becomes very close to one.

2.5 MAC Protocols

In order to use the spectrum efficiently various MAC protocols have been proposed. These protocols are used for multiple secondary Spectrum access that allows users to access the spectrum by deciding which user will access the channel for a given time. There are three categories of MAC protocols: Random Access Protocols, Time Slotted Protocols and Hybrid protocols. *Random Access Protocol* is one of the most important, simple and widely used protocol for local area networks. In this protocol the successful transmission is not guaranteed and when two transmissions are done at the same time the collision occurs.

The access for each cognitive user is random and there is no need of time synchronisation. *Time slotted protocol* needs the synchronisation for whole network where time is divided into slots and these slots are assigned to control channels and to data transmission for each user. *Hybrid protocol* is the combination of Random Access and Time slotted protocol. The control signals occur using synchronised time slots while the data transmissions are done using random access schemes.

2.5.1 Random Access Protocols

Random access protocols are famous due to their use for local area networks. As mentioned earlier, the successful transmission is not guaranteed due to the random access operation as the transmission is initiated without negotiation with other transmissions. As the result of two simultaneous transmissions, the collisions occur and to recover the lost data either retransmissions of data or erasure correction codes are used. The retransmissions are done randomly by choosing another slot time in order to further avoid collisions. We will now review various random access protocols including Aloha, Antijamming coding, Carrier Sense Multiple Access with collision detection (CSMA/CD), and Carrier Sense Multiple Access with collision avoidance (CSMA/CA).

2.5.1.1 Aloha

There is no longer a primary/secondary classification of users in Aloha protocol [83, 84] and there is no sensing : every user chooses randomly a number of slots within a frame,

as a consequence there is no cooperation and no sensing between the users. These is the possibility of collisions, they are recovered using erasure correcting codes. This approach augmented with a coarse sensing could allow a more aggressive and more effective use of the spectrum, with more collisions than with CSMA/CA, but these collisions could be recovered.

This was the first random access protocol known as Aloha introduced by Abramson and his colleagues in 1970 at the University of Hawaii [85]. The protocol was developed to have communication among several stations for wireless communication. All stations share the same radio channel and when the data is ready for transmission by any station, it starts transmission. When two or more stations start transmission simultaneously, collision occurs. The collided data frame are then retransmitted at randomly chosen time. The operation of an Aloha protocol can be described by a finite state machine.

The traffic load of each station can be represented by the arrival rate λ, the retransmission traffic is represented by r, and the total data rate of each station for Aloha system becomes: $g = \lambda + r$ frames/sec. To estimate the performance of Aloha system, it is required to chose a real traffic model and the retransmission model. Poisson process is chosen for the data transmissions of all stations for Aloha system. The arrival rate of Poisson process is λ data frames per second and the collided data frames are retransmitted at large time in future. It is assumed that the numbers of stations in the network are infinite and each station has at most one data frame in its buffer to transmit. Furthermore, the retransmission lag time can be approximated by Poisson process.

Suppose the transmission time for each data frame is T starting at time t either by load traffic or by the retransmission of station. The data frame will have no collision if no other data frame is transmitted at the same time. If the total load and retransmission traffic is done using Poisson process with arrival rate g frames/sec, then the arrival of n stations during time $2T$ is given by Poisson distribution [86].

$$P_r\{X = n\} = \frac{(2T.g)^n e^{-2T.g}}{n!} \tag{2.10}$$

Where X is Poisson random variable. For successful transmission, no other station starts its transmission if any station is transmitting. Therefore, by putting $n = 0$ in above equation, the probability of success transmission can be calculated as:

$$P_{success} = P_r\{X = 0\} = \frac{(2T.g)^0 e^{-2T.g}}{0!} = e^{-2T.g} \tag{2.11}$$

The above equation gives the arrival rate of the total traffic as g frames/sec and the rate of successful traffic then becomes: $g.P_{success}$. The throughput can be calculated in frames for the given time duration T using the following equation.

$$S = g.P_{success}.T = gTe^{-2gT} \tag{2.12}$$

Introducing $G = gT$ the equation is further simplified as:

$$S = Ge^{-2G} \tag{2.13}$$

An improved version of Aloha was performed by Roberts [87], he divided the time into discrete intervals called slots. In this scheme all stations are synchronised and they start their transmission at the beginning of slot. This scheme is known as slotted Aloha. The throughput of this modified version of Aloha is given by following equation.

$$S = Ge^{-G} \tag{2.14}$$

2.5.1.2 Antijamming coding

Antijamming coding technique [17] involves the opportunistic access to the channel but with a PU centred perspective, facing a SU which does not try to avoid collisions with PU but strives for impeding PU transmission by jamming, that is to say aiming at intentional collisions. The perspective is completely reversed in the sense that PU looks for idle part of the spectrum to avoid jamming (aiming also a low probability of detection by the SU), and implements erasure recovery to address the remaining collisions. This techniques involved are quite similar [88] to Opportunistic Spectrum Access.

PU/SU opportunistic access is extended to multiple secondary access and it is a WiFi application when multiple SUs share the same spectral resource. The cognitive radio networks is simulated without applying decentralized MAC slot structure, that is CSMA/CA based MAC and with the addition of erasure recovery the performance of multiple secondary users can be improved in-terms of spectrum re-usability.

2.5.1.3 Carrier Sense Multiple Access with collision detection

Carrier Sense Multiple Access with collision detection (CSMA/CD) is a random access approach used in wired LANs. The sensing is performed before transmission by a station

and the same time station is able to detect the collision in case it occurs. As soon as the station detects the collision, it quits the transmission in order to reduce the collision time. The retransmissions are then performed using future time slots. To detect the

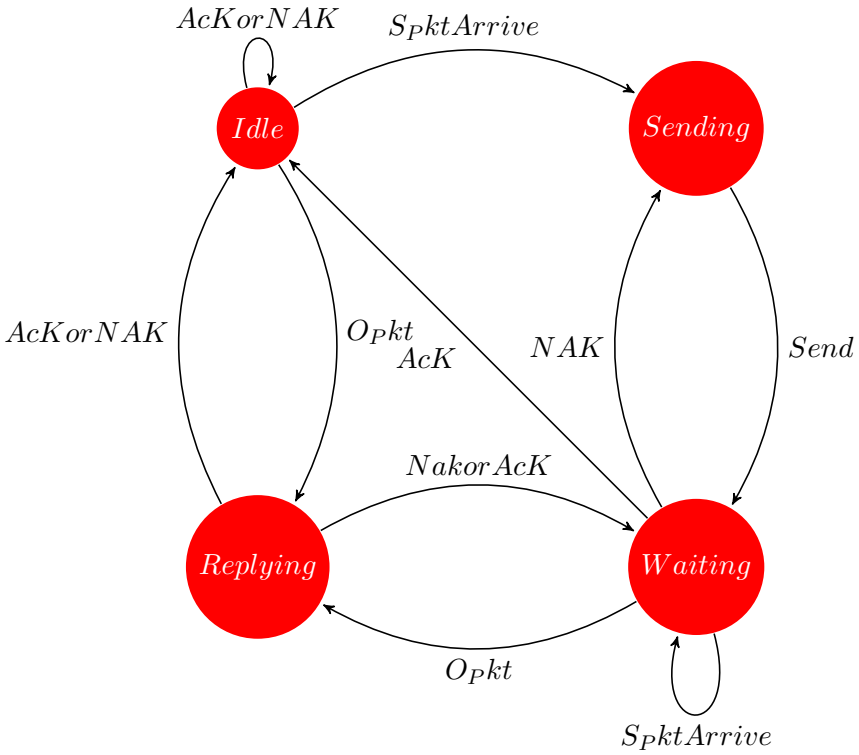

Figure 2.13: The State machine of MAC Layer

collisions each station contains an interference detector while transmitting the data frame, the station also detects the signal at broadcast channel and if the detected signal is different from the transmitted signal the station decides that the collision has occurred. The station immediately stops the transmission and sends again the collided packets using future time slots.

2.5.1.4 Sense Multiple Access with Collision Avoidance CSMA/CA

IEEE 802.11 working group has chosen the CSMA with Collision Avoidance (CSMA/CA) protocol for wireless LANs. CSMA/CA is a random access protocol that is explained in previous section. This scenario lies under unlicensed spectrum scheme. The interesting example of this scenario is WiFi (802.11af) band when there are multiple secondary users and they access the spectrum using CSMA/CA. This is carrier sense multiple access scheme

with collision avoidance for wireless data communication (e.g., Wireless LAN). In this scheme a node that wants to transmit data has to listen the channel first for a specified amount of time called DIFS in order to decide whether another node is transmitting the data on the channel within the specified wireless range. If the channel is sensed as idle then the node waits for another random amount of time called backoff (BO) in order to avoid the access of multiple nodes at the same time and starts transmission. If the channel is sensed as busy the node has to differ its transmission for random period of time. This use of collision avoidance is used to improve the performance of CSMA by equally dividing the wireless channel and the minimal occurrence of collisions.

The main difference between CSMA/CD and CSMA/CA is the detection of collisions that cannot be done in radio frequency spectrum as a far transmitter cannot be listened after the transmission because of huge difference of power with respect to the sent signal (there is a huge attenuation between the other node and sender node and this difference is several tens of dBs). Therefore, CSMA/CA scheme is used in 802.11 based wireless LANs and many other wireless communication systems. Another issue related to wireless data transmission is that it is not possible to listen while transmission of data and the hidden node may also cause a interference problem.

Interaction between Physical and MAC Layer should be independent of the hardware in order to have better performance. In order to achieve the MAC layer independent of hardware, the interactions between physical and MAC layers must be figured out. Normally, there are two kinds of interactions between PHY and MAC layers as shown in figure 2.13: control messages, such as carrier sense multiple access with collision avoidance; packet messages, such as down stream and upstream of packets. **Control Interaction** MAC layer has to know the channel status as it has to control the multiple access of various nodes in order to avoid collisions. It is therefore necessary that the PHY layer must update the carrier sensing statistics (CSS) to MAC layer. **Packet Interaction** MAC layer needs to send down stream packets to PHY layer and receive up streams packets from PHY layer. When the packet is transmitted to the PHY layer, an ACK timer is initialized, the retransmission of packet is required if the timer expires.

MAC Layer Parameters are based on given 802.11 protocol. In this protocol, the sending node has to wait for the channel to be in idle state continuously for DIFS time. If the channel is busy or the DIFS is interrupted, then the node has to wait for DIFS again. Once the channel becomes idle, the node then selects random backoff (BO) timer in order

to avoide the multiple access at the same time. Each node selects a random waiting time within the range of contention window.

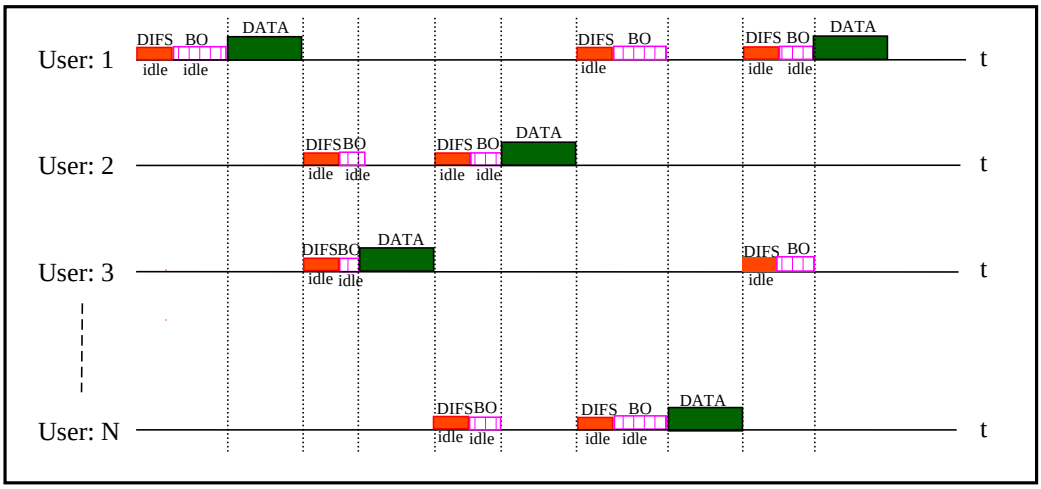

Figure 2.14: Multi Users Access Using CSMA/CA

If the random BO timer is interrupted then the BO is paused and when the channel becomes free again, it is resumed. The transmission of data is started afterwards. The ACK is sent to transmitter on successful receiving the packet. To send the ACK, the node waits only for SIFS time without interruption and the ACK can be sent without backoff. As the probability of choosing the same BO by two nodes is very small, the collisions between packets are minimized.

The state transition diagram of MAC layer is shown in figure 2.13. It has four states which are, idle, sending, replying and waiting. Sending and replying states are instantaneous that means the MAC layer stays on these states when it is either sending the packet or replying ACK. MAC layer stays on waiting state when it sends a packet but do not receive an ACK. The MAC layer stays at the idle state when initialized and also in the similar state after sending the packet and after receiving the ACK. **Transmission and Reception Flow of MAC Layer** using CSMA/CA must be presented.

The transmission flow of MAC layer is shown in figure 2.15. From the transmitting and receiving flow chart, it is clear that there are two waiting states: DIFS time without interruption and backoff (BO) time without interruption. If the backoff timer is interrupted it is paused and wait again for the channel to become idle, when the channel becomes idle, it is resumed again. After receiving the data, the receiving node checks if the packet is received

without error if yes then it waits for SIFS time and sends ACK to the transmitter. The spectrum access of multiple user using CSMA/CA is graphically described in figure 2.14. It is clear that each user has to wait DIFS and BO time before starting its transmission. The probability of waiting time will increase as the number of users of a shared resource increases. The most of time then will be used in detection of spectrum. **Throughput**

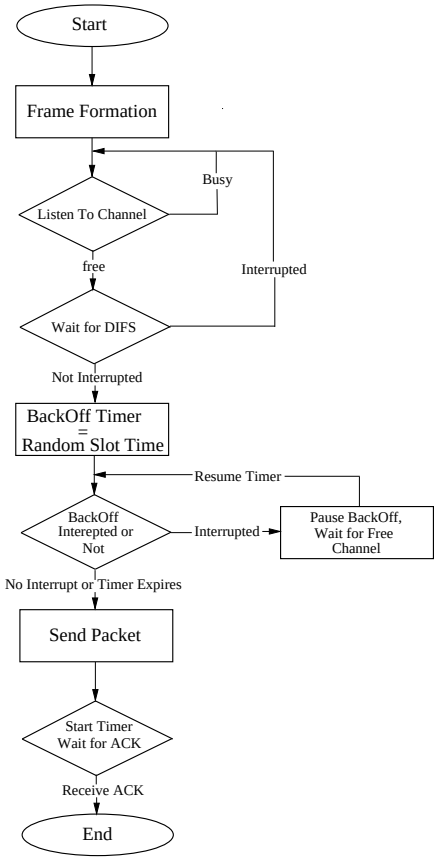

Figure 2.15: Flow Chart of usual CSMA/CA

analysis of CSMA/CA is described in [89]. Suppose τ is the maximum signal propagation delay of the broadcast channel among multiple stations, then the normalized signal propagation time a is defined as:

$$a = \tau/T \tag{2.15}$$

Where T is the data frame transmission time. Suppose the number of stations in the network are infinite and the traffic model is Poisson process. The retransmission time is very long that can be modelled using Possion process and it is independent of load traffic.

Suppose the arrival rate of load and retransmission traffic is defined as G data frames per data frame transmission time. The broadcast channel contains two repeating periods and these are idle and busy periods. The throughput can then be estimated using the following equation:

$$S = \frac{U}{B + I} \tag{2.16}$$

B is defined as the busy period and I as the duration of idle period, $B + I$ denotes the duration of each cycle. B and I are independent random variables and let U is the duration of useful period within a cycle.

2.6 Conclusion

In this chapter the spectrum access schemes are discussed and the Opportunistic spectrum access is described in detail. Various traffic models are described pertaining to opportunistic spectrum access including the On/Off model to generate the activities of primary and secondary user. To solve the problem of synchronisation between primary and secondary user sensing schemes are discussed. Receiver operating characteristic curve (ROC) is then described that gives a relationship between sensing impairments. Binary erasure channel is explained with various binary linear codes. Finally, the MAC protocols are reviewed including random, time slotted and hybrid protocols. Random Access Protocols are further explained and the CSMA/CA scheme is described that is being used for wireless LAN when there are multiple secondary/cognitive users.

Chapter 3

On the Decoding of Erasure codes and Performance measures

Contents

3.1 Introduction

In this chapter we address the decoding of erasure correcting codes to overcome the erased data due to collisions. We focus on short codes by taking advantage that their performance can be greatly improved by a proper choice of the parity check matrix. The

Tanner graph based decoding for short erasures codes is described in detail explaining how iterative erasure recovery is done to recover lost data packets. It is also explained in the chapter that all erased packets cannot be recovered and it is explained how the performance of erasure codes can be enhanced. The Tanner graph based decoding with usual and extended $\mathbf{H}$ matrix is computed and it is compared with the Exhaustive search approach for various short codes. The concatenation of short codes to construct more efficient codes is then described; for example concatenation of single parity check (SPC) codes form Single Parity Check Product (SPCPC) codes that are more powerful in-terms of erasure recovery with less encoding and decoding complexity is demonstrated. The analytical bounds for SPCPC to estimate their performance are computed and these analytical results are then compared with the simulations across various input erasure probability. The last part of the chapter is about Viterbi decoding for erasures. It is a modified Viterbi decoding that operates on erasures and it is described with examples. The decoding techniques including Tanner graph, Exhaustive search and Viterbi are then compared using various examples.

The rest of the Chapter is organised as follows: Section 3.2 describes the basic properties of codes, Binary Erasure Channel and Tanner graph based decoding of short codes in detail. It gives the iterative erasure recovery method to recover the lost data in terms of packets at the receiver without retransmission. Section 3.3 explains how the Tanner graph based decoding can be improved by increasing the number of parity check equations. The performance obtained for various codes with usual and extended $\mathbf{H}$ matrix is then compared with Exhaustive search based approach in this Section. 3.4 describes the construction of SPCPC codes and their decoding. Section 3.5 gives the detail on Viterbi decoding when dealing with erasures and section 3.6 concludes the Chapter.

3.2 Binary Erasure Channel (BEC) and codes

We are dealing with erasure channel whose properties are given in detail in the previous chapter. We now provide some basic properties of short codes for erasure channel. If we suppose two codewords $\mathbf{x}, \mathbf{y} \in \mathcal{C}$ having $k+i$ equal components, then their Hamming distance would be equal to $d(\mathbf{x},\mathbf{y}) \leq n-(k+i) < d$, which is impossible unless $\mathbf{x} = \mathbf{y}$. It means that given $k+i$ **exact** components of $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1}) \in \mathcal{C}$ then we should be able to recover $\mathbf{x}$ uniquely[1] and that it is theoretically possible to correct $n-(k+i) =$

[1] at least by an Exhaustive search over all codewords

$d-1$ erasures. Erasure correcting codes for opportunistic spectrum access were introduced in [90–92] with LT codes [79] as a solution for their recovery. These codes provide a convenient solution for delay insensitive traffic, such as streaming of multimedia data to a number of users experiencing various erasures, because they avoid acknowledgements and retransmission of data. They are generally long; for instance [91] provides simulation results for $K = 6000$ information packets (that is to say before coding). In this chapter we show that much shorter binary block codes can be envisioned for the erasure recovery. In fact any classical code (BCH or Golay codes, to name a few) can be used, for several reasons:

- Good codes of short length are well known for a long time, in particular their minimum distances are generally tabulated[2], and it is the relevant parameter for the erasure capacity of the code.
- Their Tanner graph based decoding for erasure correction is very easy to implement as it involves only XOR-ing of packets. Furthermore, since the work of Schwartz and Vardy [2] we know that it is possible to improve their erasure recovery capacity by introducing new parity check equations.
- The algorithm can be easily implemented by software, and working with small codes requires less memory and a lower CPU usage.
- The advantage of using short erasure correcting codes is their lower latency as compared to the latency of long codes.

3.2.1 Tanner graph based decoding

Tanner graphs are bipartite graphs that are used to perform erasure correction and are based on a graphical representation of the parity check matrix of the code. The nodes of the graph are separated into two distinctive sets and edges which are only connecting nodes of two different types. The two types of nodes in a Tanner graph are called variable nodes (v-nodes) and check nodes (c-nodes).

In fact, Tanner graphs provide a complete representation of the code and help to describe the decoding algorithm. For instance figure 3.1 depicts the Tanner graph associated to the

[2]Several tables of binary block codes parameters are available online, see for instance `http://www.codetables.de/` and links therein

following parity check matrix of the (7,4) Hamming code:

$$\mathbf{H} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \tag{3.1}$$

The first equation of the Tanner graph corresponds to the first row of parity check matrix $\mathbf{H}$, the second equation corresponds to the second row of $\mathbf{H}$ matrix and last equation corresponds to the third row of parity check matrix $\mathbf{H}$.

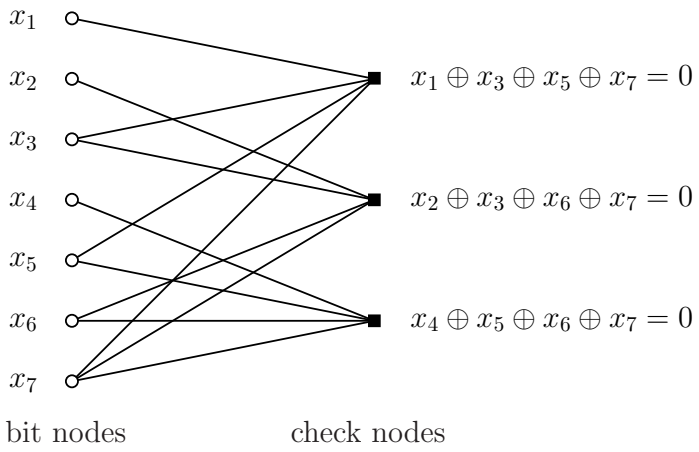

Figure 3.1: Tanner graph of the Hamming(7,4) code

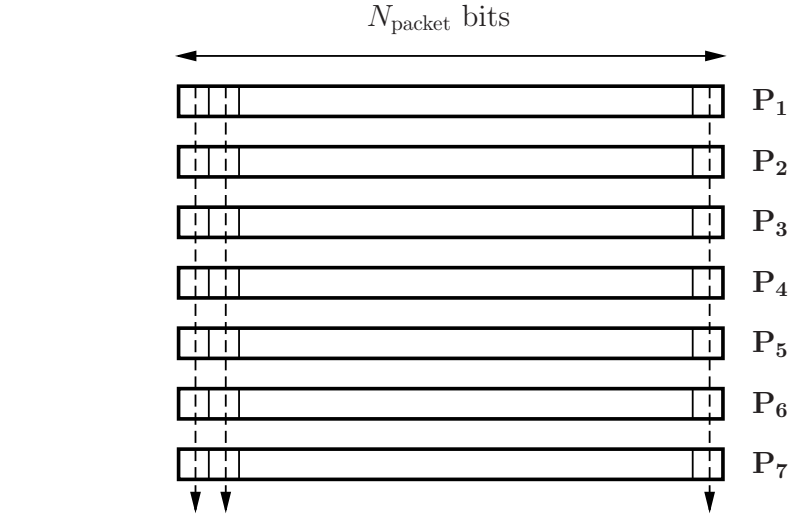

Figure 3.2: From bits to packets

The same Tanner graph based algorithm can be applied when dealing with packets rather than bits, with the difference that parity check equations involve now XOR-ing of packets; for instance, the first parity check equation becomes $\mathbf{P_1} \oplus \mathbf{P_3} \oplus \mathbf{P_5} \oplus \mathbf{P_7} = \mathbf{0}$ where $\mathbf{P_1} \ldots \mathbf{P_7}$ are such that the ensemble of the ith bits $i = 1 \ldots N$ of each packet is a codeword of the Hamming code as described in figure 3.2.

Iterative erasures recovery scheme using Tanner graph based decoding is now explained to recover the erasures. Suppose that two packets are lost in the codeword as shown in the figure 3.3, this scheme is described using Tanner graph. The missing packets are $\mathbf{P_1}$ and $\mathbf{P_3}$. It is clear that the packet $\mathbf{P_1}$ cannot be recovered as two packets are missing in the parity check equation: $\mathbf{P_1} \oplus \mathbf{P_3} \oplus \mathbf{P_5} \oplus \mathbf{P_7} = \mathbf{0}$.

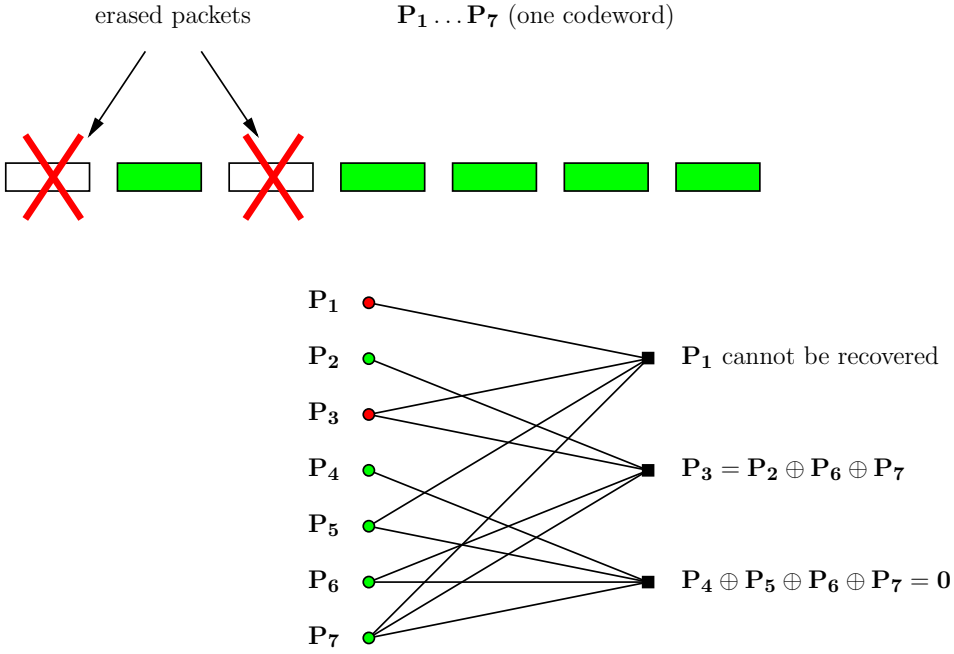

Figure 3.3: Erasure Recovery Step 1

First, $\mathbf{P_3}$ is recovered using the parity check equation $\mathbf{P_2} \oplus \mathbf{P_3} \oplus \mathbf{P_6} \oplus \mathbf{P_7} = \mathbf{0}$ by XORing all other packets as shown in figure 3.4. As if one packet is missing, all other packets can be corrected by single XOR operation.

Now $\mathbf{P_1}$ can be recovered easily using the parity check equation $\mathbf{P_1} \oplus \mathbf{P_3} \oplus \mathbf{P_5} \oplus \mathbf{P_7} = \mathbf{0}$ as shown in figure 3.5 by XORing all other packets, as there remains only one missing packet in the parity check equation.

There are some erasure patterns which are non recoverable. The phenomena is explained

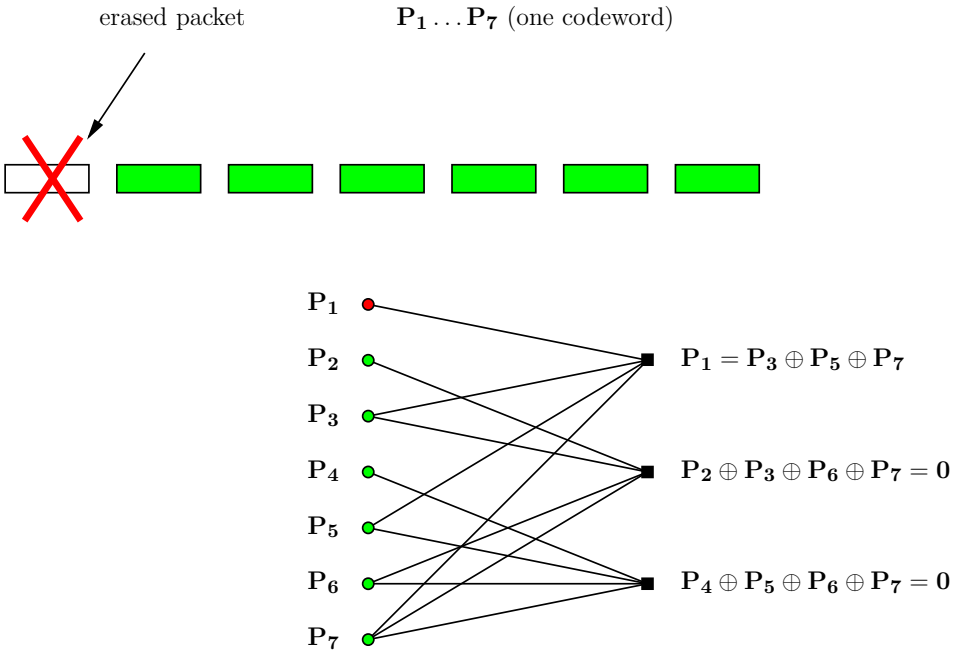

Figure 3.4: Erasure Recovery Step 2

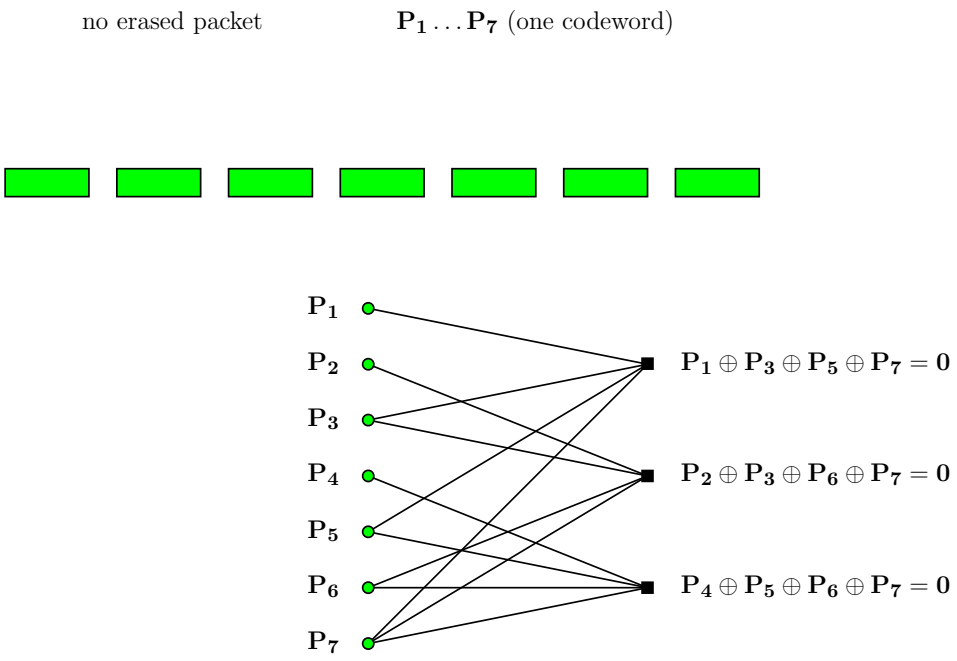

Figure 3.5: Erasure Recovery Step 3

as follows: let $\mathcal{E}$ be an array recording erased positions and $\mathcal{E}$ is of size $1 \times n$:

$$\mathcal{E}(i) = \begin{cases} 1 & \text{, if position } i \text{ is erased} \\ 0 & \text{, otherwise} \end{cases}$$

Index vector records the number of erased positions of the parity check equation. We can record all such indexes in a vector $\mathbf{I} = \mathbf{H}\,\mathcal{E}^t$ (with ordinary arithmetic) whose integer components can take the following values:

- $\mathbf{I}_j = 0$ when there is no erased bit in parity check equation j.
- A parity check equation with index $\mathbf{I}_j = 1$ contains only one erased position which can then easily be recovered.
- When $\mathbf{I}_j > 1$ there are at least two erased positions involved in the parity check equation j, no recovery is possible.
- If the index vector $\mathbf{I} \neq \mathbf{0}$ has no component equal to 1 no parity check equation contains only one erased position so that the erasure recovery fails. Such error pattern is called a stopping set. As a consequence, any codeword is a stopping set since $\mathbf{H} \cdot \mathbf{x} = \mathbf{0}$, which implies that none component of the syndrome can be odd before the modulo 2 operation.

It is unfortunately difficult to determine if an initial erasure pattern will cause a decoding failure because ending up in a stopping set, so that we cannot compute the probability of such an event.

A parity check equation with index 1 contains only one erased position that can be recovered. For example when $d \geq 3 \Rightarrow$ all erasure patterns of size 1 or 2 are recoverable, suppose $\mathcal{E} = (0 \ldots, 1, 0 \ldots)$ is a non recoverable pattern with only one erasure at position i. The index vector can only be $\mathbf{I} = \mathbf{0}$ so that $\mathcal{E}$ is a unit weight codeword, which contradicts $d \geq 3$. Likewise, if $\mathcal{E} = (0 \ldots, 1, 0 \ldots, 1, 0 \ldots)$ is a non recoverable erasure pattern with erased positions i and j then $\mathbf{I}$ has components 0 or 2 and $\mathcal{E}$ is also a weight 2 codeword, which contradicts $d \geq 3$.

The **stopping set** is defined as the index vector $\mathbf{I} \neq \mathbf{0}$ having no component equal to 1, no parity check equation contains only one erased position and the erasure recovery fails. Any codeword is a stopping set if $\mathbf{H} \cdot \mathbf{c}^{\mathbf{T}} = \mathbf{0}$ that implies none component of the syndrome can be odd before modulo 2. **Dead end sets enumerators** is the enumeration of all erasure patterns that cannot be recovered and the algorithm fails on a smaller pattern which is not recoverable. Non recoverable means there is no more parity check equation with only one erased position. As working with small codes an Exhaustive search is performed oven n patterns with 1 erasure, $\frac{n(n-1)}{2}$ patterns with 2 erasures, $\binom{n}{3}$ patterns with 3 erasures,

.... **One variable enumerator** is described as:

$$T(x) = \sum_{i=0}^{n} T_i \, x^i$$

Where T_i is the number of non recoverable erasure patterns of size i and the probability of an erasure pattern of size i is $p^i(1-p)^{n-i}$. The value of enumerator T will depend on the decoding method. For Tanner graph based decoding when using **H** matrix of erasure code we denote it as T while for extended **H** matrix we denote it as $T_{ext}(x)$ and when the decoding method is based on Exhaustive search we denote it as T_{exh}. The erasure recovery performance of Tanner graph based decoding is higher when using extended parity check matrix **H** while the erasure recovery performance is maximum when using Exhaustive search method and it provides the upper limit for any decoding scheme.

For T_i, the word erasure rate (WER) is simply obtained as:

$$WER = \sum_{i=0}^{n} T_i \, p^i (1-p)^{n-i} \tag{3.2}$$

The expression for **two variable enumerators** [42] is obtained as follows:

$$T(x,z) = \sum_{i,j=0}^{n} T_{i,j} \, z^j x^i$$

where $T_{i,j}$ is the number of non recoverable erasure patterns of initial size i and final size j. In fact T_i can be written as

$$T_i = \sum_{j>0} T_{i,j}$$

where as:

$$\frac{1}{n} \sum_{j>0} j \, T_{i,j}$$

is the mean number of residual erased bits after decoding. The final bit erasure rate BER can be calculated as:

$$BER = \frac{1}{n} \sum_{i \geq 0} \left\{ \sum_{j>0} j \, T_{i,j} \right\} p^i (1-p)^{n-i} \tag{3.3}$$

For optimal decoding an Exhaustive search is done but that is practicably possible only for very small length codes as the time complexity will increase dramatically as the length of code increases. Therefore, Tanner Graph based decoding is more practical and with

good parity check matrix it is obvious to get higher decoding performance.

3.3 Non recoverable erasure patterns

The main point is that a binary linear code of minimum distance d would allow the recovery of all erasure patterns of size $1, 2, \ldots, d-1$. Some simple examples show that decoding on the usual Tanner graph does not obey this property for $d > 3$. To this end, by taking advantage that we are working on small length codes, we have performed an exhaustive search of all erasure patterns with 1 erasure, all $\binom{n}{2}$ patterns with 2 erasures, all $\binom{n}{3}$ patterns with 3 erasures, ... and count those not completely recovered by the decoding algorithm (the algorithm fails on a pattern which is not recoverable).

3.3.1 Comparison of Tanner graph with Exhaustive search

We take as example a short code(10,5,4) that has minimum distance $d = 4$ and perform Tanner graph based decoding with usual parity check matrix $\mathbf{H}$ and with extended parity check matrix $\mathbf{H_e}$. The usual parity check matrix is given:

$$\mathbf{H_0} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

The corresponding enumerator using equation (3.2) after performing Tanner graph based decoding is given by:

$$T(x) = 2x^3 + 29x^4 + 125x^5 + 210x^6 + 120x^7 + \ldots$$

It turns out that there are two non recoverable erasure patterns of size three, which is the contrary to what can be expected ($d - 1 = 3$). Erasure recovery performances are given with curve labelled H_0 and with curve labelled H_1 (for extended H_e matrix) using WER and BER in figure 3.6

3.3.1.1 Addition of extra parity check equations

Since the work of Schwartz and Vardy [2], we know that adding redundant parity check equations to the H matrix allows to recover all erasure patterns of size up to $d - 1$, for some strongly structured codes (Reed-Muller, Golay) at least. We consider for example the

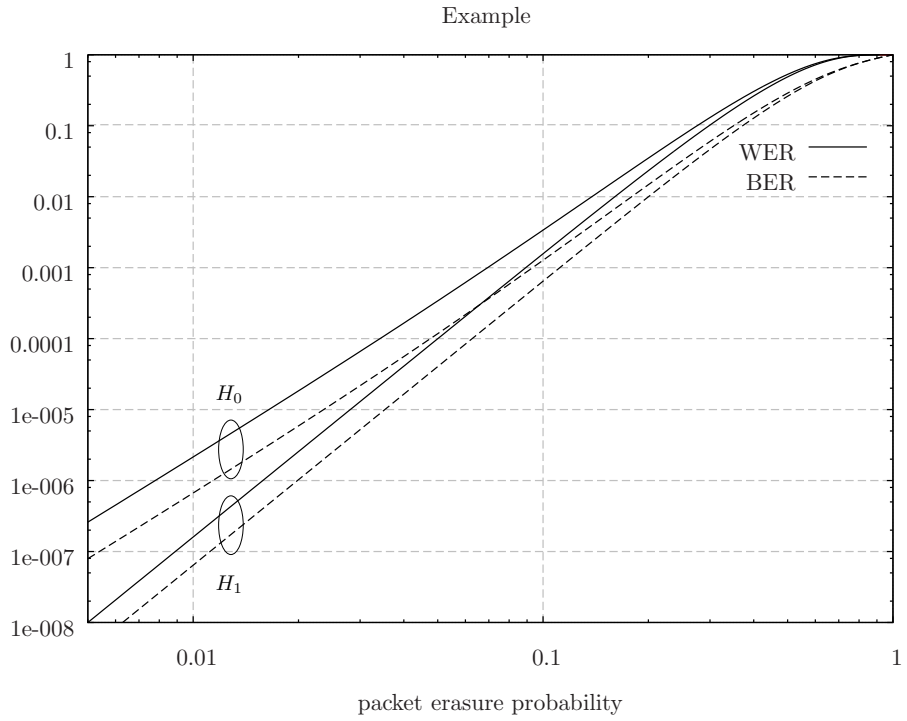

Figure 3.6: Example of erasure correction performance for short code (10,5,4)

Hamming(7,4) code with parity check matrix (3.1), with the erasure pattern:

$$\mathcal{E} = (1, 0, 0, 0, 1, 1, 1) \Rightarrow \mathbf{I} = (3, 2, 3)$$

There is no equation with one erasure and the iterative algorithm should stop here. If we add the two last rows of $\mathbf{H}$ we obtain a new parity check equation (of the same code):

$$x_2 \oplus x_3 \oplus x_4 \oplus x_5 = 0$$

. There is now only one erased position in this equation (x_5), and we can recover it by $x_5 = x_2 \oplus x_3 \oplus x_4$. We cannot go farther because the new index vector is $\mathbf{I}' = (2, 2, 2)$; $\mathcal{E}$ is a codeword, the algorithm stops. The process is described in Fig. 3.7 where red dots indicate erased packets and green dots are received or recovered packets. We now continue of apply the Tanner Graph based decoding on the extended parity check matrix $\mathbf{H}$ of Hamming code(10,5,4). Rows of the usual parity check matrix of a given code $\mathcal{C}$ are the basis vector of its dual code, they are therefore independent. We now consider an extended parity check matrix containing the original basis vector and all possible combination of two of them, we

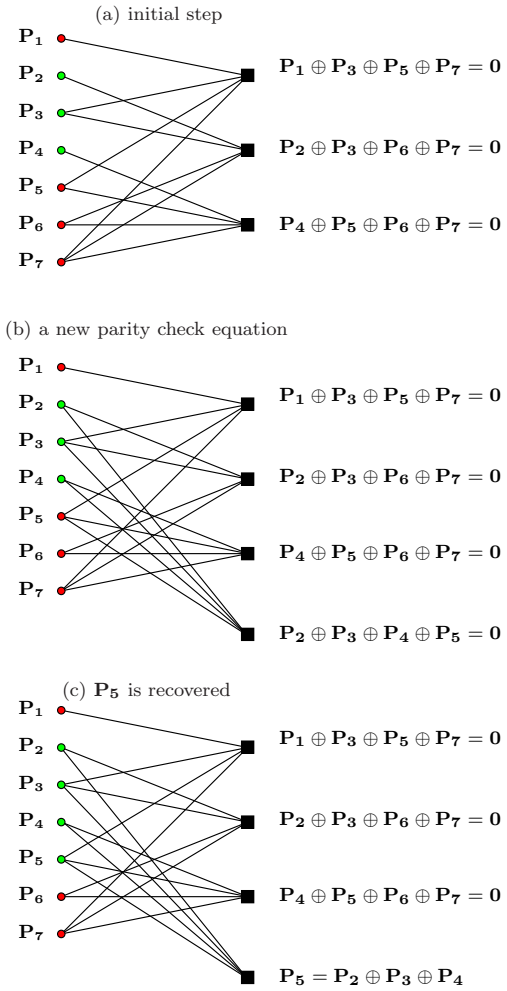

Figure 3.7: Introducing a new check equation allows recovery of packet $\mathbf{P_5}$

obtain a matrix with $5 + \binom{5}{2} = 15$ rows:

$$\mathbf{H_1} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

The corresponding two variables enumerator is now given by

$$T_{ext}(x) = 16x^4 + 100x^5 + 210x^6 + 120x^7 + \dots$$

All erasure patterns of size up to $d - 1 = 3$ are now recovered, as expected, and the performances are given by curves labelled $\mathbf{H_1}$ using WER and BER in figure 3.6. We observe a small improvement with the code under consideration code(10,5,4) being a toy example.

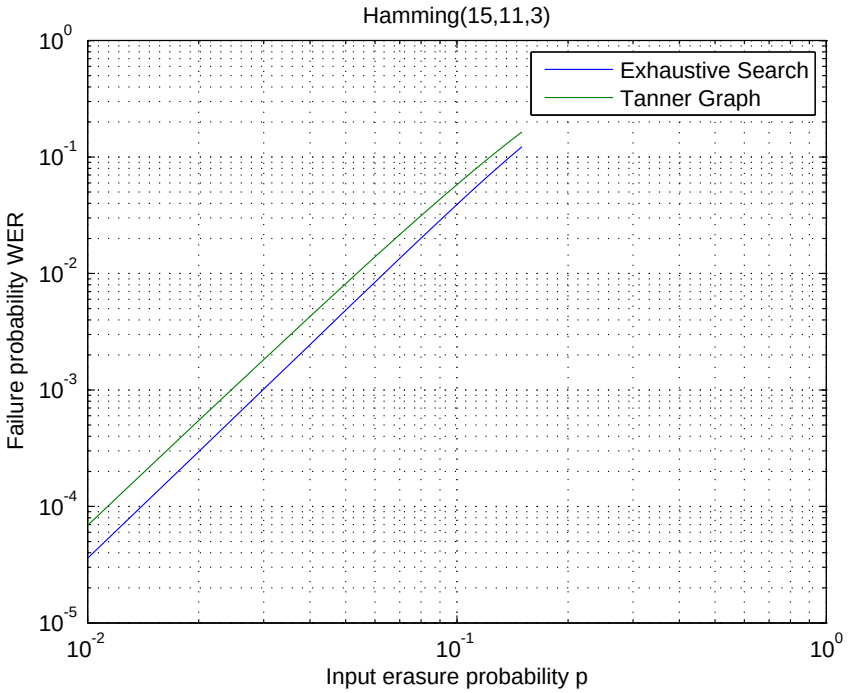

Figure 3.8: Comparison of Exhaustive Search and Tanner Graph based decoding for Hamming(7,4,3) code

Now we use the Hamming code(7,4,3) and perform the decoding using Tanner graph, we observe that all erasure patterns of weight 1 to 2 are recovered as the minimum distance $d = 3$. There are 10 erasure patterns of weight 3, 35 erasure patterns of weight 4, 21 erasure patterns of weight 5, etc,... these patterns are not recovered.

$$T(x) = 10x^3 + 35x^4 + 21x^5 + 7x^6 + x^7$$

If we decode with same Hamming code(7,4,3) at receiver side but exhaustive search, we see that all erasure patterns of weight 1 to 2 are recovered as the minimum distance $d = 3$, while there are 7 erasure patterns of weight 3, 35 erasure patterns of weight 4, 21 erasure patterns of weight 5, etc,... which are not recovered but this is the maximum erasure recovery capability that any decoding method can achieve.

$$T_{exh}(x) = 7x^3 + 35x^4 + 21x^5 + 7x^6 + x^7$$

The comparison of Tanner graph based decoding and Exhaustive search for Hamming(7,4,3)

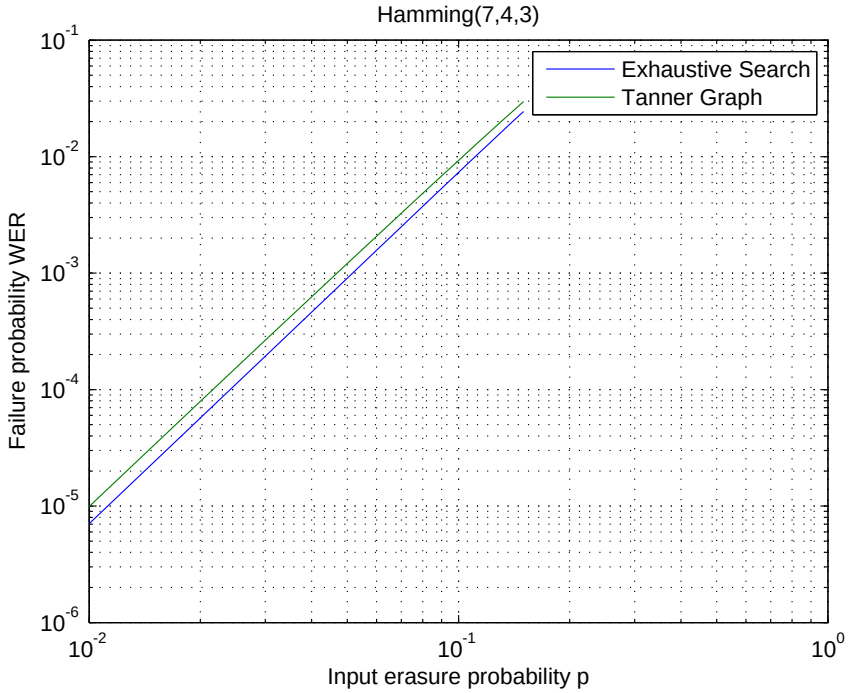

Figure 3.9: Comparison of Exhaustive Search and Tanner Graph based decoding for Hamming(15,11,3) code

code in terms of input erasure probability and failure probability is given in figure 3.8 and it is clear that there is no huge difference in performance. Now we provide the decoding using Hamming(15,11,3) code with Tanner Graph based decoding and compute the dead end set, we will observe that all erasure patterns of weight 1 to 2 are recovered as the minimum distance $d = 3$. There are 69 erasure patterns of weight 3, 822 erasure patterns of weight

4, 3003 erasure patterns of weight 5, etc,... these are non recovered erasure patterns.

$$T(x) = 69x^3 + 822x^4 + 3003x^5 + 5005x^6 \tag{3.4}$$

If we decode the same data using Hamming(15,11,3) code with exhaustive search and compute the dead end set, we will observe that all erasure patterns of weight 1 to 2 are recovered as the minimum distance $d = 3$. The interesting thing to notice is that the weights of non recoverable erasure patters of higher order are reduced, there are 35 erasure patterns of weight 3, 525 erasure patterns of weight 4, 3003 erasure patterns of weight 5, etc,... that are not recovered and this is the maximum erasure recovery capability that any decoding method can achieve.

$$\begin{aligned} T_{exh}(x) = 35x^3 + 525x^4 + 3003x^5 + 5005x^6 + 6435x^7 + 6435x^8 + 5005x^9 \\ +3003x^{10} + 1365x^{11} + 455x^{12} + 105x^{13} + 15x^{14} + x^{15} \end{aligned} \tag{3.5}$$

The comparison of Tanner graph based decoding and Exhaustive search for Hamming(7,4,3) code in terms of input erasure probability and failure probability is given in figure 3.9 and it can be observed that there is no huge difference in performance and Tanner graph based decoding method will be given preference due to lower decoding complexity.

3.3.2 Comparison of Tanner graph with Exhaustive search for Golay(24,12,8) code

We now turn to a much better code and compute the same dead-end-set enumerator of the Golay(24,12,8) code with the initial parity check matrices given in the paper [2], we obtain the polynomial $T(x)$ that is given below.

$$T(x) = 110x^4 + 2277x^5 + 19723x^6 + 100397x^7 + 343035x^8 + \dots \tag{3.6}$$

Several patterns of 4,5,6 and 7 erasures are not entirely recovered, although we have $d = 8$. But if we use extended parity check matrix $\mathbf{H}_e$, the performance of code will definitely increase. Using the extended parity check matrix of the above mentioned paper, $\mathbf{H}_e$ with 34 lines instead of 12, the two-variable enumerator becomes:

$$T_{ext}(x) = 3598z^8x^8 + 82138x^9 + \dots \tag{3.7}$$

All erasure patterns of size up to $d-1 = 7$ are now recovered. Fig. 3.10 shows the huge

improvement in performances when using the extended parity check matrix. For example a channel erasure rate $p = 0.1$ results in a WER equal to 0.01 with the usual parity check matrix and a $2\,10^{-4}$ WER for the extended matrix. We also computed the dead end set of Golay(24,12,8) code with Exhaustive search. We see that all erasure patterns of weight 1 to 7 are recovered as the minimum distance d-1 is 7. There are 759 erasure patterns of weight 8, 12144 erasure patterns of weight 9, etc,... that are not recovered and this is the maximum erasure recovery capability that any decoding method can achieve.

$$T_{exh}(x) = 759x^8 + 12144x^9 + 91080x^{10} + 425040x^{11} + \dots$$

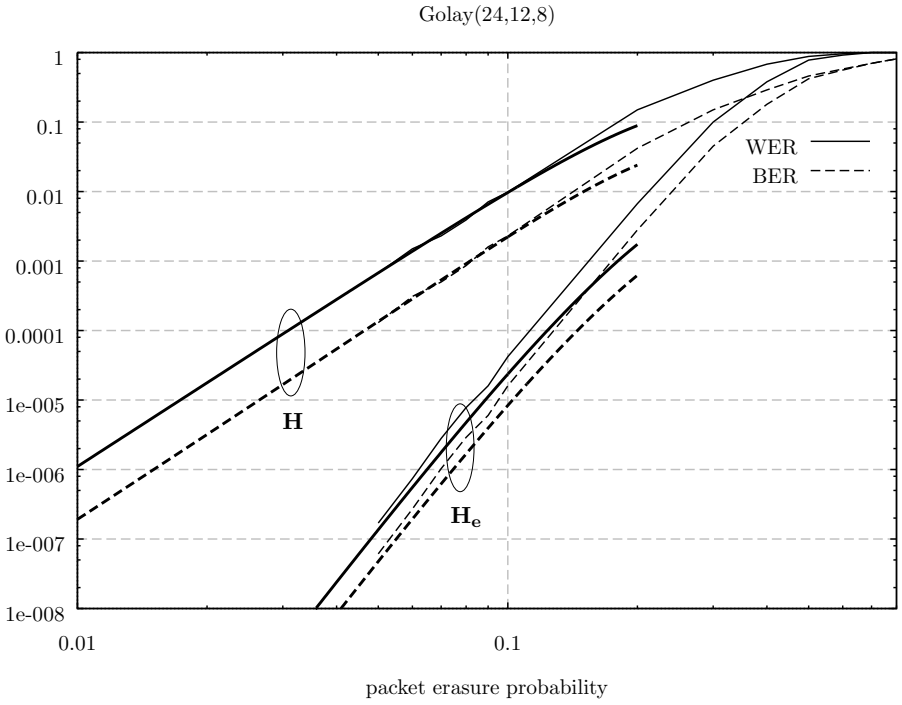

Figure 3.10: Erasure correction performance of the Golay(24,12) code with usual (**H**) and extended ($\mathbf{H_e}$) parity check matrices. Thick lines: analytical values from (3.6) and (3.7), thin lines: simulation results

Equation (3.2) and (3.3) provides a good analytical evaluation of the erasure recovery performance of the code, as depicted in fig. 3.10 where they are plotted with thick lines and simulation results are depicted with thin lines. The approximation is very accurate for channel erasure rate $p \ll 0.1$, and the discrepancy at higher values of p is due to the fact

we do not have the complete enumerator $T(x)$.

The comparison of Tanner graph based decoding and Exhaustive search for Golay(24,12,8) code with usual and extended parity check matrix in terms of input erasure probability and failure probability is given in figure 3.11. It is observed that there is huge difference in performance when using different **H** matrices. Moreover, performance achieved using Exhaustive search based decoding is compared with Tanner graph based decoding and it gives the upper bound for any decoding method. Furthermore, we can plot throughput

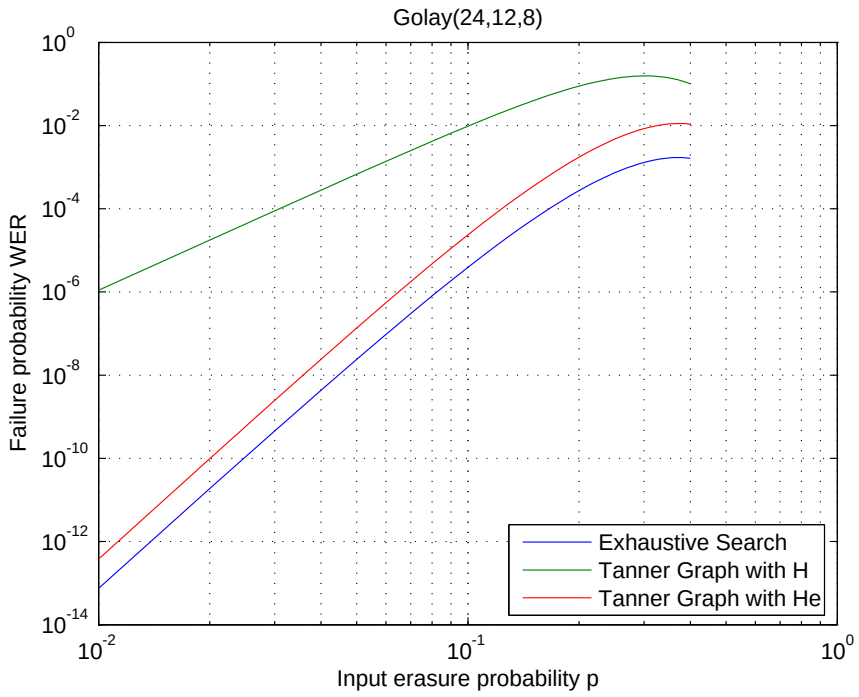

Figure 3.11: Comparison of Exhaustive Search and Tanner Graph based decoding for Golay(24,12,8) code

curves for various short codes and we observe this gain in figure 3.12 where the normalized throughputs (code rate is taken into account) of the two versions of the Golay code are shown: the curve corresponding to the extended matrix $\mathbf{H}_e$ exhibits a better performance than the curve obtained with ordinary **H** matrix. Moreover, a comparison is given with a simple Hamming(15,11) code which provides better throughput for $p < 0.2$ due to a better rate.

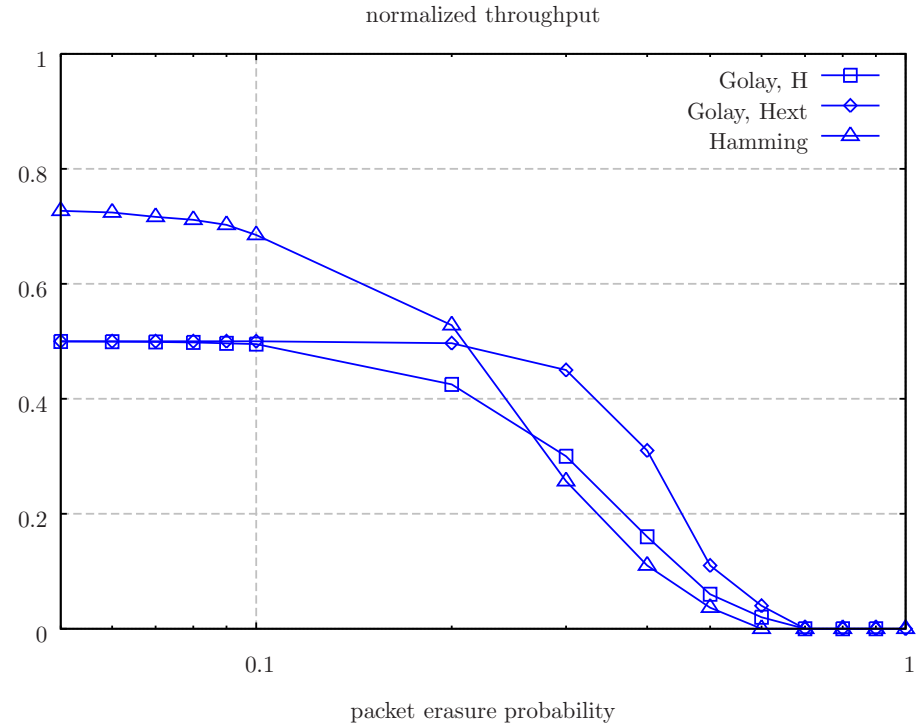

Figure 3.12: Throughput performance using Golay(24,12) code with usual (**H**) and extended ($\mathbf{H_e}$) parity check matrices, and Hamming (15,11) code, simulation results

3.3.3 Erasure recovery performance using BCH(31,21,5) code

Cyclic codes can also be used for erasure recovery and the main advantage of using these codes is their very simple implementation. Moreover, their complete extended $\mathbf{H_e}$ matrix can be obtained very easily that gives an efficient erasure recovery performance using Tanner graph based decoding off course at the expense of higher time complexity. As we work with small to moderate code length, the first few coefficients of the polynomial can be obtained easily, but, in most cases, a complete computation of the enumerator would take too long because of the explosion of the number of erasure patterns to test. We have computed this enumerator for the BCH(31,21) code and obtain:

$$T(x) = 19x^3 + 1304x^4 + 27444x^5 + 271289x^6 + 1593790x^7 + \dots$$

Figure. 3.13 compares prediction using analytical formulas (4.1a) and (4.1b) with simulation results for this BCH code, for $p \leq 0.1$. The discrepancy for greater values of p comes from the fact we have only the first coefficients of the polynomial $T(x)$.

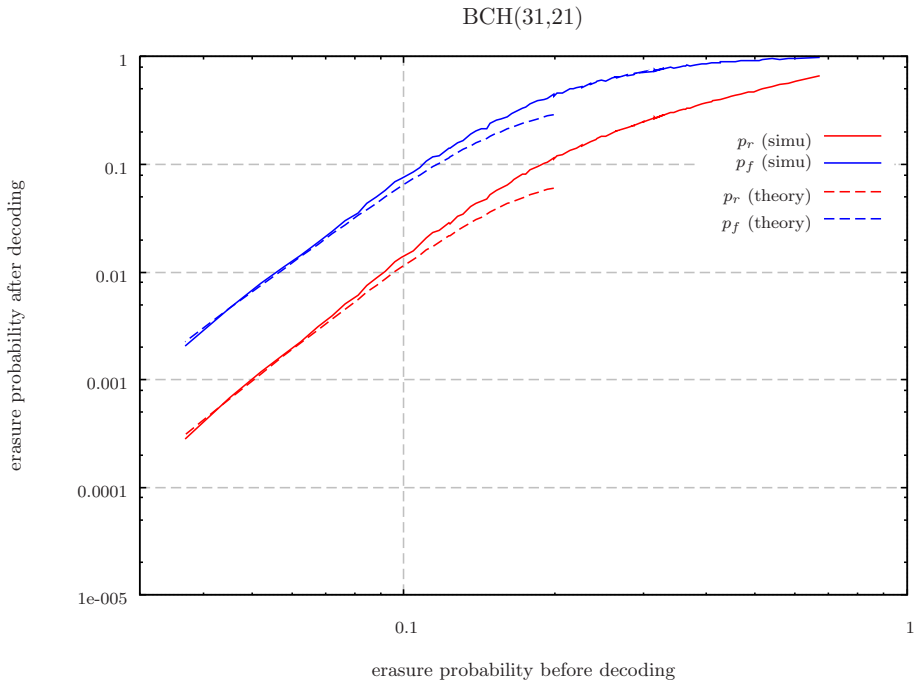

Figure 3.13: Erasure recovery performance of the BCH(31,21) code.

3.4 Single Parity Check Product Codes

We address the use of single parity check product codes (SPCPC) for erasure recovery in opportunistic spectrum access when there is a collision with the primary user due to sensing impairments. The main motivation of using SPCPC is their low decoding complexity. We derive an analytical performance bound for these product codes and give a comparison with simulation results. The main result of the using SPCPC is finding a good functioning point on the ROC curve in terms of spectrum reuse efficiency for the secondary user. Various product codes are compared with respect to their minimum distance, length and erasure recovery capability for different primary user's activity. Single Parity Check Product Codes (SPCPC) are a well known class of codes whose origin can be traced back to Elias [71]. Some decades later Battail reintroduced them in a Gaussian channel perspective [63]. The main interest of this concatenation of Single Parity Check (SPC) codes is, of course, the simplicity of their decoding, especially when using Soft-In-Soft-Out decoding. Quite naturally SPCPC were also considered as an erasure recovery scheme of ATM cells lost in congestions [93], and the SPCPC performance in a binary erasure channel were addressed in [94,95]. This chapter addresses the performance evaluation of Single Parity Check Product Codes (SPCPC)

as an erasure correction scheme to recover data lost during a collision in opportunistic spectrum access [96], [92]. Furthermore, we address the performance of single parity check (SPC) and single parity check product codes (SPCPC) with iterative decoding. Previous coding schemes are generally based on digital fountain codes [91], [97] or on ordinary short binary linear codes (Hamming, BCH, Golay) defined by a parity check matrix [3], [98]. We address the several code related parameters of erasure correcting code $\mathcal{C}(n, k, d)$ of length n, dimension k and minimum distance d:

- the code rate $R = k/n$, is related to the cost to be paid (redundancy) to make possible the erasure recovery.
- the minimum distance d, because it is theoretically possible to recover all erasure patterns of size up to $d - 1$.
- the parity check matrix has indeed an importance in this erasure recovery capacity [2]

3.4.1 Erasure decoding of concatenated codes

The decoding of **Single parity check codes** which are built with the concatenation of **Single parity Check Codes** is described as follows: the k information packets $(\mathbf{I_1}, \ldots, \mathbf{I_k})$ are appended with a parity packet $\mathbf{P} = \mathbf{I_1} \oplus \mathbf{I_2} \oplus \ldots \oplus \mathbf{I_k}$ to constitute a code word.

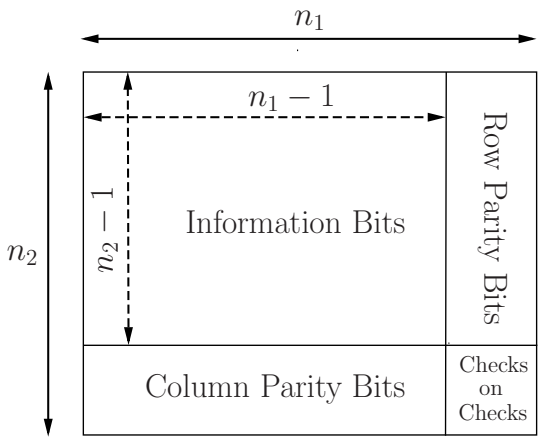

Figure 3.14: Two dimensional product codes matrix

Single parity check SPC$(n, n-1, d=2)$ codes are normally used for error detection as well as for single erasure correction since their minimum distance is $d = 2$. Multiple erasures can be corrected using the serial concatenation of two SPC codes SPC$(n_1, n_1 -$

$1,2)\times\mathrm{SPC}(n_2,n_2-1,2)$ with a very simple decoding procedure. This is a particular case of a general structure called a product code which is an array of data such that rows belong to a (n_1,n_1-1,d_1) code and columns to a possibly different (n_2,n_2-1,d_2) code. The length of this product code becomes $n=n_1n_2$, with a dimension $k=(n_1-1)(n_2-1)$ and a minimum distance $d=d_1d_2$. The block diagram of this product code (n_1n_2, $(n_1-1)(n_2-1)$, d_1d_2) is sketched in Fig. 3.14.

The erasure recovery is simple as it involves only XOR-ing of packets within a same parity check equation. By definition it is a fact that for SPC code, a single erasure is recovered easily by XOR-ing of other packets involved in the parity check equation $\mathbf{I_1}\oplus\mathbf{I_2}\oplus\ldots\oplus\mathbf{I_{n-1}}\oplus\mathbf{I_n}=\mathbf{0}$, where $\mathbf{I_1}\ldots\mathbf{I_{n-1}}$ are the information packets of the codeword and $\mathbf{I_n}=\mathbf{P}$ is the parity check packet. For instance, if it is assumed that packet $\mathbf{I_e}$ is the only erased packet, it can be recovered as follows:

$$\mathbf{I_e}=\sum_{\mathbf{j}\neq\mathbf{e}}\mathbf{I_j} \tag{3.8}$$

When there are two or more erased positions no recovery is possible. The iterative erasure recovery procedure for SPCPC ($n_1\times n_2$, $n_1-1\times n_2-1$, $d_1\times d_2$) can then be explained as follows:

First, row erasure decoding is performed on all rows. For all rows with only one erasure the erased position can be easily recovered by XOR-ing of other packets of the row as described above. After decoding of all rows, the same simple technique can then be applied on the columns of the matrix, so that some residual erasure after row decoding can be recovered thanks to columns decoding. The continuous iteration are then performed on row/column decoding until either there is no residual erasure or a non recoverable erasure pattern is found.

3.4.2 Analytical bounds of SPCPC

In this section we derive simple analytical bounds on the residual erasure rate (i.e. after decoding) of component codes (single bit parity check codes, SPC) or their serial concatenation (single parity check product codes, SPCPC).

In the particular case of SPC it is possible to derive the complete enumerator of constituent codes and the first few coefficients of their product code (SPCPC) analytically. In this very simple case all erasure patterns of size 1 are recovered and all patterns of size 2,3,

...remain unchanged because there is only one parity check equation. It means that the only non zero coefficients are $T_{i,i} = \binom{n}{i},\ i \geq 2$, so that

$$T(x,z) = (1+xz)^n - (1+n\,xz) \tag{3.9}$$

The residual erasure probability for BEC is then given by

$$\begin{aligned} p_r &= \frac{1}{n}\sum_{i\geq 2} i \binom{n}{i} p^i (1-p)^{n-i} \\ &= \frac{(1-p)^n}{n}\left.\frac{\partial T(x,z)}{\partial z}\right|_{x=\frac{p}{1-p},z=1} \\ &= p\Big[1-(1-p)^n\Big] \end{aligned}$$

All erasure patterns of size 1, 2 and 3 are recoverable, and the first non recoverable patterns are a constellation of 4 erasures at the crossing of two lines and two columns, as depicted in fig. 3.15 and also in [95].

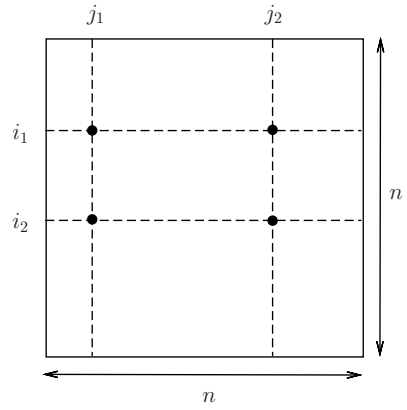

Figure 3.15: General non recoverable 4 erasure patterns

The number of such patterns is $T_{4,4} = \binom{n}{2} \times \binom{n}{2}$.

The five erasure patterns which are not completely recoverable contain a 4 erasure pattern like those depicted in fig. 3.15, the fifth erasure location being chosen among the n^2-4 remaining positions, so that $T_{5,4} = \binom{n}{2} \times \binom{n}{2} \times (n^2-4)$ The residual erasure probability can then be approximated by the following formula:

$$p_r \approx \frac{1}{n^2}\Big\{4\,T_{4,4}\,p^4(1-p)^{n^2-4} + 4\,T_{5,4}\,p^5(1-p)^{n^2-5}\Big\} \tag{3.10}$$

3.4.3 Simulation results

We now validate the developed analytical part by performing simulations. Based on the input erasure probability p for BEC. We plot bit erasure rate BER after decoding. Figure 3.16 shows the analytical and simulation curves. When $p = 2 \times 10^{-2}$, the $BER = 4 \times 10^{-3}$ using SPC (11,10,2) and using SPCPC (11×11, 10×10, 2×2), the $BER = 2 \times 10^{-4}$ after the 1st iteration for erasure decoding. As the number of iterations increase for erasure recovery, the decoding gives reduced value of BER. For example, at 3rd iteration SPCPC (11×11, 10×10, 2×2) used as erasure recovery turns $BER = 2 \times 10^{-5}$. Analytical curves upto 4 and 5 non-recoverable erasure patterns have been plotted using equation 3.10 which give the upper bound for BER after decoding.

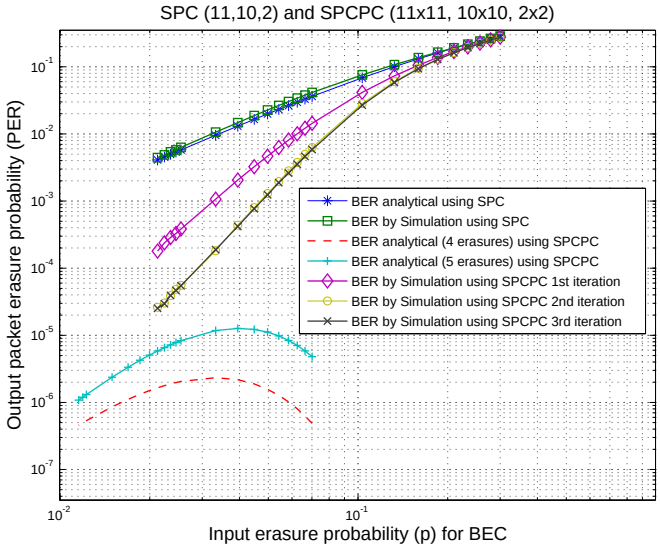

Figure 3.16: Performance of SPC (11,10,2) and SPCPC (11×11, 10×10, 2×2)

Figure 3.17 shows the analytical and simulation curves with $p = 3 \times 10^{-2}$, we notice that $BER = 6 \times 10^{-3}$ using SPC (6,5,2). While using SPCPC (6×6, 5×5, 2×2), the $BER = 1.5 \times 10^{-4}$ after the 1st iteration of erasure decoding. The higher iterations for erasure recovery decoding give the better value for BER. At 3rd iteration SPCPC (6×6, 5×5, 2×2) turns $BER = 3 \times 10^{-5}$. Analytical curves upto 4 and 5 non-recoverable erasure patterns have also been plotted.

Figure 3.18 shows the analytical and simulation curves with $p = 8 \times 10^{-2}$, we notice that $BER = 10^{-2}$ using SPC (3,2,2) which is much better code than SPC (6,5,2). While using SPCPC (3×3, 2×2, 2×2), the $BER = 2 \times 10^{-4}$ after the 1st erasure recovery decod-

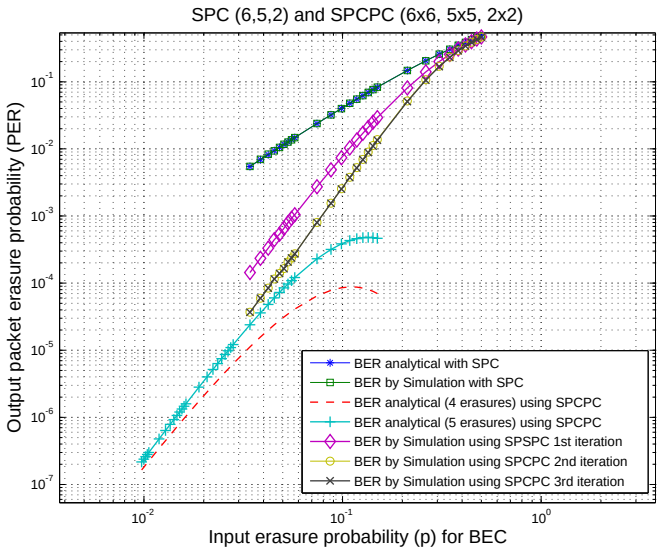

Figure 3.17: Performance of SPC (6,5,2) and SPCPC (6×6, 5×5, 2×2)

ing. After the 3rd iteration using SPCPC (3×3, 2×2, 2×2) achieves $BER = 1.5 \times 10^{-4}$. Analytical curves upto 4 and 5 non-recoverable erasure patterns have been plotted which are upper bound for BER after decoding.

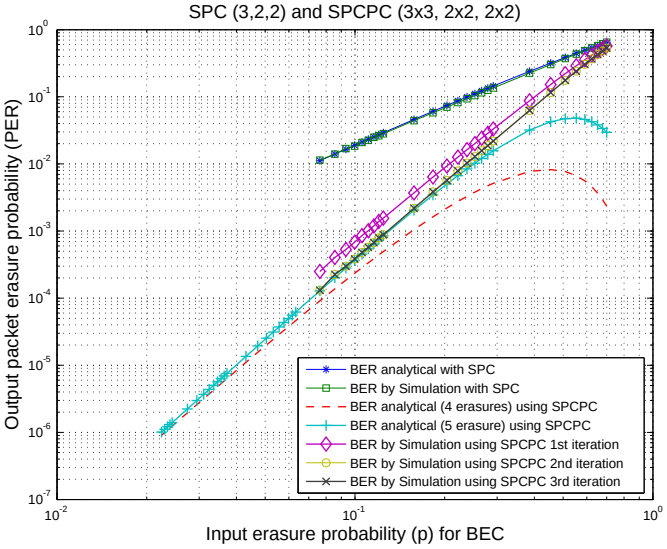

Figure 3.18: Performance of SPC (3,2,2) and SPCPC (3×3, 2×2, 2×2)

3.5 Erasure recovery with Viterbi decoding

Viterbi decoding can be understood using trellis as it is a classical way of representing codes. Trellis is a graph with nodes containing edges between nodes such that we can draw paths which are succession of edges. Suppose there are three edges in the path, then the length of the path is the summation of all these edges. We can draw complete trellis for any given code and it is possible to represent graphically all possible codewords for a given code using H matrix. It is possible to decode the codewords using trellis with Viterbi decoding. The sequence of bits is received at the receiver and decoder needs to determine the best path through trellis. The sequence of bits is received at the receiver and if there is no error then there exist a path through trellis that would match with the transmitted sequence of bits. The classical Viterbi decoder selects the maximum likelihood path that is to say the path with shortest length through the trellis. The Viterbi decoding uses two metrics: the branch metric (BM) and the path metric (PM). The branch metric is the measurement of distance between the transmitted and received bit at trellis edge, it is defined for each branch in the trellis. The value of path metric is associated to the node of trellis and it is computed incrementally using the path metrics of previously computed paths and branch metrics.

Suppose the receiver has computed the path metric PM$[s, i]$ at each path s at time i, the value of PM$[s, i]$ is the total number of erasures detected when comparing the received parity bits to the transmitted bits that have been sent by the transmitter till time step i. Furthermore, among all possible paths at time i, the most the likely path is one with the smallest path metric. If there are more than one such paths then it is decoding failure and the transmitted message cannot be decoded. We are dealing with erasures and we suppose that there are three possible values for any edge and the value of PM$[s, i]$ is calculated based on these values and in fact these can be seen as a log of equation (2.4.1).

$$l = \begin{cases} 0 & \text{if } b = r, \\ 1 & \text{if } r = X(erasure) \\ \infty & \text{if } b \neq r \end{cases}$$

Where b = Value of transmitted bit and r = value of trellis edge. The above equation shows when the received bit is equal to the transmitted bit, the value of trellis edge is zero. When the value of received bit is unknown then the value of trellis edge is written as 1 and when the value of received bit is opposite to the transmitted then the value of trellis

branch is considered as ∞. The value of path metric is computed based on these branch metric values. All possible paths at time step i are computed and most likely path is with the smallest path metric. If there are more than one such paths, we declare this case as failure and assume that the codeword cannot be decoded.

We are dealing with the case when bits are erased in the codeword and it is the modified Viterbi decoding scheme. In this scheme we suppose either the codeword is recovered correctly or it is declared as erased. We consider the case of basic Hamming(7,4,3) code to explain Viterbi decoding using trellis as shown in figure 3.19. We consider the case when there are three erasures in the codeword, bits at position [4,5,6] of the codeword are erased. The Viterbi decoding is now used to decode the transmitted codeword and it is clear from the trellis that there is only one possible path and it is the shortest path. It is, therefore, concluded that the codeword will be recovered for sure for this case of erased bits.

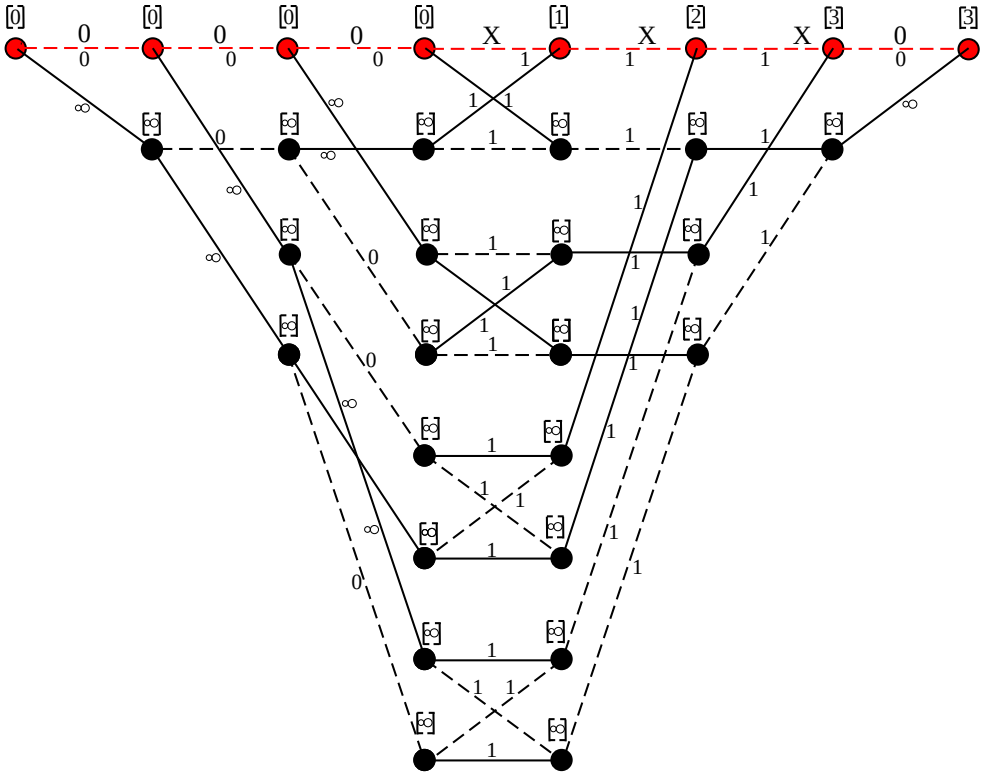

Figure 3.19: Viterbi decoding for three erasures in a codeword

The figure 3.20 shows the case when bits [3,5,6] of the codeword are erased and we see that there are two paths with equal weight of branch metrics. For classical Viterbi decoding

one of the path could be chosen but as we are dealing with modified scheme, we conclude that the codeword cannot be recovered and it is a decoding failure.

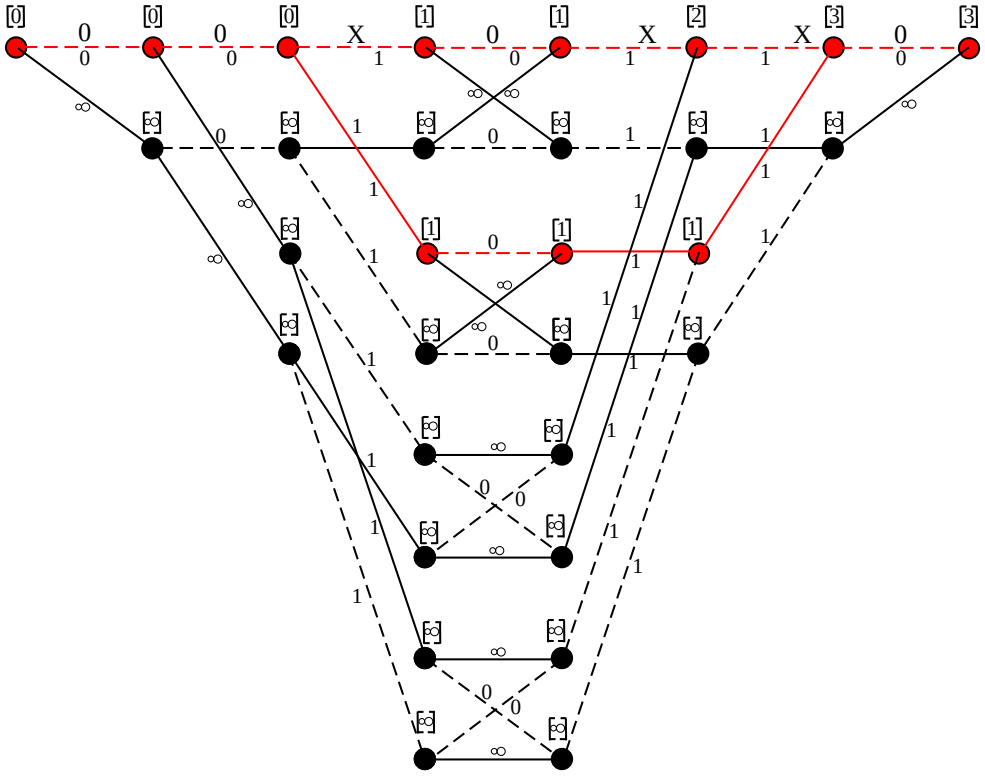

Figure 3.20: Viterbi decoding for three erasures in a codeword

The Viterbi decoding operates at bit level and when dealing with packets it complexity will be too high that is not practical, therefore, Tanner graph decoding is given preference over Viterbi decoding since its complexity is very low when dealing with packets.

3.6 Conclusion

In this chapter we have described the properties of short erasure correcting codes and their decoding using Tanner graph based approach. The way iterative erasures decoding is done at the receiver side to recover lost data packets is described. It is further explained that all erased packets cannot be recovered using Tanner graph based approach and the decoding performance of erasure codes can be enhanced. The Tanner graph based decoding is done using $\mathbf{H_e}$ to enhance the performance for various codes. The decoding performance of Tanner graph based approach with usual and extended $\mathbf{H}$ matrix is computed and it is

further compared with the Exhaustive search based approach that achieves the maximum achievable performance. With the use of $\mathbf{H_e}$ there is a huge gain in erasure recovery of lost data and this performance is comparable with Exhaustive search. Moreover, the Tanner graph based approach is given priority over Exhaustive search based decoding due to lower decoding complexity. Furthermore, the way of concatenation of short codes to construct more powerful product codes is described. These product codes are more efficient in-terms of erasure recovery with less encoding and decoding complexity. The decoding procedure of Single parity check product code (SPCPC) for erasure recovery is described in detail. The last part of the chapter describes Viterbi decoding for erasure recovery and it is, in fact, modified Viterbi decoding that is descried with examples. The three techniques are compared and it is concluded that the Tanner graph based decoding has lower complexity than Exhaustive search and it will be used in rest of the thesis. Moreover, Tanner graph based decoding is much more efficient than Viterbi decoding as well at packet level, Viterbi decoding operate at bit level and its decoding complexity will become too high at packet level and we cannot use it in practice.

Chapter 4

Application of Short Erasure Correcting Codes for Opportunistic Spectrum Access

Contents

4.1 Introduction

We address the use of short erasure correcting codes for the recovery of erased data in opportunistic spectrum access (OSA) due to sensing impairments in this chapter. Two state On/Off Gilbert model is used to generate the activities of primary and secondary users. The expression for efficiency is calculated taking in account the sensing parameters, the PU's activity and the parameters of codes used for erasure recovery. The main focus of the Chapter is to find an optimum functioning point on the receiver operating characteristic (ROC) curve in-terms of efficiency of the secondary reuse of spectrum. This optimal point depends on the sensing impairments and the parameters of the code including the length, rate and minimum distance. The erased data is recovered using Tanner Graph based decoding at receiver side without retransmission of data. Moreover, the achieved efficiency with and without erasure correcting codes is compared and the achieved gain is analysed.

The analytical approximation of efficiency is also compared with simulation results and the expression for maximum achievable efficiency is calculated. The effect of changing sensing time at the secondary spectrum efficiency is also analysed. Various erasure correcting codes are used to recover the erased data and their performances is analysed for various values of PU's activities by calculating the efficiencies for secondary spectrum access. There are different efficiency levels depending upon the code properties including length, rate and minimum distance. Single Parity Check Product codes (SPCPC) of various length are constructed and efficiencies of secondary spectrum access are plotted for various values of False alarm probabilities. Finally, the efficiencies achieved using short codes and product codes are compared with short and long LDPC codes to analyse why short code should be given preference over long codes keeping in account the decoding complexity, latency and erasure recovery performance.

The organisation of Chapter is given as: Section 4.2 describes the system model and problem definition explaining how the erasure correcting codes are used without changing the existing system. The performance analysis is done in section 4.3 and the expression for efficiency of secondary spectrum access is calculated that depends on various parameters. In section 4.4 it is described how the sensing parameters and the activity of PU affect the efficiency of secondary access. The section 4.5 is about the application of short erasure correcting codes. The simulation curves for estimating the efficiency using various short

codes are plotted and the effect of various codes is analysed. The comparison of block codes are done with short and long LDPC codes in section 4.7. The section 4.8 concludes the Chapter.

4.2 System model and problem description

We are using Opportunistic Spectrum Access scheme where primary user is the licensed user and secondary user can use the idle part of spectrum without interference to PU. The secondary user can use the spectrum when PU is not transmitting and it should stop its transmission as the PU arrives in the channel. The activity of PU can be generated as the succession of active and idle periods as the measurements reported in [36] have shown. This activity can be modelled with a two-state Gilbert model [37,38] with given transition probabilities with state *On* (while PU is active and transmitting) and the state *Off* (when PU is idle and not transmitting). Where p_1 is the transition probability from state *On* to state *Off* and p_2 is the transition probability from state *Off* to state *On*. These steady state probabilities P_{on}, P_{off} of the channel to be active or idle are given by the given classical formula :

$$P_{on} = \frac{p_2}{p_1 + p_2}, \quad P_{off} = \frac{p_1}{p_1 + p_2}$$

We cannot control the activity of PU as it is variable and it is a main challenge for SU to achieve guaranteed quality of service. For various values of P_{on}, the SU may achieve various efficiency levels. The secondary user listen continuously to the channel in order to detect the idle time slots, and sensing is normally required for this purpose. A part of the time-slot T_s is reserved for sensing the channel, while the remaining $T - T_s$ will be used for SU's transmission if no PU activity is detected. The sensing impairments including P_{FA} and P_{ND} probabilities are not independent. Their relationship can be observed using the Receiver Operating Characteristic Curve (ROC). Unfortunately, it is not possible to keep these two probabilities at a lower value. There is a need to choose a good functioning point on the ROC curve. We suppose that packets are protected by an error correcting code at the physical layer and these are decoded without errors when there is no PU but cannot be received correctly in case of non detection of the PU because the signal to noise plus interference ratio (SINR) is likely to be very low that results to collision; in this case the received packet is discarded by the SU receiver and labelled as erased and the channel in this case is Binary Erasure Channel. Moreover, we assume that packets are numbered,

so that the secondary receiver knows which packets are missing (erased). A second error control code operating at the application layer is introduced with the aim to recover erased packets: SU data are encoded in packets $\mathbf{P_1}, \mathbf{P_2}, \ldots \mathbf{P_n}$, and SU receiver is supposed to receive only a subset of them, missing packets are either not transmitted (when the channel is busy) or transmitted with a collision with PU's transmission.

We suppose that the receiver can recover all $\mathbf{P_i}$ provided it received a sufficient number of packets, thanks to the erasure correction capability of the application layer code. As there is no modification of the PHY layer this approach can be implemented on already existing systems, and does not involve any hardware changes, which is an appealing property. For broadcast applications long codes with higher delay have been used to recover lost data. We observe that short codes have lower decoding complexity and they should be given preference for OSA schemes.

Moreover, their erasure recovery performance is comparable with long codes if the collision rate is not too high. These are also efficient for delay sensitive applications like cloud gaming due to lower latency. Therefore, we have to envision the usage of short block codes, products of short codes such as SPCPC. We will perform the comparison in-terms of performance and complexity of different short codes with long codes. Furthermore, It is also possible to assess the expected performance for the secondary access depending upon the code used for erasure recovery of lost data as we can compute the joint probability successful access and the number of collisions for any given time-slots [99] under some assumptions the primary user's traffic can be modelled with a On/Off model [100, 101].

We will use Tanner graph based decoding for erasure recovery. We apply iteratively this decoding procedure until there is no erasure left or we cannot find an equation with only one erased packet. As defined in Chapter 3, the performance of a code can be estimated by a two variable polynomial enumerator, this polynomial enumerates all erasure patterns that are not recovered after decoding (i.e. dead-end sets):

$$T(x,z) = \sum_{i,j=0}^{n} T_{i,j}\, z^j x^i$$

Where the expression $T_{i,j}$ gives the number of non recoverable erasure patterns of initial

size i and final size j. From this polynomial we can derive the approximations:

$$p_r \approx \frac{1}{n} \sum_{i \geq 0} \Big\{ \sum_{j>0} j\, T_{i,j} \Big\} p^i (1-p)^{n-i} \tag{4.1a}$$

$$p_f \approx \sum_{i=0}^{n} T_i\, p^i (1-p)^{n-i}, \text{ with } T_i = \sum_{j>0} T_{i,j} \tag{4.1b}$$

The probability that all erasures are not completely recovered (a codeword recovery failure) is denoted by p_f and the residual erasure probability after decoding is denoted by p_r. The performance of the code is measured using these probabilities. The preference of short erasure correcting codes over long codes (Raptor, LT etc) for OSA has already been addressed in [102] and the analytical formulas to compute the probabilities p_f, p_r given in this Chapter are under the assumption that erasures distribution is based upon the traffic of PU and SU that is modelled using an On/Off model.

4.3 Performance Analysis

4.3.1 The Efficiency Parameters

We have to define a criteria to compare fairly erasure correction performance of various short codes (Golay, Hamming, BCH, ...) and long codes (LDPC for example). The main parameter is the rate (number of transmitted information packets) of the SU but other parameters are also important. Efficiency depends on activity of the PU i.e., the P_{on} probability of PU. With high P_{on} probability the SU has less available time period to transmit its data packets. Therefore, the value of P_{on} has a high impact on efficiency. It also depends on the sensing impairments: false alarm probability P_{FA} results in missed opportunities and a lower number of packet transmission by SU; non detection probability P_{ND} results in collision probability with the PU and the number of erasures to be recovered by the codes.

The two extreme scenarios exist: $P_{FA} = 0$ means SU will always access the channel at the cost of higher probability of collisions with the PU, and conversely $P_{FA} = 1$ means no collision with PU because $P_{ND} = 0$, at the cost of zero efficiency since the SU has no access to the channel. The erasure recovery is also a related parameter to compute the efficiency. The minimum distance d of the code is important as we know the code can correct all erasure patterns of at most $d-1$ erasures. The code rate k/n is also important, as the redundant packets are transmitted with the information packets to recover the erased data

packets. The codes with higher rate will have higher impact on efficiency.

The choice of the parity check matrix has a higher impact on the performance of erasure correction. There is also an opportunity of using cyclic codes with extended parity check matrix H_e as explained earlier and a significant improvement in the performance can be seen in-terms of erasure recovery. Here, we define a criterion that makes the effects of these parameters obvious. We introduce a reference which corresponds to an ideal detector ($P_{FA} = 0$ and $P_{ND} = 0$). In this case the SU would be able to have opportunity to use all idle periods of the PU; within a number $t \gg 1$ of consecutive time-slots, an average $t \times P_{off}$ are free and the average number of information packets correctly transmitted by SU are given by:

$$N_p(ideal) = t \times P_{off} \tag{4.2}$$

This is the best scenario that can be achieved by a SU with an ideal detector because there are no redundant packets (while there is no collision) and all opportunities are used (as no missed opportunities) to transmit the data packets of SU. While in real scenario we have to take into account sensing impairments, the average number of packets transmitted by SU over $t \gg 1$ time slots then equal to $N_p(real)$, which is given by:

$$N_p(real) = t \times \Big(P_{on}\, P_{ND} + P_{off}\ (1 - P_{FA}) \Big) \tag{4.3}$$

A part of these transmitted packets, while PU is transmitting, are consequently erased due to collisions. We have the collision probability p conditionally to SU's transmission:

$$p = \frac{P_{on}\, P_{ND}}{P_{on}\, P_{ND} + P_{off}\ (1 - P_{FA})} \tag{4.4}$$

The average number of transmitted codewords by SU is then equal to $N_p(real)/n$, and $(1 - p_f)$ is the fraction of these codewords that is entirely recovered after decoding. Last, we have to take into account the code rate, that means we have only k information packets over n transmitted packets. The average number of received information packets over $t \gg 1$ becomes:

$$N_p(info) = k \times \frac{N_p(real)}{n} \times (1 - p_f)$$

The efficiency $\eta_c = N_p(info)/N_p(ideal)$ is given by:

$$\eta_c = \frac{1}{P_{off}}\, \frac{k}{n} \Big(P_{on}\, P_{ND} + P_{off} \times (1 - P_{FA}) \Big)\ (1 - p_f) \tag{4.5}$$

The comparison in-terms of efficiency η_c for various codes having different rates is fare because the codes are compared under the same value of P_{on} (i.e., the same available idle slots) and η_c in this case is directly proportional to the throughput. Based on the above efficiency expression we can derive the efficiency without using erasure correcting codes denoted as uncoded efficiency η_u. The probability of correctly received information packets by SU without collision is $(1-p)^k$. We will multiply this probability $(1-p)^k$ instead of $(1-p_f)$ with efficiency η_c expression and after simplification we get the expression for efficiency without coding.

$\eta_u = N_p(info)/N_p(ideal)$ becomes:

$$\eta_u = \frac{{P_{off}}^{k-1}\,(1-P_{FA})^{\,k}}{\Big(P_{on}\,P_{ND} + P_{off} \times (1-P_{FA})\Big)\,k-1} \tag{4.6}$$

We plot the efficiency curves with and without erasure coding to analyse the gain. We plotted the efficiency curves using equation (4.6) for $k = 12$ and $k = 21$ as shown in figure 4.1. The maximum efficiency achieved with $k = 12 = 12\%$ and the maximum efficiency achieved with $k = 21 = 5\%$. We can see the gain when plotting the efficiencies with erasure correcting codes Golay(24,12) and BCH(31,21) using equation (4.5), the maximum achieved efficiency is significantly higher. The efficiency achieved using Golay(24,12) code is 43% and using BCH(31,21) it becomes 37%.

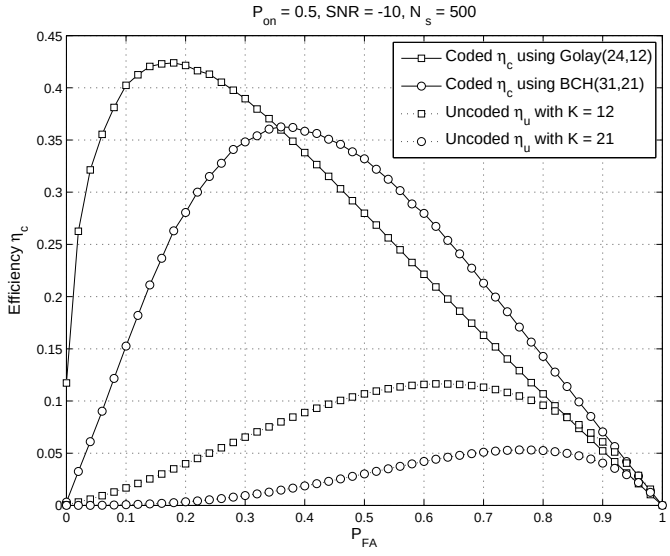

Figure 4.1: Comparison of Efficiency with and without Erasure Coding

4.3.2 Analytical approximation for efficiency

All our simulation results show the efficiency η_c as a function of false alarm probability P_{FA} and its upper bound is given by a simple function of $1 - P_{FA}$. In order to give a derivation of this property we have to proceed through some reminders on the way false alarm and non detection probabilities are computed.

We hereafter recall the general setting for the computation of these probabilities. We assume we have a number of samples $\{X_1, X_2, \ldots, X_n\}$ corresponding to two hypotheses H_0 (no signal, only noise) or H_1 (signal is present, with noise). A quantity Y is computed from these samples, for instance $Y = \frac{1}{n}\sum_{i=1}^{n} X_i^2$ for an energy detection, but any function $Y = f(X_1, X_2, \ldots, X_n)$ could be used provided we are able to compute the conditional distributions $\Pr[y|H_0]$ and $\Pr[y|H_1]$. We use the property that these two distributions are generally very different[1]: $\Pr[y|H_0]$ is rather located near the small values (there is no signal which contributes to y) while $\Pr[y|H_1]$ is rather located near greater values of y as sketched in fig. 4.2.

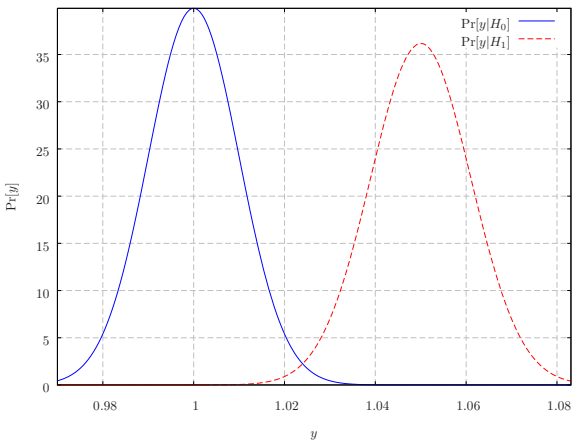

Figure 4.2: Comparison of the conditional distributions $\Pr[y|H_i]$, $i = 0, 1$

We then chose a threshold γ and decide that when $y > \gamma$ hypothesis H_1 is true, and conversely when $y < \gamma$ the hypothesis H_0 is true.

4.3.3 The gaussian approximation

When the number of samples used in $Y = \frac{1}{n}\sum_{i=1}^{n} X_i^2$ is high, Y can be considered as a Gaussian random variable (by virtue of the Central limit theorem) whose mean and

[1] if not, it means that the quantity Y we have used is not a good variable to perform detection

variance are given by :

$$m_Y = \frac{1}{n}\sum_{i=1}^{n}\mathbb{E}\left[X_i^2\right] = \sigma_X^2$$
$$\sigma_Y^2 = \mathbb{E}\left[Y^2\right] - \mathbb{E}\left[Y\right]^2 = \frac{2}{n}\sigma_X^4$$

The two possible hypotheses H_0, H_1 are then characterized by a different power for the X_i:

In the no-signal hypothesis (H_0) we have $\sigma_X^2 = \sigma^2$ (the noise variance) and Y is a normal variable (m_Y, σ_Y) with:

$$\begin{cases} m_Y = \sigma^2 \\ \sigma_Y^2 = \dfrac{2}{n}\sigma^4 \end{cases}$$

Given a threshold γ it is possible to compute the false alarm probability as :

$$P_{FA} = Q\left(\sqrt{\frac{n}{2}} \times \frac{\gamma - \sigma^2}{\sigma^2}\right)$$

where $Q(x)$ is the standard tail probability function, defined by

$$Q(x) = \frac{1}{\sqrt{2\,\pi}}\int_x^\infty e^{-t^2/2}\,dt$$

When a signal with power P is present (H_1) we have $\sigma_X^2 = P + \sigma^2$; the mean and variance of Y are now given by

$$\begin{cases} m_Y = \sigma^2 + P \\ \sigma_Y^2 = \dfrac{2}{n}\left(\sigma^2 + P\right)^2 \end{cases}$$

The non detection probability P_{ND} is then equal to

$$P_{ND} = 1 - Q\left(\sqrt{\frac{n}{2}} \times \frac{\gamma - (\sigma^2 + P)}{\sigma^2 + P}\right)$$

We will make use of the following property $Q(-x) = 1 - Q(x)$, $\forall x \in I\!R$ to write

$$1 - P_{FA} = Q\left(\sqrt{\frac{n}{2}} \times \frac{\sigma^2 - \gamma}{\sigma^2}\right) \tag{4.7a}$$

$$P_{ND} = Q\left(\sqrt{\frac{n}{2}} \times \frac{\sigma^2 + P - \gamma}{\sigma^2 + P}\right) \tag{4.7b}$$

The case $P_{FA} \to 1$ means that $m_Y - \gamma \gg \sigma_Y$, that is to say

$$1 - \frac{\gamma}{\sigma^2} \gg \sqrt{\frac{2}{n}}$$

It means that γ is such that the arguments of the two Q-functions are much greater than 1, so that we can use the approximation

$$Q(x) \approx \frac{1}{x\sqrt{2\pi}} \times e^{-x^2/2} \tag{4.8}$$

to obtain :

$$1 - P_{FA} \approx \frac{1}{\sqrt{n\pi}} \frac{\sigma^2}{\sigma^2 - \gamma} \exp\left\{-\frac{n}{4}\Big(\frac{\sigma^2 - \gamma}{\sigma^2}\Big)^2\right\} \tag{4.9a}$$

$$P_{ND} \approx \frac{1}{\sqrt{n\pi}} \frac{\sigma^2 + P}{\sigma^2 + P - \gamma} \exp\left\{-\frac{n}{4}\Big(\frac{\sigma^2 + P - \gamma}{\sigma^2 + P}\Big)^2\right\} \tag{4.9b}$$

It is advantageous to take the logarithms of both sides of (4.9a) and (4.9b) so that we can write

$$\log\Big[\sqrt{n\pi}\Big(1 - P_{FA}\Big)\Big] \approx -\frac{n}{4}\Big(1 - \frac{\gamma}{\sigma^2}\Big)^2 - \log\Big(1 - \frac{\gamma}{\sigma^2}\Big) \tag{4.10a}$$

$$\begin{aligned}\log\Big[\sqrt{n\pi}\Big(P_{ND}\Big)\Big] \approx -\frac{n}{4}\Big(1 - \frac{\gamma}{\sigma^2 + P}\Big)^2 - \\ \log\Big(1 - \frac{\gamma}{\sigma^2 + P}\Big)\end{aligned} \tag{4.11a}$$

Last, we make use of $\frac{\gamma}{\sigma^2} \ll 1$ to derive first order approximations :

$$\begin{aligned}\log\Big[\sqrt{n\pi}\Big(1 - P_{FA}\Big)\Big] \approx -\frac{n}{4}\Big(1 - 2\frac{\gamma}{\sigma^2}\Big) + \frac{\gamma}{\sigma^2} = \\ -\frac{n}{4} + \frac{\gamma}{\sigma^2}\left(1 + \frac{n}{2}\right)\end{aligned} \tag{4.12}$$

and likewise for P_{ND} :

$$\log\left[\sqrt{n\pi}\, P_{ND}\right] \approx -\frac{n}{4} + \frac{\gamma}{\sigma^2 + P}\left(1 + \frac{n}{2}\right) \tag{4.13}$$

We can now eliminate γ between these two approximations to obtain an approximation

of P_{ND} as a function of $1 - P_{FA}$:

$$\sqrt{n\pi}\, P_{ND} \approx \left[\sqrt{n\pi}\,(1 - P_{FA})\right]^{\frac{1}{1+\mathrm{SNR}}} \times \exp\left\{-\frac{n}{4} \times \frac{\mathrm{SNR}}{1+\mathrm{SNR}}\right\} \tag{4.14}$$

where we have used SNR $= P/\sigma^2$. We can use (4.14) in the formula giving efficiency and compare the simulation results with this simple analytic approximation. As shown in

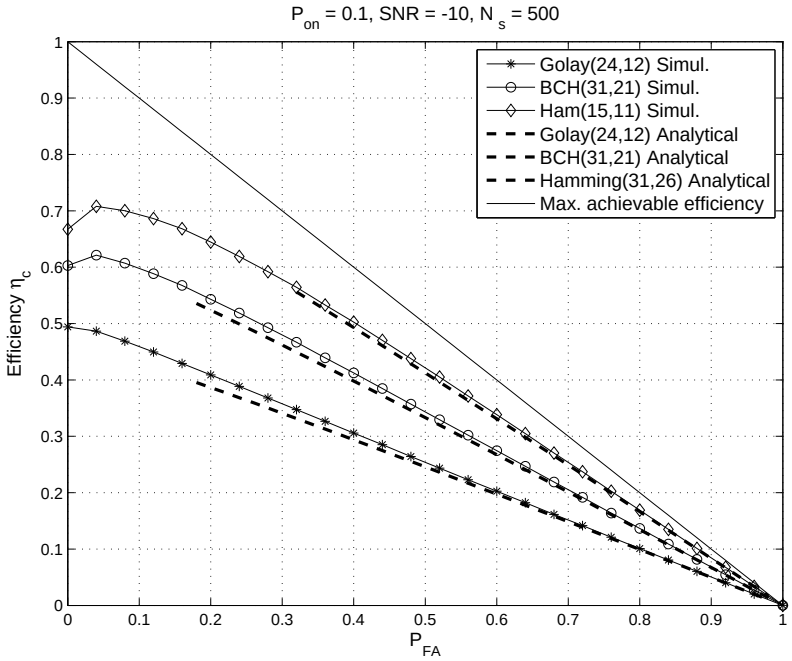

Figure 4.3: Comparison of Simulation Vs Analytical Approx. for Efficiency η_c

fig. 4.3 the agreement is very good when P_{FA} is sufficiently close to 1, that is to say in the validity range of approximation (4.8), which also ensures that decoding failure probability is such that $p_f \ll 1$, so we can discard this term by approximating the efficiency η_c.

4.3.4 Maximum achievable efficiency $\eta_{max.}$

Maximum achievable efficiency for secondary reuse can be estimated using the following derivation: The maximum number of transmitted packets by the SU are given by the expression:

$$P_{trans} = t \times \Big(P_{on}\, P_{ND} + P_{off} \times (1 - P_{FA})\Big) \tag{4.15}$$

the maximum number of correctly received packets by the secondary receiver are given:

$$\eta_{max.} = P_{trans} \times (1 - p) \tag{4.16}$$

By using the equations (4.4), (4.5) and (4.16), following expression for max. achievable efficiency is obtained after simplification:

$$\eta_{max.} = (1 - P_{FA}) \tag{4.17}$$

It will be observed from the simulation results that the code with strong parameters specially with higher erasure recovery capability and long length (for example long LDPC codes) will achieve efficiency closer to the max. achievable efficiency $\eta_{max.}$ and this is an upper limit for efficiency η_c.

4.4 Effect of sensing related parameters and PU's Activity

Several simulations corresponding to the system model described in the section 4.2 have been performed to analyse the effect of different parameters on efficiency as defined by equation (4.5). Moreover, concerning sensing, we have chosen the energy detection and we will vary the sensing time by changing the number of samples N_s to see its effect. Several short codes have been simulated, having different code rate, code length and minimum distance, that is to say different erasure correction capabilities. Finally, for various values of P_{on} the efficiencies for secondary spectrum access are plotted to see the effect of PU's activity.

4.4.1 Effect of sensing related parameters

Now we explain how the choice of a functioning point $(P_{FA}, 1 - P_{ND})$ on the ROC curve can impact the performance of the SU. As expected the number of samples N_s has a big effect on the efficiency. This can be explained clearly with the help of Fig. 4.4: for a same target value of P_{ND}, the optimum false alarm probability decreases as N_s increases, that is to say the SU loses less opportunities to access the channel.

As a consequence the collision probability p of (4.4) also decreases. Figure 4.5 depicts simulation results for Hamming(15,11) code.

We observe that efficiency η depends on P_{FA}. When $P_{FA} \approx 0$, the SU access the channel all the time, with a collision every time the PU is active, and the code (with a

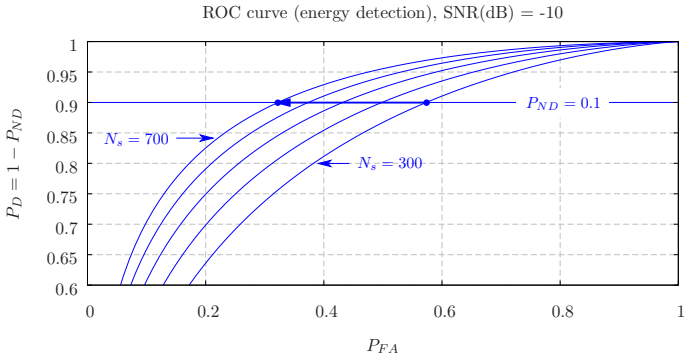

Figure 4.4: Changing the number of samples: $N_s = 300, 400, \ldots 700$

modest error correction capability since its minimum distance is $d = 3$) cannot recover the too many erasures. As a result, the SU has very few successful accesses to the channel.

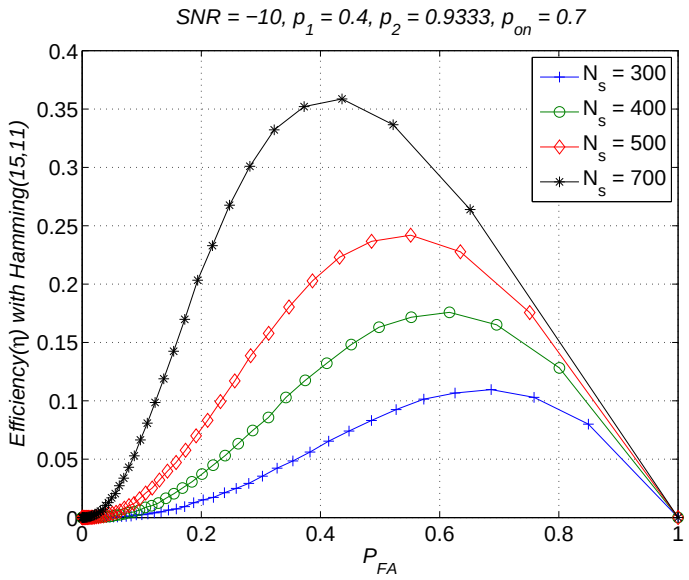

Figure 4.5: Efficiency with Hamming(15,11) code, for several values of N_s

Likewise, when $P_{FA} \approx 1$, the efficiency is close to 0, the reason being that the SU never access the channel. The maximum efficiency is the result of two contradictory effects: as P_{FA} increases some opportunities will be missed by the SU, but the number of collisions (erasures) diminishes as well and the code is able to recover erasures. If P_{FA} is too high the efficiency will suffer mainly of a reduced number of access to the channel and its value will decrease.

4.4.2 Effect of PU's activity

Although we have defined the efficiency with respect to the PU's Off probability in order to define the maximum throughput the SU could achieve without changing the sensing time, PU's activity does have an effect on the SU's efficiency. This is depicted in fig. 4.6

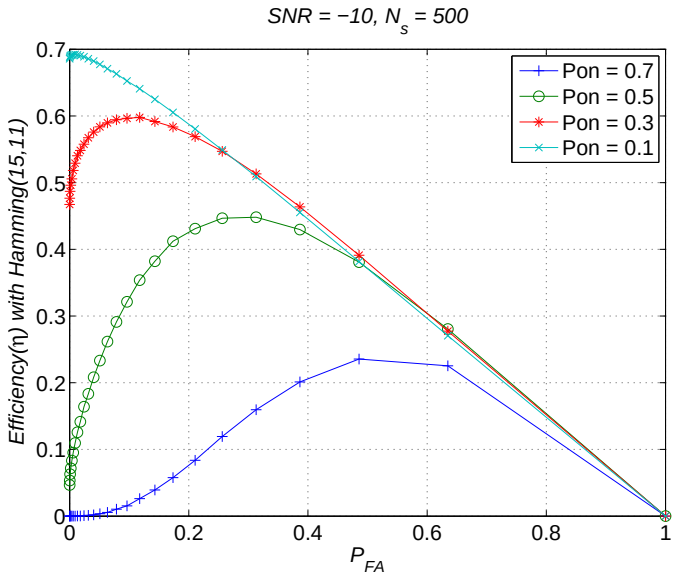

Figure 4.6: Efficiency with Hamming(15,11)

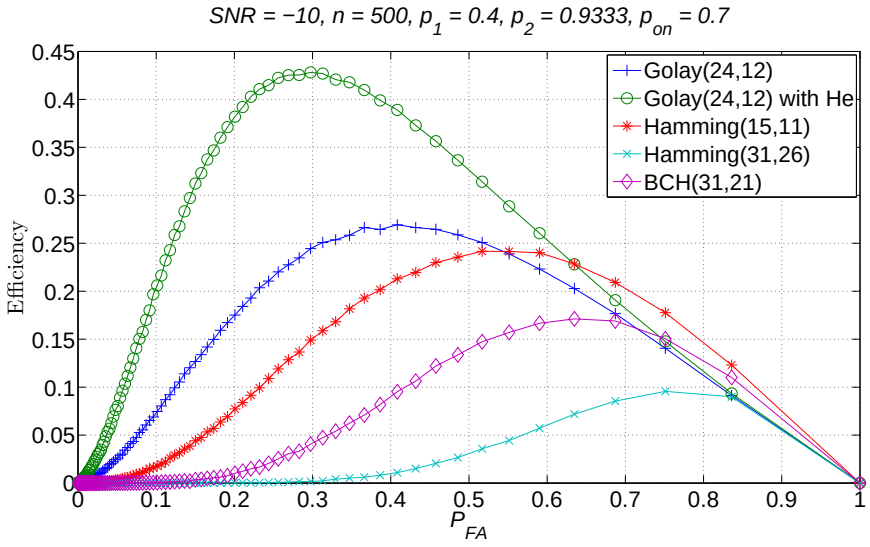

Figure 4.7: Comparison of several codes, $P_{on} = 0.7$

which shows the very different behaviour of the efficiency for $P_{on} = 0.1, 0.3, 0.5, 0.7$ for same Hamming(15,11) code. Best efficiency is achieved for $P_{on} = 0.1$ for $P_{FA} \simeq 0$ and decreases as P_{FA} increases, which is understandable: the SU uses all available opportunities without experiencing too many collisions as the PU is rarely active in the channel. As P_{on} increases, the trade off between accessing the channel (small value of false alarm probability) and recovering data lost in collisions (small non detection probability) is again the limiting factor on efficiency.

4.5 Efficiency of Secondary spectrum access using short codes

4.5.1 Influence of the rate and minimum distance of the code

We now address the influence of the code used to recover the erasures. We observe two different behaviours depending on whether the PU's activity is high or not. When PU is often active, for instance $P_{on} = 0.7$, we observe two interesting phenomena. First, there is not a great gap in efficiency between the Golay(24,12) code with ordinary parity check matrix and a Hamming(15,11) code. Both codes achieve a near 25% efficiency, despite

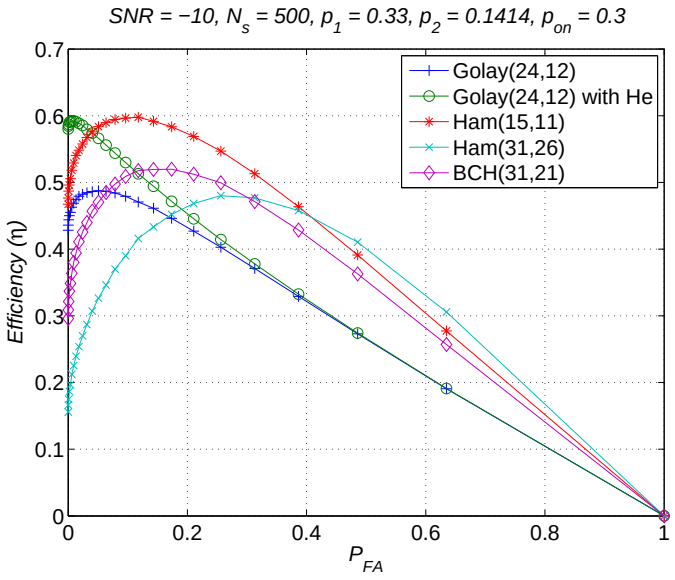

Figure 4.8: Comparison of several codes, $P_{on} = 0.3$

their different erasure correction capabilities due to different minimum distances, $d = 8$ for the Golay code to be compared with $d = 3$ for the Hamming code. In fact the limiting factor is the code rate, since working with the ordinary parity check matrix of the Golay

code leaves several erasure patterns of size less than $d-1=7$ not recovered [2,3]. Things changes greatly when using the extended parity check matrix H_e given in [2], the efficiency raises to above 40% because we can now recover all erasure patterns of size up to $d-1$, as depicted in fig. 4.7.

For lower probability of PU's transmission, for instance when $P_{on}=0.3$, the Golay code with extended parity check matrix allows a small improvement in efficiency for small values of P_{FA} as the number of collisions are higher and it can recover maximum erasures. Nevertheless, the same efficiency of 60% can be achieved with a simple Hamming(15,11) code. It is worth noticing that the maximum efficiency of the Golay code is greater than 1/2 (code rate); this can be explained as follows: for small values of P_{FA} the SU access more often to the channel than what could be expected without collisions, and the erasures can be recovered because the code is powerful and this is an extra gain to the efficiency.

4.6 Efficiency of Secondary spectrum access using Product Codes

As we discussed in previous section that several parameters affect the efficiency. We have performed many simulations and we can observe that different efficiency levels can be achieved with various value of P_{on}. When using the product codes, the properties for different SPC and SPCPC code including code rate and erasure correction capability have significant effect on efficiency.

4.6.1 Effect of P_{on}

We have performed simulations for various values of SPC and SPCPC code. The equation 4.5 shows the analytical estimation of SU efficiency for opportunistically accessing the spectrum. For same SPC and SPCPC codes, we achieve different efficiency levels for different P_{on}. Figure 4.9 shows that $\eta < 30\%$ using the SPC (6,5,2) code when $P_{on}=0.7$, number of sensing samples $N_s=500$ and $SNR=-10$. When using SPCPC (6×6, 5×5, 2×2), the efficiency is increased from 29% to 33%.

There are still several erasure patterns which are not recovered. To recover the residual erasures we increase the number of iterations, the code rate remains constant but decoding complexity will increase slightly. We notice that at the 3rd iteration, efficiency is increased to 35.5%. Figure 4.10 shows the case when $P_{on}=0.5$, achieved efficiency is $\approx 50\%$ using (6,5,2) and increases upto $\approx 57\%$ using SPCPC (6×6, 5×5, 2×2) and max. efficiency of

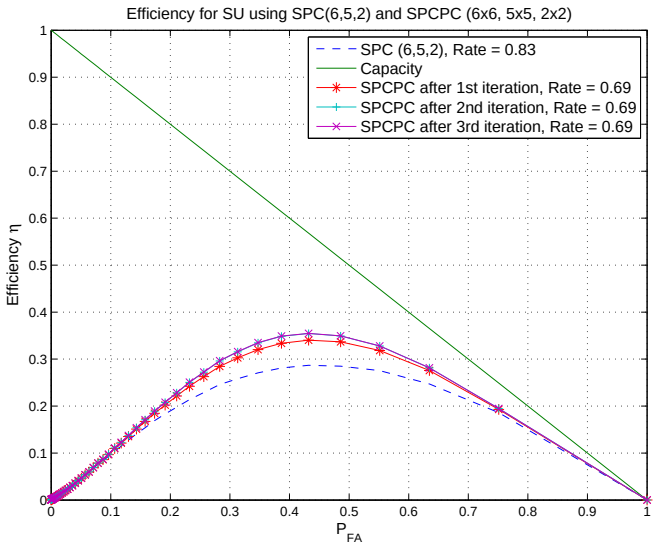

Figure 4.9: Efficiency with SPC(6,5) and SPCPC Code for $P_{on} = 0.7$, SNR = -10, $N_s = 500$

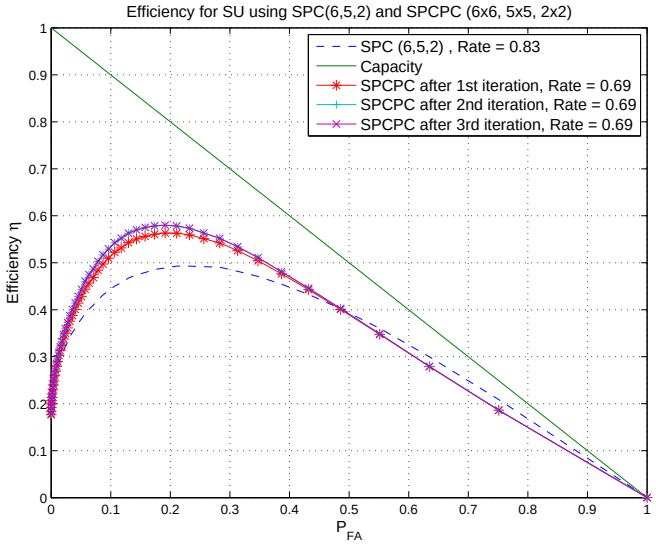

Figure 4.10: Efficiency with SPC(6,5) and SPCPC Code for $P_{on} = 0.5$, SNR = -10, $N_s = 500$

59% is achieved after 3rd iteration. If $P_{on} = 0.3$, there are less collisions resulting to less erasures and a higher efficiency of 60% is achieved using less powerful SPCPC (11×11, 10×10, 2×2) as shown in Figure 4.12.

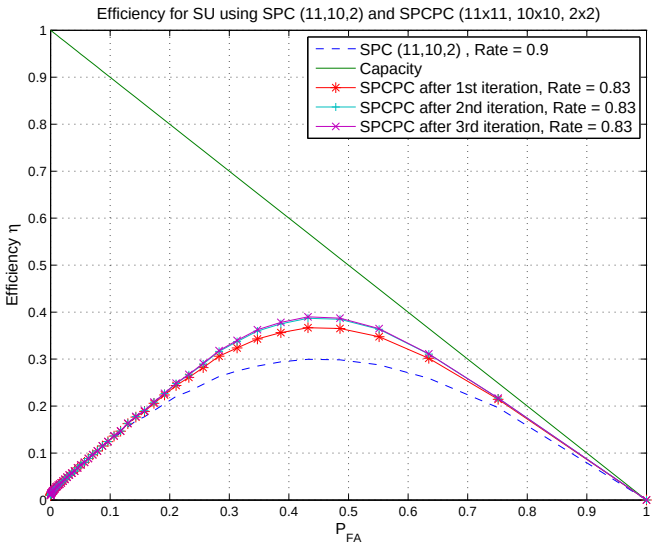

Figure 4.11: Efficiency with SPC(11,10) and SPCPC Code for P_{on} = 0.5, SNR = -10, N_s = 500

4.6.2 Effect of code properties on efficiency

The code rate (k/n), minimum distance (d) have significant effect on the efficiency. The erasure correcting code can correct upto $d-1$ erasures. The length of SPC and SPCPC

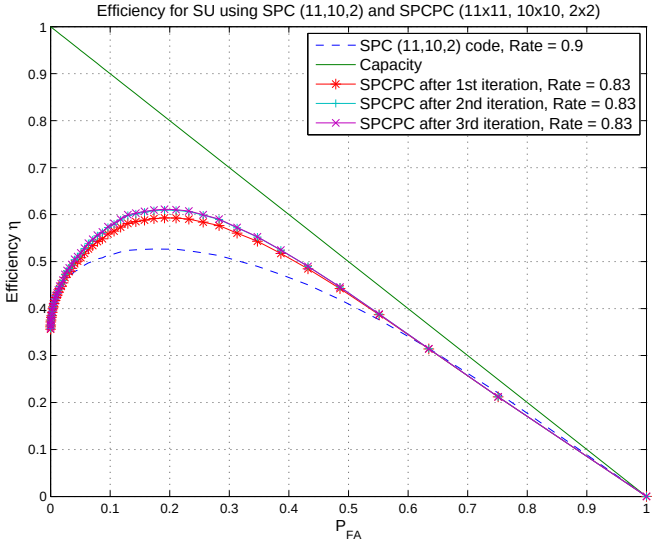

Figure 4.12: Efficiency with SPC(11,10) and SPCPC Code for P_{on} = 0.3, SNR = -10, N_s = 500

codes is also an important factor. For same minimum distance d, the SPCPC code with different code length achieve different efficiency levels. For example SPC (6,5,2) code has better efficiency then SPC (11,10,2) code because erasure recovery capability of former is better then the later. Similarly, SPCPC (6×6, 5×5, 2×2) achieves higher efficiency of 59% as shown in figure 4.10 and SPCPC (11×11, 10×10, 2×2) achieves efficiency ≈ 39% due to lower erasure recovery rate as shown in figure 4.11. The shorter SPC codes for example (3,2,2) and SPCPC (3×3, 2×2, 2×2) can achieve even higher efficiency due to better erasure recovery rate.

4.7 Comparison of Block Codes with LDPC codes

We perform many simulations for the same value of PU's activity to see the effect on efficiency using various short and long codes with different code rates, lengths and minimum distances having different erasure correction capabilities. We repeat the similar procedure for different values of P_{on} probabilities. It will be clear from simulation results that the

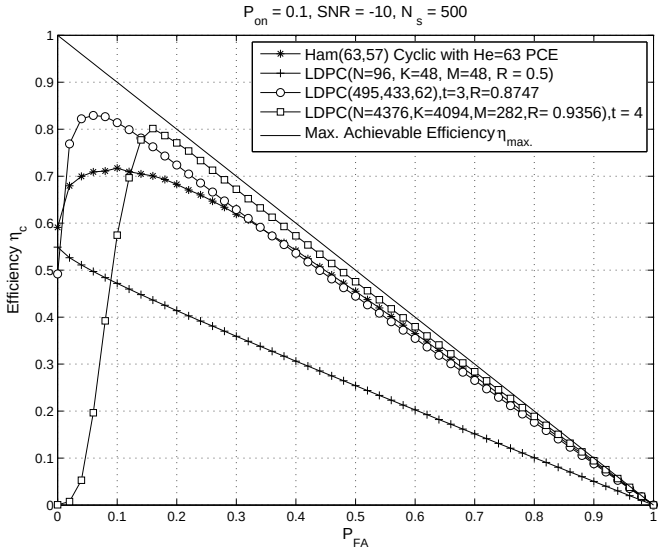

Figure 4.13: Comparison of several codes, $P_{on} = 0.1$, $N < 100$, $100 < N < 1000$, $N > 1000$, The effect of code length and PU's activity on efficiency η_c

short codes are preferable over long codes dur to low decoding complexity. Long codes are capacity achieving codes but at the expense of much higher decoding complexity. We suppose that the PU allows 10% of collisions i.e, value of p (input collision probability with PU) should not be greater than 10 % as the primary or license user will not allow very

high interference. We compare the effect of length of codes on efficiency for different class of codes including short block codes and LDPC codes. It will be observed from simulation results that the PU's activity P_{on} has an effect on the SU's efficiency. Best efficiency is achieved for $P_{on} = 0.1$ as shown in figure 4.13 when $P_{FA} \simeq 0$ and decreases as P_{FA} increases, This is due to the fact that the SU uses all available opportunities of spectrum without experiencing too many collisions because the PU is rarely active in the channel.

We compare the short codes with long erasure recovery codes when the PU's activity = 0.1 as depicted in Fig. 4.13. It is observed that the performance of short codes is comparable with long codes because there are not much collisions and short block code will recover the maximum erased data. The efficiency η_c achieved using the codes with length $N < 100$, Cyclic Hamming(63,57) with extended parity check matrix (He) for instance, is significantly higher than the η_c achieved using LDPC(96, 48) code. However, using very long codes with $N > 1000$, LDPC(4376,4094) for example, the achieved η_c is quite close to the maximum achievable efficiency $\eta_{max.}$, but these long codes should not be selected for this particular case due to much longer delay and high decoding complexity.

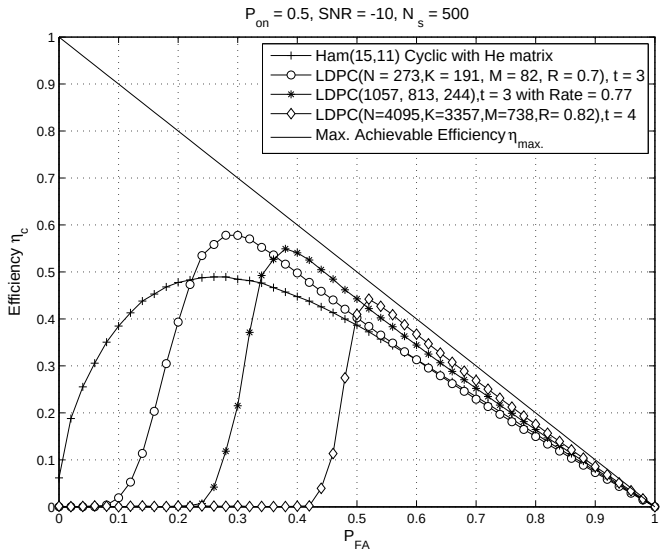

Figure 4.14: Comparison of several codes, $P_{on} = 0.5$, $N < 100$, $N < 1000$, $N > 1000$, The effect of code length and PU's activity on efficiency η_c

As P_{on} increases, there is a trade off between accessing the channel and recovering lost data due to collisions as PU is very active in the channel. This again becomes the limiting factor on achievable efficiency η_c. We perform the same comparison for higher value of

$P_{on} = 0.5$ and we observe in figure 4.14 that the achieved η_c is not that higher as with $P_{on} = 0.1$ due to the fact that channel is busy quite often. Using the block codes with length $N < 100$, the η_c achieved using Hamming(15,11) codes with H_e for instance, is comparable with LDPC(273,191) code. Therefore, Hamming(15,11) code will preferably be used for erasure recovery due to shorter delay rather using LDPC(273,191). However, LDPC(1057,813) and LDPC(4095,3357) for example achieve η_c much closer to upper limit of efficiency due to strong code parameters specially the length but these long codes have high decoding complexity and have higher latency than using short codes.

4.7.1 Comparison of short Block Codes with short LDPC Codes

Now the simulations are performed to do a fair comparison of short erasure recovery codes with only short LDPC codes. It can be observed in the figure 4.15 that all block codes

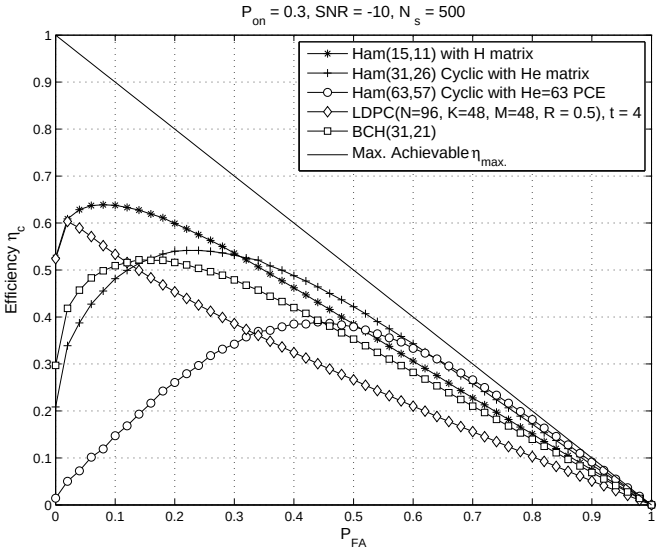

Figure 4.15: Comparison of several short codes having shorter delay ($N < 100$) with short LDPC code

including Hamming(15,11), Hamming(31,26), Hamming(63,57), BCH(31,21) have much better performance than short LDPC(96,48) code under the same value of $P_{on} = 0.3$. Hamming code (63,57) with H_e and Hamming code (31,26) with H_e are achieving the efficiency closer to the upper limit $\eta_{max.}$. It is clear from the comparison that short LDPC codes are not really interesting to use due to lower performance for erasure recovery in this particular scenario of OSA. The short block codes will preferably be selected for erasure

recovery specially in the region where $P_{FA} > 0.5$ and there are not too many collisions in this region.

4.7.2 Comparison of Product Codes with LDPC

We also do a comparison of product codes for example Hamming × Hamming or Hamming × SPC with LDPC codes. It is clear from figure 4.16 that the efficiency η_c obtained using HammingSPC(1575,1368) is comparable with the LDPC(1908,8889) that achieves η_c closer to the $\eta_{max.}$. In this case it will be more efficient to use HammingSPC(1575,1368)

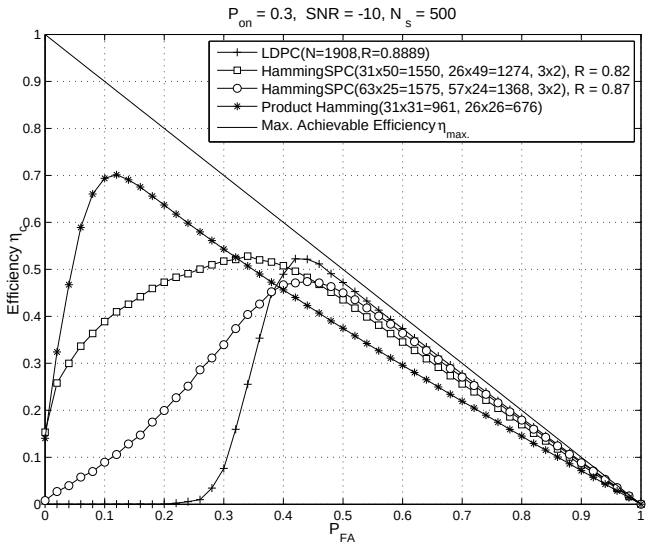

Figure 4.16: Comparison of Product Codes with LDPC codes

due to lower decoding complexity. We already discussed the advantages of using product codes in section 3.4. Furthermore, we can observe that Product Hamming ($31 \times 31 = 961$,$26 \times 26 = 676$) is achieving highest $\eta_c = 70\%$ in the region $P_{FA} = 0.1$ and there are too high collisions in this region. The erasure recovery capability of product Hamming is significantly increased due to iterative decoding. Therefore, it is more efficient to use product codes when there are higher collisions as they achieve higher performance with lower decoding complexity, rather using very long LDPC codes.

4.8 Conclusion

In this chapter we have proposed the solution to optimize the efficiency of secondary user for Opportunistic Spectrum Access. The erasure correcting codes are used to recover the

erased data for secondary user due to the interference of PU. We have defined a metric (the efficiency η_c) to compare fairly different codes having different rates in a same channel characterized by a given value of p_{on} of PU. The parameters affecting the spectral efficiency of secondary access are analysed. In fact, the efficiency depends on sensing impairments, the activity of PU and the parameters of erasure correcting codes. There is always a gain in efficiency when using the erasure correcting codes, as the missing data packets due to collisions are recovered. The way of erasures recovery using Tanner Graph based decoding is described at packet level and the expressions of failure probability of erasure correcting codes are calculated. The product codes are envisioned which are more powerful in terms of erasure recovery and they are generated by the concatenation of shorter codes. We also used cycle codes with extended parity matrix ($\mathbf{H_e}$) that have significant improvement for erasure recovery and provide better results in terms of spectral efficiency η_c. Moreover, we have analysed how the erasure correcting code can be chosen with respect to the PU transmission probability P_{on}. The efficiencies achieved using short codes are compared with long codes and it is analysed that short codes are very efficient due to lower decoding complexity and they have lower latency. There is an advantage of using short codes especially when dealing with delay sensitive applications. The short codes are given preference over longer codes which are in fact the capacity achieving codes, but at the expense of much higher decoding complexity. The main result of this chapter is to show that there exist an optimum functioning point on the ROC curve depending on the sensing parameters, and we explained it as a trade-off among secondary access to the channel (depending on the parameter P_{FA}), the collision rate experienced (relevant parameter is P_{ND}), and the choice of an erasure code having an impact on erasure recovery at the expense of the redundancy we must introduce.

Chapter 5

Performance of MAC Protocol for multiple users using Erasure Correcting codes

Contents

5.1 Introduction

In this chapter we address the application of cognitive radio networks where multiple users can access the channel for example in TV white spaces (where interesting scenario

is WiFi 802.11af) using Career Sense Multiple Access Collision Avoidance(CSMA/CA) scheme. The 802.11 protocol provides the specifications for Media Access Control (MAC) and physical layer (PHY) to implement wireless local area network (WLAN) using 2.4 or 5 GHz frequency bands. We describe the CSMA/CA scheme in detail with the interaction of PHY and MAC layer and the modifications in existing 802.11 protocol. It is observed that a lot of time is spent in the detection of channel when the no.of users increases in the system. We have proposed some modifications in 802.11a protocol by changing its parameters.

In order to see the effect of these parameters we have analytically approximated the collision probability and compared it with the simulation results. We suppose that the transmitted packets by multiple users are either received correctly at the receiver or not received and these lost packets are consider as erased. We are using the erasure channel and in order to recover the lost data due to collisions among multiple users we envision the use of erasure correcting codes. These erasure correcting codes will be useful for optimizing the global throughput of multiple secondary users at the cost of redundancy. The goal is to find an optimal point for global throughput for multiple users by reducing the value of BO to some extant and by introducing the erasure correcting codes to recover collisions. The optimal throughput depends on the parameters of MAC protocol, the parameters of the code including the length, rate and minimum distance and the number of users in the network. We also plot histograms for the input erasure probability of channel to observe the behavior and distribution of erasures.

Finally, we provide the expression for calculating the global throughput and plot various simulation curves by varying the number of users and using various erasure correcting codes. The objective is to find an optimum point by maximizing the global throughput by recovering all lost packets. We observe through simulation curves that we can choose the erasure correcting codes to recover all lost packets depending upon the MAC protocol parameters and the number of users. Moreover, if the number of users in the system increase then more efficient codes with strong code properties having better erasure correction capability are needed. The analytical model to calculate the throughput using CSMA/CA is presented in [103] and the detailed performance analysis for basic access scheme and for Request To Send or Clear To Send (RTS/CTS) is described in this article. A closer related work on fountain based transport protocol is also presented in [104] for single 802.11 WLAN cell, but our approach is to use short erasure correcting codes for erasure recovery

of multiple users for 802.11 protocol.

The organization of chapter is given as follows: The CSMA/CA for MAC protocol and the proposed modifications in this protocol are given in section 5.2. The analytical approximations for global collision rate and its comparison with simulation results is provided in section 5.3. The input erasure probability of erasure channel using various histograms is observed in section 5.4. The expression for global throughput and the simulation results to calculate the throughput for multiple users using various erasure correcting codes are provided in section 5.5. The section 5.6 is devoted to conclusions of the Chapter.

5.2 Modified Carrier Sense Multiple Access with Collision Avoidance Scheme

The Carrier Sense Multiple Access scheme with Collision Avoidance (CSMA/CA) for multiple access in wireless data communication is already explained in Chapter 2. It is obvious that as the number of users are increased in the system then the waiting time to access the channel also increases. We now propose the solution that these long delays can be reduced

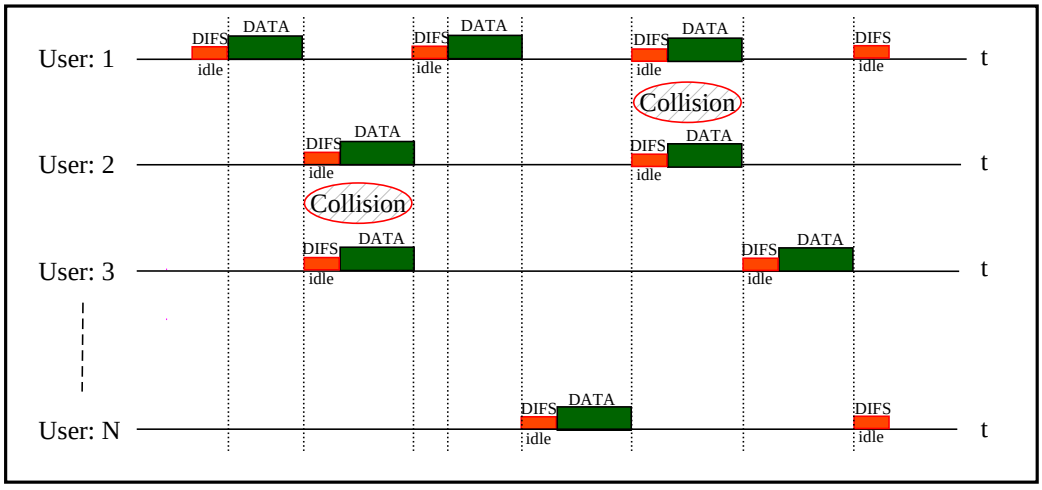

Figure 5.1: Multi users access using CSMA/CA without backOff

by decreasing the values of DIFS and BO. In case there are some collisions among multiple secondary users, the lost data due to these collisions are considered as erased. We therefore envision the use of erasure correcting codes to recover the lost data. The properties of erasures correcting codes are already given in Chapter 3. The figure 5.1 shows the case when we have reduced the value of BO to zero and users are using only DIFS to detect the

channel for transmission. The collisions among multiple users can be seen in the figure. The collisions occur when two or more users have access to the channel at the same time and they start the transmission of data. This collision results to loss of data.

5.2.1 Transmission and Reception Flow of MAC Layer with erasure recovery

The modified transmission and reception flow of MAC layer is shown in figure 5.2. It is clear from the transmitting and receiving flow chart that there are two waiting states: DIFS time without interruption and backoff (BO) time without interruption. If the backoff

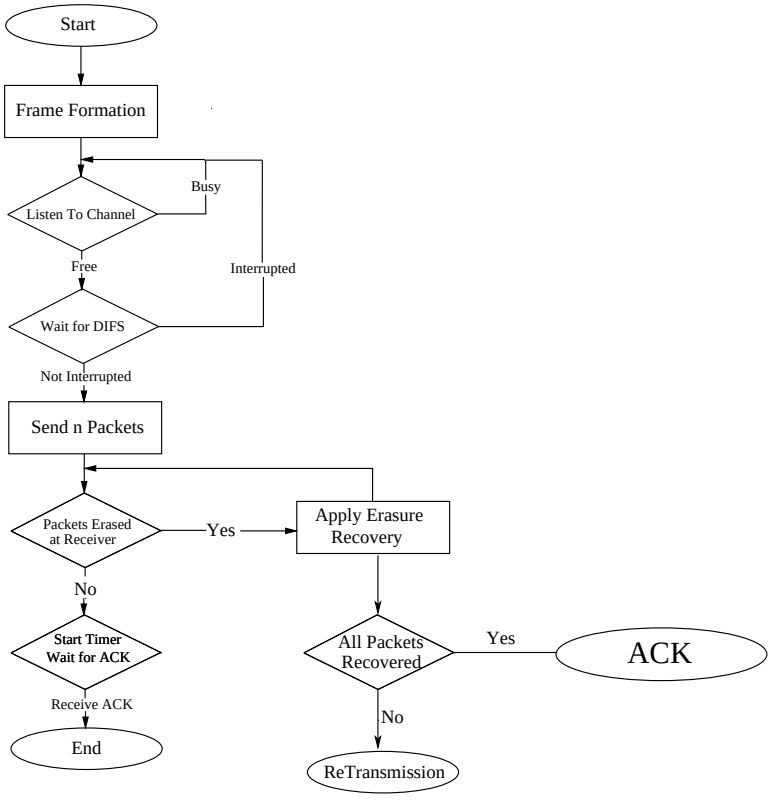

Figure 5.2: Flow chart using CSMA/CA with erasure recovery

timer is interrupted it is paused and wait for the channel to become idle again, when the channel becomes idle, it is resumed. After receiving the data, the receiving node checks if the packet is received without error. If it is true, it waits for SIFS time and sends ACK to the transmitter. If data is received with erasures then the erasure recovery to the received data is applied and checked if the data is recovered or not. If the data is recovered then the

ACK is sent. If it is not true, the re-transmission procedure is activated. This modification of the classical CSMA/CA scheme reduces the delays due to DIFS and BO times as most of the time is wasted during the detection of channel. This solution is effective specially when there is conjunction and multiple users are trying to access the channel. The idea is to allow collisions to some extent and apply erasure recovery to recover the lost data due to these collisions among multiple users. This will enhance the global throughput of multiple users.

5.3 Analytical Approximations of Collision Probability among Multiple users

In this section we calculate the analytical probability approximation for the collisions among multiple users. We suppose that the traffic model is full buffer, every user always has data in the buffer to transmit and whenever it has access to the channel it starts transmission. We give an example of WiFi scenario when there are multiple users and random value of backoff is assigned to each user. These values assigned to different users are not ordered. We use sorting to assign an order to all values of these users as the user with minimum value of backoff will get access to the channel. We suppose that the following random values of BO are assigned to five different users.

$$x_1 = 3, x_2 = 8, x_3 = 1, x_4 = 7, x_5 = 9 \tag{5.1}$$

The sorted form of the above assigned values can be written as:

$$x_{(1)} = 1, x_{(2)} = 3, x_{(3)} = 7, x_{(4)} = 8, x_{(5)} = 9 \tag{5.2}$$

The subscript (i) enclosed in the parentheses indicates the ith position of sorted users. Suppose $X_1, ..., X_n$ are random variables from discrete distribution for any given commutative distribution function $F(x)$ and probability mass function $f(x)$. To calculate probabilities of the kth order statistics, three probability values are first calculated.

$$p_1 = P(X < x) = F(x) - f(x) \tag{5.3a}$$

$$p_2 = P(X = x) = f(x) \tag{5.3b}$$

$$p_3 = P(X > x) = 1 - F(x) \tag{5.3c}$$

The cumulative distribution function of the kth order statistics can be computed as:
P $(X_{(k)} \leq x)$ = P(there are at most $n-k$ observations greater than x)

$$= \sum_{j=0}^{n-k} \binom{n}{j} p_3^j (p_1 + p_2)^{n-j} \tag{5.4}$$

Similarly, P$(X_{(k)} < x)$ = P(there are at most $n-k$ observations greater than or equal to x)

$$= \sum_{j=0}^{n-k} \binom{n}{j} (p_2 + p_3)^j (p_1)^{n-j} \tag{5.5}$$

The probability mass function of X_k is the difference of above two equations.

$P(X_{(k)} = x) = P(X_{(k)} \leq x)$ - $P(X_{(k)} < x)$

$$= \sum_{j=0}^{N-k} \binom{N}{j} (p_2 + p_3)^j (p_1)^{N-j} \tag{5.6}$$

$$= \sum_{j=0}^{n-k} \binom{N}{j} \left(p_3^j (p_1 + p_2)^{N-j} - (p_2 + p_3)^j (p_1)^{N-j} \right) \tag{5.7}$$

$$= \sum_{j=0}^{N-k} \binom{N}{j} \left((1 - F(x))^j (F(x))^{N-j} - (1 - F(x) + f(x))^j (F(x) - f(x))^{N-j} \right) \tag{5.8}$$

We start with the scenario of two users when they have collisions. As explained earlier that the traffic model is full buffered and every user has data in buffer to transmit immediately. According to CSMA/CA protocol the users waits for DIFS and the random backoff (BO) time before the transmission of data, but if the two or more users are assigned the same value of backoff then they will transmit the data packet at the same time and this results to collision and the transmitted data will be lost. $P_r(Collision) = P_r$(many users have the same min. backoff)

Suppose the value of random backoff = x, then

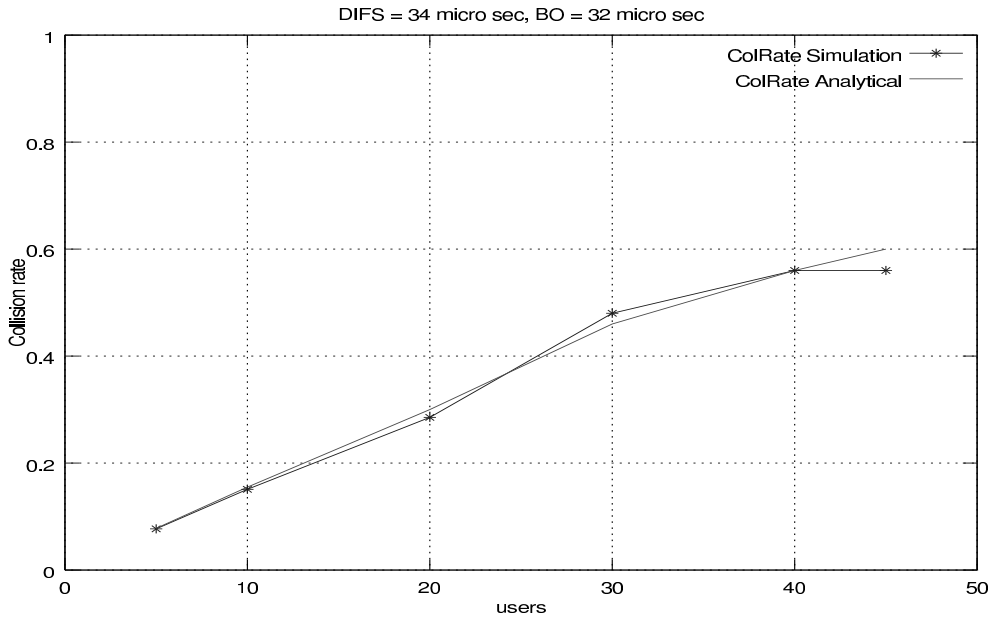

Figure 5.3: Analytical and simulation comparison of collision rate

$$P_r(Collision) = P_r(\text{min. backoff of 1st user} = x, \text{ min. backoff of 2nd user} = x)$$

$$P_r(Collision) = \sum_{i=0}^{BO-1} P_r(X_{(1)} = i) \times P_r(X_{(2)} = i \mid X_{(1)} = i) \tag{5.9}$$

$$= \sum_{i=0}^{BO-1} P_r(X_{(2)} = i, X_{(1)} = i) \tag{5.10}$$

If $P_1(X_{(1)} = 0$ in a set of size N-1) and $P_2(X_{(1)} = 0$ in a set of size N-2), then the collision probability can be generalised as:

$$= \sum_{i=0}^{BO-1} P_1(X_{(1)} = i) \cdot (P_2(X_{(1)} = i) \tag{5.11}$$

The probabilities of $P_1(X_{(1)} = i)$ and $P_2(X_{(1)} = i)$ can be calculated using equation 5.7 as:

$$P_1(X_{(1)} = i) = \sum_{j=0}^{N-1} \binom{N}{j} \left(p_3^j (p_1 + p_2)^{N-j} - (p_2 + p_3)^j (p_1)^{N-j} \right) \tag{5.12}$$

Similarly,

$$P_2(X_{(1)} = i) = \sum_{j=0}^{N-2} \binom{N-1}{j} \left(p_3^j (p_1 + p_2)^{N-1-j} - (p_2 + p_3)^j (p_1)^{N-1-j} \right) \tag{5.13}$$

The scenario of two users to calculate the collisions can be generalized for multiple users using the equation given below.

$$P_r(Collision) = \sum_{j=0}^{N-i} \binom{N-i}{j} \left(p_3^j (p_1 + p_2)^{N-i-j} - (p_2 + p_3)^j (p_1)^{N-i-j} \right) \tag{5.14}$$

Where i indicates the no.of users and ranges between $\{0, 1, 2, ..., N\}$.

The figure 5.3 shows the analytical and simulation comparison of collision rate using CSMA/CA among multiple users using equation 5.14. We see a good agreement between the simulation and analytical curve. This is the global collision rate and it is plotted across variable users. It is clear from the figure that the collision rate increases as the number of users increases, for example for 20 users the collision rate is 20% and as the number of users cross 40 the collision rate is approaching 60%.

5.4 Input Erasure Probability Histograms

The complementary cumulative distribution function (CCDF) curves of input erasure probability for code of various length are plotted. The figure 5.4 shows the input erasure probability for various values of n, where n is the length of any erasure correcting code. It

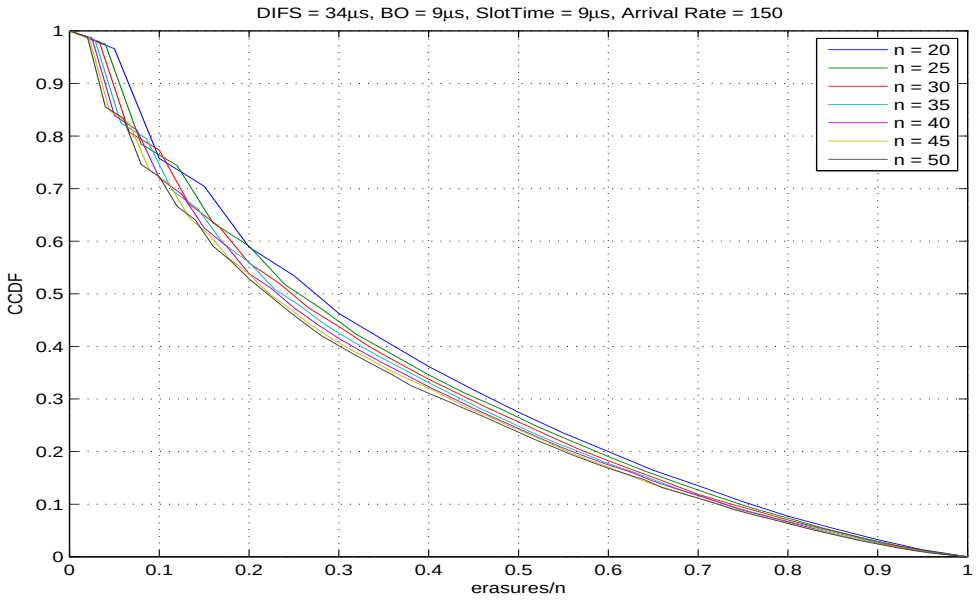

Figure 5.4: CCDF of input erasure probability for various values on n

can be observed that the input erasure probability for values $n = 20$ to $n = 50$ is plotted

and CCDF curves show that the input erasure probability remains almost the same for all values of n if we do not change any parameter of 802.11a protocol.

5.4.1 Input erasure probability and decoding effect for code with length n=15

We plot the histograms for input erasure probability of code with length $n = 15$ using parameters of 802.11a as shown in figure 5.5. The parameters of 802.11a protocol are

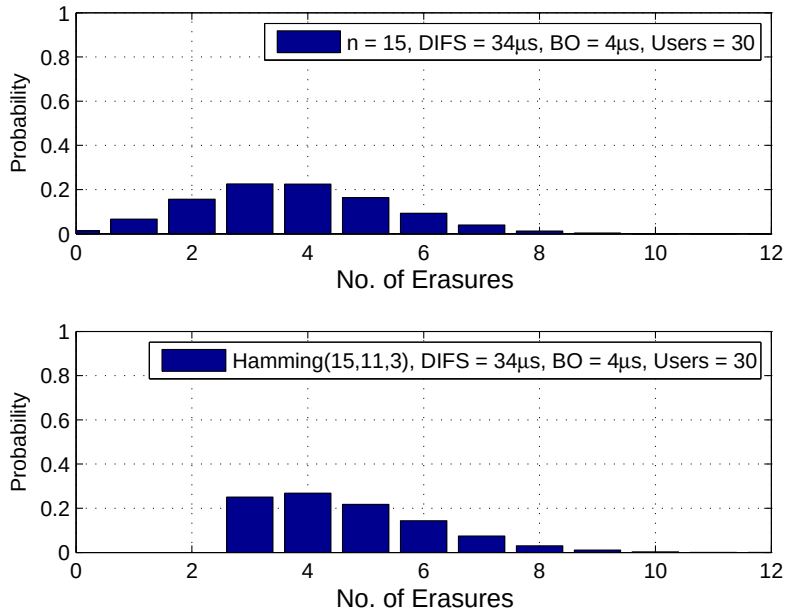

Figure 5.5: Histogram of erasure probability with $n = 15$ and residuals after decoding

selected as DIFS $= 34\mu sec$ with reduced value of backoff $= 4\ \mu sec$ for 30 number of users. The reduced value of backoff will reduce the long waiting time for multiple users to access the channel. The histogram of input erasure probability for the codewords with $0, 1, 2, ...15$ erasures is plotted. This histogram shows the behaviour of input erasure probability of the channel using any code with length $n = 15$.

The histogram for the residuals is plotted after decoding with Hamming (15,11,3) code as shown in figure. It is clear that all the codewords containing two erasures are recovered since the minimum distance for Hamming(15,11,3) code is $d = 3$. The remaining erasures can be recovered if more efficient codes with strong erasure recovery capability are used. This erasure recovery will increase the global throughput as the lost data due to collisions

are recovered using erasure correcting codes.

5.4.2 Input erasure probability and decoding effect for code with length n=31

Here we plot the histogram for input erasure probability for codeword with length $n = 31$ as shown in figure 5.6. The value of backoff is reduced in order to see the effect of collisions. The figure shows the histogram of input erasure probability of codewords with $0, 1, 2, ...31$ erasures. This histogram shows the behaviour of input erasure probability of the channel with length $n = 31$.

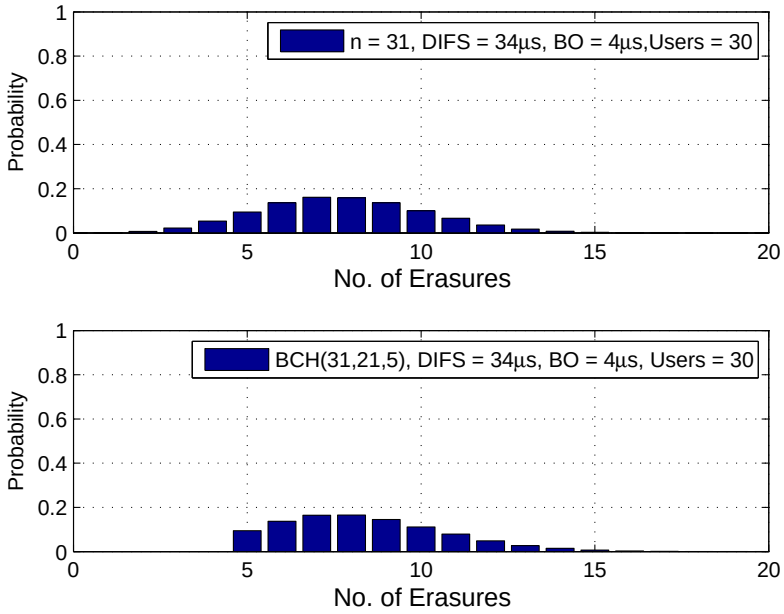

Figure 5.6: Histogram of erasure probability with $n = 31$ and residuals after decoding

For the given erasure distribution, the decoding is now performed using BCH(31,21,5) code and the histogram for the residuals is plotted after decoding as shown in Fig. 5.6. We observe that all the codewords containing upto four erasures are recovered as minimum distance $d = 5$ for BCH(31,2,5) and the histogram shows the remaining erasures that are not recovered after decoding, this erasure recovery will increase the global throughput and will reduce the retransmission requests for the lost data.

5.4.3 Input erasure probability and decoding effect for code with length n=63

The input erasure probability histogram for codeword with length $n = 63$ is plotted as shown in figure 5.7. To see the distribution of erasures the histogram for input erasure

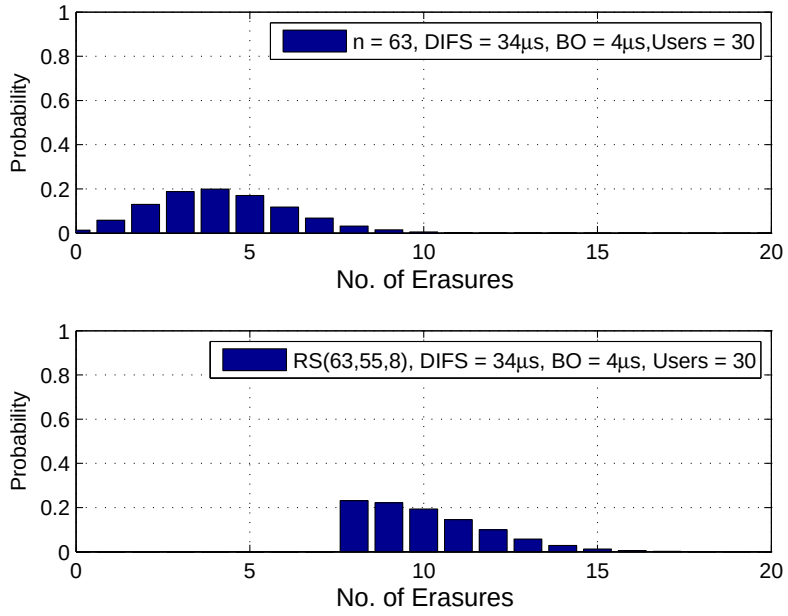

Figure 5.7: Histogram of erasure probability with $n = 63$ and residuals after recovery

probability of codewords with $0, 1, 2, ...63$ erasures is plotted. For this given erasure distribution, the erasure decoding is performed using RS(63,55,8) code and the histogram for the residuals is plotted after decoding as shown in figure. We observe that all the codewords containing upto 7 erasures are recovered as minimum distance $d = 8$ for RS(63,55,8). This will increase the global throughput for multiple secondary users in the network.

5.4.4 Input Erasure Probability and Decoding performance of Various codes

We have plotted the CCDF of normalized erasure probability and calculated the residuals probability of various codes after decoding from simulations. The objective is to show a synthesis of input erasure probability and the decoding performance of various erasure correcting codes. It is clear from figure 5.8 that the points calculated from simulations using different codes show different residuals level depending upon the parameters of codes

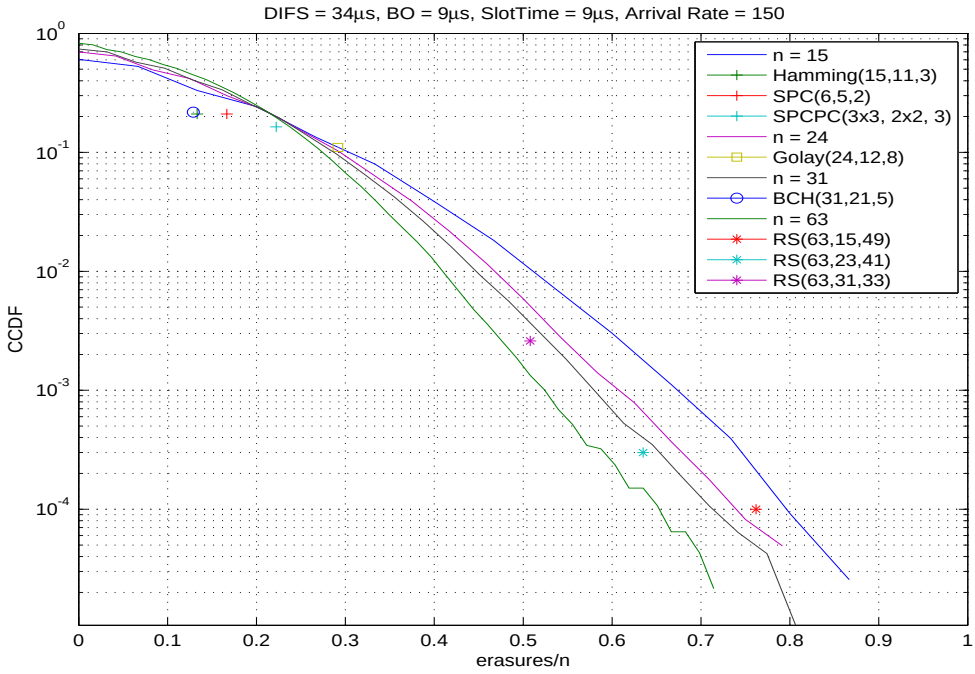

Figure 5.8: CCDF of residual erasure probability of various codes

including erasure recovery capability on the input erasure probability curves for given value of n. For example, Hamming Code has erasure recovery probability $(d-1)/n = 2/11 = 0.13$. Similarly, Golay code(24,12,8) has the erasure recovery capability $= 7/24 = 0.291$, RS Code (63,15,49) has erasure recovery capability $= 49/63 = 0.7619$.

Moreover, depending on the input erasure probability of the channel any code can be adopted keeping into account its erasure recovery capability. With higher probability of input erasures more powerful code for example RS(63,15,49) is selected and if the input erasure probability is lower then less powerful codes for example SPC(6,5,2) or Hamming codes (15,11,3) can be chosen for erasure recovery.

5.5 Simulation Results

In this section, the global throughput of CSMA/CA based MAC protocol is calculated. The general expression for throughput S is given as:

$$S = \frac{U}{B + I} \tag{5.15}$$

Where U = Successful Transmission time of secondary users, B = Busy period of the channel, I = Idle period of the channel when taking into account the MAC protocol parameters using CSMA/CA. The expression for global throughput can also be written as:

$$S = \frac{N_{OK}}{N_{OK}(DIFA + SIFS + BO + T_{packets}) + N_{NotOK}(DIFA + SIFS + BO + T_{packets})} \tag{5.16}$$

Where N_{OK} = No. of Successful received packets, N_{NotOK} = No. of Non received packets, $T_{packets}$ = Total time for transmitting a packets. We can also write the throughput expression as:

S = No. of successful packets/Total time

Where S is measured in packets/sec.

The parameters for 802.11a MAC are given in table 5.1.

Table 5.1: Parameters Configuration for 802.11 a

Symbols	**Values for given Protocol**
SlotTime	$1\mu sec$
SIFS	$16\mu sec$
DIFS	$34\mu sec$
BO	$rand() \times SlotTime$
ACK	$2\mu sec$
DATA	$1024Bytes$
DataRate	$54Mbps$

System Throughput is estimated using above parameters

We calculate the performance achieved using retransmission of data packets and using erasure correction scheme. If there are less collisions among multiple secondary users then we will have less redundancy in-terms of retransmission but still the erasure correcting code will perform better if we have very good rate code with better erasure recovery capability. In the worst case when there are a lot of collisions then the retransmission is not preferred due to very long retransmission delays.

The global throughput is now plotted for various values of BO. It is clear from figure 5.9 that the global throughput is initially higher with BO=$100\mu sec$ when there are few

number of secondary users, as the number of users increases then the global throughput starts decreasing. The global throughput is decreased from 4500 to 4000 packets/sec as the users increase from 2 to 40. The blue curve shows the global throughput of the system with retransmission, the throughput achieved with retransmission and without erasure correcting codes will cause very long delays specially with higher collision rate. The global throughput curves are then plotted using various erasure correcting codes showing that the maximum achieved throughput is comparable with the throughput achieved with retransmission of data. This difference is due to code rate but if no coding is done then various erased packets due to collisions among multiple SUs are not recoverable and the retransmissions of data is needed. The erasure recovery is performed at the receiver side and objective is to find an optimal point that gives the maximum achievable throughput with minimum packet loss.

5.5.1 The collision rate and global throughput with BO=100

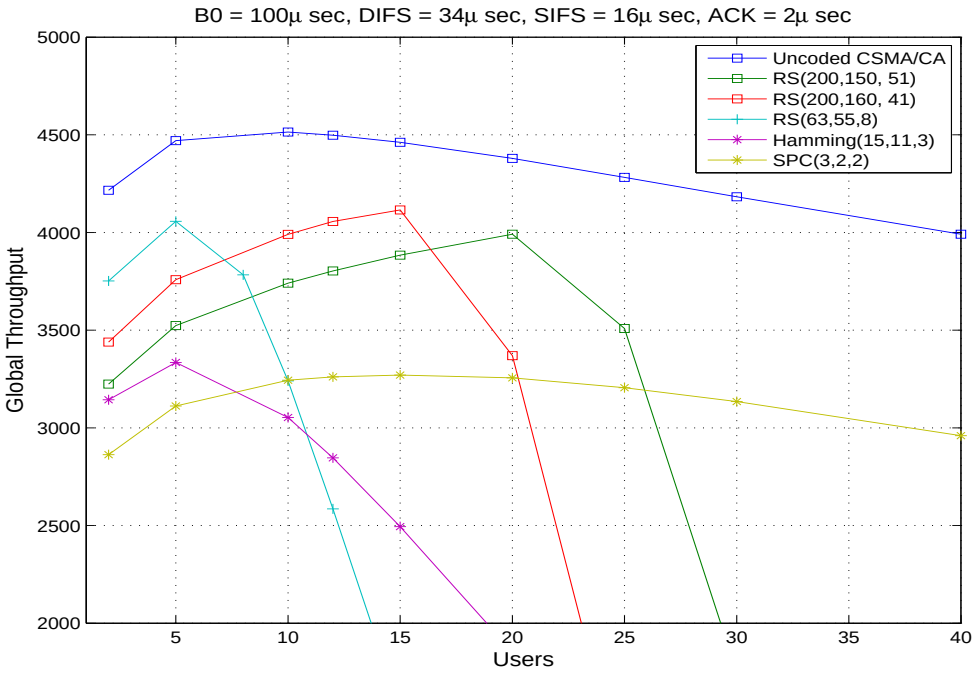

Figure 5.9: Global throughput achieved using multiple secondary users

With the same parameters as used in figure 5.9 for CSMA/CA, the collisions and residual erasure probability curves are plotted in figure 5.10 when BO=100μsec. It is clear that failure probability of RS code(200,150,51) is zero upto 20 users and all erased packets

are recovered when the collision probability is 10% as shown by the blue curve. Moreover, if the no.of users is increased for given access point then more powerful codes are needed to recover the lost data.

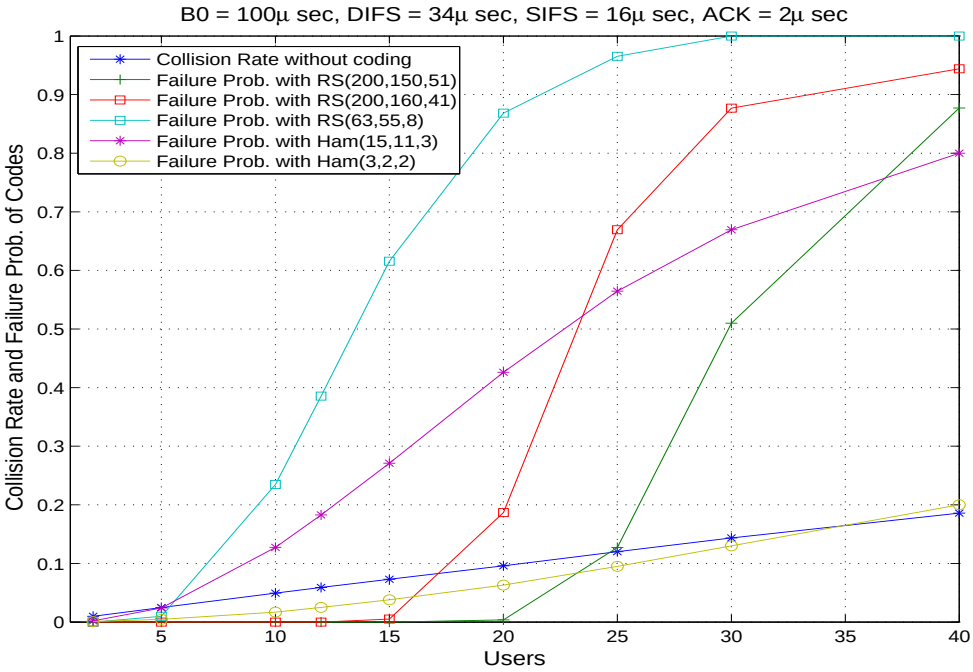

Figure 5.10: Collision rate and failure probability of codes

5.5.2 The collision rate and global throughput with BO=60

Similarly, the global throughput is estimated when BO=60 μsec. The figure 5.11 shows that the global throughput is decreased from 4500 to 3200 packets/sec as the users increase from 2 to 40. The global throughput curves are plotted for various erasure correcting codes showing that maximum achieved throughput is slightly lower than the throughput achieved without coding. However, some erased packets due to collisions among multiple SUs will not be recovered at receiver and retransmission of lost packets is mandatory. Using the erasure codes the lost data is recovered at the receiver and we try to optimize the global throughput using various codes.

The collisions and residual erasure probability curves are shown in Fig.5.12 when BO=60 μsec. We observe that the collisions are increased the BO is decreased and there is higher possibility of accessing the channel at the same time for multiple users

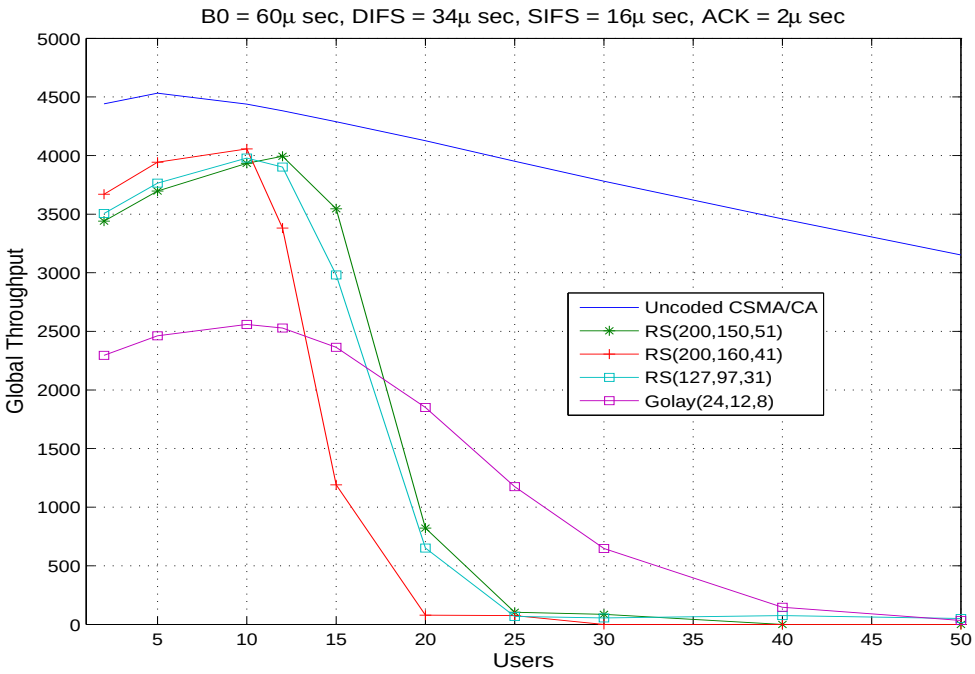

Figure 5.11: Global throughput achieved using multiple secondary users

and this increases the probability of collisions. It is clear that failure probability of RS code(200,150,51) is zero upto 12 users and all erased packets are recovered using this code when the collision probability is 10% as shown by the blue curve. If the users are increased within the access point, the collision rate is increased as well and more powerful codes are needed for erasure recovery.

5.5.3 The collision rate and global throughput with BO=32

Similarly, the global throughput is plotted when the value of BO=32 μsec. The global throughput is decreased from 4500 to 2000 packets/sec as the users increase from 2 to 40 as shown in figure 5.13. The blue curve shows the global throughput when lost data is recovered using retransmission. The global throughput curves are plotted using various erasure correcting codes showing that the optimal achieved throughput is slightly lower and comparable with the throughput achieved with retransmission of data.

The collisions and residual erasure probability curves are shown in figure 5.14 when BO=32 μsec. The collisions are further increased due to lower value of BO which can be recovered using erasure correcting codes. It is clear that the failure probability of RS

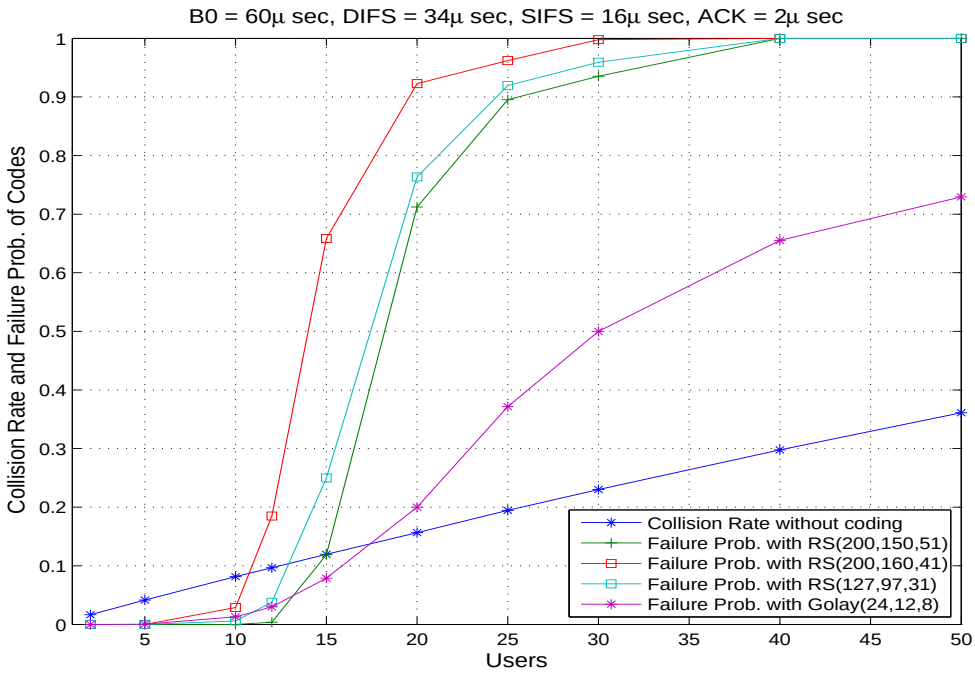

Figure 5.12: Collision rate and failure probability of codes

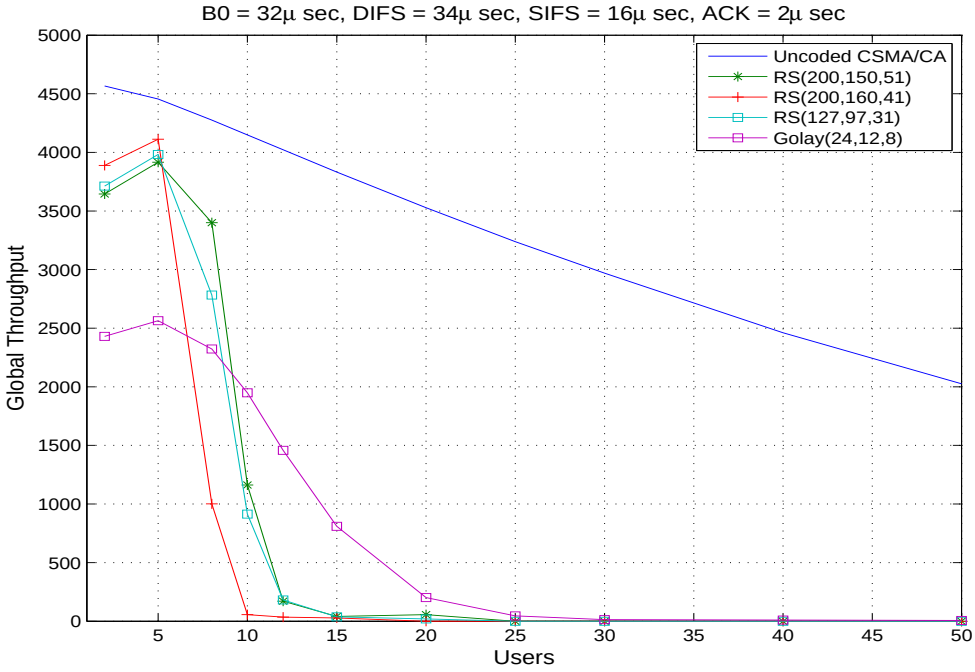

Figure 5.13: Global throughput achieved using multiple secondary users

code(200,150,51) becomes zero upto 5 users and all erased packets are recovered using this code when the collision probability is 8% as shown by the blue curve. Moreover, if the no.of users users is increased within the access point then more powerful codes are needed for erasure recovery.

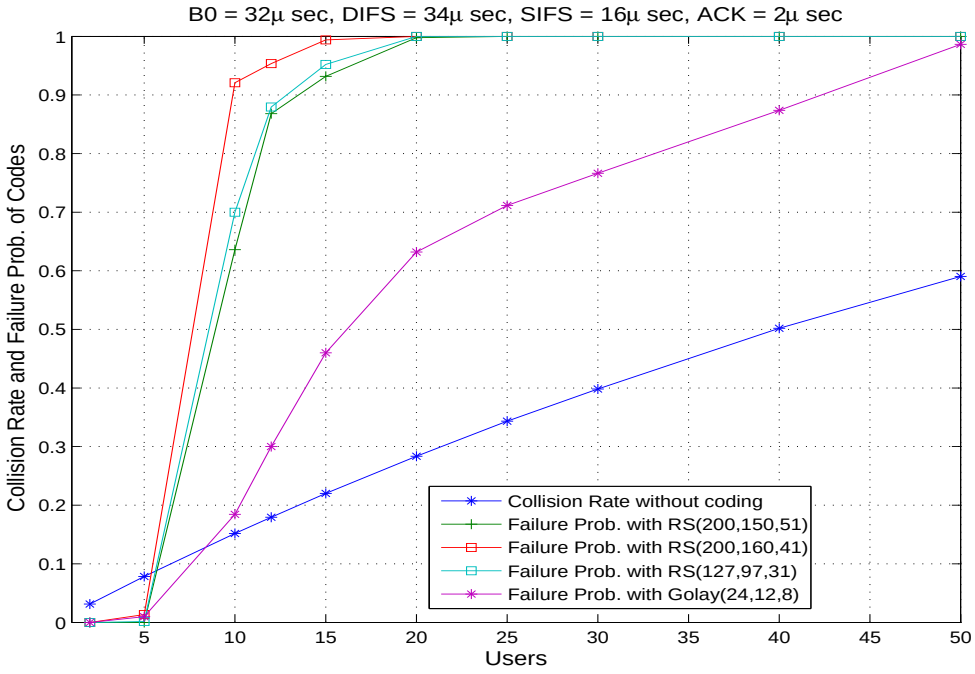

Figure 5.14: Collision rate and failure probability of codes

We summarize the simulation results for global throughput by varying the value of backoff as shown in figure 5.15. The objective is to achieve an optimal point to maximize the global throughput. We observe that when there are 5 users, the maximum achievable throughput is 4100 packets/sec but as the no.of users is increased the value of BO should be increased to get an optimal point for global throughput. When we increase the number of users from 5 to 10, the optimal point of global throughput is achieved at higher value of backoff. It is obvious because when the value of backoff is lower, there are higher collisions and the global throughput is very low. However, when there are fewer no.of users then the reduced value of backoff can be used to reduce long waiting time as the collision rate is not too high. To recover the lost data due to collisions we use erasure correcting codes, for example RS(200,150,51) is used for erasure recovery in Fig.5.15. We can achieve better throughput as we can recover the erased data due to collisions. Moreover, if strong

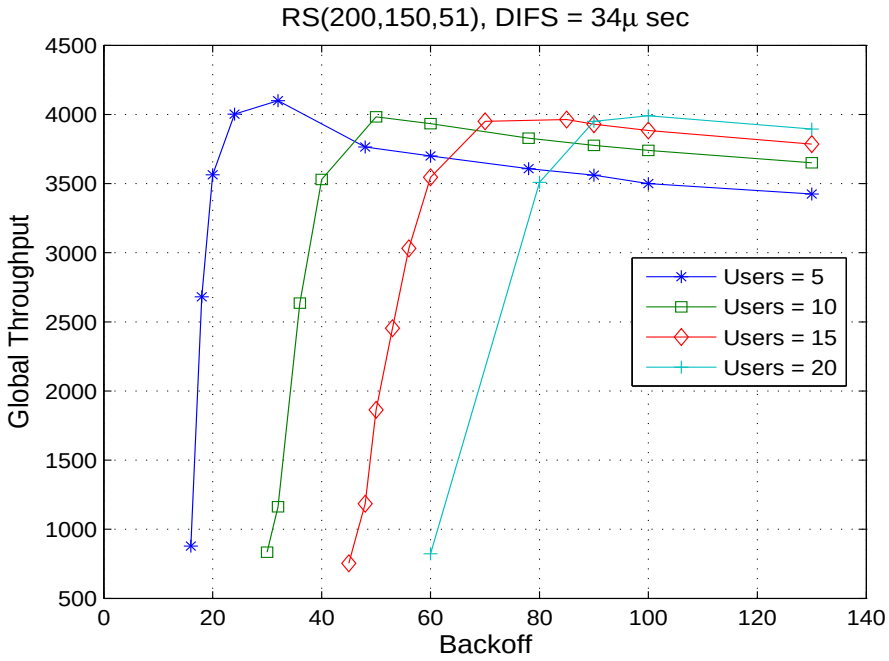

Figure 5.15: Global throughput Vs Backoff for multiple users

codes with better code properties are used, we will have significant gain in terms of global throughput. We have plotted the results upto 20 users and we see as the no.of users increase the optimal throughput point is moving at higher value of backoff. We conclude the above simulation results as: there exist an optimal point to achieve maximum global throughput that depends on the no.of users, the value of backoff and the erasure correcting codes that we must introduce for erasure recovery at the expanse of redundancy.

5.6 Conclusion

In this chapter we have studied in detail the CSMA/CA scheme for spectrum access of multiple users and analysed the performance in-terms of throughput by changing the parameters of MAC protocol and number of users. We have estimated the global collision rate of multiple users and analysed that by reducing the value of BO the collisions are increased but the overall waiting time to access the channel is reduced. The global collision rate increases as the number of users in the system increase but the collision rate per user remains constant. In order to recover the lost data due to collisions the erasure correcting codes are envisioned and we have defined a metric (the throughput S) to com-

pare throughput achieved for multiple users using different codes having different rates in a same channel with given parameters of MAC protocol. We observed that there is trade-off among secondary access to the channel (depending on the parameter DIFS and BO) and the collision rate experienced (relevant parameter is BO), and the choice of an erasure code that has significant impact on erasure recovery.

Chapter 6

Conclusions and Perspectives

Contents

6.1 Conclusions

In this thesis we have addressed the problem of spectrum scarcity and studied various spectrum access schemes including Opportunistic Spectrum Access (OSA). We proposed the solution to optimize the efficiency of secondary user using Opportunistic Spectrum Access. In this scheme the SU is able to access the idle part of spectrum when primary or licensed user is not transmitting. The secondary access is made possible using Cognitive radio that was first introduced by Mitola. Moreover, the sensing is the complimentary part for OSA scheme as there is no coordination between primary and secondary user but it is not perfect and contains two types of impairments. The limitations of spectrum sensing has to be addressed including the Non detection impairment that is the cause of collisions. We proposed to use the erasure correcting codes to recover the lost data due to collisions between primary and secondary user, the goal is to optimize the secondary spectrum access for OSA scheme.

In Chapter 3 we proposed some techniques to optimize the performance of erasure correcting codes and their decoding method. The performance of various erasure correcting codes using various decoding methods including exhaustive search and Viterbi decoding is

compared to choose the suitable decoding method for OSA scheme. The Tanner graph based approach is proposed for decoding due to lower decoding complexity and we can further enhance its performance. We deal with the erasure recovery at packet level and main advantage of using Tanner graph based approach is that its decoding complexity is lower than other decoding methods. To optimize the performance of short codes, various solutions are also proposed, for example the extended parity check matrix gives a significant gain in the performance of erasure correcting codes when using Tanner graph based decoding. The details on concatenation of short codes to construct more powerful codes in terms of erasure recovery are proposed. The analytical bounds on residual erasure rate for component codes are calculated and these analytical bounds are compared with simulation results. Moreover, we assumed that the data packets are either received correctly or these are considered as erased, i.e., we are dealing with binary erasure channel and this erasure recovery scheme will operate at application layer, this is big advantage as we do not need to modify the existing legacy system.

In Chapter 4 the main goal was to find a good functioning point on ROC curve to maximize the efficiency of secondary user for OSA scheme. We modelled the primary and secondary traffic using On/Off Gilbert model and calculated the expression for collision probability that depends upon the activity of PU and sensing impairments. The parameter efficiency is computed that is a relevant parameter for secondary spectrum access. Various simulation curves are plotted to see the effect of PU's activity, sensing impairments and code parameters on efficiency. The effect of PU's activity has impact on efficiency, it is observed that when the PU is very active in the channel the efficiency of SU is reduced, when the PU is rarely active in the channel, the SU achieves higher efficiency level. The erasure recovery performance also has higher impact on efficiency, various erasure correcting codes are used to plot efficiency curves and the achieved efficiencies using these codes are compared. The short codes and product codes are more efficient in-terms of their lower decoding complexity over very long codes. The efficiencies achieved using short and long codes are also compared, the long codes are capacity achieving codes but at the expense of higher decoding complexity. In fact, these is a trade-off among secondary access to the channel (depending on the parameter P_{FA}), the collision rate experienced (depending on the parameter P_{ND}), and the choice of an erasure code having an impact on erasure recovery at the expense of the redundancy.

Finally, in Chapter 5 we performed the throughput analysis of multiple secondary users

using MAC. The access of multiple users is addressed for Cognitive radio networks where interesting scenario is WiFi using 802.11af protocol. Another interesting scenario for multiple users is WiFi using 802.11 protocol operating at 2.4 and 5 GHz frequency bands. We have proposed a solution to optimize the global throughput of multiple secondary users in the network. We calculated the global collision rate analytically and compared it with simulation results for multiple secondary users, it is observed that the collision rate increases as the waiting time to access the channel is reduced and the number of users are increased. In order to recover the lost data due to collisions we proposed the solution of using short erasure correcting codes, the short codes will be useful if the collision rate is not to high but more powerful codes will be used if the collision rate is too high. Moreover, as the no.of users is increasing in the network then the value of BO can be increased to reduce very high collision rate and the global throughput can be enhanced. The envision of erasure codes will enhance the global throughput as well and will reduce the extra delays due to retransmission of lost data. We summarized the throughput analysis as: in order to achieve an optimal point for global throughput there is always a trade-off among multiple secondary users, the value of BO and the erasure correcting codes that we must introduce for erasure recovery at the expanse of redundancy.

6.2 Perspectives

Directions for the future work of this thesis are listed:

- The access point and multiple users scenario can be implemented using the system simulator OMNeT++ to design a network and the parameters of 802.11 protocol can be modified to see the effect on global throughput. We can adjust the values of DIFS or BO and select various erasure correcting codes to see the effect on global throughput.

- The analytical expressions for the throughput achieved using multiple users can be calculated to compare it with simulation results to see the effect of various erasure correcting codes, the parameters of 802.11 protocol and varying the no.of users in the network.

- The hidden node problem can be addressed by extending the network to multiple access points and the effect of erasure recovery can be addressed. The gain in system

performance can be analysed using erasure correcting codes for the recovery of lost data. This can be possible using any system simulator OMNeT++ for example.

- The WiFi can be implemented using Universal Software Radio Peripheral (USRPs) hardware and the global throughput achieved using erasure recovery scheme can be compared with the throughput achieved using existing WiFi standards to estimate the gain by designing a short network with access point and multiple users.

- The decoding performance of short erasure recovery codes can be further enhanced by provided some techniques to construct good extended parity check matrix. Some heuristic approaches can be used to add the linear combinations of parity check equations in $\mathbf{H}$ matrix. Various algorithms for example Tabu search or simulated annealing can be used to get good parity check matrix $\mathbf{H}$.

Chapter B

Thesis Publications

Conference Publications:

- P. Tortelier and M. M. Azeem,"Improving the erasure recovery performance of short codes for opportunistic spectrum access." in the 14th International Symposium on Wireless Personal Multimedia Communications, WPMC, 2011, Brest, France.
- M. Azeem, P. Tortelier, and D. Le Ruyet, "On the interplay of sensing and erasure correction in opportunistic spectrum access." in 76th IEEE Vehicular Technology Conference (VTC Fall), 2012, Quebec city, Canada.
- M. M. Azeem, P. Tortelier, and D. L. Ruyet, "Single parity check product codes for erasure recovery in opportunistic spectrum access." in The Ninth International Symposium on Wireless Communication Systems: ISWCS, 2012, Paris, France.

Journal Article:

- Muhammad Moazam Azeem, P. Tortelier, and D. Le Ruyet, "On the use of short erasure correcting codes for Opportunistic Spectrum Access." Submitted in Journal Annals of Telecommunications, 2014.

Patent Submission:

- Patrick Tortelier, Muhammad Moazam Azeem, and Didier Le Ruyet, "Systeme de Transmission de Paquets de Donnees Selon un Protocole d'acces Multiple."

Deliverables to Orange Labs:

- P. Tortelier and M. M. Azeem. "Erasure Codes for Opportunistic Spectrum Access".
- M.M.Azeem and P. Tortelier. "Application of Short Erasure Correcting Codes for Enhanced Multimedia Broadcast Multicast Services (eMBMS) for LTE."

Tutorial Talk:

- Muhammad Moazam Azeem,"Application of Short Erasure Correcting Codes for Opportunistic Spectrum Access and Cognitive Radio MAC." Tutorial Presentation at Global Wireless Summit (GWS), 24-27 July 2013, Atlantic City, New Jursey, USA

Bibliography

[1] J. Mitola, "Cognitive radio: An integrated agent architecture for software defined radio," Ph.D. dissertation, KTH Royal Inst. of Technol. Stockholm, Sweden, 2000.

[2] M. Schwartz and A. Vardy, "On the stopping distance and the stopping redundancy of codes," *IEEE Trans. Information theory*, vol. 52, no. 3, pp. 922–932, 2006.

[3] P. Tortelier and M. Azeem, "Improving the erasure recovery performance of short codes for opportunistic spectrum access," in *14th International Symposium on Wireless Personal Multimedia Communications (WPMC 2011)*. Brest, France: IEEE, 2011.

[4] M. Buddhikot, "Understanding dynamic spectrum access: Models, taxonomy and challenges," in *Proceedings of IEEE DySPAN 2007*, Dublin, Ireland, April 17-21 2007.

[5] "Spectrum policy task force report," FCC Doc. ET Docket No. 02-135, Nov. 2002.

[6] Q. Zhao and A. Swami, "A survey of dynamic spectrum access: signal processing and networking perspectives," in *Acoustics, Speech and Signal Processing, 2007. ICASSP 2007. IEEE International Conference on*, vol. 4. IEEE, 2007, pp. IV–1349.

[7] Q. Zhao and B. Sadler, "A survey of dynamic spectrum access," *Signal Processing Magazine, IEEE*, vol. 24, no. 3, pp. 79–89, 2007.

[8] "Darpa: The next generation (xg) program," 2005. [Online]. Available: http://www.darpa.mil/ato/programs/xg/index.html

[9] B. Wang and K. J. R. Liu, "Advances in cognitive radio networks: A survey," *IEEE Journal of Selected Topics in Signal Processing, Vol. 5, No. 1*, February, 2011.

[10] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Computer Networks, 2006 - Elsevier*, January 2006.

[11] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *Communications Surveys & Tutorials, IEEE*, vol. 11, no. 1, pp. 116–130, 2009.

[12] A. Chia-Chun Hsu, D. Weit, and C. Kuo, "A cognitive mac protocol using statistical channel allocation for wireless ad-hoc networks," in *Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE*. IEEE, 2007, pp. 105–110.

[13] J. Mitola, "Software radios: Wireless architecture for the 21st century," *John Wiley & Sons Inc*, 2000.

[14] "Regulatory aspects of software defined radio," SDR Forum, SDRF-00-R-0050-v0.0.

[15] D. Willkomm, J. Gross, and A. Wolisz, "Reliable link maintenance in cognitive radio systems," in *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on*. IEEE, 2005, pp. 371–378.

[16] Y. G., W. X., and M. M., "Design of anti-jamming coding for cognitive radio," in *Global Telecommunications Conference, 2007. GLOBECOM'07. IEEE*. IEEE, 2007, pp. 4190–4194.

[17] G. Yue, "Antijamming coding techniques," *Signal Processing Magazine, IEEE*, vol. 25, no. 6, pp. 35–45, 2008.

[18] S. Huang, X. Liu, and Z. Ding, "Opportunistic spectrum access in cognitive radio networks," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. IEEE, 2008, pp. 1427–1435.

[19] Q. Zhao, S. Geirhofer, L. Tong, and B. Sadler, "Optimal dynamic spectrum access via periodic channel sensing," in *Wireless Communications and Networking Conference, 2007. WCNC 2007. IEEE*. IEEE, 2007, pp. 33–37.

[20] T. Shu, S. Cui, and M. Krunz, "Wlc05-3: medium access control for multi-channel parallel transmission in cognitive radio networks," in *Global Telecommunications Conference, 2006. GLOBECOM'06. IEEE*. IEEE, 2006, pp. 1–5.

[21] R. Urgaonkar and M. Neely, "Opportunistic scheduling with reliability guarantees in cognitive radio networks," *Mobile Computing, IEEE Transactions on*, vol. 8, no. 6, pp. 766–777, 2009.

[22] W. Wang and X. Liu, "List-coloring based channel allocation for open-spectrum wireless networks," in *IEEE Vehicular Technology Conference*, vol. 62, no. 1. Citeseer, 2005, p. 690.

[23] D. Xu, E. Jung, and X. Liu, "Optimal bandwidth selection in multi-channel cognitive radio networks: how much is too much?" in *New Frontiers in Dynamic Spectrum Access Networks, 2008. DySPAN 2008. 3rd IEEE Symposium on*. IEEE, 2008, pp. 1–11.

[24] S. Huang, X. Liu, and Z. Ding, "Optimal transmission strategies for dynamic spectrum access in cognitive radio networks," *Mobile Computing, IEEE Transactions on*, vol. 8, no. 12, pp. 1636–1648, 2009.

[25] V. Blaschke, H. Jaekel, T. Renk, C. Kloeck, and F. Jondral, "Occupation measurements supporting dynamic spectrum allocation for cognitive radio design," in *Cognitive Radio Oriented Wireless Networks and Communications, 2007. CrownCom 2007. 2nd International Conference on*. IEEE, 2007, pp. 50–57.

[26] S. Yin, D. Chen, Q. Zhang, M. Liu, and S. Li, "Mining spectrum usage data: a large-scale spectrum measurement study," *Mobile Computing, IEEE Transactions on*, vol. 11, no. 6, pp. 1033–1046, 2012.

[27] L. Yang, W. Hou, L. Cao, B. Zhao, and H. Zheng, "Supporting demanding wireless applications with frequency-agile radios," in *Proc. of NSDI*, 2010.

[28] M. Wellens, A. de Baynast, and P. Mahonen, "Performance of dynamic spectrum access based on spectrum occupancy statistics," *Communications, IET*, vol. 2, no. 6, pp. 772–782, 2008.

[29] V. Kone, L. Yang, X. Yang, B. Zhao, and H. Zheng, "The effectiveness of opportunistic spectrum access: A measurement study," 2012.

[30] S. Mishra, D. Cabric, C. Chang, D. Willkomm, B. Van Schewick, S. Wolisz, and B. Brodersen, "A real time cognitive radio testbed for physical and link layer experiments," in *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on.* IEEE, 2005, pp. 562–567.

[31] T. Rondeau, B. Le, C. Rieser, and C. Bostian, "Cognitive radios with genetic algorithms: Intelligent control of software defined radios," in *Software Defined Radio Forum Technical Conference.* Citeseer, 2004, pp. C3–C8.

[32] D. Raychaudhuri, I. Seskar, M. Ott, S. Ganu, K. Ramachandran, H. Kremo, R. Siracusa, H. Liu, and M. Singh, "Overview of the orbit radio grid testbed for evaluation of next-generation wireless network protocols," in *Wireless Communications and Networking Conference, 2005 IEEE*, vol. 3. IEEE, 2005, pp. 1664–1669.

[33] C. Cordeiro, K. Challapali, D. Birru, and N. Sai Shankar, "Ieee 802.22: the first worldwide wireless standard based on cognitive radios," in *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on.* IEEE, 2005, pp. 328–337.

[34] C. Cordeiro, K. Challapali, and M. Ghosh, "Cognitive phy and mac layers for dynamic spectrum access and sharing of tv bands," *Proc. ACM TAPAS*, 2006.

[35] M. Muck, S. Buljore, P. Martigne, A. Kousaridas, E. Patouni, M. Stamatelatos, K. Tsagkaris, J. Yang, and O. Holland, "Ieee p1900. b: Coexistence support for reconfigurable, heterogeneous air interfaces," in *New Frontiers in Dynamic Spectrum Access Networks, 2007. DySPAN 2007. 2nd IEEE International Symposium on.* IEEE, 2007, pp. 381–389.

[36] P. M. Mattias Wellens, Janne Riihijarvi, "Modelling primary system activity in dynamic spectrum access networks by aggregated on/off-processes," 2009.

[37] E. Elliott, "Estimates of error rates for codes on burst noise channels," *BSTJ*, vol. 42, pp. 1977–1997, september 1963.

[38] L. Kanal and A. Sastry, "Models for channels with memory and their applications to error control," *Proc. of the IEEE*, vol. 66, no. 7, pp. 724–744, july 1978.

[39] Q. Zhao, L. Tong, A. Swami, and Y. Chen, "Decentralized cognitive mac for opportunistic spectrum access in ad hoc networks: A pomdp framework," *IEEE journal on Selected Areas in Communications*, vol. 25, April 2007.

[40] H. Kushwaha, Y. Xing, R. Chandramouli, and H. Heffes, "Reliable multimedia transmission over cognitive radio networks using fountain codes," *Proceedings of the IEEE*, vol. 96, no. 1, pp. 155–165, January 2008.

[41] Q. Zhao, S. Geirhofer, L. Tong, and B. Sadler, "Opportunistic spectrum access via periodic channel sensing," *Signal Processing, IEEE Transactions on*, vol. 56, no. 2, pp. 785–796, 2008.

[42] P. Tortelier, "Analytic performance evaluation of opportunistic spectrum access with detection errors," in *ValueTools*, 2011.

[43] M. Wellens, J. Riihijärvi, and P. Mähönen, "Empirical time and frequency domain models of spectrum use," *Elsevier Physical Communications*, vol. 2, no. 1–2, pp. 10–32, 2009.

[44] M. Wellens, J. Riihijarvi, and P. Mahonen, "Modelling primary system activity in dynamic spectrum access networks by aggregated on/off-processes," in *Sensor, Mesh and Ad Hoc Communications and Networks Workshops, 2009. SECON Workshops' 09. 6th Annual IEEE Communications Society Conference on.* IEEE, 2009, pp. 1–6.

[45] Xiaoliang, "On/off model: A new tool to understand bgp update burst."

[46] Q. Zhao, S. Geirhofer, L. Tong, and B. M. Sadler, "Optimal dynamic spectrum access via periodic channel sensing," in *WCNC*, 2007.

[47] S. G. L. T. B. M. Sadler, "Dynamic spectrum access in the time domain: Modeling and exploiting white space," *IEEE Communications Magazine*, May 2007.

[48] P. Bahl, R. Chandra, T. Moscibroda, R. Murty, and M. Welsh, "White space networking with wi-fi like connectivity," *Computer communication review*, vol. 39, no. 4, p. 27, 2009.

[49] S. Deb, V. Srinivasan, and R. Maheshwari, "Dynamic spectrum access in dtv whitespaces: design rules, architecture and algorithms," in *Proceedings of the 15th annual international conference on Mobile computing and networking*. ACM, 2009, pp. 1–12.

[50] T. Yücek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Communications surveys and tutorials*, vol. 11, no. 1, pp. 116–130, 2009.

[51] D. Hu and S. Mao, "A sensing error aware mac protocol for cognitive radio networks," *in Proc. IEEE GLOBECOM*, pp. 5514–5519, 2009.

[52] S. Haykin, D. Thomson, and J. Reed, "Spectrum sensing for cognitive radio," *Proceedings of the IEEE*, vol. 97, no. 5, pp. 849–877, 2009.

[53] N. Shankar, C. Cordeiro, and K. Challapali, "Spectrum agile radios: utilization and sensing architectures," in *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on*. IEEE, 2005, pp. 160–169.

[54] H. Urkowitz, "Energy detection of unknown deterministic signals," in *Proceedings of the IEEE*, vol. 55, Apr. 1967., pp. 523–531.

[55] J. J. L. M. J. H. Saarnisaari; and S. Koivu, "Threshold setting strategies for a quantized total power radiometer," *IEEE Signal Processing Letters*, vol. vol. 12, pp. 796–799, Nov. 2005.

[56] J. Plank, A. Buchsbaum, R. Collins, and M. Thomason, "Small parity-check erasure codes-exploration and observations," in *Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on*. IEEE, 2005, pp. 326–335.

[57] J. Plank, "T1: erasure codes for storage applications," in *Proc of the 4th USENIX Conference on File and Storage Technologies. San Francisco:[sn]*, 2005, pp. 1–74.

[58] M. Blaum, J. Brady, J. Bruck, and J. Menon, "Evenodd: An efficient scheme for tolerating double disk failures in raid architectures," *Computers, IEEE Transactions on*, vol. 44, no. 2, pp. 192–202, 1995.

[59] L. Xu and J. Bruck, "X-code: Mds array codes with optimal encoding," *Information Theory, IEEE Transactions on*, vol. 45, no. 1, pp. 272–276, 1999.

[60] C. Huang and L. Xu, "Star: An efficient coding scheme for correcting triple storage node failures," *Computers, IEEE Transactions on*, vol. 57, no. 7, pp. 889–901, 2008.

[61] J. Hafner, "Weaver codes: Highly fault tolerant erasure codes for storage systems," in *Proceedings of the 4th conference on USENIX Conference on File and Storage Technologies*, 2005, pp. 16–16.

[62] ——, "Hover erasure codes for disk arrays," in *Dependable Systems and Networks, 2006. DSN 2006. International Conference on*. IEEE, 2006, pp. 217–226.

[63] G. Battail, "Building long codes by combination of simple ones, thanks to weighted-output decoding," *Proc, URSIISSSE*, pp. 634–637, 1989.

[64] P. Tortelier and M. M. Azeem, "Improving the erasure recovery performance of short codes for opportunistic spectrum access." *WPMC*, 2011.

[65] M. Azeem, P. Tortelier, and D. Le Ruyet, "On the interplay of sensing and erasure correction in opportunistic spectrum access," in *Vehicular Technology Conference (VTC Fall), 2012 IEEE*. IEEE, 2012, pp. 1–5.

[66] L. Pamies-Juarez, A. Datta, and F. Oggier, "Rapidraid: Pipelined erasure codes for fast data archival in distributed storage systems," *arXiv preprint arXiv:1207.6744*, 2012.

[67] J. Luo, L. Xu, and J. Plank, "An efficient xor-scheduling algorithm for erasure codes encoding," in *Dependable Systems & Networks, 2009. DSN'09. IEEE/IFIP International Conference on*. IEEE, 2009, pp. 504–513.

[68] J. Plank, C. Schuman, and B. Robison, "Heuristics for optimizing matrix-based erasure codes for fault-tolerant storage systems," in *Dependable Systems and Networks (DSN), 2012 42nd Annual IEEE/IFIP International Conference on*. IEEE, 2012, pp. 1–12.

[69] M. Uppal, G. Yue, Y. Xin, X. Wang, and Z. Xiong, "A dirty-paper coding scheme for the cognitive radio channel," in *Communications (ICC), 2010 IEEE International Conference on*. IEEE, 2010, pp. 1–5.

[70] X. Chen and I. Reed, *Error-control coding for data networks*. Kluwer Academic Publishers, 1999.

[71] P. Elias, *Error-free coding*. Research Laboratory of Electronics, Massachusetts Institute of Technology, 1954.

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

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

[74] C. Berrou and A. Glavieux, "Near optimum error correcting coding and decoding: Turbo-codes," *Communications, IEEE Transactions on*, vol. 44, no. 10, pp. 1261–1271, 1996.

[75] L. Lan, L. Zeng, Y. Tai, L. Chen, S. Lin, and K. Abdel-Ghaffar, "Construction of quasi-cyclic LDPC codes for AWGN and binary erasure channels: A finite field approach," *Information Theory, IEEE Transactions on*, vol. 53, no. 7, pp. 2429–2458, 2007.

[76] V. Roca, M. Cunche, C. Thiénot, J. Detchart, and J. Lacan, "RS + LDPC-staircase codes for the Erasure Channel: Standards, Usage and Performance," in *The 9th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, 7-9 October 2013.

[77] H. Kushwaha, Y. Xing, R. Chandramouli, and K. Subbalakshmi, *Cognitive Networks: Towards Self-Aware Networks*. Wiley, 2007, ch. Erasure tolerant coding for cognitive radios.

[78] A. Shokrollahi, "Raptor codes," *IEEE Trans. Information Theory*, vol. 52, no. 6, pp. 2551–2567, 2006.

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

[80] M. Luby, M. Mitzenmacher, M. Shokrollahi, and D. Spielman, "Efficient erasure correcting codes," *Information Theory, IEEE Transactions on*, vol. 47, no. 2, pp. 569–584, 2001.

[81] J. S. G. J. J. B. Rhim; and D. Wang, "Fountain codes," December 2010.

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

[83] E. Paolini, G. Liva, and M. Chiani, "High Throughput Random Access via Codes on Graphs: Coded Slotted ALOHA," in *proc. IEEE ICC 2011*, 2011.

[84] M. Chiani, G. Liva, and E. Paolini, "The marriage between random access and codes on graphs: Coded slotted aloha," in *Proc. of the IEEE First AESS European Conference on Satellite Telecommunications (ESTEL)*. IEEE, october 2012.

[85] N. Abramson, "The aloha system - another alternative for computer communications," in *Fall Joint Comput. Conf. AFIPS*, 1970.

[86] C. H. Foh, "Performance analysis and enhancement of mac protocols," Ph.D. dissertation, The university of Melbourne, November 2002.

[87] L. G. Roberts, "Aloha packet system with and without slots and capture," *SIGCOMM Comput. Commun. Rev.*, vol. 5, no. 2, pp. 28–42, Apr. 1975. [Online]. Available: http://doi.acm.org/10.1145/1024916.1024920

[88] A. Asterjadhi and M. Zorzi, "JENNA: A Jamming evasive network-coding neighbor-discovery algorithm for cognitive radio networks," *IEEE Wireless Communications*, vol. 17, no. 4, pp. 24–32, august 2010.

[89] L. K. F. A. Tobagi, "Packet switching in radio channels: Part i-carrier sense multiple-access modes and their throughput-delay characteristics," *IEEE Transactions on Communications*, vol. 23, p. 12, 1975.

[90] H. Kushwaha and R. Chandramouli, "Secondary spectrum access with lt codes for delay-constrained applications," in *proc. IEEE Consumer Communications and Networking conference (CCNC)*, Las Vegas, 2007.

[91] H. Kushwaha, Y. Xing, R. Chandramouli, and H. Heffes, "Reliable multimedia transmission over cognitive radio networks using fountain codes," *Proceedings of the IEEE*, vol. 96, no. 1, pp. 155–165, January 2008.

[92] H. Kushwaha, Y. Xing, R. Chandramouli, and K. Subbalakshmi, *Cognitive Networks: Towards Self-Aware Networks*. Wiley, 2007, ch. Erasure tolerant coding for cognitive radios.

[93] M. A. Kousa and A. H. Muqaibel, "Cell loss recovery using two-dimensional erasure correction for ATM networks," *7th International Conference on Telecommunication Systems Modeling and Analysis*, March 18-21 1999.

[94] M. Kousa, "A novel approach for evaluating the performance of SPC product codes under erasure decoding," *IEEE Trans. on communications*, vol. 50, no. 1, pp. 7–11, january 2002.

[95] A. Al-Shaikhi and J. Ilow, "Improved upper bounds for erasure recovery in binary product codes," in *IEEE 16th international Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2005.

[96] Q. Zhao and B. Sadler, "A survey of dynamic spectrum access," *IEEE Signal Processing magazine*, vol. 24, no. 3, pp. 79–89, may 2007.

[97] X. Shao, H. S. Cronie, F. W. Hoeksema, and C. H. Slump, "Fountain codes for frequency occupancy information dissemination," in *17th Annual Workshop on Circuits, Veldhoven, The Netherlands*. Utrecht: Technology Foundation STW, November 2006, pp. 196–203.

[98] M. M. Azeem, P. Tortelier, and D. L. Ruyet, "Single parity check product codes for erasure recovery in opportunistic spectrum access," in *The Ninth International Symposium on Wireless Communication Systems: ISWCS2012*, Paris, France.

[99] P. Tortelier, "Analytic performance evaluation of opportunistic spectrum access with detection errors," in *ValueTools*, 2011.

[100] M. Wellens, J. Riihijärvi, and P. Mähönen, "Empirical time and frequency domain models of spectrum use," *Elsevier Physical Communications*, vol. 2, no. 1–2, pp. 10–32, 2009.

[101] M. Wellens, J. Riihijärvi, and Mähönen, "Modelling primary system activity in dynamic spectrum access networks by aggregated on/off-processes," in *Proc. of 4th IEEE Workshop on Networking Technologies for SDR Networks*, june 2009.

[102] M. Azeem, P. Tortelier, and D. Le Ruyet, "Single parity check product codes for erasure recovery in opportunistic spectrum access," in *Wireless Communication Systems (ISWCS), 2012 International Symposium on*. IEEE, 2012, pp. 76–80.

[103] G. Bianchi, "Performance analysis of the ieee 802.11 distributed coordinated function." *IEEE JSAC*, vol. 18, pp. 535–547, March 2000.

[104] D. Kumar, T. Chahed, and E. Altman, "Analysis of a fountain codes based transport in an 802.11 wlan cell," in *Proceedings of the 21st International Teletraffic Congress*, 2009., pp. 1–8.

le cnam	Muhammad Moazam Azeem Erasure Correcting Codes for Opportunistic Spectrum Access	le cnam

Résumé:
Cela passe en particulier par de nouvelles méthodes pour gérer la manière dont plusieurs utilisateurs se partagent une même ressource spectrale. Les années récentes ont vu l'explosion du trafic sur les réseaux mobiles depuis l'apparition de nouveaux terminaux (smartphones, tablettes) et des usages qu'ils permettent, en particulier les données multimédia, le trafic voix restant sensiblement constant. Une conséquence est le besoin de plus de spectre, ou la necessité de mieux utiliser le spectre déjà alloué. Comme il n'y a pas de coordination entre les utilisateurs secondaire(s) et primaire, avant toute transmission les premiers doivent mettre en oeuvre des traitements pour détecter les périodes dans lesquelles l'utilisateur primaire transmet, ce qui est le scénario considéré dans cette thèse. Nous considérons donc une autre approche, reposant sur l'utilisation de codes correcteurs d'effacements en mode paquet. La dernière partie de la thèse aborde un scénario dans lequel il n'y a plus d'utilisateur primaire, tous les utilisateurs ayant le même droit à transmettre dans le canal. Nous décrivons une modification de la couche MAC du 802.11 consistant à réduire les différents temps consacrés à attendre (SIFS, DIFS, backoff, ...) afin d' accèder plus souvent au canal, au prix de quelques collisions supplémentaires qu'il est possible de récupérer en mettant en œuvre des codes correcteurs d'effacements.

Mots-clés: La radio cognitive, Opportuniste du spectre accès, Canal à effacement binaire, Codes correcteurs d'effacements, Graphe de Tanner, Les codes de produit, L'efficacitè spectrale, Processus de dètection, CSMA/CA, Protocoles MAC.

Abstract:
The emergence of new devices especially the smartphones and tablets having a lot of new applications have rocketed the wireless traffic in recent years and this is the cause of main surge in the demand of radio spectrum. There is a need of either more spectrum or to use existing spectrum more efficiently due to dramatic increase in the demand of limited spectrum. Among the new dynamic access schemes designed to use the spectrum more efficiently opportunistic spectrum access (OSA) is currently addressed when one or more secondary users (SU) are allowed to access the channel when the PU is not transmitting. The erasure correcting codes are therefore envisioned to recover the lost data due to sensing impairments. We define the parameter efficiency of SU and optimize it in-terms of spectrum utilization keeping into account sensing impairments, code parameters and the activity of PU. Finally, the spectrum access for multiple secondary users is addressed when there is no primary and each user has equal right to access the channel. The interesting scenarios are Cognitive radio networks and WiFi where 802.11 protocol gives the specification for MAC layer. The throughput curves achieved by retransmission and using various erasure correcting codes are compared. This modification in MAC layer will reduce the long waiting time to access the channel, as the number of users are increased.

Keywords: Opportunistic Spectrum Access, Cognitive Radio, Binary Erasure Channel, Erasure Correcting Codes, Tanner graph, Product Codes, Spectral Efficiency, Spectrum Sensing, CSMA/CA, MAC Protocols.